



26 Security Hardening Tips for Modern Linux Servers

Ravi Saive | Last Updated: July 19, 2024 | Read Time: 16 mins | [Linux Commands](#) | [78 Comments](#)

Everybody says that [Linux](#) is secure by default, and to some extent, this is agreed upon (it's a debatable topic). However, Linux has an in-built security model in place by default.

You need to tune and customize it according to your needs, which can help in making the system more secure. Linux is more challenging to manage but offers greater flexibility and configuration options.

Securing a system in 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 useful tips and tricks to secure your Linux system. Hope, below tips and tricks will help you some extend to secure your system.

1. Physical System Security – Setting a GRUB Password

One effective way to enhance security is by setting a GRUB password, which is a boot loader used by [most Linux distributions](#) to load the operating system when the computer starts up.

By [setting a GRUB password](#), you add an extra layer of defense against unauthorized users who might attempt to tamper with or gain unauthorized access to your system.

Log into your Linux server and open the GRUB configuration file, which is located in different paths as shown.

- For Ubuntu/Debian: `/etc/default/grub`
- For CentOS/RHEL: `/etc/grub2.cfg` or `/boot/grub/grub.cfg`

Next, use a text editor like [nano](#) or [vi](#) to edit this file with [root privileges \(sudo\)](#).

Look for the line that starts with `GRUB_CMDLINE_LINUX` or similar and append `GRUB_PASSWORD=<password>` to the end of this line.

```
GRUB_CMDLINE_LINUX="quiet splash"  
GRUB_PASSWORD=password123
```

After editing the configuration file, update GRUB to apply the changes.

```
sudo update-grub    # For Ubuntu/Debian  
sudo grub2-mkconfig -o /boot/grub2/grub.cfg    # For CentOS/RHEL 7  
sudo grub2-mkconfig -o /boot/grub/grub.cfg    # For CentOS/RHEL 8
```

Restart your server to apply the GRUB password.

```
sudo reboot
```

2. Creating Different Partitions for Higher Data Security

It's important to have different partitions to obtain higher data security in case any disaster happens. By creating different partitions, data can be separated and grouped.

When an unexpected accident occurs, only data from that partition will be damaged, while the data on other partitions will survive. Make sure you have the following separate partitions and that [third-party applications](#) should be installed on separate file systems under `/opt`.

```
/  
/boot  
/usr
```

```
/var  
/home  
/tmp  
/opt
```

Most Linux distributions allow you to create and configure partitions during the installation process using the guided or manual partitioning options.

Post-installation, you can use tools like [fdisk](#), [parted](#), or graphical tools like GParted to create and manage partitions.

Example using fdisk:

```
sudo fdisk /dev/sda
```

Follow the prompts to create new partitions and assign them to the appropriate file systems.

3. Minimize Packages to Minimize Vulnerability: Remove Unwanted Services

One of the key strategies in securing a Linux system is to minimize the number of installed packages and running services. Each package and service can potentially introduce vulnerabilities, so keeping your system lean and efficient is a crucial step in hardening your server.

Start by identifying the packages and services that are not needed for your server's specific function, which can be done using [package management tools](#) such as [dpkg](#) or [rpm](#) and service management utilities.

```
dpkg --get-selections | grep install # For Debian-based systems  
rpm -qa                             # For Red Hat-based systems  
systemctl list-units --type=service --state=running
```

Once you have identified the unnecessary packages, you can remove them using your package manager such as [apt](#) or [yum](#).

```
sudo apt remove package_name    # For Debian-based systems
sudo yum remove package_name    # For Red Hat-based systems
```

After [removing the unwanted packages](#), the next step is to [disable and stop services](#) that are not needed.

```
sudo systemctl stop service_name
sudo systemctl disable service_name
```

4. Check Listening Network Ports in Linux

Monitoring and managing network ports is a crucial aspect of securing a Linux system and knowing which ports are open and listening can help you identify potential vulnerabilities and ensure that only necessary services are accessible.

To check network ports, we will use [netstat](#) or [ss](#) command-line tools, which provide various network-related information, including open ports and listening services.

```
sudo netstat -tuln
OR
sudo ss -tuln
```

5. Use Secure Shell (SSH) for Enhanced Security

Secure Shell (SSH) is a widely used protocol that offers a secure way to access and manage your Linux servers. However, to maximize security, there are [several best practices](#) you should follow, such as disabling root login, allowing only specific users, using SSH protocol 2, and changing the default SSH port.

Disabling root login forces users to log in with their user accounts, providing better accountability and reducing the risk of unauthorized access.

```
sudo nano /etc/ssh/sshd_config
```

Find the line that says `PermitRootLogin` and change its value to `no`:

```
PermitRootLogin no
```

[Restricting SSH access](#) to specific users adds a layer of security by ensuring that only authorized users can log in.

Add a line at the end of the file to specify the allowed users:

```
AllowUsers user1 user2
```

Changing the [default SSH port](#) (22) to a non-standard port can help reduce the number of automated attacks on your server.

```
Port 2222
```

Restart the SSH service to apply the changes:

```
sudo systemctl restart sshd
```

6. Keep Your System Up-to-Date

Regularly update your Linux distribution and all installed packages to the latest security patches and bug fixes using your system default package manager, such as `apt` for [Debian-based distributions](#) or `yum` for [Red Hat-based systems](#).

```
sudo apt update      # For Debian-based systems
sudo yum update      # For Red Hat-based systems
```

7. Managing Cron Job Permissions

[Cron](#) is a powerful utility in Unix-like operating systems that allows users to schedule jobs to run at specific intervals.

However, there might be situations where you need to control who can or cannot create and run cron jobs on your system. Cron has built-in features to manage these permissions using the `/etc/cron.allow` and `/etc/cron.deny` files.

To allow specific users to use cron, edit `/etc/cron.allow` file and the usernames of the users you want to deny, one per line.

```
user1  
user2
```

To deny specific users to use cron, edit `/etc/cron.deny` file and the usernames of the users you want to allow, one per line.

```
user3  
user4
```

To completely disable all users from using cron, you can add the `ALL` line to the `/etc/cron.deny` file.

```
ALL
```

8. Disable USB Storage Detection

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 `'nano /etc/modprobe.d/no-usb.conf'` and adding the below line will not detect USB storage.

```
blacklist usb_storage
```

After creating the blacklist file, update the `initramfs` (initial RAM filesystem) to ensure the blacklisted module is not loaded during the boot process:

```
sudo update-initramfs -u
```

Reboot your system for the changes to take effect.

9. Turn on SELinux Protection

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

SELinux provides three basic modes of operation and they are.

- **Enforcing:** This is the default mode that enables and enforces 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 terms of troubleshooting SELinux-related issues.
- **Disabled:** SELinux is turned off.

You can view the current status of SELinux mode from the command line using `'system-config-selinux'`, `'getenforce'`, or `'sestatus'` commands.

```
# sestatus
```

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

```
# setenforce enforcing
```

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

10. Removing X Desktops on a Linux Server

There is no need to run X Window desktops like KDE, GNOME, or XFCE on your dedicated [LAMP](#) server. You can remove or disable them to increase the security of the server and performance.

Before removing any desktop environment, identify which one is installed on your server.

```
dpkg -l | grep desktop  
OR  
yum grouplist | grep -i desktop
```

Once identified, you can remove the desktop environment along with any associated packages.

Remove GNOME Desktop Environment:

```
sudo apt-get purge gnome-shell gnome-session gnome-terminal # For Debian-  
sudo yum groupremove "GNOME Desktop Environment" # For Red Hat
```

Remove KDE Plasma Desktop Environment:

```
sudo apt-get purge kde-plasma-desktop # For Debian-ba  
sudo yum groupremove "KDE Plasma Workspaces" # For Red Hat-
```

Remove Xfce Desktop Environment:

```
sudo apt-get purge xfce4 # For Debian-ba  
sudo yum groupremove "Xfce" # For Red Hat-
```

If your server also has the X Server installed, which is the display server system for GUIs, you can remove it to further reduce potential security risks.


```
sudo apt-get purge xserver-xorg-core xserver-xorg # For Debian
sudo yum remove xorg-x11-server-Xorg xorg-x11-server-common # For Red Hat
```

Ensure that the server boots into a text-based console rather than starting a graphical desktop environment.

```
sudo systemctl set-default multi-user.target # For systemd-based systems
sudo systemctl set-default graphical.target # To revert back to graphical
```

After removing the desktop environment and optionally the X Server, reboot your server to apply the changes.

11. Disabling IPv6 Protocol on a Linux Server

If you're not using an IPv6 protocol, then you should disable it because most of the applications or policies do not require IPv6 protocol and currently, it isn't required on the server.

You need to edit the network configuration file to disable IPv6.

```
sudo nano /etc/sysctl.conf
```

Add the following lines to the end of the file:

```
# Disable IPv6
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
```

Next, apply the changes to the running system.

```
sudo sysctl -p
```

Verify that IPv6 is disabled by checking the network interfaces and configuration.

```
ip addr show
```

You should see only IPv4 addresses assigned to your network interfaces. IPv6 addresses should not be present.

12. Restricting Users from Using Old Passwords on Linux

This is very useful if you want to disallow users to use the same old passwords. The old password file is located at `/etc/security/opasswd`. This can be achieved by using the PAM module.

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

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

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

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

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

```
auth        sufficient    pam_unix.so likeauth nullok
```

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

```
password    sufficient    pam_unix.so nullok use_authtok md5 shadow remember
```

Only the last 5 passwords are remembered by the server. If you try to use any of the last 5 old passwords, you will get an error like.

Password has been already used. Choose another.

13. How to Check Password Expiration of User

In Linux, the user's passwords are stored in a '/etc/shadow' file in an encrypted format. To check the password expiration of users, you need to use the 'chage' command, which displays information on password expiration details along with the last password change date. These details are used by the 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.

```
#chage -l username
```

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

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

Break down of the command:

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

14. Lock and Unlock the Account Manually

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

```
passwd -l accountName
```

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

```
su - accountName  
This account is currently not available.
```

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

```
passwd -u accountName
```

15. Enforcing Stronger Passwords

Many users use soft or weak passwords and their passwords might be hacked with dictionary-based or [brute-force](#) attacks.

The 'pam_cracklib' module is available in the PAM (Pluggable Authentication Modules) module stack which will force users to set strong passwords.

Open the following file with an editor.

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

And add a line using credit parameters such as (lcredit, ucredit, dcredit, and/or ocredit respectively lower-case, upper-case, digit, and other)

```
/lib/security/$ISA/pam_cracklib.so retry=3 minlen=8 lcredit=-1 ucredit=-2 dcredit=-1 ocredit=-1
```

16. Enabling and Configuring Firewalls: firewalld and ufw

Firewalls are essential for securing Linux servers by controlling incoming and outgoing network traffic based on predetermined security rules. There are two most widely used

firewall solutions for Linux are firewalld for [RHEL-based distributions](#) and ufw for [Debian-based systems](#).

If firewalld or ufw is not already installed on your system, you can install it using the package manager.

Install Firewalld:

```
sudo dnf install firewalld
sudo systemctl enable firewalld
sudo systemctl start firewalld
```

Install Ufw:

```
sudo apt-get install ufw
sudo ufw enable
sudo ufw status
```

17. Disabling Ctrl+Alt+Delete on Linux

In [most Linux distributions](#), pressing 'CTRL-ALT-DELETE' will take your system to the reboot process. So, it's not a good idea to have this option enabled at least on production servers, if someone mistakenly does this.

To disable Ctrl+Alt+Delete, create or edit the override file for the Ctrl+Alt+Delete key combination.

```
sudo systemctl edit ctrl-alt-del.target
```

Add the following lines to the override file to disable the key combination:

```
[Service]
ExecStart=
```

After making changes, reload the systemd configuration and mask the `ctrl-alt-del.target` ensures that it cannot be triggered:

```
sudo systemctl daemon-reload
sudo systemctl mask ctrl-alt-del.target
```

18. Checking Accounts for Empty Passwords on Linux

Any account having an empty password means it's 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 passwords, use the following command.

```
sudo cat /etc/shadow | awk -F: '($2==""){print $1}'
```

19. Display SSH Banner Before Login

Displaying a [banner message before the SSH login](#) prompt can be a useful way to provide legal notices, warnings, or information to users attempting to access your Linux server.

To set such banners, you need to create a text file that contains the message you want to display.

```
sudo nano /etc/ssh/ssh-banner
```

Add your banner message:

```
*****
WARNING: Unauthorized access to this system is prohibited.

All activities on this system are logged and monitored. By logging in,
you acknowledge that you are authorized to access this system and agree
to abide by all relevant policies and regulations.
```

```
Unauthorized users will be prosecuted to the fullest extent of the law.  
*****
```

Next, you need to configure the SSH server to display the banner before the login prompt.

```
sudo nano /etc/ssh/sshd_config
```

Find and modify the Banner directive:

```
Banner /etc/ssh/ssh-banner
```

After making these changes, restart the SSH service to apply the new configuration.

```
sudo systemctl restart sshd
```

20. Monitor User Activities on Linux

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

There are two useful tools called 'psacct' and 'acct' are used for monitoring user activities and processes on a system. These tools run in a system background and continuously track each user activity on a system and resources consumed by services such as Apache, MySQL, SSH, FTP, etc.

For more information about installation, configuration, and usage, visit the below url.

- [Monitor User Activity with psacct or acct Commands](#)

21. Monitor Linux Logs Regularly

Reviewing logs on a regular basis is an important part of managing and securing a Linux system, as logs provide detailed records of system events, user activities, and potential security incidents.

By regularly checking these logs (usually stored in the `/var/log` directory), you can identify issues early, respond to security threats, and ensure the system runs smoothly.

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

22. Backup Files in Linux Using rsync

Backing up files in Linux using [rsync](#) is an efficient and reliable method, as it synchronizes files and directories between two locations, making it perfect for backups.

To back up files on the local system, use the following command:

```
rsync -av --delete /source/directory/ /backup/directory/
```

To back up files on the remote system, use the following command:

```
rsync -avz -e ssh /source/directory/ user@remote_host:/backup/directory/
```

23. NIC Bonding

In Linux, NIC Bonding is a feature that allows you to combine multiple network interfaces into a single bonded interface to improve network reliability, redundancy, and performance.

Below guides, you'll find a simple explanation of how NIC Bonding works in Linux, including configuration details for the two common modes.

- [How to Create NIC Teaming or Bonding in CentOS 8 / RHEL 8](#)
- [A Beginner's Guide to Creating Network Bonding and Bridging in Ubuntu](#)

24. Keeping /boot as Read-Only in Linux

The /boot directory in Linux [contains essential files](#) needed to boot the operating system, such as the kernel, initial ramdisk (initrd), and bootloader configuration files.

Ensuring that /boot is mounted as read-only can enhance system security and integrity by preventing unauthorized modifications to these critical 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    ext4    defaults,ro    1 2
```

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

25. Ignoring ICMP or Broadcast Requests in Linux

In Linux, you can configure your system to ignore ICMP (Internet Control Message Protocol) or broadcast requests to enhance security and reduce unwanted network traffic.

Open the /etc/sysctl.conf file using a text editor:

```
sudo nano /etc/sysctl.conf
```

Add or modify the following line to set the ICMP echo ignore flag:

```
net.ipv4.icmp_echo_ignore_all=1
```

Apply the changes:

```
sysctl -p
```

26. Implement Intrusion Detection and Prevention

To enhance network security, install and configure an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) to monitor traffic and detect potential attacks.

IDS options like Snort and Suricata analyze network packets for suspicious activity and provide alerts. Snort offers flexible, rule-based detection, while Suricata supports multi-threaded processing and advanced protocols.

For a proactive defense, consider [Fail2ban](#), which detects and responds to suspicious behavior by blocking offending IPs. Each tool can be configured to suit your specific security needs, providing robust protection against intrusions and helping maintain network integrity.

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 discussions for improvement.

Hey TecMint readers,

Exciting news! Every month, our top blog commenters will have the chance to win fantastic rewards, like free Linux eBooks such as RHCE, RHCSA, LFCS, Learn Linux, and Awk, each worth \$20!

Learn [more about the contest](#) and stand a chance to win by [sharing your thoughts below!](#)



PREVIOUS ARTICLE:

[OBS Studio: Free Live Streaming & Screen Recording in Linux](#)

NEXT ARTICLE:

11 Lesser Known Useful Linux Commands



Ravi Saive

I am an experienced GNU/Linux expert and a full-stack software developer with over a decade in the field of Linux and Open Source technologies

Each tutorial at TecMint is created by a team of experienced Linux system administrators so that it meets our high-quality standards.

Join the [TecMint Weekly Newsletter](#) (More Than 156,129 Linux Enthusiasts Have Subscribed)

Was this article helpful? Please [add a comment](#) or [buy me a coffee](#) to show your appreciation.

Related Posts

```
tecmin@tecmin ~/testing $ find . -type f \( -name "*.txt" -o -  
name "*.sh" -o -name "*.c" \)  
./emails.txt  
./script-1.sh  
./header.c  
./examples.txt  
./script.sh  
./expenses.txt
```

Find Multiple Filenames (File Extensions) Using 'find' Command in Linux

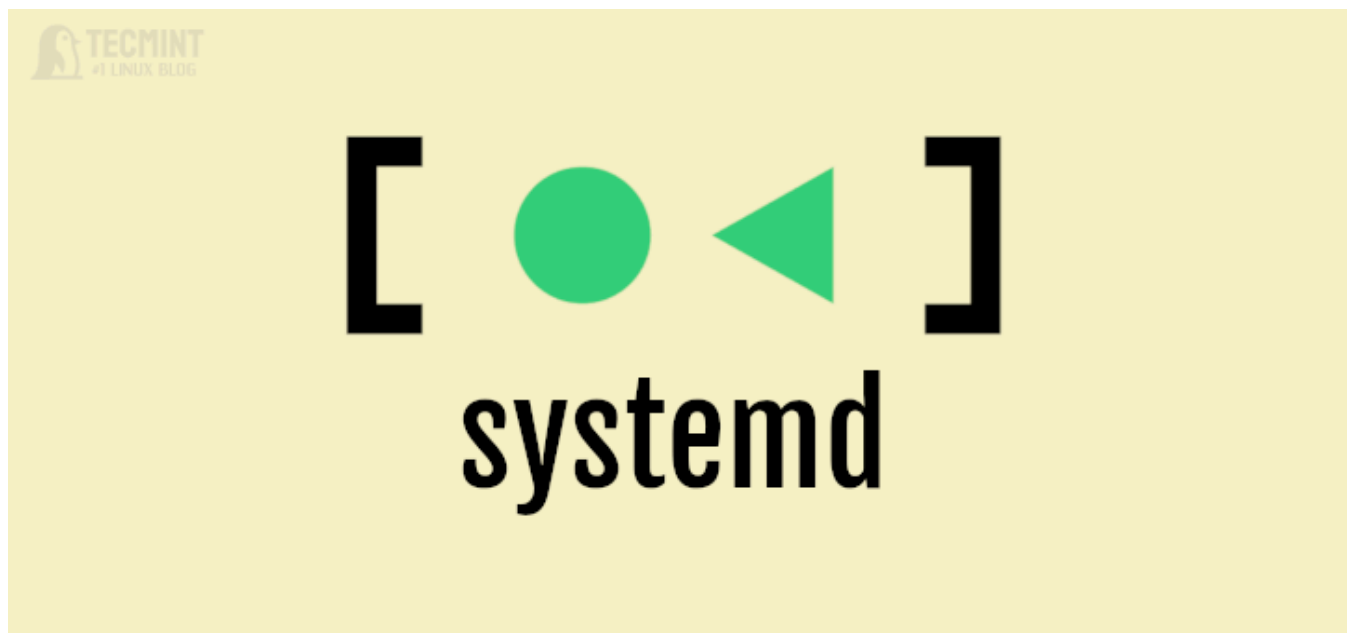
How to Search Files by Name or Extension Using find Command



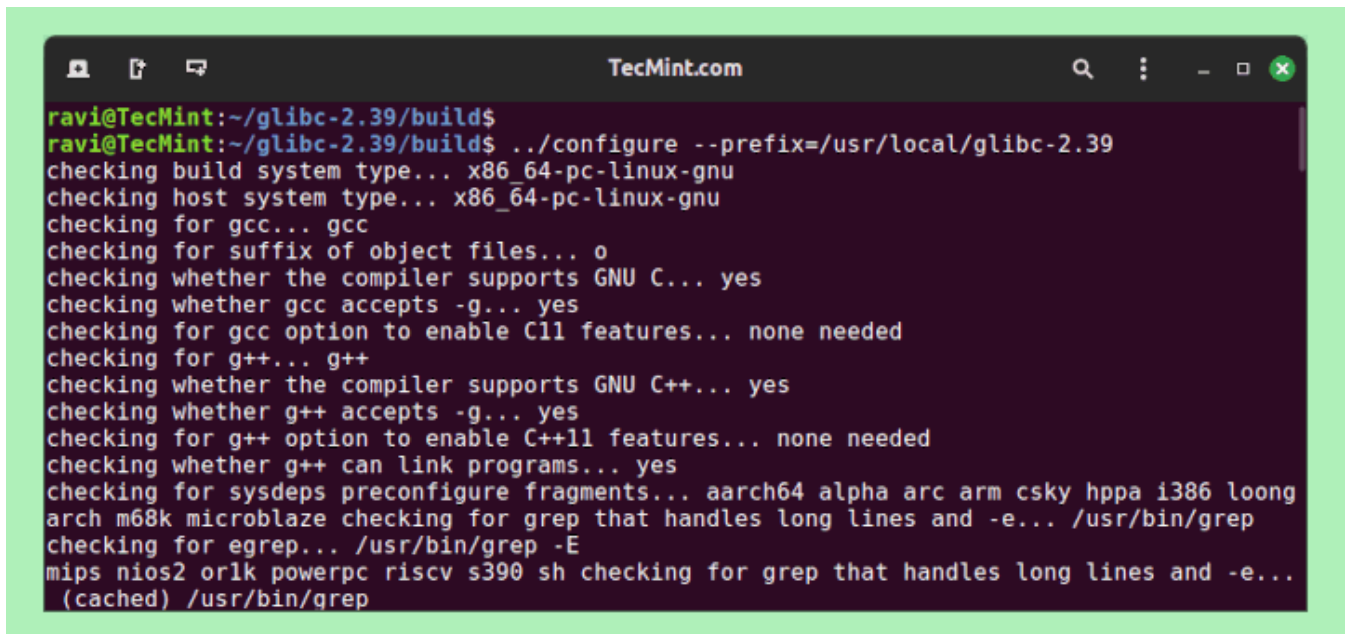
10 Lesser Known Linux Commands – Part 2



11 Lesser Known Useful Linux Commands

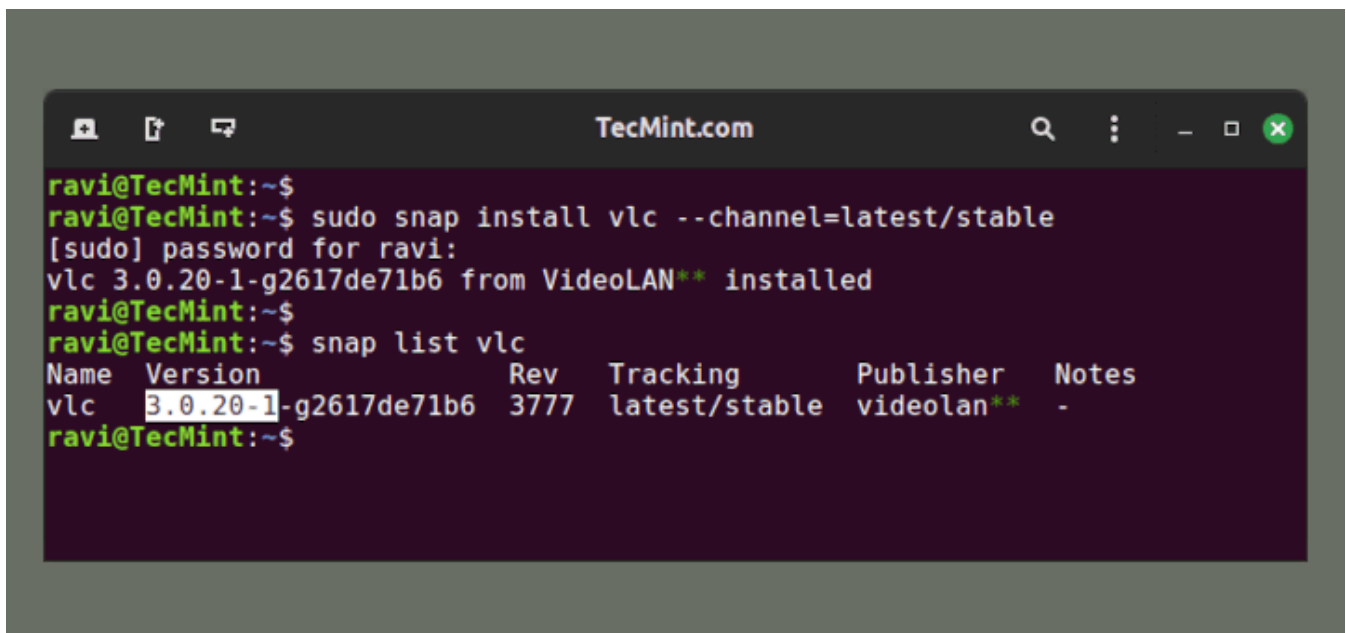


How to Remove Systemd Services on Linux

A terminal window titled 'TecMint.com' showing the configuration of glibc-2.39. The user is in the directory ~/glibc-2.39/build and runs './configure --prefix=/usr/local/glibc-2.39'. The output shows various checks for build system type, host system type, compiler (gcc), and linker (g++). It also checks for various architectures and features. The output is as follows:

```
ravi@TecMint:~/glibc-2.39/build$  
ravi@TecMint:~/glibc-2.39/build$ ../configure --prefix=/usr/local/glibc-2.39  
checking build system type... x86_64-pc-linux-gnu  
checking host system type... x86_64-pc-linux-gnu  
checking for gcc... gcc  
checking for suffix of object files... o  
checking whether the compiler supports GNU C... yes  
checking whether gcc accepts -g... yes  
checking for gcc option to enable C11 features... none needed  
checking for g++... g++  
checking whether the compiler supports GNU C++... yes  
checking whether g++ accepts -g... yes  
checking for g++ option to enable C++11 features... none needed  
checking whether g++ can link programs... yes  
checking for sysdeps preconfigure fragments... aarch64 alpha arc arm csky hppa i386 loong  
arch m68k microblaze checking for grep that handles long lines and -e... /usr/bin/grep  
checking for egrep... /usr/bin/grep -E  
mips nios2 orlk powerpc riscv s390 sh checking for grep that handles long lines and -e...  
(cached) /usr/bin/grep
```

How to Install and Run Multiple glibc Libraries in Linux

A terminal window titled 'TecMint.com' showing the installation of VLC using Snap. The user runs 'sudo snap install vlc --channel=latest/stable'. The output shows the password prompt and the installation of VLC 3.0.20-1-g2617de71b6 from VideoLAN. The user then runs 'snap list vlc' and the output shows the installed version and tracking channel. The output is as follows:

```
ravi@TecMint:~$  
ravi@TecMint:~$ sudo snap install vlc --channel=latest/stable  
[sudo] password for ravi:  
vlc 3.0.20-1-g2617de71b6 from VideoLAN** installed  
ravi@TecMint:~$  
ravi@TecMint:~$ snap list vlc  
Name Version Rev Tracking Publisher Notes  
vlc 3.0.20-1-g2617de71b6 3777 latest/stable videolan** -  
ravi@TecMint:~$
```

How to Install Particular Versions of Packages with Snap

 **78 Comments**

[Leave a Reply](#)

Trevor Chandler

July 31, 2024 at 3:03 am

In the article , the first sentence begins with 'Everybody says that Linux is secure by default,...' Call me petty, but not quite everybody says this! Maybe the majority in the Linux space feels this way, but certainly not everybody. Okay, enough on that.

Very nice, practical tips on securing a Linux system!

[Reply](#)

Author



Ravi Saive

July 31, 2024 at 10:12 am

@Trevor,

Thank you for your feedback! We appreciate your attention to detail and are glad you found the tips helpful.

[Reply](#)

dragonmouth

July 23, 2024 at 1:18 am

"unexpected accident"

Most accidents are unexpected. :-)

"3. Minimize Packages to Minimize Vulnerability: "

From my experience, it is next to impossible to uninstall any packages install by default on *buntu systems without disabling the system. Even the most insignificant package has some system file as a dependency.

Why do you use `/etc/cron.allow` to DENY users and `/etc/cron.deny` to ALLOW users?

"8. Disable USB Storage Detection"

Another important reason to disable USB storage is to prevent inadvertent or intentional malware installation.

"19. Display SSH Banner Before Login"

Suppose you have multiple banners to display depending on conditions. How is that handled?

Of course, none of the systemd commands will work on a non-systemd distro such as Devuan.

[Reply](#)



Tobias LinuxServer

September 20, 2021 at 5:31 am

Thanks for the tips. I just rented a VServer, the first time that a Linux server of mine hangs freely on the Internet. Of course, you have to pay more attention to the security.

[Reply](#)

Qamre alam

April 23, 2021 at 4:50 pm

Thanks Team,

It was great and useful.

[Reply](#)**Mohammad Khalid**

January 25, 2019 at 3:56 pm

I am also administrating Linux servers for my client websites and facing too many security threats.

Sometimes server got down after website update.

I will also use above tips to secure my servers.

Thanks for the tips.

[Reply](#)**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](#)

Aleksander Strusinski

February 5, 2017 at 3:09 pm

Hello, For me SELinux do not work at all. Don't know where to get help. Tried everything. My Linux say all the time, after sestatus, disabled, even if I edit etc /selinux/config.

[Reply](#)

Aleksander Strusinski

February 5, 2017 at 3:11 pm

Ps. unfortunately, I 'm beginner in Linux, so probably doing something wrong.

[Reply](#)

Author

**Ravi Saive**

February 6, 2017 at 3:42 pm

@Aleksander,

Try to restart the machine after disabling SELinux.

[Reply](#)**Ashutosh Upadhyay**

November 1, 2016 at 10:48 am

Liked the efforts to write such a very useful article. Thanks.

I've a situation where I want to ensure that a particular group of IT staff is not able to perform any execute or write on production servers. Is there a quick way to do so by adding them to "deny" files etc?

[Reply](#)

Author

**Ravi Saive**

November 2, 2016 at 11:14 am

@Ashutosh,

Yes that can be possible, just go through this article, you will get idea on how to do that..

<https://www.tecmint.com/manage-users-and-groups-in-linux/>

[Reply](#)

Greg

October 19, 2016 at 8:31 pm

centos (and fedora etc.) now uses systemd. It will help to update this page by adding the systemctl commands.

Thank you

[Reply](#)

Author

**Ravi Saive**

October 20, 2016 at 11:52 am

@Greg,

Yes, we aware that RHEL, CentOS and Fedora, in fact all modern distributions are switched to SystemD, thats the reason we've created a separate articles on how to secure CentOS systems here:

[How to Harden and Secure CentOS 7 – Part 1](#)

[How to Harden and Secure CentOS 7 – Part 2](#)

[Reply](#)

Khushal Bisht

September 3, 2016 at 5:45 am

Hi Ravi,

Any server-hardening-security-tips article then suggested me...because this article is very basic times. We need more security in servers.....also Suggested me any PAM article

[Reply](#)

Author



Ravi Saive

September 3, 2016 at 10:55 am

@Khusal,

Here are the ultimate guides to secure and harden your CentOS 7 server, as well as RHEL 7..

[The Mega Guide to Harden and Secure CentOS 7 – Part 1](#)

[The Mega Guide to Harden and Secure CentOS 7 – Part 2](#)

[Reply](#)

Dave

August 18, 2016 at 9:44 am

I stopped reading at number 2. Different partitions do nothing for security or protection. If anything it can cause problems by having a partition that can become too small and fill. With current systems you can use raid 1 or do a rsync of the entire disk daily. The only real disk that needs to be protected is /home.

[Reply](#)**medhat ahmed**

August 16, 2016 at 7:02 pm

number 8 in this list doesn't work "disable usb"

[Reply](#)**Gareth**

July 5, 2016 at 5:54 pm

One caveat on the way the SELinux tip was worded: just enabling it on its own does not instantly and magically give you any extra security, but it will slow your system down. If you're not making explicit use of the features that it offers then disabling it will not reduce your security.

SELinux is a module that provides more fine-grained access control over security policies. Before enabling it find out what it is and whether you will use that extra

level of control, and balance that need against the fact that it does come with some amount of negative performance impact.

But don't just treat "Enable SELinux" as a checklist item to get out of the way and quickly move on, every installation.

[Reply](#)

Tanveer

May 26, 2016 at 2:02 pm

Awesome...Appreciate your efforts...Looks like you can help me with my dilemma..I have installed RHEL 7.1 & 6.5 on VM in VMware work station. But I am not able to create repository..In fact, rpm also does not work. Any comments please? I am not able to move forward with setting up my server.

[Reply](#)

Author



Ravi Saive

May 26, 2016 at 4:12 pm

@Tanveer,

You need to register your RHEL 7.1 & 6.5 to RedHat Network subscription to get the package updates, please follow the below article to register your RHEL OS versions to RedHat subscription and enable system repositories

<https://www.tecmint.com/enable-redhat-subscription-repositories-and-updates-for-rhel-7/>

[Reply](#)

Tanveer

May 26, 2016 at 4:42 pm

Dear Ravi,

Appreciate your prompt response. But, I just want to inform that I am not looking to get package updates. I am trying to set up repository with the default available packages. With RHEL 7.1, it does now show that repository is enabled. But, in RHEL 6.5 it does show repo is enabled, and 'yum install' takes me to a prompt asking for y/n for installation. But, when y is presses, then nothing happens. Also, like in RHEL 5, where we use rpm to install 'createrepo' or 'vsftpd' before creating a repo, I cant even rpm in both 7 & 6. Please comment.

[Reply](#)

Author

**Ravi Saive**

May 26, 2016 at 5:09 pm

@Tanveer,

You mean local CD/DVD repository or network repository, hope these following articles will helpful to you, just go through it and let me know..

<https://www.tecmint.com/setup-yum-repository-in-centos-7/>

<https://www.tecmint.com/install-gui-in-rhel-centos-7/>

[Reply](#)**MOHD TAUHEED**

April 18, 2016 at 4:44 pm

Hi,

I want to block all user for cp and scp from our remote server to my local machine.
please suggest me ..

Thanks

[Reply](#)

Author



Ravi Saive

April 19, 2016 at 10:09 am

@Mohd,

In sshd_config file, just comment out the following line to disable scp connections.

```
## override default of no subsystems
#Subsystem      sftp    /usr/libexec/openssh/sftp-server
```

[Reply](#)

Akshay Chakre

April 11, 2016 at 10:02 pm

Very easy to understand...Too Good

[Reply](#)

ravindra

March 5, 2016 at 9:54 am

assign single user mode password

[Reply](#)**Sothy**

January 29, 2016 at 9:42 am

Great post.

Thanks for this post. I am using and learning about Linux.

[Reply](#)**MD**

January 27, 2016 at 9:25 am

Thank you for this great post!

I'm still learning Linux, and this is a GIANT help for me!

Keep it up!

[Reply](#)**Mike lam**

January 18, 2016 at 6:03 am

FOR # 3, ubuntu has done away with chkconfig, it is now sysv-rc-config

[Reply](#)

Author



Ravi Saive

January 18, 2016 at 1:58 pm

@Mike,

Thanks for the tip and we are well aware of it, in fact we're in process to update this article to match the newest technologies..

[Reply](#)



24x7servermanagement

January 17, 2016 at 10:05 pm

This indeed is very well versed documented article for linux server hardening and shows to harden your core operating system. Thanks for sharing this nice information.

[Reply](#)

Joe

January 15, 2016 at 8:34 pm

Great Article!

[Reply](#)**Paul C**

January 12, 2016 at 12:01 am

Could you update these for systemd/systemctl ? initab, checkconfig are less common.

[Reply](#)

Author

**Ravi Saive**

January 12, 2016 at 1:55 pm

@Paul,

Give us some time to update this article to support systemd/systemctl based distributions..

[Reply](#)**Ragnarok**

January 10, 2016 at 12:02 am

Good, needs more in depht points but is great.

[Reply](#)

sadmanrock

January 9, 2016 at 6:18 pm

Great job guy

[Reply](#)



Chirag Nayyar

December 29, 2015 at 3:48 pm

Fantastic article ...keep it up

[Reply](#)

Ali

August 19, 2015 at 7:05 am

Good one.. thanks mate..:)

[Reply](#)

simon

May 28, 2015 at 4:01 pm

Great article – very useful. I would go as far as to say force users to use key based authentication if possible as SSH brute force attacks are relentless these days. Also it is worth considering using a real time security monitoring tool to identify malicious activity. Tools like siemless are easy to set up and operate a freemium operating model so home users and SME's can be covered by 24/7 security monitoring for no fee.

[Reply](#)

karthikeyan

April 16, 2015 at 8:01 pm

nice information

i would like to one more point. i give below like for protection linux server

<http://tecadmin.net/mac-address-filtering-using-iptables/>

[Reply](#)

Omar

April 2, 2015 at 3:30 pm

@Hextreme

Absolutely right.

[Reply](#)

nitin raj

March 12, 2015 at 4:52 pm

upload,,,how to store a backup on linux server

[Reply](#)**gowrish**

March 9, 2015 at 4:33 pm

Wonderful and please add FTP chroot also.

[Reply](#)**Yo**

March 3, 2015 at 6:11 pm

@Hextreme – Really using ICMP for diagnostics??? Have you heard of LEM and SNMP? Or actively monitoring your servers?? Good article for people like Hextreme that has a lot to learn.

[Reply](#)**guest**

January 31, 2015 at 12:01 am

thanks mate ;)

[Reply](#)

Hextreme

January 28, 2015 at 11:30 pm

At least half the things in this list are completely bogus and certainly don't increase security. Password protecting GRUB or the BIOS? If they have physical access to the machine, that's trivial to get around. Disabling ICMP and broadcasts? That just breaks network diagnostics and doesn't increase security at all. Empty passwords? That means NO LOGIN, which is certainly more secure than setting a password! NIC bonding isn't security, it's reliability...

CTRL-ALT-DEL is a great shortcut for rebooting the system properly, turning it off doesn't increase security in any way. If you can touch the keyboard you can just as easily pull the power cord.

[Reply](#)

pinky

October 21, 2015 at 3:40 pm

gosh okay so what should we do to increase security since you clearly know what your talking about.

[Reply](#)

Rainer

January 19, 2015 at 3:14 pm

very usefull thanks

I use public private key authentication where ever possible. Especially on SSH and suppress password login. So I can allow SSH root login and have root as the only user on servers. Additionally I send a login notification automatically with the .bash_profile to my mailbox. So I can see if there is a unauthorized login by a foreign IP address. So I also have to surveille only one user

[Reply](#)

Syed

November 24, 2014 at 5:35 pm

Hi,

Thanks for sharing information. i have one query, while adding below lines in /etc/pam.d/system-auth file. Is there any problem in system booting.

```
password sufficient pam_unix.so nullok use_authtok md5 shadow remember=5  
/lib/security/$ISA/pam_cracklib.so retry=3 minlen=8 lcredit=-1 ucredit=-2  
dcredit=-2 ocredit=-1
```

[Reply](#)

vaibhav

November 24, 2014 at 4:27 pm

“Minimize Packages to Minimize Vulnerability”

in this which which package/services i have to remove/stop can you please tell me

[Reply](#)

Author



Ravi Saive

November 24, 2014 at 4:54 pm

@Vaibhav,

These two articles will help you out..

<https://www.tecmint.com/remove-unwanted-services-from-linux/>

<https://www.tecmint.com/remove-unwanted-services-in-centos-7/>

[Reply](#)

Pugazhendhi

November 14, 2014 at 5:26 pm

Hi can u suggest from where can i get more on pam authentication. I googled but unable to grab one

[Reply](#)

Author



Ravi Saive

November 14, 2014 at 9:06 pm

@Pugazhendhi,

Here is the link to the complete guide on the PAM module..

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Managing_Smart_Cards/Pluggable_Authentication_Modules.html

[Reply](#)

Karthick.Ar

November 13, 2014 at 11:06 pm

Good one. Excellent. But a few tips can be added which are related to basic services.

[Reply](#)

Author



Ravi Saive

November 14, 2014 at 9:19 pm

@Karthick,

We glad that if you could provide those basic few tips, so that we could include in the article...Thanks.

[Reply](#)

Lasse

November 11, 2014 at 9:36 am

Great article! Way too many people do not even know how vulnerable they are.

You should really work on your English though.

[Reply](#)

Greg

July 20, 2014 at 12:29 am

Ravi, your article does not even touch the surface of linux hardening. Even distros where syslinux is not available can be maintained in many ways not mentioned in article. Starting from file system encryption and ending on warnings about specific services (i.e. mail servers should be tested for open relay, web servers should be kept in chrooted environment etc. etc.)

[Reply](#)

Purushotham

May 30, 2014 at 11:22 pm

I would like to shift over from Windows to Linux, i have gone through ur valuable tips... can i get any links or suggestion for achieving the Certification in Linux..... kindly help... preparing for RHCSA...

[Reply](#)

Author



Ravi Saive

May 31, 2014 at 12:21 pm

You will find many ebooks and learning sites for such linux certification. Go through following link for such ebooks.

<http://tecmint.tradepub.com/c/search.mpl?keyword=LINUX+CERTIFICATION>.

[Reply](#)

Mayur

May 21, 2014 at 9:42 pm

I want to but linux whm server so let me know which port open in configserver firewall and ad which to be block

Can you explain me the steps

Regards

Mayur

[Reply](#)

iron

May 9, 2014 at 2:43 am

Please remove the part that says to disable ipv6. This does not harden a server and is grossly untrue as to say it is not needed.

Some isp's use ipv6.

It has its place.

When an isp has ipv6, and it is setup correctly on the pc's, it doesn't slow things down, cause stalls, etc etc.

That happens when the isp in use doesnt support the potocol and the pc's are searching for it.

[Reply](#)

Bash

April 22, 2014 at 1:43 am

Thanks. Would you please explain how to setup a firewall from A to Z? It is so hard and I need your support. Thanks.

[Reply](#)

Steve

February 26, 2014 at 6:37 pm

Hi Ravi,

This is an excellent article for someone new to Linux, I have a question with regard to No 3 how do I know what is needed and what is not, as I have quite few services running. Playing around with owncloud as a practical introduction to Linux.

[Reply](#)

Alex

February 25, 2014 at 3:02 am

Use tcp wrappers to allow and deny connections and have an email notification when someone is trying to access from not allowed locations.

[Reply](#)

Ali

January 30, 2014 at 5:23 pm

Hello,

Thanks for writing such an informative post on Linux server security.

[Reply](#)

icefyre

December 6, 2013 at 7:06 pm

Great article, one note though. 'chkconfig' is a Red Hat tool, that command won't work on Ubuntu, you would need to follow a different process to stop/remove services for other distros.

[Reply](#)

Author



Ravi Saive

December 7, 2013 at 3:30 pm

Yes you right the chkconfig command won't work on Debian based distro's. You need to follow some other tactics to on/off services.

[Reply](#)

Alex

February 25, 2014 at 2:56 am

rcconf in debian

[Reply](#)

massy

November 3, 2013 at 4:38 pm

Thank you.

[Reply](#)



Michael

October 18, 2013 at 9:55 pm

Well done Ravi, a nice start for hardening/securing a Linux system!
If you want a more extensive audit, consider my open source tool Lynis:
<http://www.rootkit.nl/projects/lynis.html>

[Reply](#)**Vareg**

September 16, 2013 at 8:22 pm

Thanks for the tips,
but .., beware tip #24, as it sent me in maintenance mode, and i'm running CentOS 6.4, the ext2 filesystem type should have rung a bell but didn't and before i know it, i lost control of my system, although i learned something valuable outta this:

If you're stuck in maintenance mode (during bootstrap) and you get a root shell but everything's read-only, and you can't edit the file that sent you here, use the following command

```
mount -o remount,rw /
```

Many people go automatically fetch their livecd for that matter but i don't think it's adequate, this way, you don't even to mount sysimage using your install cd. Hope it helps

[Reply](#)**Chelton**

September 12, 2013 at 6:45 pm

Comment on 5. Never log in as root and use sudo, sudo encourages a weak passwords and hence weaker security (For example a 30+ password on root would be tedious, but this is what I have on my servers)

Better to log in to root and do complex work than running multiple sudo commands. While you do get a sudo log, in my opinion working in this way on non trivial tasks is

ridiculous.

[Reply](#)

Shane

December 13, 2013 at 2:27 pm

Why does sudo encourage weak passwords? If you find yourself constantly being timed out in sudo, and having to constantly enter your password, you can increase the timeout value.

It's safer to prevent root SSH login. SSH in as a different user, and su to root if you need to.

[Reply](#)



Siddesh

August 14, 2013 at 9:15 am

Excellent Article. Thanks so much :))

[Reply](#)

Ganesh

June 24, 2013 at 6:54 pm

Thanks Ravi for sharing such an important doc.

Here we are missing on

- 1.ftp service :- Disabling the ftp services eg.vsftpd if it is not required..
- 2.WWW files:- Secondly monitor the WWW files /folders, if possible pls set strong umask . We should not have any system config files with WWW permissions,
- 3.Enable audit and seconday login logs if you are using SUDO access,
- 4.Stop sharing the users id's, every end users should have his named id instead of using the genric user id's..eg. on database servers normally we are having oracle / db2 / sybase user id's used for binary installation purpose. We should disable the direct logins post the installation gets over and enable db team to have sudo su – , this will help us to segrate ownership.

[Reply](#)

Got Something to Say? Join the Discussion...

Thank you for taking the time to share your thoughts with us. We appreciate your decision to leave a comment and value your contribution to the discussion. It's important to note that we moderate all comments in accordance with our [comment policy](#) to ensure a respectful and constructive conversation.

Rest assured that your email address will remain private and will not be published or shared with anyone. We prioritize the privacy and security of our users.

☐ Save my name, email, and website in this browser for the next time I comment.

Post Comment

Search...

Do You Enjoy My Blog?

Support from readers like YOU keeps this blog running. Buying me a cup of coffee is a simple and affordable way to show your appreciation and help keep the posts coming!

Buy Me a Coffee

Linux Commands and Tools

[How to Add or Remove Linux User From Group](#)

[4 Ways to Send Email Attachment from Linux Command Line](#)

[How to Transfer Files Between Two Computers using nc and pv Commands](#)

[15 Useful 'Sockstat Command Examples' to Find Open Ports in FreeBSD](#)

[6 Best CLI Tools to Search Plain-Text Data Using Regular Expressions](#)

[How to Watch TCP and UDP Ports in Real-time](#)

Linux Server Monitoring Tools

[3 Tools to Monitor and Debug Disk I/O Performance in Linux](#)

[How to Monitor Website and Application with Uptime Kuma](#)

[How to Install Nagios XI on Ubuntu 22.04](#)

[Psensor – Monitor Linux Hardware Temperature \[Motherboard and CPU\]](#)

[Sysdig – A Powerful System Monitoring and Troubleshooting Tool for Linux](#)

[Duf – A Better Linux Disk Monitoring Utility](#)

Learn Linux Tricks & Tips

[How to Christmassify Your Linux Terminal and Shell](#)

[How to Disable SELinux Temporarily or Permanently](#)

[Assign Read/Write Access to a User on Specific Directory in Linux](#)

[6 Best CLI Tools to Search Plain-Text Data Using Regular Expressions](#)

[How to Use 'at' Command to Schedule a Task on Given or Later Time in Linux](#)

[How to Monitor Progress of \(Copy/Backup/Compress\) Data using 'pv' Command](#)

Best Linux Tools

[The 27 Best IDEs and Code Editors for Linux](#)

[10 Best Open Source Forum Software for Linux in 2024](#)

[5 Top Open-Source Microsoft 365 Alternatives for Linux](#)

[5 Best Command Line HTTP Clients for Linux](#)

[6 Best Command-Line FTP Clients for Linux Users](#)

[11 Best Graphical Git Clients and Git Repository Viewers for Linux](#)

Tecmint: Linux Howtos, Tutorials & Guides © 2024. All Rights Reserved.

The material in this site cannot be republished either online or offline, without our permission.

Hosting Sponsored by : [Linode Cloud Hosting](#)