

Hardening Linux

Lance Albertson - lance@ksu.edu
UNIX System Administrator

Dan Lang - dlang@ksu.edu
UNIX System Administrator

Summary

- General
- Packages
- Services
- 10 Basic Steps
- Apache Tips

Choosing the right Distribution

- Choose a widely used Linux distribution
- Release security updates in a timely manner
- Choose something that is easy to use
- Suggestions:
 - Redhat, Debian, Suse, Gentoo (for advanced users)

Plan Filesystem Layout

- Avoid single partition approach
- Use LVM to help divide up directories
- Create volumes for at least:
 - /, /boot, /tmp, /var, /usr, /home*
- Set safe mount options for /tmp and /home
 - noexec, nodev, nosuid

* Only if you have a lot of users on the system

Avoid Unnecessary Packages

- First, know how to use the package management system for your distro
- Try and keep a minimal set of packages
- Remove anything you know you don't need
- Avoid binaries that have setuid root
- Avoid X, compilers, dev tools

Passwords, Creating Users

- Review `/etc/passwd` and `/etc/shadow` for default users
- Lock out non-interactive accounts
 - Add `!!` in the password field
 - Replace shell with `/bin/false`
- Configure and use `sudo` (audit trail)

Passwords, Creating Users (cont'd)

```
# Example of locked system user  
ntp:! :13371:0:99999:7:::
```

```
# Locking out a user  
passwd -l userfoo
```

```
# Changing shell for a user  
usermod -s /bin/false ntp
```

```
# Adding a user to a group  
gpasswd -a foouser foogroup
```

Disable Unnecessary Daemons / Network Services

- Check what is enabled for the default runlevel (chkconfig for Redhat, rc-status for Gentoo)
- Disable things you don't need like telnetd
- Disable inetd services you don't need
- Use netstat/ps to check for listening services
 - netstat -anlp (check for listening programs)
 - ps -ef (check for processes running)

Disable Unnecessary Daemons / Network Services (cont'd)

```
ignite ~ # netstat -tnulp
```

```
Active Internet connections (only servers)
```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	127.0.0.1:3306	0.0.0.0:*	LISTEN	15053/mysqld
tcp	0	0	127.0.0.1:53	0.0.0.0:*	LISTEN	6322/named
tcp	0	0	38.99.66.48:53	0.0.0.0:*	LISTEN	6322/named
tcp	0	0	38.99.66.47:53	0.0.0.0:*	LISTEN	6322/named
tcp	0	0	0.0.0.0:25	0.0.0.0:*	LISTEN	22572/master
tcp	0	0	127.0.0.1:953	0.0.0.0:*	LISTEN	6322/named
tcp	0	0	:::993	:::*	LISTEN	18978/couriertcpd
tcp	0	0	:::80	:::*	LISTEN	31967/apache2
tcp	0	0	:::22	:::*	LISTEN	13894/sshd
tcp	0	0	:::1:953	:::*	LISTEN	6322/named
tcp	0	0	:::443	:::*	LISTEN	31967/apache2
udp	0	0	0.0.0.0:33410	0.0.0.0:*		6322/named
udp	0	0	0.0.0.0:161	0.0.0.0:*		21937/snmpd
udp	0	0	127.0.0.1:53	0.0.0.0:*		6322/named
udp	0	0	38.99.66.48:53	0.0.0.0:*		6322/named
udp	0	0	38.99.66.47:53	0.0.0.0:*		6322/named

Disable Unnecessary Daemons / Network Services (cont'd)

```
ignite ~ # ps -ef | grep ^root | less
root      20165      1    0 Sep20 ?           00:00:53 /usr/sbin/syslog-ng
root      29660      1    0 Sep20 ?           00:00:00 /usr/sbin/ntpd
root      27329      1    0 Sep20 ?           00:00:00 /usr/sbin/cron
root       9669      1    0 Sep20 tty1         00:00:00 /sbin/agetty 38400 tty1 linux
root       7168      1    0 Sep20 tty2         00:00:00 /sbin/agetty 38400 tty2 linux
root      22350      1    0 Sep20 tty3         00:00:00 /sbin/agetty 38400 tty3 linux
root       7838      1    0 Sep20 tty4         00:00:00 /sbin/agetty 38400 tty4 linux
root      22638      1    0 Sep20 tty5         00:00:00 /sbin/agetty 38400 tty5 linux
root      29160      1    0 Sep20 tty6         00:00:00 /sbin/agetty 38400 tty6 linux
root      11927      1    0 Sep20 ?           00:00:00 sshd: lance [priv]
root       6307  22529    0 Sep20 pts/5        00:00:00 su -
root      32760    6307    0 Sep20 pts/5        00:00:00 -su
root      13894      1    0 Sep20 ?           00:00:11 /usr/sbin/sshd
root      31967      1    0 Sep20 ?           00:00:03 /usr/sbin/apache2 -D DEFAULT_VHOST -D SSL -
D SSL_DEFAULT_VHOST -D USERDIR -D PHP4 -d
/usr/lib/apache2 -f /etc/apache2/httpd.conf -k start
root      22572      1    0 Sep20 ?           00:00:13 /usr/lib/postfix/master
root      15550      1    0 Sep20 ?           00:00:00 /usr/sbin/courierlogger -pid=/var/run/
authdaemon.pid -start /usr/lib/courier/courier
-authlib/authdaemond
root       6331  15550    0 Sep20 ?           00:00:00 /usr/lib/courier/courier-authlib/
authdaemond
root       2118    6331    0 Sep20 ?           00:00:00 /usr/lib/courier/courier-authlib/
authdaemond
```

Safe sshd Settings

```
# Disable Remote Root Logins
PermitRootLogin no
# Enable privilege separation
UsePrivilegeSeparation yes
# Force version 2
Protocol 2
# May want to disable these if not
# using them
AllowTcpForwarding no
X11Forwarding no
# Enforce file permission checks
StrictModes yes
# Disable host-based auth
IgnoreRhosts yes
HostbasedAuthentication no
RhostsRSAAuthentication no
```

Firewall (iptables)

- Configure and enable iptables
- Find a script package (shorewall, etc)
- Lock down everything and add things you need open
- Be selective on what you open to the world
- Maintain logs

Firewall (iptables), (cont'd)

Very Basic iptable Rule

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -A OUTPUT -i lo -j ACCEPT
iptables -A OUTPUT -d your_dns_server -p udp --dport 53 -j
ACCEPT
iptables -A OUTPUT -d your_dns_server -p tcp --dport 53 -j
ACCEPT
iptables -A OUTPUT --state ESTABLISHED, RELATED -j ACCEPT
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -s your_administration_box -p tcp --dport
22 -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED, RELATED -j
ACCEPT
```

Enable Security Related Kernel Parameters

- Enable syncookies
- Disable responses for pings to the broadcast
- Enable ip spoof protection
- Disable ICMP redirects
- Disable source routing

Enable Security Related Kernel Parameters

Adding following lines to `/etc/sysctl.conf`

```
net.ipv4.tcp_syncookies = 1
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.accept_source_route = 0
```

Run `sysctl -p` to enable the settings

Host Based IDS

- Install an HIDS (Samhain, Tripwire, etc)
- Look into Role Based Access Control
 - SELinux
 - grsecurity
- Loghost for logs
- Log analyzer (tenshi, logwatch, etc)

Apply Latest Updates

- Keep up on updates
- Keep a test system to check for any issues for updates
- Have a cronjob setup to notify you via email for updates daily/weekly
- Subscribe to security announcement mailing lists

Apache Tips

- Permissions on ServerRoot Directories
- Server Side Includes (SSI)
 - Increased load
 - Like a CGI, same risks
 - Enable suexec
 - Disable ability to run scripts (IncludesNOEXEC)

Apache Tips (cont'd)

- CGI in General
 - Trust writers
- Dynamic Content (mod_perl, mod_php, etc)
- Protecting files
- Watch logs
- Use mod_security and gotroot.com rules

Credits

- <http://www.puschitz.com/SecuringLinux.shtml>
- <http://flaviostechnotalk.com/wordpress/index.php/2005/06/16/hardening-linux-a-10-step-approach-to-a-secure-server/>
- http://httpd.apache.org/docs/2.0/misc/security_tips.html