The Ideal Linux Blog for Sysadmins & Geeks

LINUX COMMANDS 72

I ❤ TecMint :

25 Hardening Security Tips for Linux Servers

by Ravi Saive | Published: June 24, 2013 | Last Updated: January

Download Your Free eBooks NOW - 10 Free Linux eBooks for Administrators | 4 Free Shell Scripting eBooks

Everybody says that **Linux** is secure by default and agreed to some extend (It's debatable topics). However, Linux has in-built security model in place by default. Need to tune it up and customize as per your need which may help to make more secure system. Linux is harder to manage but offers more flexibility and configuration options.

25 Linux Security and Hardening Tips

Securing a system in a production from the hands of **hackers** and **crackers** is a challenging task for a **System Administrator**. This is our first article related to "**How to Secure Linux box**" or "**Hardening a Linux Box**".

In this post We'll explain 25

How to Add Linux Host to Nagios Monitoring Server Using NRPE Plugin

How to Install Nagios 4.3.4 on RHEL, CentOS and Fedora

Install Cacti (Network Monitoring) on RHEL/CentOS 7.x/6.x/5.x and Fedora 24-12

Google Chrome 70 Released – Install on RHEL/CentOS and Fedora

How to Install Ubuntu 16.10/16.04 Alongside With Windows 10 or 8 in Dual-Boot secure your Linux system. Hope, below tips & tricks will help you some extend to secure your system.

1. Physical System Security

Configure the **BIOS** to disable booting from **CD/DVD**, **External Devices**, **Floppy Drive** in **BIOS**. Next, enable **BIOS** password & also protect **GRUB** with password to restrict physical access of your system.

- Set GRUB Password to Protect Linux Servers

2. Disk Partitions

It's important to have different partitions to obtain higher data security in case if any disaster happens. By creating different partitions, data can be separated and grouped. When an unexpected accident occurs, only data of that partition will be damaged, while the data on other partitions must have following separate partitions and sure that third party applications should be installed on separate file systems under /opt.

```
/
/boot
/usr
/var
/home
/tmp
/opt
```

3. Minimize Packages to Minimize Vulnerability

Do you really want all sort of services installed?. It's recommended to avoid installing useless packages to avoid vulnerabilities in packages. This may minimize risk that compromise of one service may lead to compromise of other services. Find and remove or disable unwanted services from the server to minimize vulnerability.

find out services which are running on **runlevel 3**.

```
# /sbin/chkconfig --lis
```

Once you've find out any unwanted service are running, disable them using the following command.

```
# chkconfig serviceName
```

Use the **RPM** package manager such as "**yum**" or "**apt-get**" tools to list all installed packages on a system and remove them using the following command.

```
# yum -y remove package
```

```
# sudo apt-get remove p
```

- 5 chkconfig Command Examples
- 20 Practical Examples of RPM Commands

Commands for Linux Package Management

- 25 APT-GET and APT-CACHE Commands to Manage Package Management

4. Check Listening Network Ports

With the help of '**netstat**' networking command you can view all open ports and associated programs. As I said above use '**chkconfig**' command to disable all unwanted network services from the system.

```
# netstat -tulpn
```

- 20 Netstat Commands for Network Management in Linux

5. Use Secure Shell(SSH)

Telnet and **rlogin** protocols uses plain text, not encrypted format which is the security breaches. SSH encryption technology during communication with server.

Never login directly as **root** unless necessary. Use "**sudo**" to execute commands. sudo are specified in **/etc/sudoers** file also can be edited with the "**visudo**" utility which opens in **VI** editor.

It's also recommended to change default **SSH 22** port number with some other higher level port number. Open the main **SSH** configuration file and make some following parameters to restrict users to access.

```
# vi /etc/ssh/sshd_conf
```

Disable root Login

```
PermitRootLogin no
```

Only allow Specific Users

```
AllowUsers username
```

version

```
Protocol 2
```

- 5 Best Practices to Secure and Protect SSH Server

6. Keep System updated

Always keep system updated with latest releases patches, security fixes and kernel when it's available.

```
# yum updates
# yum check-update
```

7. Lockdown Cronjobs

Cron has it's own built in feature, where it allows to specify who may, and who may not want to run jobs. This is controlled by the use of files called **/etc/cron.allow** and **/etc/cron.deny**. To lock a user using cron, simply add user names in **cron.deny**

cron add in **cron.allow** file. If you would like to disable all users from using cron, add the '**ALL**' line to **cron.deny** file.

```
# echo ALL >>/etc/cron.
```

- 11 Cron Scheduling Examples in Linux

8. Disable USB stick to Detect

Many times it happens that we want to restrict users from using **USB** stick in systems to protect and secure data from stealing. Create a file '**/etc/modprobe.d/no-usb**' and adding below line will not detect **USB** storage.

```
install usb-storage /bi
```

9. Turn on SELinux

Security-Enhanced Linux (SELinux) is a compulsory mechanism provided in the kernel. Disabling **SELinux** means removing security mechanism from the system. Think twice carefully before removing, if your system is attached to internet and accessed by the public, then think some more on it.

SELinux provides three basic modes of operation and they are.

- **Enforcing**: This is default mode which enable and enforce the **SELinux** security policy on the machine.
- **Permissive**: In this mode, **SELinux** will not enforce the security policy on the system, only warn and log actions. This mode is very useful in term of troubleshooting **SELinux** related issues.
- **Disabled**: **SELinux** is turned off.

You can view current status of **SELinux** mode from the command line using 'getenforce' or 'sestatus' commands.

```
# sestatus
```

If it is disabled, enable **SELinux** using the following command.

```
# setenforce enforcing
```

It also can be managed from '**/etc/selinux/config**' file, where you can enable or disable it.

10. Remove KDE/GNOME Desktops

There is no need to run **X Window** desktops like **KDE** or **GNOME** on your dedicated LAMP server. You can remove or disable them to increase security of server and performance. To disable simple open the file '**/etc/inittab**' and set run level to **3**. If you wish to remove it completely from command.

```
# yum groupremove "X Wi
```

11. Turn Off IPv6

If you're not using a **IPv6** protocol, then you should disable it because most of the applications or policies not required **IPv6** protocol and currently it doesn't required on the server. Go to network configuration file and add followings lines to disable it.

```
# vi /etc/sysconfig/net
```

```
NETWORKING_IPV6=no
IPV6INIT=no
```

12. Restrict Users to Use Old Passwords

This is very useful if you want to disallow users to use same old passwords. The old password file is

/etc/security/opasswd. This can be achieved by using **PAM** module.

Open '**/etc/pam.d/system-auth**' file under **RHEL / CentOS / Fedora**.

```
# vi /etc/pam.d/system-
```

Open **'/etc/pam.d/common-password**' file under **Ubuntu/Debian/Linux Mint**.

```
# vi /etc/pam.d/common-
```

Add the following line to '**auth**' section.

```
auth            sufficient
```

Add the following line to '**password**' section to disallow a user from re-using last **5** password of his or her.

```
password    sufficient
```

remember by server. If you tried to use any of last **5** old passwords, you will get an error like.

```
Password has been alrea
```

13. How to Check Password Expiration of User

In Linux, user's passwords are stored in '**/etc/shadow**' file in encrypted format. To check password expiration of user's, you need to use '**chage**' command. It displays information of password expiration details along with last password change date. These details are used by system to decide when a user must change his/her password.

To view any existing user's aging information such as **expiry date** and **time**, use the following command.

To change password aging of any user, use the following command.

```
#chage -M 60 username
#chage -M 60 -m 7 -W 7
```

Parameters

- -M Set maximum number of days
- -m Set minimum number of days
- -W Set the number of days of warning

14. Lock and Unlock Account Manually

The lock and unlock features are very useful, instead of removing an account from the system, you can lock it for an week or a month. To lock a specific user, you can use the follow command.

```
# passwd -l accountName
```

still available for **root** user only. The locking is performed by replacing encrypted password with an (!) string. If someone trying to access the system using this account, he will get an error similar to below.

```
# su - accountName
This account is current
```

To unlock or enable access to an locked account, use the command as. This will remove (!) string with encrypted password.

```
# passwd -u accountName
```

15. Enforcing Stronger Passwords

A number of users use soft or weak passwords and their password might be hacked with a **dictionary based** or brute-force attacks. The '**pam_cracklib**' module is available in PAM (Pluggable module stack which will force user to set strong passwords. Open the following file with an editor.

Read Also:

```
# vi /etc/pam.d/system-
```

And add line using credit parameters as (**lcredit**, **ucredit**, **dcredi**t and/or **ocredit** respectively lower-case, upper-case, digit and other)

```
/lib/security/$ISA/pam_
```

16. Enable Iptables (Firewall)

It's highly recommended to enable **Linux firewall** to secure unauthorised access of your servers. Apply rules in **iptables** to filters **incoming**, **outgoing** and **forwarding** packets. We can specify the source and destination add port number.

- Basic IPTables Guide and Tips

17. Disable Ctrl+Alt+Delete in Inittab

In most Linux distributions, pressing '**CTRL-ALT-DELETE**' will takes your system to reboot process. So, it's not a good idea to have this option enabled at least on production servers, if someone by mistakenly does this.

This is defined in '**/etc/inittab**' file, if you look closely in that file you will see a line similar to below. By default line is not commented out. We have to comment it out. This particular key sequence signalling will shut-down a system.

```
# Trap CTRL-ALT-DELETE
#ca::ctrlaltdel:/sbin/s
```

Accounts for Empty Passwords

Any account having an empty password means its opened for unauthorized access to anyone on the web and it's a part of security within a Linux server. So, you must make sure all accounts have strong passwords and no one has any authorized access. Empty password accounts are security risks and that can be easily hackable. To check if there were any accounts with empty password, use the following command.

```
# cat /etc/shadow | awk
```

19. Display SSH Banner Before Login

It's always a better idea to have an legal banner or security warnings before SSH authentication. To set such banners read the following article.

- Display SSH Warning Message to Users

20. Monitor User Activities

If you are dealing with lots of users, then its important to collect the information of each user activities and processes consumed by them and analyse them at a later time or in case if any kind of performance, security issues. But how we can monitor and collect user activities information.

There are two useful tools called '**psacct**' and '**acct**' are used for monitoring user activities and processes on a system. These tools runs in a system background and continuously tracks each user activity on a system and resources consumed by services such as **Apache**, **MySQL**, **SSH**, **FTP**, etc. For installation, configuration and usage, visit the below url.

- Monitor User Activity with psacct or acct Commands

21. Review Logs Regularly

Move logs in dedicated log server, this may prevents intruders to easily modify local logs. Below are the Common Linux default log files name and their usage:

- /var/log/message – Where whole system logs or current activity logs are available.
- /var/log/auth.log – Authentication logs.
- /var/log/kern.log – Kernel logs.
- /var/log/cron.log – Crond logs (cron job).
- /var/log/maillog – Mail server logs.
- /var/log/boot.log – System boot log.
- /var/log/mysqld.log – MySQL database server

- /var/log/secure – Authentication log.
- /var/log/utmp or /var/log/wtmp : Login records file.
- /var/log/yum.log: Yum log files.

22. Important file Backup

In a production system, it is necessary to take important files backup and keep them in safety vault, remote site or offsite for Disasters recovery.

23. NIC Bonding

There are two types of mode in **NIC** bonding, need to mention in bonding interface.

- **mode=0** – Round Robin
- **mode=1** – Active and Backup

NIC Bonding helps us to avoid single point of failure. In **NIC** bonding, we bond two or more **Network Ethernet Cards** together and make one single virtual Interface address to talk with other servers. Our network will be available in case of one **NIC Card** is down or unavailable due to any reason.

Read Also : Create NIC Channel Bonding in Linux

24. Keep /boot as read-only

Linux kernel and its related files are in **/boot** directory which is by default as **read-write**. Changing it to **read-only** reduces the risk of unauthorized modification of critical boot files. To do this, open "**/etc/fstab**" file.

```
# vi /etc/fstab
```

Add the following line at the bottom, save and close it.

```
LABEL=/boot     /boot
```

Please note that you need to reset the change to read-write if you need to upgrade the kernel in future.

or Broadcast Request

Add following line in "**/etc/sysctl.conf**" file to ignore **ping** or **broadcast** request.

```
Ignore ICMP request:
net.ipv4.icmp_echo_igno

Ignore Broadcast reques
net.ipv4.icmp_echo_igno
```

Load new settings or changes, by running following command

```
#sysctl -p
```

If you've missed any important security or hardening tip in the above list, or you've any other tip that needs to be included in the list. Please drop your comments in our comment box. **TecMint** is always interested in receiving comments, suggestions as well as discussion for improvement.

If You Appreciate What We Do Here On TecMint, You Should Consider:

1. Stay Connected to: Twitter | Facebook | Google Plus
2. Subscribe to our email updates: Sign Up Now
3. Get your own self-hosted blog with a Free Domain at ($3.45/month).
4. Become a Supporter - Make a contribution via PayPal
5. Support us by purchasing our premium books in PDF format.
6. Support us by taking our online Linux courses

We are thankful for your never ending support.

Ravi Saive **View all Posts**

I am Ravi Saive, creator of TecMint. A Computer Geek and Linux Guru who loves called Linux. **Follow Me**: Twitter, Facebook and Google+

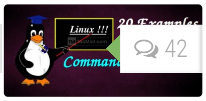
Your name can also be listed here. Got a tip? Submit it here to become an TecMint author.

PREVIOUS STORY
Hands On 'C' Programming Language

NEXT STORY
FireSSH – A Web Browser SSH Client Plugin for Firefox

YOU MAY ALSO LIKE...

6



42

4

Useful 'host' Command Examples

20 Practical Examples of RPM Commands in Linux

10 APR 2013

Understanding Shared Libraries in Linux

Querying
DNS
Lookups

16 MAY, 2017

72 RESPONSES

Comments 3 Pingbacks 0

Jota Esse November 3, 2017 at 12:08 am
Thanks for the tutorial. You may change the step 1. Md5 is deprecated and now the command is grub-mkpasswd-pbkdf2

Reply

Arsalan September 3, 2017 at 1:30 pm
kindly correct the english grammer mistakes and recheck for other errors. Otherwise a very good article for linux security. Recommended!

Reply

Gaurav Bhatkar
February 7, 2017 at 11:32 am
Hi,

Kindly help me understand tip number 15.
lcredit=-1 ucredit=-2 dcredit=-2 ocredit=-1 why these parameters have -1/-2 value.

Thanks in advance
Gaurav

Reply

« Older Comments

GOT SOMETHING TO SAY? JOIN THE DISCUSSION.

Name *

Email *

Website

☐ **Notify me of followup comments via e-mail. You can also subscribe without commenting.**

Post Comment

This site uses Akismet to reduce spam. Learn how your comment data is processed.

LINUX MONITORING TOOLS

How to Monitor Nginx Performance Using Netdata on CentOS 7

Netdata – A Real-Time Performance Monitoring Tool for Linux Systems

How to Use 'fsck' to Repair File System Errors in Linux

LINUX INTERVIEW QUESTIONS

10 Useful 'Interview Questions and Answers' on Linux Shell Scripting

10 Advance VsFTP Interview Questions and Answers – Part II

Basic Linux Interview Questions and Answers – Part II

OPEN SOURCE TOOLS

11 Best Graphical Git Clients and Git Repository Viewers for Linux

8 Best Screen Recorders for Desktop Screen Recording in Linux

4 Best Linux Apps for Downloading Movie Subtitles

Troubleshooting and Debugging Linux Processes

ctop – Top-like Interface for Monitoring Docker Containers

Questions for Beginners and Intermediates

10 MySQL Database Interview Questions for Beginners and Intermediates

Linux Desktop

9 Tools to Take or Capture Desktop Screenshots in Linux