How to improve security on your Linux box

Yoonsuck Choe

The University of Texas at Austin

Sep 22, 1998

What this talk IS about

- Detecting a novice intruder
- Recovering (if broken into)
- Preventing easy break-ins

What this talk is NOT about

- Detecting a MASTER HACKER
- Recover to make your system 100% FOOL-PROOF
- Preventing ALL future break-ins

Why all this?

- More Linux boxes are being setup at home
- Over-featured Linux distributions
- Longer on-line time than ever
- Easily available tools for hacking

The three steps to secutiry

- Detection
- Recovery
- Prevention

Detection

Simple skills of detection can save your day (and your computer).

Major things to keep track of:

- System log files
- Configuration files
- Binary files
- Network traffic

Detection: System log files

Important files:

- /var/log/messages (general)
- /var/log/secure (network connection)
- /var/log/xferlog (ftp)
- /var/log/wtmp (login)
- and others (of course) :-)

Detection: System logs: What to look for

- Short or incomplete logs
- Strange timestamps
- Records of reboots or restarting of services
- Missing log
- su entries or logins from strange places

Detection: System logs: Examples

```
[EX1: ILLEGAL USER]
Aug 27 14:19:11 lite syslog: FAILED LOGIN 1 FROM lite FOR rewt,
User not known to the underlying authentication module

[EX2: suspicious su]
Aug 27 14:18:21 lite PAM_pwdb[23619]: 1 authentication failure;
yschoe(uid=504) -> root for su service
Sep 21 15:57:47 lite PAM_pwdb[26536]: (su) session opened for user
root by yschoe(uid=0)

[EX3: syslogd restarted]
Sep 20 01:02:03 lite syslogd 1.3-3: restart.

[EX4: /var/log/secure, access log]
Aug 25 22:52:46 lite in.ftpd[15049]: refused connect from dial-127-4.
ots.utexas.edu
Aug 27 14:19:07 lite in.telnetd[23626]: connect from evil.com
Aug 23 02:12:09 lite in.fingerd[774]: connect from 128.83.141.173
```

Detection: Configuration files

System configuration files that can lead to a hole in security.

- /etc/passwd
- /etc/inetd.conf
- /etc/hosts.allow /etc/hosts.deny
- /etc/crontab
- /etc/ftpusers
- /etc/syslog.conf

Detection: Config files: /etc/passwd

/etc/passwd file format

userid:encrypted-passwd:UID:GID:info:home-dir:shell

```
- new account
  hacker:sXfkjsj.dflj:999:100:Lord of Hell,,,,:/home/hacker:/bin/bash

- account with no password,
  root::0:0:root:/root:/bin/sh

- unusual user shell

- accounts that usually are not allowed to be logged on having a passwor
  bin:*:1:1:bin:/bin:

- commented out entry (with '#').
  #hacker:sXfkjsj.dflj:999:100:Lord of Hell,,,,:/home/hacker:/bin/bash
```

Detection: Config files: /etc/inetd.conf, /etc/hosts.allow, /etc/hosts.deny

- /etc/inetd.conf specifies what network services are available
- /etc/hosts.allow and hosts.deny controls access to (1) certain $\underline{Services}$ from (2) certain $\underline{Domains}$.

Detection: Config files:

/etc/inetd.conf

tcpd is used to selectively allow/deny access to these services

```
#
# These are standard services.
#
# <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

#
# Pop and imap mail services et al
#
pop-2   stream  tcp     nowait  root    /usr/sbin/tcpd evil-ipop2d
pop-3   stream  tcp     nowait  root    /usr/sbin/tcpd evil-ipop3d
imap    stream  tcp     nowait  root    /usr/sbin/tcpd evil-imapd
```

Detection: Config files: /etc/crontab

Run stuff at a regular interval.

Intruder can UNDO all changes if crontab was not checked.

```
[FORMAT: /etc/crontab]
<minute> <hour> <day-o-month> <month> <weekday> command arg(s)

[EX1. /etc/crontab]
# run five minutes after midnight, every day
5 0 * * *       $HOME/bin/daily.job >> $HOME/tmp/out 2>&1

# run at 2:15pm on the first of every month
15 14 1 * *     $HOME/bin/monthly

23 0-23/2 * * * echo "run 23 minutes after midn, 2am, 4am ..., everyday"

5 4 * * sun     echo "run at 5 after 4 every sunday"

30 1 * * *  /bin/cp /dev/.evil/login /bin/login  # plant trojan
```

Detection: Config files:

/etc/syslog.conf

Syslog configuration could have been changed to conceal intruder’s activity.

```
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;news.none;authpriv.none       /var/log/messages

# The authpriv file has restricted access.
# authpriv.*                                     /var/log/secure

# Blackhole!
authpriv.*                                     /dev/null
```

Detection: Binaries

Replaced system programs can be an IMMEDIATE risk.

(1) Illegal Access (2) Hide Activity (3) User to ROOT

```
*** BINARY ***              *** ADDED FUNCTION ***
/bin/login                  remote access (as root)
/bin/ps                     hide processes
/bin/top                    hide processes
/bin/ls                     hide files
/usr/bin/du                 hide files
/bin/netstat                hide network activity
/sbin/ifconfig              hide sniffing
/usr/bin/passwd             user->root
/bin/chfn                   user->root
/bin/chsh                   user->root
/usr/bin/last               hide lastlog
/usr/sbin/inetd             remote access
/usr/sbin/in.rshd           remote access
/usr/sbin/syslogd           hide system log
/usr/sbin/tcpd              hide connections, avoid denies
```

Detection: Binaries: setuid

File: $\underline{trojan}$ Owner: $\underline{root}$ Setuid: $\underline{ON}$ $\rightarrow$ any user running $\underline{trojan}$ runs it under $\underline{root}$ privileges.

- Find all setuid programs

```
$ /bin/ls -l /bin/login
-rwsr-xr-x   1 root     root        18732 Jul  1 02:11 /bin/login

$ /bin/find / -perm +4000 -exec ls -l '{}' ';'
...

$ /bin/find /bin -perm +4000 -exec ls -l '{}' ';'
-rwsr-xr-x   1 root     root        12448 Sep 22  1997 /bin/ping
-rwsr-xr-x   1 root     root        29732 Feb  7  1997 /bin/mount
-rwsr-xr-x   1 root     root        16376 Feb  7  1997 /bin/umount
-rwsr-xr-x   1 root     root        26136 Apr 18  1997 /bin/su
-rwsr-xr-x   1 root     root        18732 Jul  1 02:11 /bin/login
```

Detection: Binaries: What to check

Check for these things:

- File size (ls -l filename)
- md5sum (md5sum filename)
- RPM verification (rpm -Va) – covers all the above.

Detection: Binaries: How to check

- Check the MD5 checksum

```
$ /usr/bin/md5sum /bin/login
623f6bce62fc6588975d35c5ca197689  /bin/login
```

- Verifying the installed RPMs

```
*** Example ***                   *** Symbols ***
$ /bin/rpm -Va
S.5....T c /etc/exports           5      MD5 sum
SM5....T c /etc/hosts.allow       S      File size
SM5....T c /etc/hosts.deny        M      mode
.......T   /usr/bin/biff          T      Mtime
.......T   /usr/bin/finger        c      it may be a config file
S.5....T   /bin/login
.......T   /usr/bin/ftp
```

Detection: Network traffic

Check if suspicious activity is going on at the moment.

- /bin/netstat (check all network connections)

```
$ /bin/netstat -a
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address           Foreign Address        Stat
tcp        0      0 dial-10-11.ots.ute:1023 cheddar.cs.utexas.ed:22 ESTB
tcp        0      0 dial-10-11.ots.utexa:22 evil.com:36096         ESTB
```

- /sbin/ifconfig (check network card interface)

```
$ /sbin/ifconfig
eth0      Link encap:10Mbps Ethernet  HWaddr 00:A0:24:64:66:B3
          inet addr:172.16.1.1  Bcast:172.16.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:12251 errors:0 dropped:0 overruns:0
          TX packets:11998 errors:0 dropped:0 overruns:0
          Interrupt:5 Base address:0x300
```

Detection: Miscellaneous

- .rhosts (allows access w/o passwd verification)

```
$ find /home -name .rhosts -exec ls -l '{}' ';'
...
```

- /dev/ directory (check for regular files)

```
[Legal]
crw-rw-rw-   1 root     tty        2, 176 Aug  2  1996 ptya0
crw-rw-rw-   1 root     tty        2, 177 Aug  2  1996 ptya1
crw-rw-rw-   1 root     tty        2, 178 Aug  2  1996 ptya2

[Illegal]
$ find /dev -mode f -exec ls -l '{}' ';'
-rw-------   1 root     root           81 Jul  1 15:58 ptyp
-rw-------   1 root     root           75 Jul  1 15:58 ptyq
-rw-------   1 root     root           67 Jul  1 15:58 ptyr
-rw-------   1 root     root           56 Jul  1 15:58 ptys

Regular files often contain config info for hacker's tools.
```

Recovery

After an intrusion has been detected, follow these steps:

- Preserve the evidence
- Reinstall OS
- *or* Reinstall damaged components

Recovery: Preserving the evidence

Preserve all peices of evidence before removing anything. (timestamp and mode are important)

- log files
- copies of trojaned binaries (be careful with setuid programs)
- altered config files
- other files left behind by the intruder

Recovery: Reinstall OS or replace damaged components

- Reinstalling the OS is recommended
- Don’t forget to apply security patches
- Great care should be taken if only recovering damaged components only
- Follow guidelines in ”Prevention ...”

Prevention

Some simple changes can dramatically improve security on your system.

- Do not run unnecessary services (httpd, named, ..)
- Restrict remote access (tcdp)
- Install security patches
- Use SSH, the Secure SHell
- Continuous (or occasional) monitoring
- Conceal your identity (/etc/issue.net)

Prevention: Unnecessary services I

In /etc/inetd.conf, comment out unnecessary services:

Most stuff are not necessary except for (1)telnet and (2) ftp:

- imap/ipop
- tftp
- auth
- gopher etc.

* Comment out with '#' at the beginning, and restart inetd.

Prevention: Unnecessary services II

To stop certain services from running at boot time: (1) Edit /etc/rc.d/rc[n].d/* (2) or, use Run-level-editor

- httpd (Web server)
- named (DNS server)
- nfs, nfsfs (NFS service)
- smb (Samba : Windows connectivity)
- news (NNTP service)

* Don't forget to stop currently running ones

Prevention: Restricting Access

Use *tcpd* to selectively block access.

(1) /etc/hosts.allow (2) /etc/hosts.deny

```
File format:
<service> : <domain> [ : <action> ]

#
# /etc/hosts.allow
#
ALL : 128.83.141. .csres.utexas.edu .cs.utexas.edu 127.0.0.1

#
# /etc/hosts.deny
#
ALL : ALL \
: spawn (/usr/sbin/safe_finger -l @%h | \
/bin/mail -s "%d->%h" yschoe@cs.utexas.edu ) &

* accesses (denied or allowed) are logged to /var/log/secure .
* restart inetd after configuring these files.
```

Prevention: Install Security Patches

Security patches are avaiable from RedHat, in RPM format.

- Download from *http://www.redhat.com/linux-info/security/*
- Then, run
  rpm -Uvh *filename*
- Also, check the newsgroup for recent news
  comp.security.announce

Prevention: Use SSH

Secure SHell encrypts everything. More and more institutions are making the use of SSH mandatory.

- http://www.cs.hut.fi/ssh/
- http://www.cs.utexas.edu/users/nn/pages/private-pages/ssh.html

Prevention: Continuous monitoring

Regularly do steps described in ”Detection ...”.

- Check log files / config files
- Check binaries
- Check access logs
- Check network
- Install monitoring tools (COPS/tripwire)

Resources

Web pages, magazines, books, etc.

- http://www.cert.org/
- http://www.redhat.com/linux-info/security/
- http://www.linuxjournal.com/
- http://www.rootshell.com/
- Linux Security-HOWTO

* Complete list at http://www.cs.utexas.edu
/users/nn/pages/private-pages/redhat-security.HOWTO.html

Tools

```
cops  : does a general security check of your system

           ftp://ftp.cert.org/pub/tools/cops

sudo  : SUperuser DO -- lets regular users run certain commands
           as root.  Useful if you have to grant root privileges to
           regular users.

           ftp://sunsite.unc.edu/pub/Linux/system/Admin

tripwire : keeps checksums of important system files (hence the
           name 'tripwire') and check for the integrity from
           time to time.

           ftp://coast.cs.purdue.edu/pub/COAST/Tripwire

saint : checks network security

           http://www.wwdsi.com/saint
```

Minimal security checklist

```
=========================+=======================================
file/dir                 | what to do
=========================+=======================================
/etc/inetd.conf          : remove unnecessary services (*)
-------------------------+---------------------------------------
/etc/hosts.allow         : tcpd -- allow services to other hosts (*)
/etc/hosts.deny          : tcpd -- deny services to other hosts (*)
-------------------------+---------------------------------------
/etc/issue.net           : conceal your identity
/etc/rc.d/rc.local       : prevent from overwriting /etc/issue.net
-------------------------+---------------------------------------
/etc/rc.d/rc<n>.d/       : remove unnecesary server scripts (**)
-------------------------+---------------------------------------
(*): restart inetd.
(**): stop servers /etc/rc.d/init.d/<serverscriptname> stop
```