Installing & Hacking From 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 assighned 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 responisble 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