



# UNIX Security Tips

Produced by the CyberNEXS Team

**Siobhan Moran**  
August 2009

# Now What About UNIX?



More and more attacks are being targeted toward the variations of UNIX

- Solaris 10
- Open BSD
- Red Hat Linux
- Mac OS
- Ubuntu
- Open source

# Defending Your UNIX Box



- Simple hardening steps
  - Understand boot process, Remove unneeded accounts and groups, restrict root
- Patching
  - Keep up to date with latest patch releases
- Disable unnecessary services
  - If a service is not needed, shut it off
- Secure configuration
  - Strong passwords
  - File permissions
  - Proper configuration of services (Apache, MySQL, etc.)
- Logging
  - Configuring and monitoring Syslogs
- SANS Top Ten Vulnerabilities
  - Mitigate most common vulnerabilities

# Boot Process Review (Linux)



- BIOS\*
- First stage boot loader
- Second stage boot loader (/boot/)
  - Kernel loaded
  - /initrd loaded
    - Root file system (/) mounted read only
- /sbin/init
  - /etc/rc.d/rc.sysinit
  - /etc/inittab
  - Services loaded
  - Mount /etc/fstab partitions
- Virtual Console or shell
  - \*Basic Input/Output System

# Securing the BSD BootLoader



- /boot/loader.conf
  - Can have password protection
- Or just use GRUB\*, it's honestly easier and a better loader
- Though Loader does remember last booted OS

\*Grand Unified Bootloader

# Securing the Linux Boot Loader



- Timeout
- Password protect
  - LILO\*
    - `restricted`
    - `password = <password>`
  - GRUB
    - `/sbin/grub-md5-encrypt`
    - `password -md5 <password-hash>`
    - Use `lock` for dual boot menus
- `chmod 600 grub.conf or lib.conf`

\*Linux LOader

# UNIX Permissions



- `rwx-`
- `owner,group,world`
- `ls -l`
- `setuid*`, `rwsrwxrwx`
- `setgid**`, `rwxrwsrwx`
- sticky bit, `rwxrwxrwt`
- `chattr` and `lsattr`
- `Umask`

\*Set UserID

\*\*Set GroupID

# Permissions (continued)

- chgrp\*
- chmod\*\*
- chown\*\*\*
- Right-click → **Properties**

\*Change Group

\*\*Change Mode

\*\*\*Change Ownership

# /etc/passwd

- root:x:0:0:root:/root:/bin/bash
- Username
- Password
- User ID (UID)
- Group ID (GID)
- GECOS\*
- Home Directory
- Shell

\*General Electric Comprehensive Operating System

- juan:\$1\$. QKDPc5E\$S WlkjR WexrXYgc98F.:11956:0:90:5:30:12197:
- Username
- Encrypted password
- Date password last changed
- Minimum password age
- Maximum password age
- Number of days before a password expiration warning
- Number of days before expired password account will be disabled
- Days the account has been disabled
- Extra field

# Remove Default Users/Groups



- Users that may be removed:

- adm
- lp\*
- shutdown
- halt
- news
- mail
- uucp\*\*
- operator
- games
- gopher
- ftp\*\*\*

- Groups that may be removed:

- adm
- lp
- news
- mail
- uucp
- games
- dip

- Common UNIX uids

\*Line Printer

\*\*UNIX-to-UNIX Copy Program

\*\*\*File Transfer Protocol



## Current kernel state files (some writeable)

- /proc/meminfo
- /proc/ide
- /proc/cpuinfo
- /proc/sys
  - echo hostname > /proc/sys/kernel/hostname

# Pluggable Authentication Module (PAM)



- Advantages:
  - Provides common authentication scheme
  - Modular
  - Application independent
  - Supports many applications
  - Developer doesn't need to implement authentication, just PAM-aware

# Passwd Filters



- `passwd` is PAM aware
- `pam_cracklib.so`
  - Palindrome of old password?
  - Case change of old password?
  - Same characters as old password?
  - Is the new password too small?
  - Is it the rotated old password?
  - Has the password been used previously?

# Password Cracking



- John the Ripper
- Crack

# Limiting root Access



- Password protect the boot loader
- Disable root SSH\* logins
- Disallow root login/shell
- Prevent root login on devices
- Prevent root access to services through PAM
- Does not affect su\*\*, sudo\*\*\*, or other setuid programs

\*Secure Shell

\*\*Super User

\*\*\*"su do"

# Limiting `root` Access (continued)



- `su`
  - Use “wheel” to limit `su` access
  - `/etc/pam.d/su`
- `sudo`
  - Use `visudo` to add users to `/etc/sudoers`
  - `sudo` available for five minute session (default)
  - Logged to `/var/log/messages` and `secure`

# Runlevels



- 0 – Halt
- 1 – Single User Mode
- 2 – Multi-User Mode w/o Networking
- 3 – Full Multi-User Mode w/ Networking
- 4 – User Defined
- 5 – Full Multi-User Mode (X Windows)
- 6 – Reboot
- Using `init*/telinit`

\*Initialization

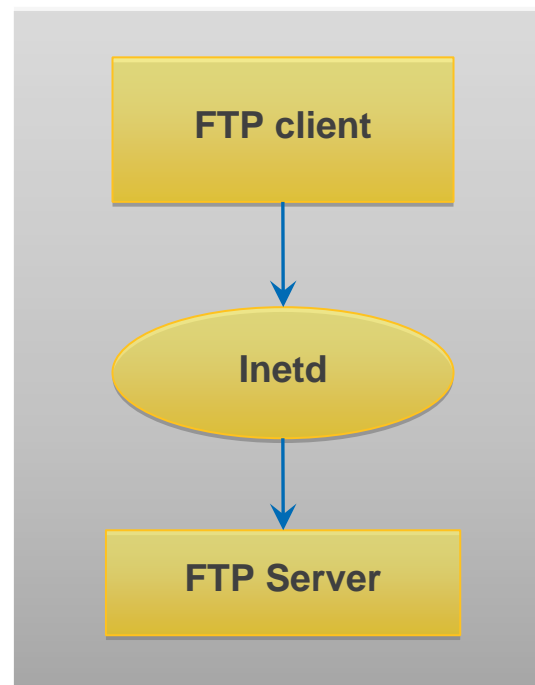
# /etc/inittab



- Default RunLevel
  - `id:5:initdefault:`
- Disable Shutdown via Ctrl-Alt-Del
  - `ca::ctrlaltdel:/sbin/shutdown -a t3 -r now`
  - `/etc/shutdown.allow`

# Inetd-based Daemons

- Inetd is a “super-daemon.” It sits in the systems process space and handles user requests by running other daemons.
- This way, memory and resources are not wasted when nobody has connected to the service.





- eXtended inetd
- Once a popular service (e.g., POP, telnet, ftp) is called, `xinetd` checks host access control information, the number of current instances of the requested service, and any other specified rules before granting access.
- Once access is granted `xinetd` is not called until the next applicable service request.

# Insecure Services



- rlogind
- rshd
- rwhod
- telnetd
- vsftpd
- wu-ftp
- sendmail
- identd

# Firewalls Should Protect These Services



- finger
- identd
- netdump
- netdump-server
- nfs
- portmap
- rwhod
- sendmail
- smb (Samba)
- yppasswdd
- ypserv
- ypxfrd

# Securing Services



## Securing X-Windows

- If you don't need X-Windows (most people don't) don't use it. There is no reason to run X-Windows if no person needs X-Window access to the machine (from the console or remotely.)

## Securing NFS\*

- If NFS is unnecessary, don't use it.
- Never mount your own exports, this is extremely dangerous.
- If you don't need anyone to write to your exports, mount them read-only.

## Securing sendmail servers

- If you don't need Sendmail, don't use it!
- Running Sendmail in server mode is not necessary to send mail from your local machine. It is only necessary when receiving email from other machines.

## Securing Web servers

- Make sure you have installed the latest version of the web-server. Previous versions usually have security fixes.

\*Network File System

# What is Running On My Machine?



- Now we know the difference between necessary and unnecessary services...how do we know what network daemons are running on our machine?
- We can use two methods
  - “netstat -a”
  - A port scanner
- Netstat\* will give us a look at what is running on the machine, but the results are difficult to read and understand. A port scanner is easier.
- lsof -i
  - List open files

\*Network Statistics

# Sun Microsystems' Patch Methods



- Sun Packages their patches using two methods:
  - Individual Patches
  - Patch Clusters
- Both Individual patches and patch clusters use the same sort of installation mechanism, but patch clusters may or may not contain all the necessary patches.

# Securing OpenSSH



- `/etc/ssh/sshd_config`
  - `ListenAddress`
  - `ServerKeyBits`
  - `LoginGraceTime`
  - `PermitRootLogin`
  - `IgnoreRhosts`
  - `PermitEmptyPasswords`

# Finding Solaris Patches and Advisories



- Recommended Security Patches can be found at:  
<http://sunsolve.sun.com/show.do>
- You can download the individual patches by clicking your OS version number on the OS column.
- Patch clusters are available by clicking on the “Download Cluster” link.

# Using Sun's Patchdiag Tool



- Sun has provided a simple tool which compares the current system patch environment with the latest patch environment Sun has available.
- To use this software, you just need to download the latest patchdiag.xref file from Sun's server.
- This command can be easily automated along with the wget command to download the latest patchdiag.xref file each night, run patchdiag, and then return the results to the user via email.

# BSD Package Tools



- port
  - Installs a source code repository
  - Then compiles, tests, installs and cleans.
- pkg\_add
  - Installs pre-compiled binaries

# Linux RPM Package Manager (RPM)



- Determine what packages are currently installed.
  - `rpm -qa`
- Package Details
  - `rpm -qi <package name>`
- Remove Package
  - `rpm -e <package name>`

# yum (Yellowdog Updater Modified)



- Command line
  - yum update (update all packages on system)
- Handles dependencies
- Utilizes repositories to provide added applications
- Also provides ability to easily install software

# Using Syslog



- Most UNIX-like OSs offer a system logging tool called syslog.
- This tool is turned on by default, but offers little monitoring capabilities when not custom configured.
- Syslog is configured by editing the file `/etc/syslog.conf`. The service must be restarted before modifications made take hold.

# Syslog Messages



## • Facilities

- Auth - Authentication log messages
- Cron - Cron log messages
- Daemon - Services log messages
- Kern - Kernel log messages
- Lpr - Print spooler log messages
- Mail - Mail spooler log messages
- Mark - Timestamp for syslog
- News - News spooler log messages
- User - Log messages for User processes
- UUCP - UUCP spooler log messages
- local - 8 locally defined log messages
- \* - Everything except mark

## • Levels

- Emerg - For panic conditions
- Alert - Errors that need to be corrected immediately
- Crit - Warnings about critical hardware/software conditions
- Err - Other error messages
- Warning - Warning messages
- Notice - Not error conditions, but requires special handling
- Info - Routine messages
- Debug - Debugging messages
- None - When used, turns off a certain facility

# Using Remote Syslog



- Two reasons for a remote syslog server
  - remote server is more secure, so logs can't be changed after the fact
  - remote server collects logs from several machines for central analysis (or maybe just because it has enough storage)
- An entry in syslog.conf that logs to a different machine instead of a file
  - Remember that this information is not encrypted
  - Remember an attacker could try and fill the disk
  - It may be necessary to tell the recipient syslog to allow it

# Bottom Line



This concludes your Unix Tips

You can't always be totally secure, but follow these simple practices and you get pretty close...

# Attribution and Trademark Statements

The Linux trademark is owned by Linus Torvalds in the U.S., Germany, the European Community, and Japan.

Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Red Hat, Red Hat Network, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc. in the United States and other countries.

SSH and Secure Shell are trademarks of SSH Communications Security, Inc.

Sun and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. or its subsidiaries in the United States and other countries.

Ubuntu is a registered trademark of Canonical Ltd.

UNIX is a registered trademark of The Open Group in the U.S. and other countries.

yum is a Gnu Public License (GPL) tool; it is freely available and can be used, modified, or redistributed without any fee or royalty provided that the terms of its associated license are followed.

All other trademarks, tradenames, or images mentioned herein belong to their respective owners.