Linux Security

By: Matthew Porter

"[UNIX] was not designed from the start to be secure. It was designed with the necessary characteristics to make security serviceable."

- Dennis Ritchie

Basic Security Guidelines

- Trust No One!
  - Only trust those who directly have something to lose.
  - You may be putting your job in that person's hands.
- No Box Is Too Small.
- Pay Attention!

Physical Security

- One of the most ignored areas of security.
- Possible theft of computer and/or hard drive(s).
- Ten seconds to denial-of-service?
  - Unplug the wires
  - Reboot the server
- Estimated that insiders initiate 80% of all intrusions.

Physical Security

- BIOS Passwords are a necessary evil, but no guarantee.
  - BIOS passwords can be wiped out via shorting the battery or a manufacturer-provided jumper switch.
  - Programs such as !BIOS by Bluefish or AMIDECOD defeat most modern BIOS password protection.
- Use LILO Passwords!
  - RedHat and Mandrake's infamous 'linux single' boot option.

Physical Security

- Why use LILO Passwords?
  - Further protection against certain physical security attacks.
  - RedHat and Mandrake's infamous 'linux single' boot option.
- Three easy steps...
  - Add the line 'password=xxxxx' in the lilo.conf file
  - Execute 'chmod 600 lilo.conf'
  - Execute 'lilo'

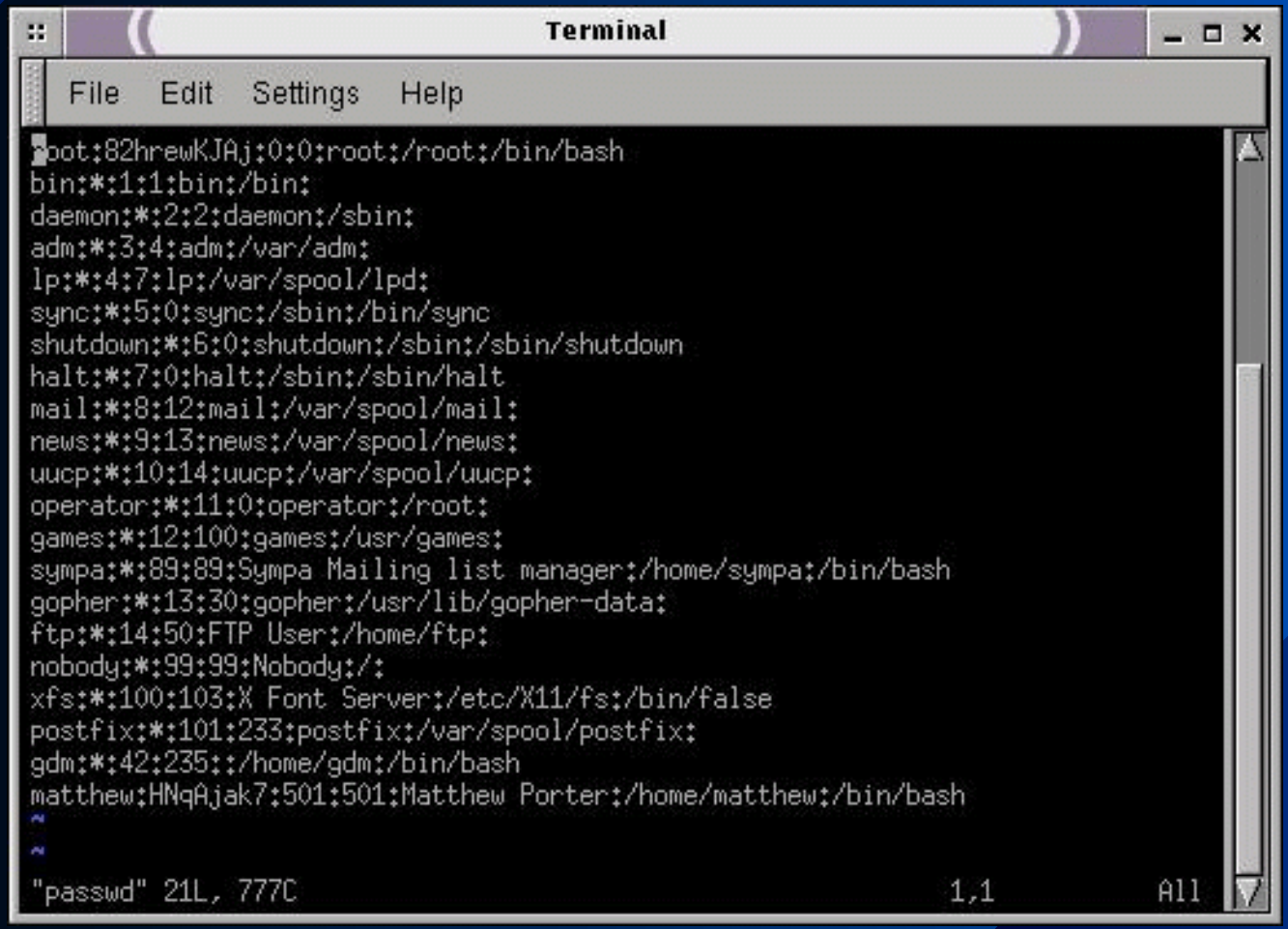
Installation Options

- Some Distributions Provide 'Hardening/Secure' Options
  - SuSE provides numerous packages
    - Secumod = kernel module, including recent setuid fix
    - Seccheck = security-checking scripts
  - Mandrake offers 'Secure' setting option

Password Security

- Passwords are traditional stored in /etc/passwd in encrypted format.
- However, this is unsafe since /etc/passwd is (and MUST BE) readable.
- Therefore, any user can view its contents.

Password Security



Password Security

The Passwords Are Encrypted, So Who Cares?

- People Often Chose Passwords That Are Easy To Remember
  - In other words, passwords that are based-on dictionary words, birthdates, names, etc.
- "Script kiddies" Have Access To Password Cracker Programs
  - Crack - http://www.users.dircon.co.uk/~crypto/index.html
  - John the Ripper - http://www.bullzeye.net/tools/crackers/john.zip

Password Security

Protection From Password Attacks

- Shadow Password Suite
  - Comes with most Linux distributions.
  - Other shadow suites available, i.e. Shadow In A Box by Michael Quan.
- Proactive Password Checkers
  - Checking the password when the user chooses a password.
- Hacking Your Own System
  - HOWEVER, ensure that the powers that be approve!!

Network Security

The Basics - Inet and Tcpwrappers

- Inetd - The Internet Super-Server
- Most distributions add more programs and services than needed.
  - Classic examples are bind, sendmail, pop3, and imap.
  - Remove and/or disable unneeded services and daemons.
  - Audit the system's /etc/inetd.conf file.

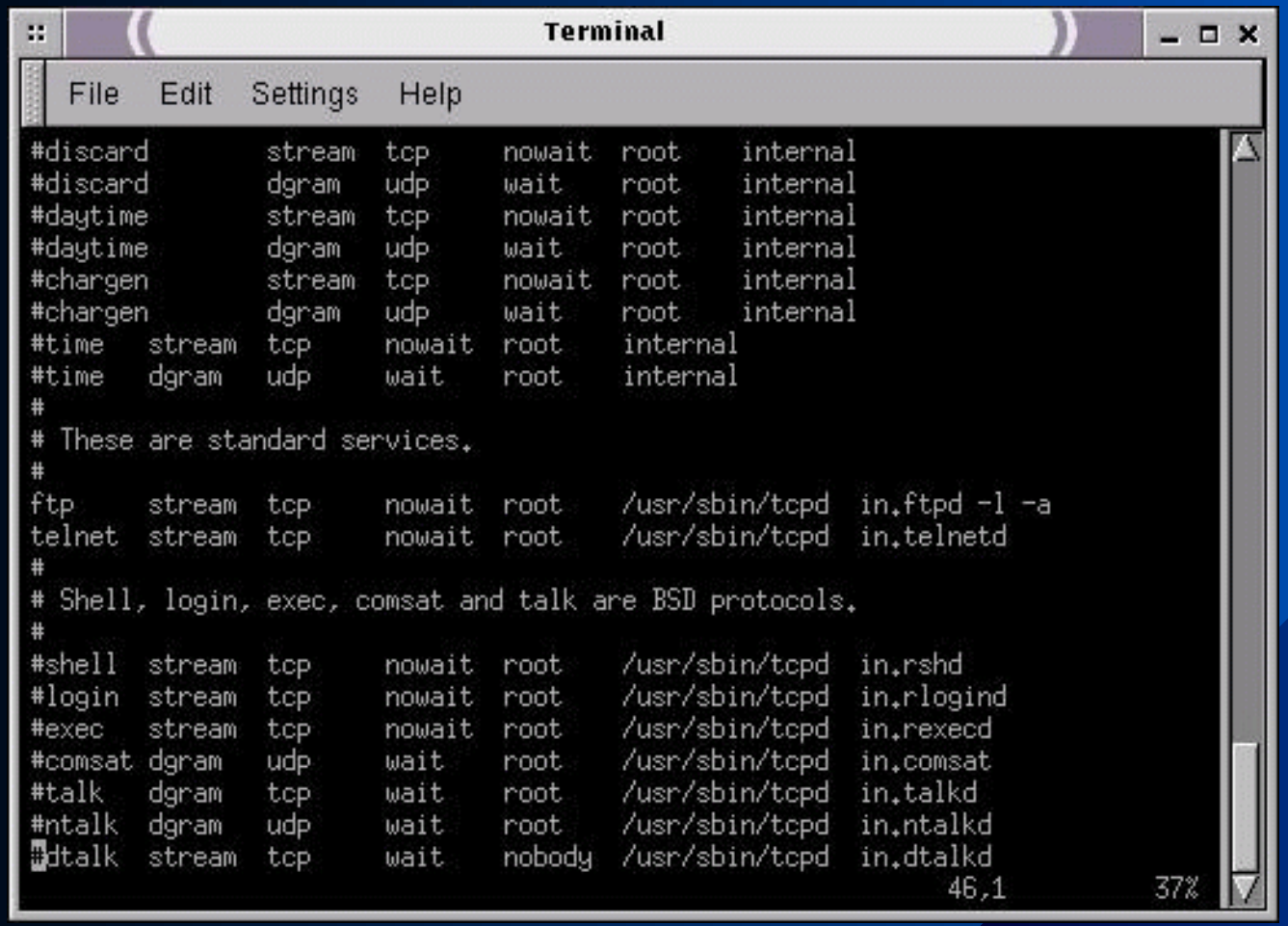
Network Security

The Basics - Inet and Tcpwrappers

- TCP Wrappers
  - Monitors and controls remote access to services implemented using inetd.
  - Control to services administered via hosts.allow and hosts.deny, in that order.

Network Security

The Basics - Inet and Tcpwrappers



Network Security

Network Sniffing At Its Finest

- What is Network Sniffing?
  - The process in which communication packets are read without the consent and/or knowledge of the user(s).

Network Security

Great the sniffer has packets, who cares?

- Why would someone sniff?
  - Unencrypted packets include numerous plaintext information (i.e. passwords, credit cards, etc.), among other goodies.
  - When installed on a gateway (internet or intranet), the sniffer can listen to all packets through the gateway.

Network Security

How Sniffers Work?

- By default, computers listen and respond only to packets addressed to them.
- Sniffers open the NIC card into promiscuous mode.
  - In this mode, the computer monitors and captures all network traffic and packets passing by- despite their true destination.

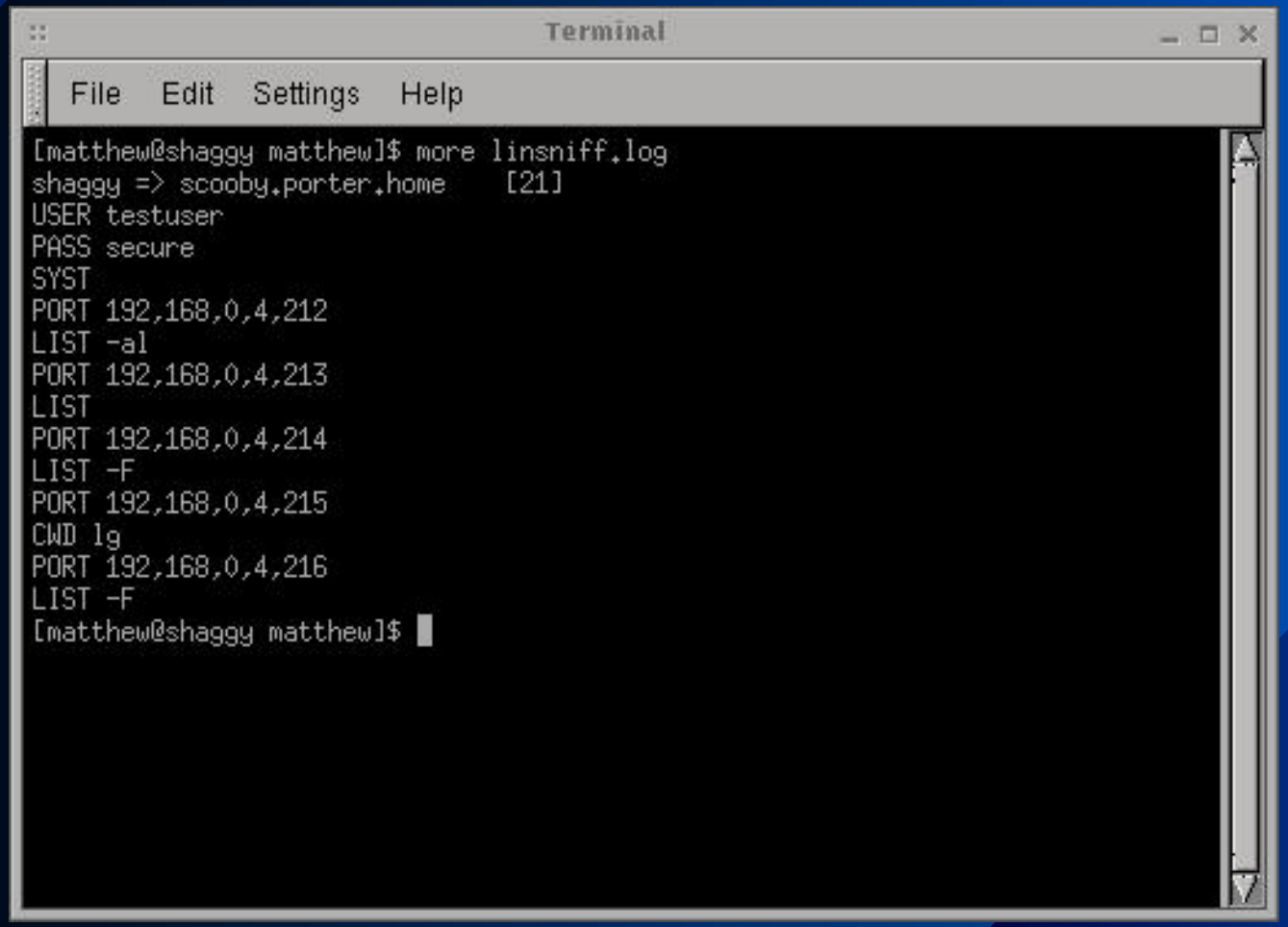
Network Security

Network Sniffers Available

- Sniffit by Richard Claerhout - http://reptile.rug.ac.be/~coder/sniffit/sniffit.html
- Linsniffer by Mike Edulla - http://agape.trilidun.org/hack/network-sniffers/linsniffer.c
- Linux_sniffer by loq - http://www.ryanspc.com/sniffers/linux_sniffer.c
- Hunt by Paul Krauz - http://www.cri.ca/kra/index.html

Network Security

Sniffit Sample Output



Network Security

How To Protect Against Network Sniffers?

- Encryption, Encryption, Encryption
  - FreeS/WAN - http://www.freeswan.org
  - Secure Shell - http://www.ssh.org
  - Open Secure Shell - http://www.openssh.com
  - PGP - http://www.pgp.com
  - GnuPG - http://www.gnupg.org

Network Security

A Detector - PortSentry by Psionic

- What is PortSentry?
  - An advanced tool that reached beyond simple port scanning. It actually attempts to identify and block the attacker in real-time.

Network Security

A Detector - PortSentry by Psionic

- PortSentry Features
  - Extensive stealth detection support for FIN, half-open, NULL, “oddball packets”, SYN, and X-MAS-style attacks.
  - Simultaneous TCP and UDP monitoring of multiple sockets.
  - State maintenance (remembering hosts that previously connected) for automagically assigning offending hosts a deny entry in TCP Wrappers.

Network Security

Port Scanning

- Scan the network for potential vulnerabilities and exploits.
- Important tools are PortSentry, SAINT, SATAN, and nmap.
- On-line tools available:
  - Http://crypto.yashy.com/nmap.php3

Denial of Service

Where did the server go?

- What is A Denial-of-Service Attack?
  - Any action, initiated by a human or otherwise, that incapacitates a host's hardware, software, or both, rendering the system unreachable and therefore denying service to legitimate users.

Denial Of Service

Examples

- Lpd Bogus Print Requests - Dec. 1998
  - Attackers send requests to server which they have no account. Lpd cannot resolve or authenticate the user. It then hangs and prevents previous and future print jobs.
- Teardrop.c - Nov. 1997
- Ping Flood

Denial Of Service

How To Protect?

- Denial of Service attacks are widely varied. Therefore, there is no unified combat tactic.
- Some Major Measures:
  - Patch the software/kernel to solve known problems.
  - Partition the hard disk in such a way that hackers cannot overflow the partition to cause excpetions in programs.
  - Set limits to the amount of utilizable resources per each user.

File Integrity

- Linux root kits are tools that can be installed on a compromised server to replace all important utilities with a changed version.
- The main purpose is to hide every information which suggests that the server has been hacked.
- Available at http://www.rootshell.com/archive-j457nxigi3gq59dv/199812/lrk4.tgz.html

Security Auditing

Linux Log Files and Third-Party Utilities

- Most Unix/Linux Programs Use The Native System Logger (syslog)
  - Three primary portions: the syslogd daemon, klogd kernel daemon, and the syslog.conf configuration file.
  - Examples of program usage:
    - Sendmail
    - Cron
    - Inn

Security Auditing

Linux Log Files and Third-Party Utilities

- TripWire free for non-commercial use
  - A flexible, easy-to-use file integrity tool that employs several algorithms (MD4, MD5, CRC32, SHA).
  - Each file has a unique fingerprint taken at the initial installation.
  - Files are checked to ensure that their fingerprints have not changed.
  - *The Design and Implementation of Tripwire: A File System Integrity Checker* -http://www.ja.net/CERT/Software/tripwire/TripWire.PS

Security Auditing

Linux Log Files and Third-party Utilities

- Open Source Tripwire Clones
  - AIDE
  - Tripwall
  - Toby IDS
  - ViperDB

Hacked! Now What?

- Call the FBI?!
  - Must show a monetary loss of at least $20,000.
- Selective Enforcement
  - Look at the log files and enforce the law against everyone.

Secure Distributions

- Bastille Linux - http://www.gl.umbc.edu/~jbeale1/
  - A comprehensive hardening program for RedHat 6.0.
- Trustix Secure Linux - http://www.trustix.net
- Secure Linux - http://www.reseau.nl/securelinux/

References

- Books
  - *Maximum Linux Security* by Anonymous
  - *Running Linux* by Welsh, Dalheimer, & Kaufman
  - *Red Hat 6 Unleashed* by Pitts and Ball

References

- Websites
  - “Improving the Security of Your Site by Breaking Into It” -http://www.securit.net/breakin.html
  - Linux Security - http://www.linuxsecurity.com
  - Security Focus (BugTraq Mailing List) - http://www.securityfocus.com
  - Security News - http://www.securitynews.org
  - CERT - http://www.cert.org
  - HERT - http://www.hert.org
  - Nmap Scan - http://crypto.yashy.com/nmap.php3