

Securing Your Machine: UNIX

This document contains the following sections:

- [Basic Guidelines](#)
- [Security Updates](#)
- [Account and Password Security](#)
- [Network Services](#)
- [Tripwire](#)
- [Log Files](#)

For information related to this topic refer to:

- [Security: General Practices](#)
(<http://www.cmu.edu/computing/doc/security/general/index.html>)
- [Information Security Office](#) (<http://www.cmu.edu/computing/security/>)

Last Updated: May 26, 2004

Securing UNIX Systems: Basic Guidelines

UNIX systems were created to use the network, but that doesn't mean that the network is a safe place for them to be. UNIX systems are capable of running a wide array of network services, and because of this, are vulnerable to a large number of attacks and exploits.

This document provides some general guidelines on how to keep your UNIX system safe from harm. It is not exhaustive, and is not a "how to" guide. Because UNIX is available in so many flavors and colors, it is not reasonable to create a single "how to" web page. We recommend "Practical UNIX & Internet Security" and "Computer Security Basics", both available from [O'Reilly's Security Section \(http://security.oreilly.com\)](http://security.oreilly.com).

The following is a list of concerns for UNIX system security:

- Security Updates
- Account and Password Security
- Network Services
- Tripwire
- Log Files

Last Updated: May 26, 2004

Security Updates

Most UNIX or Linux operating system vendors release security patches regularly. You should check the vendor websites for new patches at least weekly, and immediately after any announcement of a new vulnerability.

Most vendors also allow users to subscribe to security mailing lists for their operating systems. Doing so is a good idea.

Last Updated: May 26, 2004

Account and Password Security

All active accounts should be given strong passwords. Any account left on with a weak, or nonexistent password is an invitation for hackers to compromise your system.

Some UNIX systems come "out of the box" with a number of accounts created and active that you may not need. Accounts like "printer" and "guest" are good examples. If you do need "default" accounts, you should set strong passwords for them.

It is a good practice to periodically check your password file for unexpected accounts. Any account in group 0, or with a UID of 0, which you did not create, or are unaware of, is highly suspect and could mean that the system has been compromised.

Last Updated: May 26, 2004

Network Services

Any services which are not needed for your day-to-day use should be disabled. Most operating systems turn on too many services by default. This includes services such as SMTP, IMAP, POP, telnet (ssh is more secure), ftp (scp is more secure), http, DNS, and others. If you aren't sure that you need it, you most likely don't. While it may seem obvious to some, remember to check `/etc/inetd.conf`. This file allows services to start "as needed" when a request hits the machine from the network. So a service that you think is disabled may not be if it's still available through this service. For some flavors of Linux/UNIX, there is an excellent tool called [Bastille Linux](http://www.hardworking.com/live/modules.php?op=modload&name=News&file=index&catid=&topic=3) (<http://www.hardworking.com/live/modules.php?op=modload&name=News&file=index&catid=&topic=3>). This tool "hardens" various UNIX operating systems.

Last Updated: May 26, 2004

Tripwire

Tripwire (<http://www.tripwire.org/>) is another useful tool for UNIX systems. Tripwire checks the various system files on a UNIX system to see what, if anything, has changed. Hackers change things in order to introduce more vulnerabilities or to create back door access for themselves. Tripwire helps to detect these changes.

Last Updated: May 26, 2004

Log Files

UNIX systems are able to log a wide variety of activities on the system. These include system events (device failures, reboots, etc.), user logins, and in some cases, security alerts for potential attacks. System log files should be viewed with some regularity and frequency in order for the system administrator to be aware of what is happening on and to the system. Some security guidelines recommend that the log files be stored on a different machine, or on write-once devices (CD-Rs) so that an intruder cannot erase the log of their actions.

At the very least, you should be aware of what log files are your system, what is being logged, and you should arrange to view the files periodically.

Last Updated: May 26, 2004