===

CA-95:01 CERT Advisory
January 23, 1995

IP 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 a 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. If you have experienced a root compromise, see Section C for general instructions on how to recover.

C. Recovery from a UNIX root compromise

1. 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).

Internet E-mail: cert@cert.org
Telephone: +1 412-268-7090 (24-hour hotline)
           CERT personnel answer 8:30 a.m.-5:00 p.m. EST(GMT-5)/EDT(GMT-4),
           and are on call for emergencies during other hours.
Fax: +1 412-268-6989

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.