This guide is to familiarize you with your new Linux machine, as well as the software that has been installed. The software is hand picked, free and open source and provides a complete set of tools for you to be productive. This includes web browsing, email, VPN, image and video viewing/editing, PDF document handling and many other system utilities to both harden your machine, as well as provide functionality.

Your machine has been configured with a number of privacy and security hardening features, beyond a VPN of your choice which is a basic first step to connect to the internet in a more privacy friendly way. In addition to masking your true IP address with your VPN, we also have enabled and tuned the firewall, disabled IPv6 on the system and tweaked the browsers to be as privacy and security conscious as possible, while maintaining a balance of usability.

As you'll see later in this guide, you have various browsers to use that offer a continuum of maximum hardened configuration to moderate hardening with better functionality across more websites. Many websites break or do not load properly when using these more privacy friendly browsers, which can be frustrating, so having multiple browsers will come in very handy for when sites do not load properly. Simply switch to another browser, chances are, any site that breaks with one browser, will likely work just by using a different browser.

Clearing the cache/history and relaunching also can be quite helpful for sites that don't cooperate for you. This (hopefully minor) inconvenience is highly worth it though, when compared to the massive data harvesting and snooping happening when using stock Google Chrome, Microsoft Edge or Safari browsers, especially better off since you are also on a hardened version of Linux.

Let's dive into the applications that have been installed on your machine and explain briefly what each of them do, and a little bit of how to use them. We'll explain a few tips and tricks where we feel it's helpful to the average user, especially those new to Linux.

Applications Installed on your Computer

There are several ways to access the Applications menu to find the various software installed on your machine, and it's a little different depending on which type of Linux you have. Pop!_OS for example, you can click the top left of your screen where it says 'Applications' or simply hit the super key (The Windows logo key in lower left of keyboard). Other Linux distros such as Zorin or Linux Mint, you can simply click the main system menu icon in the lower left corner.

VPN (Virtual Private Network)

We recommend using one of only three VPN's, while there are other good ones out there, this short list are our top choices for folks to use. Generally, we want to stay connected behind a VPN at all times, with few exceptions. While you are not limited to purchasing only one VPN provider, you can only run one of these at a time on your machine.

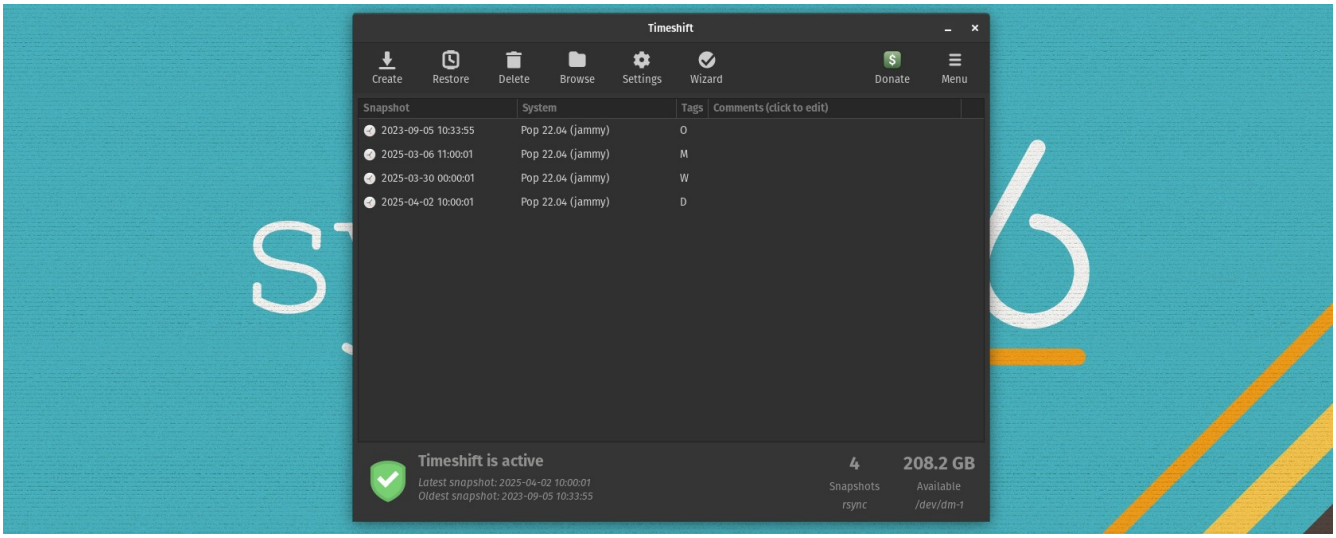
Proton VPN	Mullvad VPN	IVPN

Simply visit your Applications menu and select your provider, enter your credentials, and click connect. Choose a server of your choice, this can be in the United States or any other country provided by your VPN provider. Some services online may not be available in one country or another, switching your VPN to a country that is supported is fairly easy to do. Generally though, for US users, you'll want to connect to a US server for fastest speeds and for general use.

Timeshift

This application comes native on some Linux systems, this is essentially a backup and restore feature for your machine, should you break it bad enough (very rare). You can visit the settings within the app to adjust how many snapshots are taken, these snapshots allow us to roll back to a known good point and undo any damage that may have been done. While this is not usually necessary, it's nice to have. Set it and forget it, you won't ever have to think about it or really manage it at all, it's just there in the background running locally on your machine.

Timeshift pictured below



Flatpak Compatibility
Some Linux distros such as Pop!_OS and ZorinOS come with native Flatpak support, however if your distro did not, we have added that to your machine. This allows you to install and use Flatpak versions of software, as many of the apps installed are Flatpaks, and you may wish to install and use other Flatpaks in the future, there's many out there (Flathub.org is a large repository of software)

In addition, your machine has some Flatpak tools to help manage the apps, these include `Flatseal` and `Warehouse`. Opening these two applications offers you easy GUI (Graphical User Interface) based dashboards to help manage your Flatpak applications if you desire.

AppImage Launcher
This utility allows for easy integration of AppImage applications into your system application menu. AppImages on many Linux distros do not integrate and can be difficult to find on your system. `AppImage Launcher` utility fixes that for us and allows us to find any AppImages easily in your native applications menu on your system.

Browsers and Search Engines
Your system has five browsers installed, and while this may seem overkill, it is often necessary to overcome the various websites out there that tend to break and not load properly in one browser. Switching browsers can often alleviate this headache.

The other major thing this does for us is *browser isolation*, a technique to enhance your privacy when visiting lots of websites, especially those that you log into. While many of these browsers block some of the cross tab tracking and spying, we can be certain our activities remain isolated by using an entirely different browser for a new task, to avoid sites seeing other sites you have open.

Example, if you open Firefox browser and login to your Facebook account, then open a new tab and start shopping for new underwear from Walmart and Victoria's Secret, Facebook might see (log) your search for underwear and the sites you visit. This data is collected and sold, to try and target you with ads and who knows for what other purposes. By using different browsers for those two tasks, you ensure that they remain isolated from each other. These are the browsers we install by default:

`Brave Browser` (Brave search engine)

`Firefox Browser` (Duck Duck Go search engine)

`LibreWolf Browser` (Duck Duck Go search engine)

`Mullvad Browser` (Duck Duck Go search engine)

`Tor Browser` (Duck Duck Go search engine)

Brave and Firefox are good choices for general use, and tend to work best across the most amount of websites out there. LibreWolf and Mullvad are hardened versions of Firefox, but tend to break more sites, which you'll quickly see when searching. However these are still excellent choices, and even if you don't need or desire the extra privacy on these browsers, they are helpful for browser isolation as mentioned previously. Plus, having different browsers can help you organize your tasks.

Tor is its own animal, this provides ‘dark web’ or .onion domain hidden web services function, but we can still use it to browse the ‘normal’ internet as well. Some sites block Tor connections, however we strongly encouraged you to use Tor as much as possible for things like general searches. Tor is not ideal for logging into services tied directly to you, such as your known email accounts, or social media accounts. Tor is excellent however for anonymous web searching, it routes your traffic across several proxy servers with layers of encryption at each step to hide your IP address and true identity.

Using Tor will provide many of the same benefits as a VPN, better in some ways. It’s not magic, nor bulletproof, but it’s pretty good at keeping you anonymous, with our without a VPN turned on. The more of us using Tor, the easier it is for all of us to hide in the anonymous traffic on the Tor network. The only real downside to Tor is the speed, since you’re hopping through multiple random Tor nodes around the world, pages will take much longer to load than normal.

BleachBit
You may have heard of this one back around the 2016 US election cycle, and while it is great at shredding and deleting files securely from your illegal private server in your bathroom, it’s main purpose for us is as a system cleaner. This is an open source tool to easily clean up your system with just a few clicks, run this often to help keep your machine tidy and running smooth. This is the better alternative to something like C-Cleaner that you may have used.

Photo and Images Viewing and Editing
Your machine has been loaded with a number of photo and image viewing and editing software, from lightweight/basic to heavier and much more advanced, with some balanced right in the middle. You’ll likely find one that is your favorite for quickly viewing photos, but another for doing various editing tasks. You may have an additional viewer on your system depending on what comes native on your Linux distro. Let’s briefly describe each one.

`Nomacs` – Light to medium weight, excellent default Image Viewer

`Krita` – Medium weight, excellent all around viewer and editor

`Darktable` – Medium to somewhat heavy weight, excellent all around viewer and editor

`GIMP` – Heavy weight editor, similar to Photoshop

Others you may wish to install: `Inkscape` (similar to Adobe Illustrator), `Pinta`, `DigiKam`

Make sure to go to Settings > Default Applications on your machine and set your default Image Viewer to the one you most prefer. The lightweight ones such as Nomacs open much faster than something like GIMP, so if you just need to browse through photos quickly, the lighter weight tools will be much better. For heavier editing tasks, GIMP or Inkscape will be the power house here, however they also have a steep learning curve, as they are loaded with tools.

PDF Document Viewing and Editing
This is a bit of a change from using Adobe for everything PDF, there is no Adobe support for Linux anymore, and it’s closed source, abusive software anyway. On Linux, we have a number of PDF tools

to use, there isn't quite a direct replacement for Adobe, but by combining several of the tools listed below, you'll have everything you'll need to create, manage, view, sign, and edit your PDF's.

`Document Viewer` - (lightweight viewer, native on many Linux distros, also called Evince)

`PDF Mix Tool` - (Lightweight editor great for combining/splitting/arranging PDF's)

`PDF Arranger` - (Lightweight but very handy tool for many basic editing tasks)

`Xournal ++` - (Medium weight but fairly powerful editor, excellent for touch screen/stylus use also)

`Scribus` – (Heavy weight, very powerful PDF tool, for creating and doing heavy edits)

`LibreOffice Draw` – (Native on nearly all Linux distros. Very powerful at editing PDFs)

`Calibre` – (PDF book viewer, also handles ePUB and other eBook formats)

Other PDF applications: GIMP and Inkscape handle PDF also, not just images. `Okular` is another medium weight PDF editor great for annotations and signatures, including digital signatures. One PDF tool that comes close to Adobe is a closed source proprietary one, but very easy to use- a full featured application called `Master PDF Edit`. You can use a restricted version free that has a watermark, but the software is a one time purchase license that costs about $70. To learn more about all of these and other PDF tools on Linux, watch our video here on Rumble.

MetaData Cleaner
This tool will strip the metadata from your files prior to sharing with others, especially for anything posted online. Each image or document we create has a lot of information about the device used to create or edit that image embedded within the file, use this tool to delete that metadata. You should create a backup of any files first just to be safe, then use the tool to clean the metadata on a copy. This ensures that if `MetaData Cleaner` breaks a file or image, you have a clean original copy still.

Audio / Video Tools
Installed for you are some popular, powerful and very useful tools for viewing and editing all audio and video files, there are many more out there, but these below are excellent to have at a minimum.

`FFmpeg` – A powerful utility that powers a number of other tools for audio/video

`Audacity` – Edit any audio like a pro with this well known audio editor

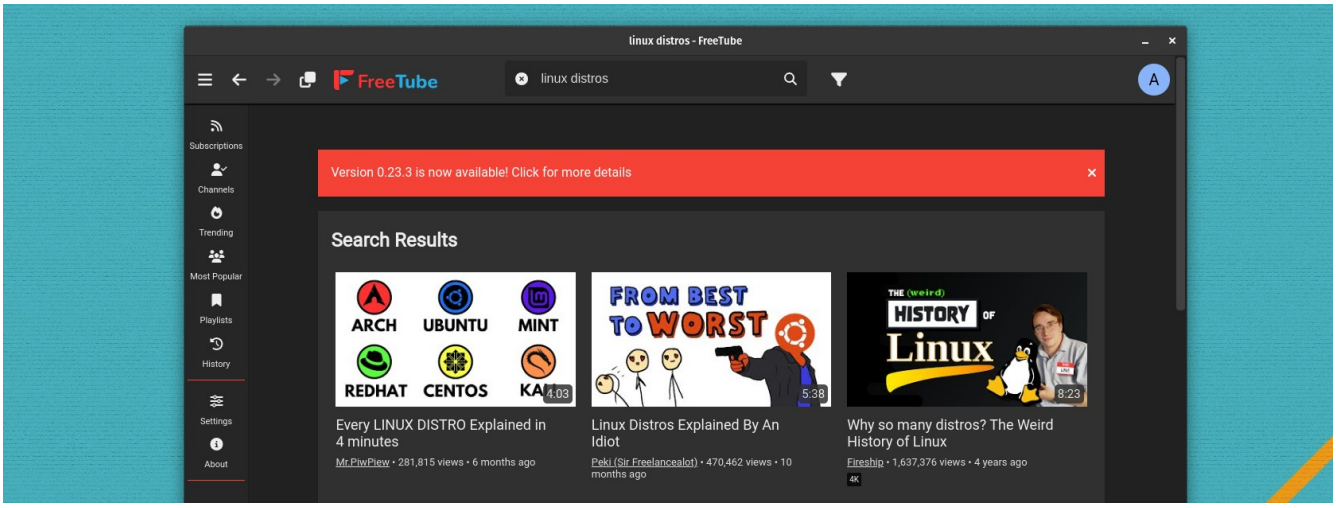
`SoundConverter` – Easily convert file formats of any audio file

`VLC` – Powerful and robust, easy to use app for all audio/video needs

All Linux distros also come with a native audio/video tool in addition to these apps and utilities, the combination of that plus these additional applications should be all you need to get started. For anyone who needs video editing, consider `Kdenlive`, this is a very robust option should you need heavy duty video editing.

YouTube Front End
YouTube's parent company Google (which in turn is owned by Alphabet) collects staggering amounts of data when we use their service online, especially when signed in. While there are a ton of YouTube front ends (proxy services that fetch YouTube videos for us privately), this one is now cross platform and arguably the most robust and easy to use one that runs on Linux, as well as your mobile device.

`FreeTube` – Play, share, download and manage all of your YouTube needs



Encryption Tools
Your machine, unless otherwise specified, comes with Full Disk Encryption (FDE) which requires a password to decrypt any data stored on your computer's hard drive. This is a huge layer of protection for any data stored on your machine. In addition to your computer hard drive, you may wish to encrypt other data using any of these applications listed, VeraCrypt is very well liked, Cryptomator is probably the easiest if you need to use encryption across all platforms including Apple iOS and macOS.

`LUKS` – Native Linux disk encryption that can be read by nearly all types of computers

`VeraCrypt` – Powerful encryption software for creating and opening encrypted data

`Cryptomator` – Another tool nearly identical to VeraCrypt for encrypting your data easily

Communication Applications
There are many other communication apps that you may want, however these are best left up to you to determine which ones you need. The ones listed below though we feel are robust must haves, even if it's only for occasional use. We encourage folks to use these tools where possible, instead of abusive software such as Zoom, WhatsApp, etc.

`Signal` – Excellent replacement for native SMS and voice / video calling. Supports up to 1000 people on group chats, and up to 40 people on voice / video calls. Open source and fully encrypted end to end communication.

Onionshare – while many do not need this, or at least not often, this is an excellent way to share files anonymously over the Tor network. Open source, free, and unlimited file size, share as many files as you want without attaching any identity. Requires a Tor browser for the receiving party to view your files that you host or send to them.

Additional Applications
Below are other software applications installed on your system to achieve further functionality.

Standard Notes – Encrypted note taking application, free and paid tiers. Paid tiers offer Two Factor Authentication codes (2FA), and all content of your notes are zero knowledge encryption, meaning even Standard Notes cannot see your content, only you. Very robust and useful notes app.

RSS Guard – RSS feeds are still a thing, these offer a very good way to achieve a couple of things. One, increased privacy, RSS allows you to view news articles and updates from most sites without giving them your true identity. RSS also allows you to neatly organize all of those feeds to easier digest the content you want to stay up to date with.

Transmission – If you need a torrent application, this one is an easy top choice. Simple, lightweight and open source, pull any file you want easily with this application.

KeePassXC – Offline password manager. While we recommend an encrypted cloud based password manager for the average person (Bitwarden, Proton Pass), this offline encrypted manager is still an excellent tool to use for just about any type of note taking as well. Easily organize any project you have going in this secure, offline database that you view using KeePassXC.

GNOME Maps – a basic map application that can be used offline. Organic Maps is another mapping application that can also be configured for easy offline use if you want a similar option. Mapping on Linux is generally easiest to use online maps through a browser rather than an installed application.

Balena Etcher – This is a necessary tool for creating bootable media, such as computer boot drives. A boot drive allows you to run and/or install a computer operating system on another computer. This is how your computer was created, a Linux boot disk was made using Balena Etcher to install Linux.

Additional System Utilities
In addition to the software applications covered, you also have a number of other utilities installed to further help you get as much functionality out of your system as possible. These are all very lightweight on your system, but offer powerful features and tweaks.

YT-DLP – A utility that downloads YouTube videos via the terminal, see documentation

HTOP, BTOP – These utilities can be accessed via the terminal, simply type in ‘htop’ or ‘btop’ and hit enter, shows a number of details about your system such as load on your processor, memory and running applications. Useful for troubleshooting and viewing system resources use.

Hardinfo – another terminal tool, simply open a terminal and type ‘hardinfo’ and it will launch a window showing all of the information about your system. This is very similar to Device Manager on Windows, very useful for viewing the exact components of your system.

Stacer – Shows system resources in use, similar to Task Manager. Access Stacer via Applications menu.

curl/wget – allows you to download files through the terminal, useful for various installations.

Fdupes – a terminal based tool for finding duplicate files on your system to clean up your disk.

Gnome-tweaks – type ‘gnome-tweaks’ into your terminal to launch, adds additional ability to tweak the appearance and behavior of your system.

mLocate – System tool to help you find files on your system via the terminal.

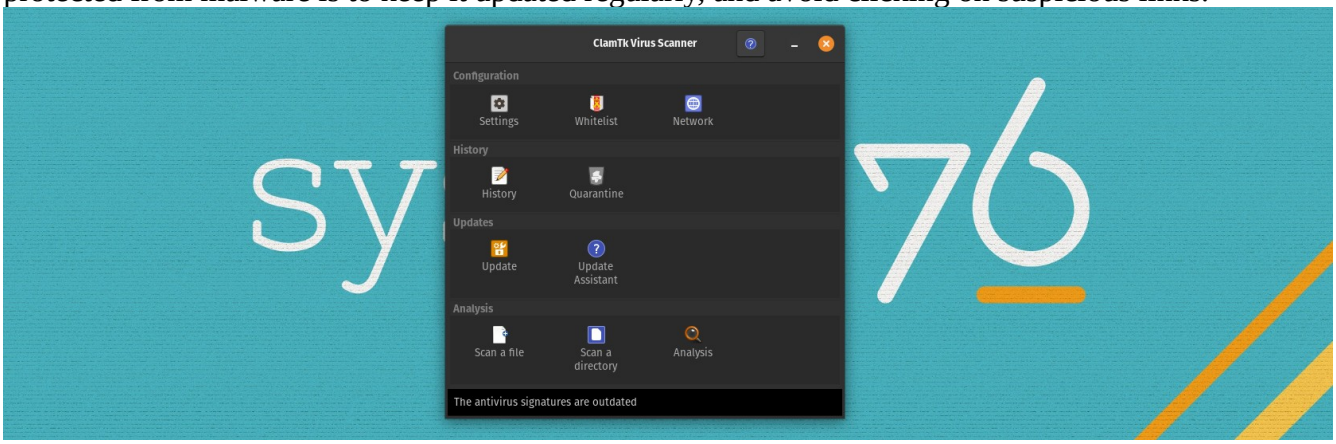
Delete Permanently Right Click feature – adds an additional option when right clicking on a file. Normally you can only move a file to the trash (same as Delete in Windows), your system now has the ability to permanently delete files from right click menu if desired.

Anti-Virus on Linux

ClamTK – Anti-Virus for your system. This is a topic that many find quite strange, generally we do not run active anti-virus on Linux. ClamTK, and it’s terminal based version ClamAV application are not active, however they will scan your system or a specific folder or drive when you wish. This is much different than what you are used to on other operating systems where anti-virus is running continuously in the background looking for any malware signatures in real time.

With active anti-virus, you are trusting your entire system including the root (administrator) file system to a third party (the anti-virus service), on Linux we want to maintain full control of our system and not allow any third party full access to our system. With ClamTK, the only time it touches the internet is when you pull updated signatures. The scanning is happening locally via the application, not an online connected third party. ClamAV can be configured to run automatically if desired at set intervals via something called ‘cron jobs’ if you desire automated scans.

While there are certainly viruses for Linux, they are extremely rare with users on desktop, and with proper digital hygiene, there is really no need to run active anti-virus for most of us. The open source nature of Linux, its permissions and file structure and software repository management makes your system inherently very secure as is. The number one thing we can do to ensure our systems our protected from malware is to keep it updated regularly, and avoid clicking on suspicious links.



Other Useful System Maintenance

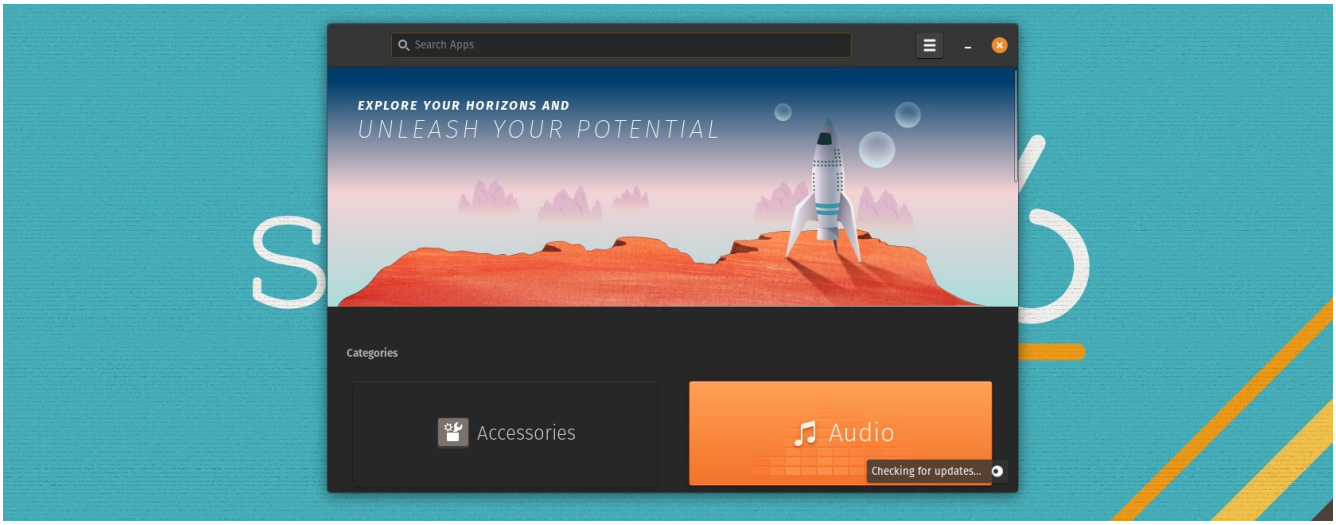
Keeping your machine updated is paramount, this provides security patches daily, as well as bug fixes to ensure your machine and all of its software are running the most up to date versions. This not only keeps your system running smooth, but provides a better secure system for you as you do your daily compute tasks. Linux is powerful, just keep it updated and it will do the rest to keep you secure and trouble free!

One of the more common issues we see is folks running out of date software, please update your system regularly to take advantage of the security and bug fixes, in the following section we will discuss how to do this in several ways. Do not be adverse to the terminal on Linux, it is much easier than you think!

For easy GUI updates of your system, visit the software management center of your distro and follow the prompts to update your system. Alternatively on any Debian based Linux distro (almost assuredly one that is provided to you by us, we rarely sell any other type of Linux distro) you can easily copy/paste the following commands into the terminal and achieve the same results in a much quicker and more efficient manner. The GUI tool provided with your distro is completely fine, but most of you will appreciate the speed of the terminal over the initial comfort of the GUI tool. Neither is a wrong answer, but those who can explore the Linux terminal will gain very useful insight into the powerful world of Linux and all it can offer us for secure computing.

Initially the terminal seems ‘dangerous’ but it is extremely difficult to break your system using the terminal, it offers immense power well beyond any Windows or Apple experience you’ve ever had. While Linux has bridged the usability gap in recent years and becoming extremely user friendly, the terminal still offers us God like powers over our systems, so please learn the few basic commands to take advantage of your system. If you are totally adverse to the terminal, Linux has grown quite easy to use with a GUI interface on most distros, so you really have the option to cheat on most distros if you never wish to use the terminal at all.

Example Software and Update Interface (Pop!_OS Linux)

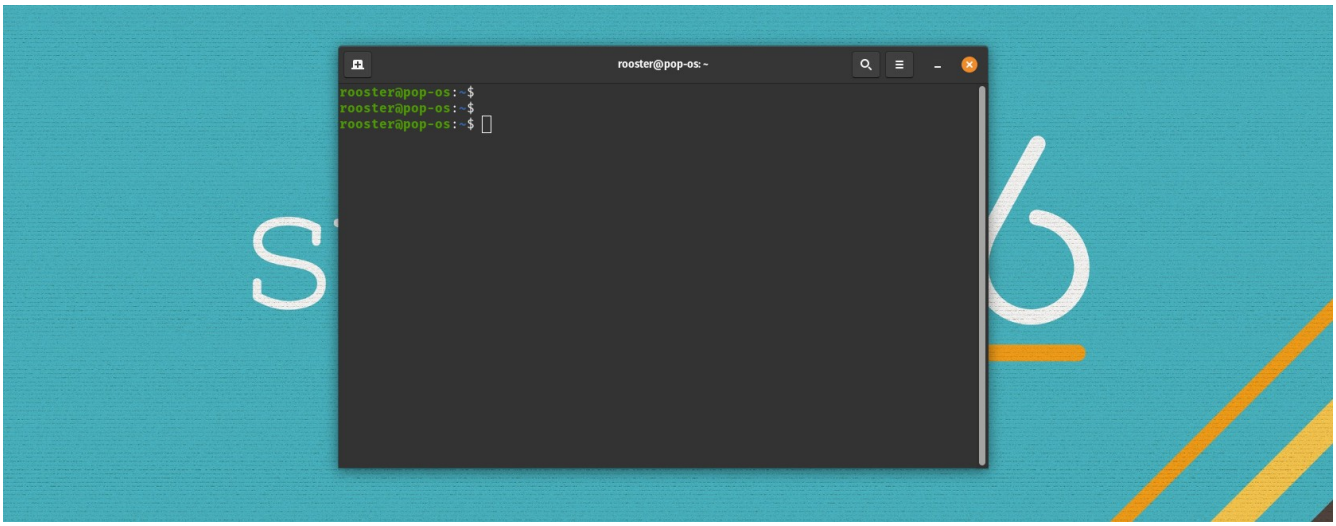


To update and clean your system, run the following commands as often as you can (daily is best, but at least weekly is recommended), run each line one at a time in your terminal, or you can copy all five commands at once and run them (copy/paste into a terminal window and press enter):

```
sudo apt update
sudo apt upgrade -y
sudo apt autoremove -y
sudo apt autoclean

flatpak update -y
```

Example of what the terminal looks like on Linux



Your System Firewall

Installed on most Linux distros is an active firewall called UFW or Uncomplicated Firewall. This is a very simple way to manage a very complex set of IP tables to handle all traffic coming in and out of your machine, you can use UFW to fine tune rules to enhance security.

GUFW is a GUI based version of UFW and is an even easier method to manage your firewall. The default is 'active' (on) and 'Allow all outgoing', 'Deny all incoming' and you may wish to disable specific IP addresses, ports or to whitelist specific services you need. Generally you don't need to mess with this very often as there are better tools like custom DNS to further take control of all incoming and outgoing traffic. The only thing you'll want to check periodically is to ensure that UFW is on, or active. You'll find GUFW in your Applications menu, simply open it and ensure your firewall is active.

Custom DNS

We are assuming you are using a VPN most of the time, your firewall is active, and you can periodically scan for malware using ClamTK or ClamAV. Another excellent service to install and use is

a custom DNS service. NextDNS is one of many such services, usually during the ordering process, we will ask if you want this configured or not.

DNS is the Domain Naming System, or in plain speak, it's the phone book of the internet. Just like you don't memorize all of your contacts phone numbers, but rather their name, DNS is very similar. It takes a domain name (like GrapheneGoat.com) and translates it into an IP address (198.46.93.53) and makes the connection to that web service. Normally your ISP (Internet Service Provider) handles your DNS queries (and therefore can see every connection you make), when we use a VPN, the VPN provider takes over the DNS queries. While not every VPN / Custom DNS service combination works well together, we have tested NextDNS with Proton VPN, Mullvad VPN and IVPN and works well.

The benefit of NextDNS (or any other privacy respecting DNS service) is that it allows the user to fine tune all connections between your computer and the internet. You can block entire domains such as facebook.com, you can whitelist any URL or site you wish, which is excellent for parental controls, as well as prevent any connections to undesired services online. NextDNS also has a ton of blocklists that you can toggle on that filter out ads, known malware and suspicious or malicious sites for you automatically, this makes for a much safer and more ad free experience.

IPv6 Disable
We configure all of our machines for customers to block all IPv6 traffic unless otherwise specified. IPv4 is the traditional IP address which is a 32 bit format (198.46.93.53), where IPv6 is a 128 bit format that looks like this: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

The main difference is how unique you look to online services. An IPv4 address means you are one in 4.3 billion, whereas with IPv6 addressing, you are one in 340+ undecillion (340 x 10 to the 36^{th} power), or in other words, very, very unique. This is poor for privacy, so we disable this type of addressing on your system and force IPv4 addresses only to connect to the internet, which is much more desirable.

To check to ensure you are using IPv4 only, visit: https://deviceinfo.me/

If you see an IP address that looks like this format, you are protected: 198.46.93.53

WebRTC Disable
Your machine can be configured to block WebRTC leaks from happening. When using various services such as video teleconferencing (VTC), gaming or some streaming services, WebRTC can leak your true IP address, even when behind a VPN. While we can disable this manually through your browsers, some of your browsers already block WebRTC by default, and using Proton, Mullvad or IVPN VPN already blocks WebRTC leaks, so we leave this feature alone. However you may still wish to manually disable WebRTC in your various browsers, namely Firefox and Brave. LibreWolf, Mullvad and Tor browsers should block it by default. More information on how to do this is in the link below.

To learn more about VPN's, Firewalls, Custom DNS, IPv6 Disable, and WebRTC disabling, you can read more about each of those on our page here:

https://graphenegoat.com/linux-operating-systems/hardening-linux/

Password Managers
If you do nothing else, please make sure that you are using a Password Manager, and Two Factor Authentication (2FA) for all of your accounts and login information. This is absolutely critical in

today's age, especially with the growing number of online services required to do all of the important things in our lives beyond email and social media. Our banking, healthcare and many other important aspects hinge on us having proper security on those accounts, failing to secure them can cause catastrophic damage to our well being.

Using a Password Manager and 2FA takes your risk of a breached account to as close to zero as we can get. ***Ensure you are using a long, strong, unique password for each account*** (the password manager can auto generate a strong password for you), and enable some form of 2FA. Password Manager apps that we recommend listed below, but more important than which one, is simply that you should be using one, whatever that is. This means you only have to remember the password/login to the password manager, from there it's simply copy/paste or autofill your credentials, without the need to memorize them. Never lose a password again, since they all will be centralized in one application in one place.

`Proton Pass` (Free, open source, encrypted, cloud based/syncs automatically)

`Bitwarden` (Free, open source, encrypted, cloud based/syncs automatically)

`KeePassXC` (Free, open source, encrypted, offline only)

2FA Applications

`Standard Notes` (Paid tiers only, open source, encrypted, cross platform)

`Aegis` (Free, open source, encrypted, Android only)

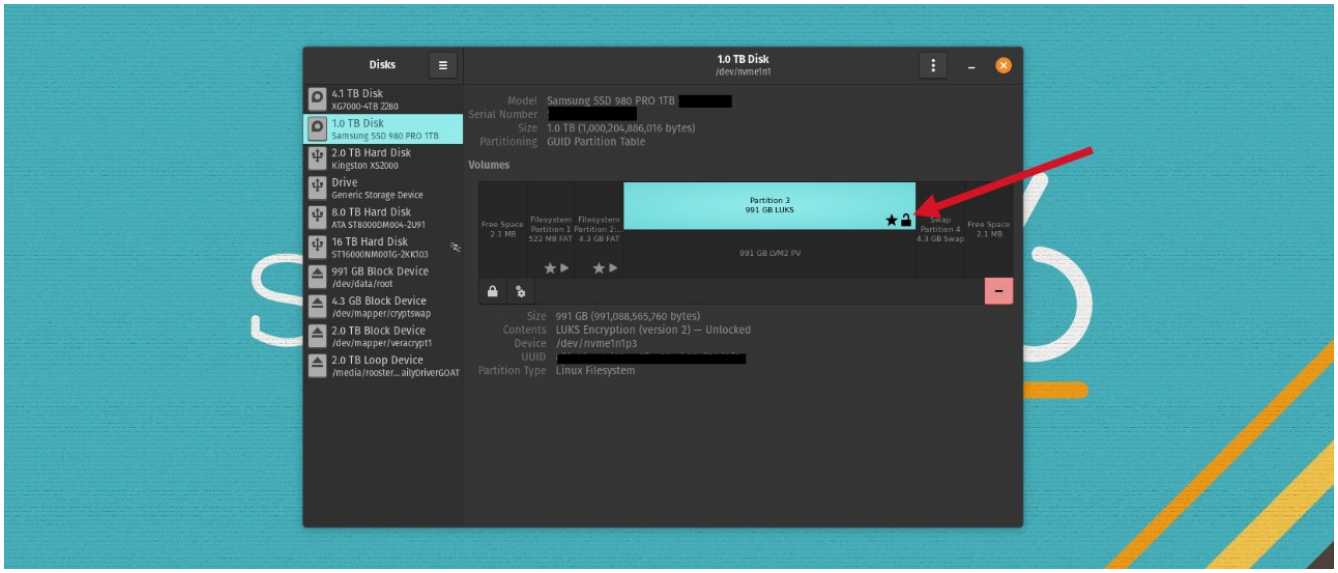
`Ente Auth` (Free, open source, encrypted, cross platform)

Changing Login Passwords
Your machine shipped, with your password(s) sent separately to you via email, this is to help guard against any possible tampering during transit to ensure your machine is secure. However you should change those passwords upon receiving your new device. Each Linux distro is a little bit different, and if you opted for Full Disk Encryption (FDE), you'll want to change that in addition to your user password to login to your machine.

To change the FDE passphrase, this is nearly identical on all distributions, let's look at the example below with Pop!_OS using the GUI application called `'Disks'`.

Pop!_OS
For FDE password change, open the application called `'Disks'`
Select your hard drive on the left pane
Next select the partition with the lock icon, this is your LUKS partition (red arrow)
Next click on the gears icon in lower left corner
Select 'Change Passphrase' and enter current password
Enter your new desired password twice and click Save

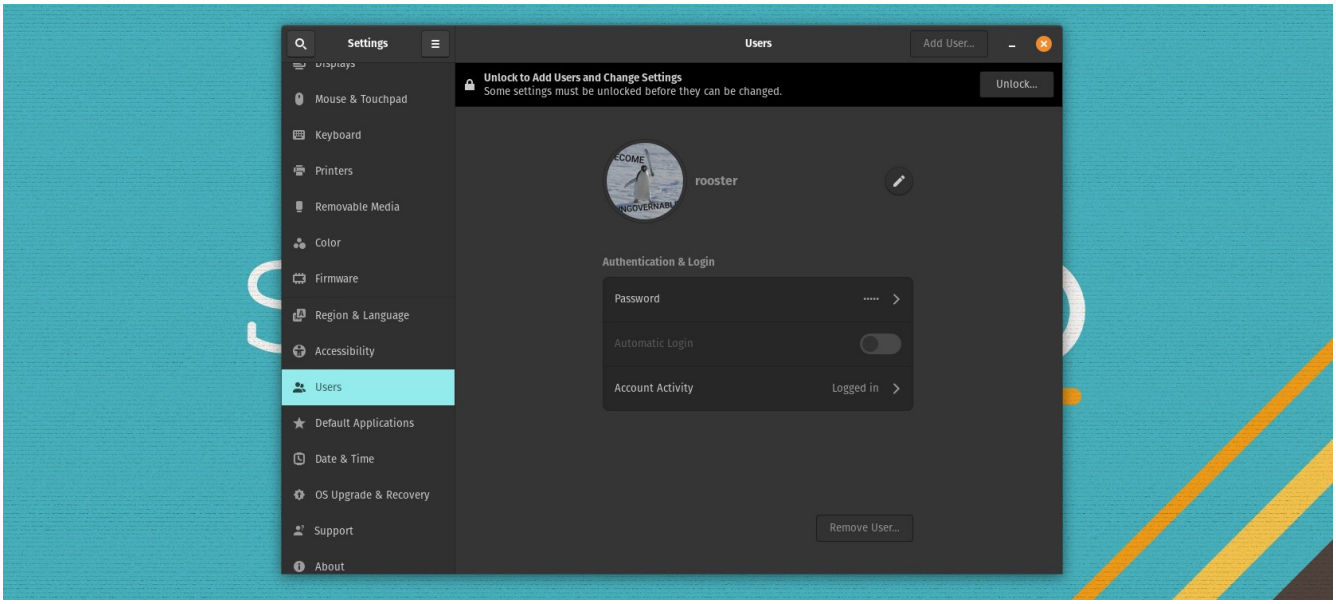
Below is a screenshot of the Disks application with the correct partition highlighted



Changing the User Password

This one is also located in a similar spot on most Linux distros, select Settings from your application menu and look for a setting called ‘Users’ or something similar.

You’ll need to enter the current user password to unlock this section, select ‘Password’ and enter your new desired password for that user twice and click save. (Pictured below)



This page left intentionally blank for user notes