Cal State Fullerton

CPSC 254

Software Development With Open Source Systems - Linux Security

Instructor: Tejaas Mukunda Reddy

Top 10 Best Methods on how to improve Linux security

- This blog post is created in order to help you significantly improve Ubuntu-based Linux security and to avoid the general bruteforcing, phishing as well as other types of attacks that may be targeted towards your desktop.
- According to recent statistics at Berkeley Linux Users group, the market share of Linux usage has been growing, even though not at an amazing rate. One possible reason for that is the security issues which many enterprises experienced in recent years. Besides the number of targeted attacks with various forms of banking malware, worms as well as spyware, many ransomware infections like WannaCry and EternalPetya have proven that even often-used and often-patched operating systems such as Windows 10 can be affected big time. This has driven many personal as well as enterprise users to seek alternative methods and solutions, turning their heads to Linux-based operating system. The biggest share of those have the Ubuntu-based Linux OS's. If you are a beginner Linux user and are looking for the methods to improve your security, we recommend implementing the below-suggested ones to turn your Linux distribution into a software fortress.

Prepared By: Tejaas Mukunda Reddy, Shivansh Vijay Nathan

Reference Prof. David Heckathorn

Top 10 Best Security tools and methods for Linux

- To best provide you with the methods we have decided to divide them chronologically. This basically means that the methods that we have explained first are more important and essential for your security. Let's begin with the necessary command after installation, which is the necessary:
  - $sudo apt-get update && time
  - $sudo apt-get dist-upgrade
- In addition to this, we also do not include services that can be set up separately, like **VPN**, which is essential for Linux security and if you aim for protection you should be familiar with VPN services for Linux distros and the methods on how to set them up.
- After having those essential elements of security, you can proceed with doing other modifications on your Linux distribution.

Encrypt your drive (full disk encryption)

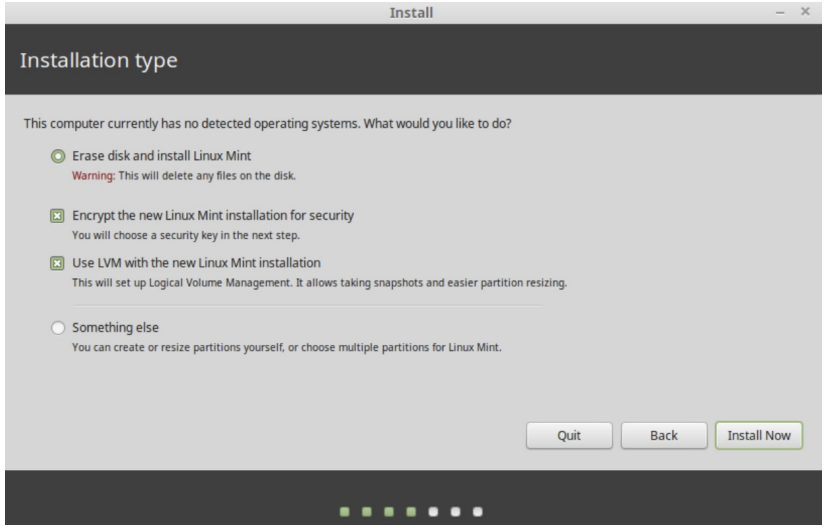
When you install your new Linux distribution, whether it is Gnome, Kubuntu, BackTrack or any other type, it's newer versions will always ask you If you would like to encrypt your drive. Whether it is an SSD drive or Hard Drive, if it is encrypted, your data remains almost 100% safe. Yes, you will be asked a password to decrypt your drive upon login, but this is the price of having a drive that only you can access to if you are familiar with your password that is. This is especially useful when you are mobile and working on a laptop.

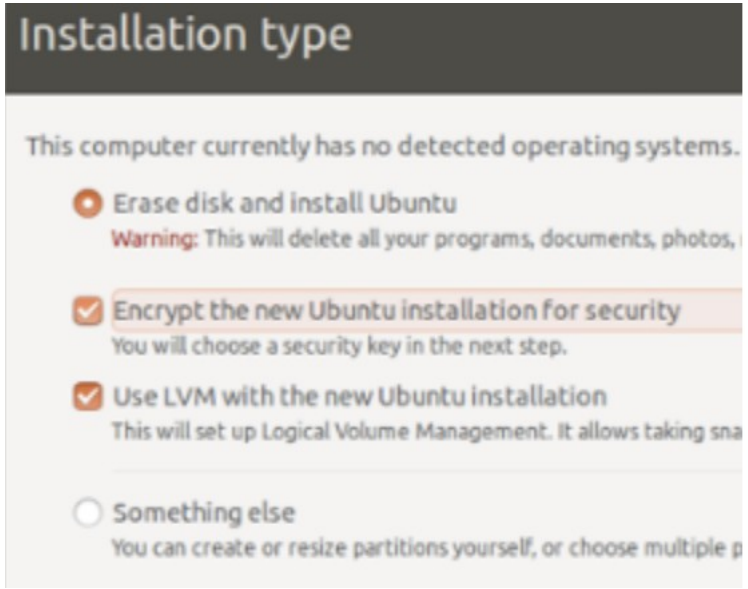
Prepared By: Tejaas Mukunda Reddy, Shivansh Vijay Nathan

Reference Prof. David Heckathorn

Top 10 Best Security tools and methods for Linux

- If your drive is encoded and the laptop gets stolen, there is likely nothing that the criminals can do to even access your important data. Furthermore, if a hacker has physical access to your laptop and knows your account password, for example, the code required to decrypt the drive will obstruct him into entering your drive. The same principle goes if someone stole your hard drive. In addition to full disk encryption, Linux also offers to encrypt your Home folder, meaning that even if someone has access to your computer, they will not be able to tamper with everything within this crucial for Linux directory.





Prepared By: Tejaas Mukunda Reddy, Shivansh Vijay Nathan

Reference Prof. David Heckathorn

Top 10 Best Security tools and methods for Linux

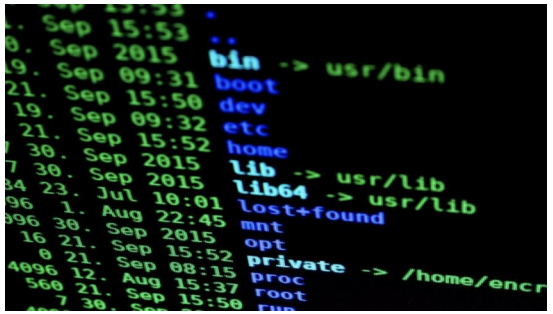
Enable Your Firewall

- Basically, this is one thing that every self-respecting Linux user should do when they install a Linux distribution. It more of a security ethic advise, primarily because, even with the firewall disabled, Linux has all the ports locked down either way. But, you never know, if your computer will be targeted sooner or later, because someone with hardened security obviously has something to hide and people quickly realize this. To enable your Linux firewall, you must run the Linux Terminal after which type: $sudo apt-get install guf
- GUFW stands for “Graphical Uncomplicated Fire Wall”. The command will install it and after it has finished doing so, you should open it, by typing in your terminal it’s abbreviation and hitting Enter: $gufw
- After you open GUFW you will see it’s simple user interface. From there simply click on the slider button next to Status to turn it from OFF to ON:

Prepared By: Tejaas Mukunda Reddy, Shivansh Vijay Nathan

Reference Prof. David Heckathorn

Top 10 Best Security tools and methods for Linux



Disable SSH Login via Root

- In order to disable anyone logging in via SSH, you should access the file that is responsible for the configuration of SSH. The file has the following location:
  - → /etc/ssh/sshd_config
- After you have found this file, open it with the text editor app and find the following line of code and when you do, remove the # symbol from it:
  - →#PermitRootLogin no

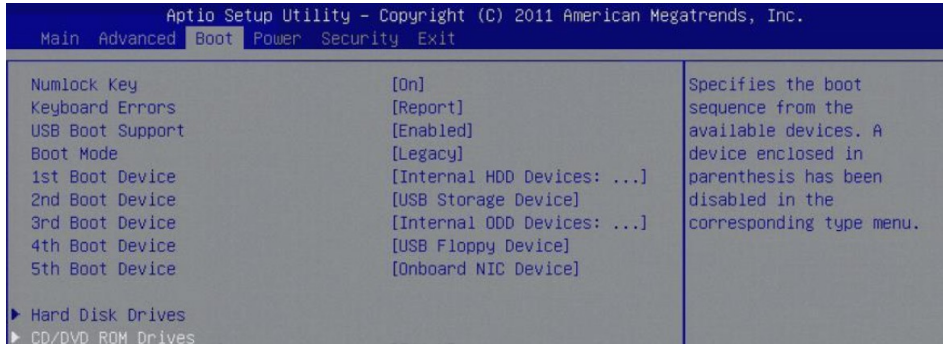
Make your BIOS More Secure

- This tip may not be directly Linux related but it is considered as a general security risk for most Linux distributions. After installing Linux on your computer, it is a good idea to disable any possibility of your computer to boot via USB, CD/DVD or other external drives. This means that nobody can overwrite your Linux and hence damage it or even try to access your drive by booting a Live OS. And this is just the tip of the iceberg of security threats when external boot is enabled. This is why, you should access BIOS on your system start up and go to the Boot tab from which disable the booting option from external drives:

Prepared By: Tejaas Mukunda Reddy, Shivansh Vijay Nathan

Reference Prof. David Heckathorn

Top 10 Best Security tools and methods for Linux



In addition to these measures, add a BIOS password, which will stop someone with a physical access to your computer to enter the BIOS:

- IMPORTANT TIP! Make sure to find a way to memorize all the passwords, especially the firmware BIOS one, because there is no way of recovering it!.

Disable USB Mount

- One crucial method by which you can ensure higher security, especially against someone who can physically tamper with your computer is to ban them from using USB to attack it. There are many sophisticated USB-based malware which is activated automatically when the pen drive is inserted in your USB port, so this is a crucial tip to strengthen your Linux security. The only price you have to pay is to quit using USB drives all the time and find another method to safely transfer data. Here is how to do it:
- Step 1: Open any text editor and write:
  - → install usb-storage /bin/true
- Step 2: Save the file as a .conf type of file and save in the following location:
  - → /etc/modprobe.d/
- Step 3: Restart your computer and test if you are able to mount a USB drive

Prepared By: Tejaas Mukunda Reddy, Shivansh Vijay Nathan

Reference Prof. David Heckathorn

Top 10 Best Security tools and methods for Linux

Use Firejail Sandboxing When You Try New Applications

- In general, Linux operating systems are designed in order to be secure by default. But this does not mean that your online browsing is not exposed against any sniffing or phishing attacks – the main reason why you need to secure yourself against new browser extensions or apps that may be unwanted on your Linux machine. Firejail is one security app that is very simple to set up and works on the latest Linux distros. Here is how to set it up on 16.04 LTS Ubuntu:
  - → sudo apt-get update
  - sudo apt-get install firejail
  - ls /etc/firejail
- Now you have successfully entered a page where you should see the profiles of all the programs installed on your computer. They should look somewhat like the following:
  - → skype.profile
  - dropbox.profile
  - icedove.profile
  - Tor.profile
- If we would like to secure Tor web browser, for example, we can use the “firejail” command in the following syntax:
  - → firejail firefox
- After entering this command, the next time you run Tor browser, the events that are happening are recorded on a log file. Here is more information on how to tinker with Firejail, kindly provided by OSTechNix.

Prepared By: Tejaas Mukunda Reddy, Shivansh Vijay Nathan

Reference Prof. David Heckathorn

Top 10 Best Security tools and methods for Linux

Use Anti-Virus

- “Anti-Virus for Linux?” you would ask yourself in a critical manner… While some consider anti-virus to be completely unnecessary for a Linux, because most malware is generally designed for Windows and will not be activated on your system. This is true, however there are also arguments that there are sophisticated attacks and malware for Linux OS’s out there and they are increasing and you have no way of defending yourself once you get attacked by them, even if the probability is low. You can never be safe enough, right? There are many Linux anti-virus programs out there, and you can use Google to find the ones which are suitable most for your situation. Furthermore, we will soon post a comparison between the best anti-virus programs for Linux-based OS’s, so we suggest that you follow our blog regularly. In the meantime, you can go ahead an check MakeUseOf’s post.

Top 10 Best Security tools and methods for Linux

Enable Root Mode and Secure it

- The root access is essential to administrative control of your Linux operating system and it's enabling it crucial for it too. To enable logins via root, you should use the following commands:
  - → sudo passwd root
- After this has been done,, you should type your password. Then, type the following command:
  - → sudo passwd -u root
- In order to enter the root mode, simply type:
  - → sudo -i
- When you type it, you will be requested to enter your password and you will be in privileged root mode afterwards.

Top 10 Best Security tools and methods for Linux

Improve Your Browsing Security

- The most disregarded aspect of online security is the web browser, since it is the most often method by which malware may slither onto your computer system. JavaScripts, drive-by downloads, worms and many other types of malware may find their way onto your Linux system.
- There are multiple ways to improve browser security. For starters, you can add browser extensions(Add-ons) which can contribute to the improvement of security and preventing attacks from suspicious third-parties. Here we have some suggestions on such:
- Adblock Plus – an add-blocker which can disable any pop-ups, redirects and other types of advertisements. Available for most web browsers.
- Disconnect – A browser extension which aims to make your web browsing private, since it aims to prevent third-parties to track your browsing history.
- Privacy Badger – Created by the notorious EFF (Electronic Frontier Foundation), this browser add-on helps to block malicious adverts as well as tracking technologies and categorizes the danger of every site, based on colors (green, yellow, red).
- NoScript – Possibly the most useful browser add-on for Firefox. It aims to block absolutely any script that is executed from websites you do not trust. This basically means that you can use the script to white-list multiple sites you visit often and trust and when it comes to the new websites, they will be blocked. Significantly increases security.

Prepared By: Tejaas Mukunda Reddy, Shivansh Vijay Nathan

Reference Prof. David Heckathorn

Top 10 Best Security tools and methods for Linux

Improve Your Browsing Security

- However, if you still feel that your web browser is not secure enough, because you have read about bug bounties and other details that decrease your trust in your browser, you can try and download web browsers which are specifically oriented towards security. This is why we have the following suggestions which you can try and choose the best security browser for Linux that will suit your activity:
  - Elinks
  - Konqueror
  - Midori
  - Opera
  - Slimboat

Prepared By: Tejaas Mukunda Reddy, Shivansh Vijay Nathan

Reference Prof. David Heckathorn