Securing your Linux System for the Internet

SHARE 98

Nashville, TN

Session 5512

Abstract

- You've gotten your Linux system installed, and are ready to connect it to the Internet. What should you do now? What can you expect to happen when you plug it into the net? What tools are available to make sure your system is secure? If you don't know the answers to these questions, then this session is for you.

The Speaker

Harold Pritchett

The University of Georgia

(706) 542-5110

harold@uga.edu

Disclaimer

Everybody has lawyers:

The ideas and concepts set forth in this presentation are solely those of the respective authors, and not of the companies and or vendors referenced within and these organizations do not endorse, guarantee, or otherwise certify any such ideas or concepts in application or usage. This material should be verified for applicability and correctness in each user environment. No warranty of any kind available.

Introduction

- Who am I?
- What makes me qualified to talk about this subject?
  - 25 Years working with computers
  - 10 Years experience with Unix
  - Unix Security Administrator
  - Security Incident Handling Team for UGA

The One Minute Security Manager

- Common Sense Security
  - Passwords
    - Use good passwords
    - Use a Shadow password file
    - Check for accounts without passwords
  - Superuser accounts
    - root
    - root equivalent accounts

The One Minute Security Manager

- Common Sense Security (cont)
  - File Permissions
    - Read, Write, Execute
    - User, group, others
    - The “chmod” command
    - The “umask” command

The One Minute Security Manager

- Common Sense Security (cont)
  - The “path”
    - Just what are you running?
    - “dot” in the path
      - Convenient for general users
      - Really bad for super users

The One Minute Security Manager

- Special Access Permission files
  - .rhosts
  - /etc/hosts.equiv
  - The “+” sign
- Security Patches
  - updateme
    - RedHat 6.1+ comes with up2date which is getting better but still requires a “ton” of prereqs

The One Minute Security Manager

- Physical Security
- Backups
- Logs
- Make sure a human reads mail sent to “root” and “postmaster”
  - /etc/aliases
  - newaliases

Things you probably don't want to do

- Anonymous FTP
- Sendmail
- Superfluous internet daemons

Things you might want to do but should think about first

- Anonymous ftp
- Web server (httpd)
- Sendmail
  - Deserves a session of its own
    - And it has one
      - Fortunately, it’s tomorrow at 9:30 in this room

Things you Really, Really should do

- Shadow Passwords
- Clean up /etc/inetd
- Clean up /etc/rc.d
- TCP Wrappers
- Secure Shell (SSH)
- Logcheck/Logrotate
- NTP
- Backups

Shadow Passwords

- Unix password file
  - Old style password file
    - World readable
    - Contains much information about users
    - Used by many programs/utilities
    - Contains encrypted passwords
  - How can I tell if I have shadow passwords?
    - grep ^root /etc/passwd

Shadow Passwords

panic$ **grep ^root /etc/passwd**

root:x:0:0:root:/root:/bin/bash

rottweiler$ **grep ^root /etc/passwd**

root:Qdr4zlDATfLWg:0:0:root:/root:/bin/bash

rottweiler$ **pwconv**

rottweiler$ **grep ^root /etc/passwd**

root:x:0:0:root:/root:/bin/bash

Shadow Passwords

- This is on by default in RedHat 6.0+
- passwords are stored in /etc/shadow
- /etc/shadow is only readable by root

```
panic$ ls -Fla shadow
-r--------   1 root     root          514 Feb 10 09:27 shadow
```

System Startup

- There are three places where programs are started when you boot your system
- /etc/inittab
- /etc/rc.d
- /etc/inetd.conf

How to find what's running

- ps –ax | more
  - Displays processes running on the system
- netstat –l | more
  - Displays processes which are "listening" on network sockets

Output from “netstat –l”

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:smtp                  *:*                     LISTEN
tcp        0      0 *:printer               *:*                     LISTEN
tcp        0      0 *:telnet                *:*                     LISTEN
tcp        0      0 *:auth                  *:*                     LISTEN
tcp        0      0 *:1006                  *:*                     LISTEN
tcp        0      0 *:sunrpc                *:*                     LISTEN
udp        0      0 *:1004                  *:*
udp        0      0 *:1024                  *:*
udp        0      0 *:sunrpc                *:*
raw        0      0 *:icmp                  *:*                     7
raw        0      0 *:tcp                   *:*                     7
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node Path
unix  0      [ ACC ]     STREAM     LISTENING     520    /dev/printer
```

inetd

- The “Internet Daemon”
- Runs the majority of internet services
- RedHat 5 and 6
- Uses /etc/inetd.conf
- Edit inetd.conf to remove ALL unwanted or unneeded services
- Take no prisoners!

Inetd.conf

```
ftp    stream tcp nowait root /usr/sbin/tcpd in.ftpd -l -a
telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd
gopher stream tcp nowait root /usr/sbin/tcpd gn
shell  stream tcp nowait root /usr/sbin/tcpd in.rshd
login  stream tcp nowait root /usr/sbin/tcpd in.rlogind
talk   dgram  udp wait   root /usr/sbin/tcpd in.talkd
ntalk  dgram  udp wait   root /usr/sbin/tcpd in.ntalkd
pop-2  stream tcp nowait root /usr/sbin/tcpd ipop2d
pop-3  stream tcp nowait root /usr/sbin/tcpd ipop3d
imap   stream tcp nowait root /usr/sbin/tcpd imapd
finger stream tcp nowait root /usr/sbin/tcpd in.fingerd
```

Inetd.conf

```
ftp     stream tcp nowait root /usr/sbin/tcpd in.ftpd -l -a
telnet  stream tcp nowait root /usr/sbin/tcpd in.telnetd
#gopher stream tcp nowait root /usr/sbin/tcpd gn
#shell  stream tcp nowait root /usr/sbin/tcpd in.rshd
#login  stream tcp nowait root /usr/sbin/tcpd in.rlogind
#talk   dgram  udp wait   root /usr/sbin/tcpd in.talkd
#ntalk  dgram  udp wait   root /usr/sbin/tcpd in.ntalkd
#pop-2  stream tcp nowait root /usr/sbin/tcpd ipop2d
#pop-3  stream tcp nowait root /usr/sbin/tcpd ipop3d
imap    stream tcp nowait root /usr/sbin/tcpd imapd
#finger stream tcp nowait root /usr/sbin/tcpd in.fingerd
```

xinetd

- The “Internet Daemon”
- Runs the majority of internet services
- RedHat 7
- Uses /etc/xinetd.conf and /etc/xinetd.d
- Use the chkconfig command to disable ALL unwanted or unneeded services
- Take no prisoners!

chkconfig and xinetd

```
[root@grumpy /etc]# chkconfig --list
atd             0:off   1:off   2:off   3:on    4:on    5:on    6:off
arpwatch        0:off   1:off   2:off   3:off   4:off   5:off   6:off
xinetd based services:
        rexec:  off
        rlogin: off
        telnet: off
        rsync:  off
[root@grumpy /etc]#
```

chkconfig and xinetd

```
[root@grumpy /etc]# chkconfig --list time
time            off
[root@grumpy /etc]# chkconfig --level 345 time on
[root@grumpy /etc]# chkconfig --list time
time            on
[root@grumpy /etc]# chkconfig --level 345 time off
[root@grumpy /etc]# chkconfig --list time
time            off
[root@grumpy /etc]#
```

/etc/rc.d

- Controls services which run as daemons
- Hierarchy of directories based upon run level
- Can both start and stop services when run level changes
- One set of scripts located in /etc/rc.d/init.d

ls –F /etc/rc.d

init.d/
rc0.d/
rc1.d/
rc2.d/
rc3.d/
rc4.d/
rc5.d/
rc6.d/
rc*
rc.local*
rc.sysinit*

ls -F /etc/rc.d/init.d

atd*
crond*
functions*
gpm*
halt*
identd*
inet*
ipchains*
kdcrotate*
lpd*
netfs*
network*
nfs*
nfslock*
pcmcia*
portmap*
random*
rstatd*
rusersd*

Runlevels

- 0 - Halt
- 1 – Down to Single User
- 2 – Multiuser (no networking)
- 3 – Full Multiuser mode
- 4 – Not used
- 5 – Multiuser mode with X11
- 6 - Reboot
- S – Single user mode

ls -F /etc/rc.d/rc3.d

K20nfs@
K20rstatd@
K20rusersd@
K20rwalld@
K20rwhod@
K34yppasswdd@
K50snmpd@
K84ypserv@
K92ipchains@
S05kudzu@
S10network@
S11portmap@
S16apmd@
S20random@
S25netfs@
S30syslog@
S35identd@
S40atd@
S80sendmail@
S99local@

Turning off services

- chkconfig --del service
- Edit script in /etc/rc.d/init.d
  - Add exit 0 at beginning of script
- Rename script in /etc/rc.d/init.d
  - mv service service.old
  - echo “exit 0” > exit.script
  - ln –s exit.script service

/etc/inittab

- Some services are started here
- Comment out lines to prevent starting of services
- There is usually nothing in inittab which needs to be changed.

TCP Wrappers

- Started from inetd
- Controls access to other daemons started from inetd
- Uses configuration files to determine access
  - /etc/hosts.deny
  - /etc/hosts.allow

TCP Wrappers

- /etc/hosts.deny

```
#
# hosts.deny
#       This file describes the names of the hosts which
#       are *not* allowed to use the local INET services,
#       as decided by the '/usr/sbin/tcpd' server.
#
ALL:    ALL
```

TCP Wrappers

- /etc/hosts.allow

```
#
# hosts.allow
#
sshd:          128.192.6. 128.192.254. 24.2.26.138
sshd:          128.192.1.
in.ftpd:       128.192.6. 128.192.254. 24.2.26.138
```

TCP Wrappers

- /etc/inetd.conf

```
#
# inetd.conf
#
# <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
ftp       stream  tcp     nowait  root    /usr/sbin/tcpd  in.ftpd -l -a
telnet    stream  tcp     nowait  root    /usr/sbin/tcpd  in.telnetd
```

Secure Shell

- An implementation of the Secure Socket Layer (SSL)
- Free for Educational and non-commercial use
- Commercial version available
- Developed at The Helsinki University of Technology
- Available on the Internet
- Included with RedHat Linux 7.0

Secure Shell

- Automatic authentication of users
- Multiple strong authentication methods
- Authentication of both ends of connection
- Automatic authentication using agents
- Encryption and compression of data
- Tunneling and encryption of arbitrary connections

Secure Shell

- Cryptographic algorithms available
  - Triple DES (Default)
  - Blowfish
  - Twofish
  - Arcfour
  - Idea
  - Cast
  - RSA

LogCheck

- Linux logs a tremendous amount of info
- People just don’t read logs
- Most of what is in the logs is normal
- The normal stuff hides the important stuff
- Let the computer read the logs and separate the important stuff from the junk

LogCheck

- Written by Craig Rowland
- Scans logs for interesting entries
- Free
- Now called LogSentry
- Available for download at
  - http://www.psionic.com/abacus/logcheck/

LogCheck

- LogCheck uses four configuration files
  - logcheck.hacking
  - logcheck.violations
  - logcheck.violations.ignore
  - logcheck.ignore
- Files are applied in the order shown
- Every line is a “regular expression”

LogWatch

- Another Log Analyzer
  - Distributed standard with RedHat 7.2
  - Written by Kirk Bauer <kirk@kaybee.org>
  - http://www.kaybee.org/~kirk
  - Configuration files in /etc/log.d
  - Does not appear to be as easily configured as logcheck

TCPLOGD

- Port scanners
- Three way handshake required for logging
- Tcplogd can log on single “syn” packet
- http://www.tigerteam.net/linuxgroup/tcplogd/

TCPLOGD

```
tar -zxf tcplogd-0.1.5pre1.tar.gz
cd tcplogd-0.1.5
./configure
./make
su -
make install
make cf-install
make rh-install
vi /etc/syslog.conf
vi /usr/local/etc/tcplogd.cf
/etc/rc.d/init.d/tcplogd.init start
```

Logrotate

- Comes with RedHat Linux
- Debian does something Different
- Slackware doesn’t do this at all
- YMMV
- Freely available from Redhat.com
  - Should build on any version of Linux

Logrotate

- Check and update /etc/logrotate.conf
  - Allows for keeping old logs
  - Keeps logs from filling up disk
  - Different logs can have different parameters
  - Can also use files in the directory /etc/logrotate.d

Updateme

- Locally written UGA utility
- Checks for new versions of software
- Can be configured to use any RedHat distribution site
  - Configuration file
  - Command line argument

/usr/local/etc/updateme.cf

site=acs-mirror.ucsd.edu

updatedir=/linux/redhat/updates/7.2/en/os/i386

site=sunsite.unc.edu

updatedir=/pub/linux/distributions/redhat/updates/7.2/en/os/i386

Alternatives to updateme

- up2date
  - Comes with RedHat 6.2+
  - Has a LOT of prereqs
- AutoRPM
  - By Kirk Bauer
  - Can download updates for later installation
  - Can download and install updates

Tripwire

- Monitors system for modified files
- Many versions, most commercial
- Tripwire for linux is open source under GPL
  - http://sourceforge.net/projects/tripwire
- Distributed with RedHat 7.2
  - tripwire-2.3.1-5.i386.rpm

Tripwire

- Uses passwords and cryptographic signatures to protect configuration files
- Default configuration may take some fixing
  - Comes with many non-existent files defined
  - Run it once and use the output to edit the twpol.txt file. You probably also want to remove /var/log from checking.
- Run from cron once a day to audit system

Tripwire

- rpm -Uvh tripwire-2.3.1-5.i386.rpm
- /etc/tripwire/twinstall.sh
  - Answer prompts
  - Use good passphrases
- tripwire --init
- tripwire --check
  - Check output and edit twpol.txt, removing all files reported as missing and fixing the HOSTNAME variable
- tripwire --update-policy –Z all twpol.txt
- tripwire --check

Tripwire

- When something changes
  - Tripwire will find it.
  - If it's OK, then run:
    - tripwire --update –r /full/path/to/latest/report.twr
  - If it's NOT OK, then replace the files from the backup tape.

Network Time Protocol

From NBS Special Publication 432 (out of print)

Do you know what time it is?

Better still,

does your computer know what time it is?

NTP

- Network Time Protocol
- Developed by Dave Mills at The University of Deleware (mills@udel.edu)
- Sets computer clock automagically
- Previous version is xntp-3.5.93 and is on the RedHat 6.1 CDROM
- Current version is ntp-4.0.99k and is on the RedHat 7.1 CDROM

NTP

- Can set the clock from various sources
  - Reference Time Standards
  - Broadcast Standards (WWVB)
  - GPS receivers
  - Network
- Configuration File
  - /etc/ntp.conf

NTP

- Network Time Standards
  - Public vs Private
  - Primary vs Secondary
  - Server List
    - http://www.eecis.udel.edu/~mills/ntp/servers.htm
    - Pick a server near you
    - Use a “Public” server
    - Do NOT use a “Primary” Server

Backups

- Not really optional
- Two reasons
  - Catastrophic failure of a system
  - Oops...
- Run from “cron”
- Format
  - tar (unix Tape ARchive command)
  - dump

Backups

- Media
  - Fixed
    - Local Disk
    - Remote Disk (networked)
  - Removable
    - Tape
    - Disk (Zip or Jaz)
    - Floppy

Backups

- Stearns' Law
- Cost of drive vs cost of media
- Tape robots
- Some types of drives
  - Exabyte (8mm)
  - DAT (4mm)
  - DLT
  - Travan
  - LTO
  - ?

Backups

```
#!/bin/sh

/bin/mt -f /dev/st0 rewind
cd /
tar --exclude proc -cvf /dev/st0 . | gzip > /local/backup.log.gz
status=$?
if [ $status != 0 ]
then
  echo "backup had trouble.  tar exit status was $status."
fi
```

References

- LINUX HOWTO documents
  - Should be on your Install CD, or from http://metalab.unc.edu/LDP/

References

- SSH
  - http://www.ssh.com/ (commercial version)
  - http://www.ssh.org/ (educational version)
- LogCheck
  - http://www.psionic.com/abacus/logcheck/
- NTP
  - RFC 1796
  - http://www.eecis.udel.edu/~ntp/

References

- TCPLOGD
  - http://www.tigerteam.net/linuxgroup/tcplogd
- Some unofficial RPMs (Built for RH 6.2)
  - ftp://linuxserv.uga.edu/pub/unix/linux/uga

References

- General Security References
  - //www.alw.nih.gov/Security/security.html
  - //www.usg.edu/oiit/support/security/
  - //csrc.ncsl.nist.gov/
  - //www.cert.org/

Session 5512
Th-th-th-that's all folks

- Questions?

Survey – Optional question 3

- How would you prefer to receive the handouts
  - 1-up – check the “Excellent” box
  - 2-up – check the “Good” box
  - 3-up – check the “Average” box
  - 4-up – check the “Below Average” box
  - 6-up – check the “Poor” box