1997 CERT Tech Tip: UNIX Configuration Guidelines

Original publication date: October 2, 1997

This document describes commonly exploited UNIX system configuration problems and recommends practices that can be used to help deter several types of break-ins. We encourage system administrators to review all sections of this document and modify their systems to fix potential weaknesses.

In addition to the information in this document, we provide three companion documents that may help you.

- http://www.cert.org/tech_tips/intruder_detection_checklist.html
  contains suggestions for determining if your system may have been compromised
- http://www.cert.org/tech_tips/win-UNIX-system_compromise.html
  contains suggested steps for recovering from a root compromise on a UNIX and Windows NT systems

Also, please see our CERT advisory page, our CERT incident notes page, and our CERT vulnerability notes page which contain brief descriptions of all past CERT advisories, incident notes, and vulnerability notes. These files are available from

- http://www.cert.org/advisories/
- http://www.cert.org/incident_notes/
- http://www.cert.org/vul_notes/

We encourage you to review the documents that pertain to your system(s), and to consider taking the suggested steps to protect your system(s) from attack. We also encourage you to check with your vendor(s) regularly for any software updates or new software patches that relate to your systems.

A. Commonly Exploited Configuration Problems

1. Poor Password Security

   The basic form of authentication used to control access to a UNIX host is a username and password combination. Intruders have established mechanisms and tools to compromise password information by leveraging a variety of common problems.

   a. Weak passwords

      Encourage your users to choose passwords that are difficult to guess (for example, words that are not in any dictionary of any language; no proper nouns, including names of "famous" real or fictitious characters; no acronyms that are commonly used by computer professionals; no simple variations of first or last names.) Furthermore, inform your users not to leave any cleartext username/password information in files on any system.

      A good heuristic for choosing a password is to choose an easy-to-remember phrase, such as "By The Dawn's Early Light", and use the first letters to form a password. Add some punctuation or mix case letters as well. For the phrase above, one example password might be: bt}DeL{. (DO NOT use this sample phrase for your password.)

      If intruders can get a password file, they usually move or copy it to another machine and run password-guessing programs on it. These programs involve large dictionary searches, and they run quickly even on slow machines. Most systems that do not put any controls of the type of passwords used probably have at least one password that can be easily guessed. CERT Incident Note IN-98.03 describes intruder activity that is based on a stolen password file.

      http://www.cert.org/incident_notes/IN-98.03.html

If you believe that your password file may have been taken, change all the passwords on the system. At the very least, you should change all system passwords because an intruder may concentrate on those and may be able to guess even a reasonably "good" password. Intruders often use compromised accounts to attempt to gain privelaged access on vulnerable systems, so we encourage you to follow the steps in

- http://www.cert.org/tech_tips/intruder_detection_checklist.html
- http://www.cert.org/tech_tips/win-UNIX-system_compromise.html

For further information about protecting your system from password-based attacks, see

- http://www.cert.org/tech_tips/passwd_file_protection.html

a. Accounts with default passwords

Intruders exploit system default passwords that have not been changed since installation, including accounts with vendor-supplied default passwords. In some cases, accounts do not have a password assigned by default. CERT Incident Note IN-98.01 describes intruder activity that is based on exploitations of accounts without passwords.

http://www.cert.org/incident_notes/IN-98.01.irix.html

Be sure to change all default passwords on computer systems and networking equipment prior to deployment. Also, be aware that product upgrades can quietly change account passowrds to a new default. It is best to change the passwords of default accounts after applying updates.

Scan your password file for extra UID 0 accounts, accounts with no password, or new entries in the password file. Do not allow any accounts without passwords. Remove entries for unused accounts from the password file. To disable an account, change the password field in the /etc/passwd file to an asterisk '*' and change the login shell to /bin/false to ensure that an intruder cannot login to the account from a trusted system on the network.

a. Reusable and shared passwords

Even excellent passwords are not safe. They can be captured by programs such as packet sniffers if the passwords are sent across networks in cleartext (whether on a subnet, a local network, or the Internet). It is common for intruders to use packet sniffers on compromised systems to harvest passwords.

CERT Incident Note IN-99-06 describes widespread intruder activity involving distributed sniffers used to harvest username and password information from a network.

http://www.cert.org/incident_notes/IN-99-06.html

At the very least, a single password should not be used to protect multiple accounts. If an intruder is able to compromise a shared password just once, all of the accounts sharing the password are compromised. Each account, or resource, protected by a password should have it's own unique password.

To overcome the threat posed by packet sniffers, we recommend using one-time passwords, especially for authenticated access from external networks and for access to sensitive resources like name servers and routers. For more information, see Appendix B of the following advisory:

http://www.cert.org/advisories/CA-94.01.ongoing.network.monitoring.attacks.html

Another approach is to use a strong authentication mechanisms such as secure shell, SSL, or kerberos. Secure shell, or ssh, is widely available for many different platforms. For more information about secure shell, see

- http://www.ssh.com/index.html
- http://www.openssh.com/

1. Use of TFTP (Trivial File Transfer Protocol) to obtain 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 on the network can probably get your password file. To avoid the problem, disable tftpd. If you must have tftpd, ensure that it is configured with restricted access. For further information, see

http://www.cert.org/advisories/CA-91.18.Active.Internet.tftp.Attacks.html

As mentioned in Section 1 above, if you believe your password file may have been taken, the safest course is to change all passwords in the system.

2. Vulnerabilities in sendmail

There have been a number of vulnerabilities identified over the years in sendmail(8). To the best of our knowledge, the current version of sendmail addresses those known vulnerabilities.

To determine which version of sendmail is running, use telnet to connect to the SMTP port (25) on your system:

```
telnet  25
```

We encourage you to keep up to date with the latest version of sendmail from your vendor, and ensure that it is up to date with security patches or workarounds detailed in CERT advisories advisories and bulletins. In addition, we encourage you to use the following tools, both of which are distributed with the latest versions of sendmail:

a. smrsh, the sendmail restricted shell, controls the way o that incoming mail messages can interact with your operating system. For instance, when configured correctly, smrsh can prevent an intruder from using pipes to execute arbitrary commands on your system.
b. mail.local can be used to control the way in which the /bin/mail program is used on your system. This tool is described in CERT advisory CA-95:02.

> *http://www.cert.org/advisories/CA-1995-02.html*

3. Misconfigured anonymous FTP

   In addition to making sure that you are running the most recent version of ftpd, check your anonymous FTP configuration. It is important to follow the instructions provided with the operating system to properly configure the files and directories available through anonymous FTP (for example, file and directory permissions, ownership and group). Note that you should not use your system's standard password file or group file as the password file or group file for FTP. The anonymous FTP root directory and its two subdirectories, etc and bin, should not be owned by ftp. For more information about configuring anonymous FTP, see

   > *http://www.cert.org/tech_tips/anonymous_ftp_config.html*

4. Inappropriate network configuration file entries

   Several vendors supply /etc/hosts.equiv files with a '+' (plus sign) entry. The '+' entry should be removed from this file because it means that your system will trust all other systems. Other files that should not contain a '+' entry include all .rhosts files on the system. These files should not be world-writable.

   If your /usr/lib/X11/xdm/Xsession file includes an 'xhost' command with a '+' entry, such as

   ```
   /usr/bin/X11/xhost +
   ```

   remove that line. (Note that the 'xhost' command may be in a different directory tree on your system.) If such a line remains intact, anyone on the network can talk to the X server and potentially insert commands into windows or read console keystrokes.

5. Inappropriate 'secure' settings in /etc/ttys and /etc/ttytab

   Check the file /etc/ttys or /etc/ttytab (depending on the release of UNIX being used). The ONLY terminal that should be set to 'secure' should be the console.
6. Inappropriate entries in /etc/aliases (or /usr/lib/aliases)

   Examine the /etc/aliases (or /usr/lib/aliases) mail alias file for inappropriate entries. Some alias files include an alias named 'uudecode' or just 'decode.' If this alias exists on your system and you are not explicitly using it, then you should remove it.
7. Inappropriate file and directory protections

   Check your system documentation to establish the correct file and directory protections and ownership for system files and directories. In particular, check the '/' (root) and '/etc' directories, and all system and network configuration files. Examine file and directory protections before and after installing software or running verification utilities. These procedures can cause file and directory protections to change.
8. Old versions of system software

   Older versions of operating systems often have security vulnerabilities that are well known to intruders. To minimize your vulnerability to attacks, keep the version of your operating system up to date and apply security patches appropriate to your system(s) as soon as they become available.
9. Use of setuid shell scripts

   Setuid shell scripts (especially setuid root) can pose potential security problems, a fact that has been well documented in many UNIX system administration texts. Do not create or allow setuid shell scripts, especially setuid root.
10. Inappropriate export settings

    Use the showmount(8) utility to check that the configuration of the /etc/exports files on your hosts are correct.

    - Wherever possible, file systems should be exported read-only.
    - Do not self-reference an NFS server in its own exports file. That is, the exports file should not export an NFS server to itself nor to any netgroups that include the NFS server.
    - Do not allow the exports file to contain a "localhost" entry.
    - Export file systems only to hosts that require them.
    - Export only to fully qualified hostnames.
    - Ensure that export lists do not exceed 256 characters (after the aliases have been expanded) or that all security patches relating to this problem have been applied.

    The CERT Coordination Center is aware that intruders are using tools that exploit a number of NFS vulnerabilities. This can result in a root compromise, depending on the vulnerability being exploited. We encourage you to limit your exposure to these attacks by implementing the security measures outlined in CERT advisory CA-94:15. For this and other information about the NFS vulnerability, see

    > *http://www.cert.org/advisories/CA-1994-15.html*

11. Vulnerable protocols and services

    You may want to consider filtering certain TCP/IP services at your firewall or router. For some related suggestions, please refer to "Packet Filtering For Firewall Systems," available from

    > *http://www.cert.org/tech_tips/packet_filtering.html*

For a list of some recommended books and articles on computer security topics, see the CERT(sm) Coordination Center FAQ, available from

- http://www.cert.org/faq/cert_faq.html

Revision History	
Oct 02, 1997	Initial Release
Feb 12, 1999	Converted to new web format
Jun 04, 2003	Updated broken links
Apr 24, 2006	