Linux Commands

Introduction to Linux Server Security Hardening

4 years ago • by Usama Azad

Securing your Linux server(s) is a difficult and time consuming task for System Administrators but its necessary to harden the server's security to keep it safe from Attackers and Black Hat Hackers. You can secure your server by configuring the system properly and installing as minimum softwares as possible. There are some tips which can help you secure your server from network and privilege escalation attacks.

Upgrade your Kernel

Outdated kernel is always prone to several network and privilege escalation attacks. So you can update your kernel using **apt** in Debian or **yum** in Fedora.

```
$ sudo apt-get update
$ sudo apt-get dist-upgrade
```

Disabling Root Cron Jobs

Cron jobs running by root or high privilege account can be used as a way to gain high privileges by attackers. You can see running cron jobs by

```
$ ls /etc/cron*
```

Strict Firewall Rules

You should block any unnecessary inbound or outbound connection on uncommon ports. You can update your firewalls rules by using **iptables**. Iptables is a very flexible and easy to use utility used to block or allow incoming or outgoing traffic. To install, write

```
$ sudo apt-get install iptables
```

Here's an example to block incoming on FTP port using iptables

```
$ iptables -A INPUT -p tcp --dport ftp -j DROP
```

Disable unnecessary Services

Stop any unwanted services and daemons running on your system. You can list running services using following commands.

```
ubuntu@ubuntu:~$ service --status-all

[ + ]  acpid
[ - ]  alsa-utils
[ - ]  anacron
[ + ]  apache-htcacheclean
[ + ]  apache2
[ + ]  apparmor
[ + ]  apport
[ + ]  avahi-daemon
[ + ]  binfmt-support
[ + ]  bluetooth
[ - ]  cgroupfs-mount

…snip...
```

OR using the following command

```
$ chkconfig --list | grep '3:on'
```

To stop a service, type

```
$ sudo service [SERVICE_NAME] stop
```

OR

```
$ sudo systemctl stop [SERVICE_NAME]
```

Check for Backdoors and Rootkits

Utilities like rkhunter and chkrootkit can be used to detect known and unknown backdoors and rootkits. They verify installed packages and configurations to verify system's security. To install write,

```
ubuntu@ubuntu:~$ sudo apt-get install rkhunter -y
```

To scan your system, type

```
ubuntu@ubuntu:~$ sudo rkhunter --check

[ Rootkit Hunter version 1.4.6 ]

Checking system commands...

Performing 'strings' command checks
Checking 'strings' command                          [ OK ]

Performing 'shared libraries' checks
Checking for preloading variables                   [ None found ]
Checking for preloaded libraries                    [ None found ]
Checking LD_LIBRARY_PATH variable                   [ Not found ]

Performing file properties checks
Checking for prerequisites                          [ OK ]
```

```
/usr/sbin/adduser                                          [ OK ]
/usr/sbin/chroot                                           [ OK ]

...snip...
```

Check Listening Ports

You should check for listening ports that aren't used and disable them. To check for open ports, write.

```
azad@ubuntu:~$ sudo netstat -ulpnt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address      Foreign Address   State      PID/Program name

tcp        0    0 127.0.0.1:6379        0.0.0.0:*        LISTEN     2136/redis-server 1

tcp        0    0 0.0.0.0:111           0.0.0.0:*        LISTEN     1273/rpcbind

tcp        0    0 127.0.0.1:5939        0.0.0.0:*        LISTEN     2989/teamviewerd

tcp        0    0 127.0.0.53:53         0.0.0.0:*        LISTEN     1287/systemd-resolv

tcp        0    0 0.0.0.0:22            0.0.0.0:*        LISTEN     1939/sshd

tcp        0    0 127.0.0.1:631         0.0.0.0:*        LISTEN     20042/cupsd

tcp        0    0 127.0.0.1:5432        0.0.0.0:*        LISTEN     1887/postgres

tcp        0    0 0.0.0.0:25            0.0.0.0:*        LISTEN     31259/master

...snip...
```

Use an IDS (Intrusion Testing System)

Use an IDS to check network logs and to prevent any malicious activities. There's an open source IDS Snort available for Linux. You can install it by,

```
$ wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
$ wget https://www.snort.org/downloads/snort/snort-2.9.12.tar.gz
$ tar xvzf daq-2.0.6.tar.gz
$ cd daq-2.0.6
$ ./configure && make && sudo make install
$ tar xvzf snort-2.9.12.tar.gz
$ cd snort-2.9.12
$ ./configure --enable-sourcefire && make && sudo make install
```

To monitor network traffic, type

```
ubuntu@ubuntu:~$ sudo snort

Running in packet dump mode
--== Initializing Snort ==--

Initializing Output Plugins!
pcap DAQ configured to passive.

Acquiring network traffic from "tun0".
Decoding Raw IP4

--== Initialization Complete ==--

...snip...
```

Disable Logging as Root

Root acts as a user with full privileges, it has power to do anything with the system. Instead, you should enforce using sudo to run administrative commands.

Remove no owner Files

Files owned by no user or group can be security threat. You should search for these files and remove them or assign them a proper user a group. To search for these files, type

```
$ find /dir -xdev \( -nouser -o -nogroup \) -print
```

Use SSH and sFTP

For file transferring and remote administration, use SSH and sFTP instead of telnet and other insecure, open and unencrypted protocols. To install, type

```
$ sudo apt-get install vsftpd -y
$ sudo apt-get install openssh-server -y
```

Monitor Logs

Install and setup a log analyzer utility to check system logs and event data regularly to prevent any suspicious activity. Type

```
$ sudo apt-get install -y loganalyzer
```

Uninstall unused Softwares

Install softwares as minimum as possible to maintain small attack surface. The more softwares you have, the more chances of attacks you have. So remove any unneeded software from your system. To see installed packages, write

```
$ dpkg --list
$ dpkg --info
$ apt-get list [PACKAGE_NAME]
```

To remove a package

```
$ sudo apt-get remove [PACKAGE_NAME] -y
$ sudo apt-get clean
```

Conlusion

Linux server security hardening is very important for enterprises and businesses. Its a difficult and tiresome task for System Administrators. Some processes can be automated by some automated utilities like SELinux and other similar softwares. Also, keeping minimus softwares and disabling unused services and ports reduces the attack surface.

ABOUT THE AUTHOR

Usama Azad

A security enthusiast who loves Terminal and Open Source. My area of expertise is Python, Linux (Debian), Bash, Penetration testing, and Firewalls. I'm born and raised in Wazirabad, Pakistan and currently doing Undergraduation from National University of Science and Technology (NUST). On Twitter i go by @UsamaAzad14

View all posts

RELATED LINUX HINT POSTS

- Check Listening Ports on Linux
- How to Use Topgrade to Update Packages in Linux
- Linux sysfs File System
- OProfile Tutorial
- Syslog Tutorial
- How to Create a New File Using Linux Touch Command
- Stealth Scans With Nmap

Linux Hint LLC, editor@linuxhint.com
1309 S Mary Ave Suite 210, Sunnyvale, CA
94087