CERT Advisory CA-1990-02 Internet Intruder Warning

Original issue date: March 19, 1990
Last revised: September 17, 1997
Attached copyright statement

A complete revision history is at the end of this file.

There have been a number of media reports stemming from a March 19 New York Times article entitled "Computer System Intruder Plucks Passwords and Avoids Detection." The article referred to a program that attempts to get into computers around the Internet.

At this point, the Computer Emergency Response Team Coordination Center (CERT/CC) does not have hard evidence that there is such a program. What we have seen are several persistent attempts on systems using known security vulnerabilities. All of these vulnerabilities have been previously reported. Some national news agencies have referred to a "virus" on the Internet; the information we have now indicates that this is NOT true. What we have seen and can confirm is an intruder making persistent attempts to get into Internet systems.

It is possible that a program may be discovered. However, all the techniques used in these attempts have also been used, in the past, by intruders probing systems manually.

As of the morning of March 19, we know of several systems that have been broken into and several dozen more attempts made on Thursday and Friday, March 15 and 16.

Systems administrators should be aware that many systems around the Internet may have these vulnerabilities, and intruders know how to exploit them. To avoid security breaches in the future, we recommend that all system administrators check for the kinds of problems noted in this message.

The rest of this advisory describes problems with system
configurations that we have seen intruders using. In particular, the intruders attempted to exploit problems in Berkeley BSD derived UNIX systems and have attacked DEC VMS systems. In the advisory below, points 1 through 12 deal with Unix, points 13 and 14 deal with the VMS attacks.

If you have questions about a particular problem, please get in touch with your vendor.

The CERT makes copies of past advisories available via anonymous FTP (see the end of this message). Administrators may wish to review these as well.

We've had reports of intruders attempting to exploit the following areas:

1. Use TFTP (Trivial File Transfer Protocol) to steal password files.
   To test your system for this vulnerability, connect to your system using TFTP and try "get /etc/motd". If you can do this, anyone else can get your password file as well. To avoid this problem, disable tftpd.

   In conjunction with this, encourage your users to choose passwords that are difficult to guess (e.g. words that are not contained in any dictionary of words of any language; no proper nouns, including names of "famous" real or imaginary characters; no acronyms that are common to computer professionals; no simple variations of first or last names, etc.) Furthermore, inform your users not to leave any clear text username/password information in files on any system.

   If an intruder can get a password file, he/she will usually take it to another machine and run password guessing programs on it. These programs involve large dictionary searches and run quickly even on slow machines. The experience of many sites is that most systems that do not put any controls on the types of passwords used probably have at least one password that can be guessed.

1. Exploit accounts without passwords or known passwords (accounts with vendor supplied default passwords are favorites).
   Also uses finger to get account names and then tries simple passwords.

   Scan your password file for extra UID 0 accounts, accounts with no password, or new entries in the password file. Always change vendor supplied default passwords when you install new system software.

1. Exploit holes in sendmail.

   Make sure you are running the latest sendmail from your vendor. BSD 5.61 fixes all known holes that the intruder is using.

1. Exploit bugs in old versions of FTP; exploit mis-configured anonymous FTP

   Make sure you are running the most recent version of FTP which is the Berkeley version 4.163 of Nov. 8 1988. Check with your vendor for information on configuration upgrades. Also check your anonymous FTP configuration. It is important to follow the instructions provided with the operating system to properly configure the files available through anonymous ftp (e.g., file permissions, ownership, group, etc.). Note especially that you should not use your system's standard password file as the password file for FTP.

1. Exploit the fingerd hole used by the Morris Internet worm.

   Make sure you're running a recent version of finger. Numerous Berkeley BSD derived versions of UNIX were vulnerable.

   Some other things to check for:

1. Check user's .rhosts files and the /etc/hosts.equiv files for systems outside your domain.

   Make sure all hosts in these files are authorized and that the files are not world-writable.

1. Examine all the files that are run by cron and at.

We've seen intruders leave back doors in files run from cron or submitted to at. These techniques can let the intruder back on the system even after you've kicked him/her off. Also, verify that all files/programs referenced (directly or indirectly) by the cron and at jobs, and the job files themselves, are not world-writable.

1. If your machine supports uucp, check the L.cmds file to see if they've added extra commands and that it is owned by root (not by uucp!) and world-readable.

   Also, the L.sys file should not be world-readable or world-writable.

1. Examine the /usr/lib/aliases (mail alias) file for unauthorized entries.

   Some alias files include an alias named "uudecode'; if this alias exists on your system, and you are not explicitly using it, then it should be removed.

1. Look for hidden files (files that start with a period and are normally not shown by ls) with odd names and/or setuid capabilities.
   These can be used to "hide" information or privileged (setuid root) programs, including /bin/sh. Names such as '.. ' (dot dot space space), '...', and . xx have been used, as have ordinary looking names such as '.mail'. Places to look include especially /tmp, /usr/tmp, and hidden directories (frequently within users' home directories).

1. Check the integrity of critical system programs such as su, login, and telnet.
   Use a known, good copy of the program, such as the original distribution media and compare it with the program you are running.

1. Older versions of systems often have security vulnerabilities that are well known to intruders.
   One of the best defenses against problems is to upgrade to the latest version of your vendor's system.

   VMS SYSTEM ATTACKS:

1. The intruder exploits system default passwords that have not been changed since installation.
   Make sure to change all default passwords when the software is installed. The intruder also guesses simple user passwords. See point 1 above for suggestions on choosing good passwords.

1. If the intruder gets into a system, often the programs loginout.exe and show.exe are modified.
   Check these programs against the files found in your distribution media.

Revision History

```
September 17, 1997  Attached Copyright Statement
```