**Kali Linux**

**Here are the top 10 things you should do to get it ready for use**

**1. Change the Default Password**

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2024/11/Change-the-Default-Password.png)

The first thing you should do is change the default password. **Security risk**: Kali Linux uses “kali” for both the username and password by default. This is widely known, making it extremely easy for anyone to access your system if left unchanged. ‘root’ is the superuser account in Linux systems. It has unrestricted access to all commands, files, and resources.

To change it:

1. Open the terminal

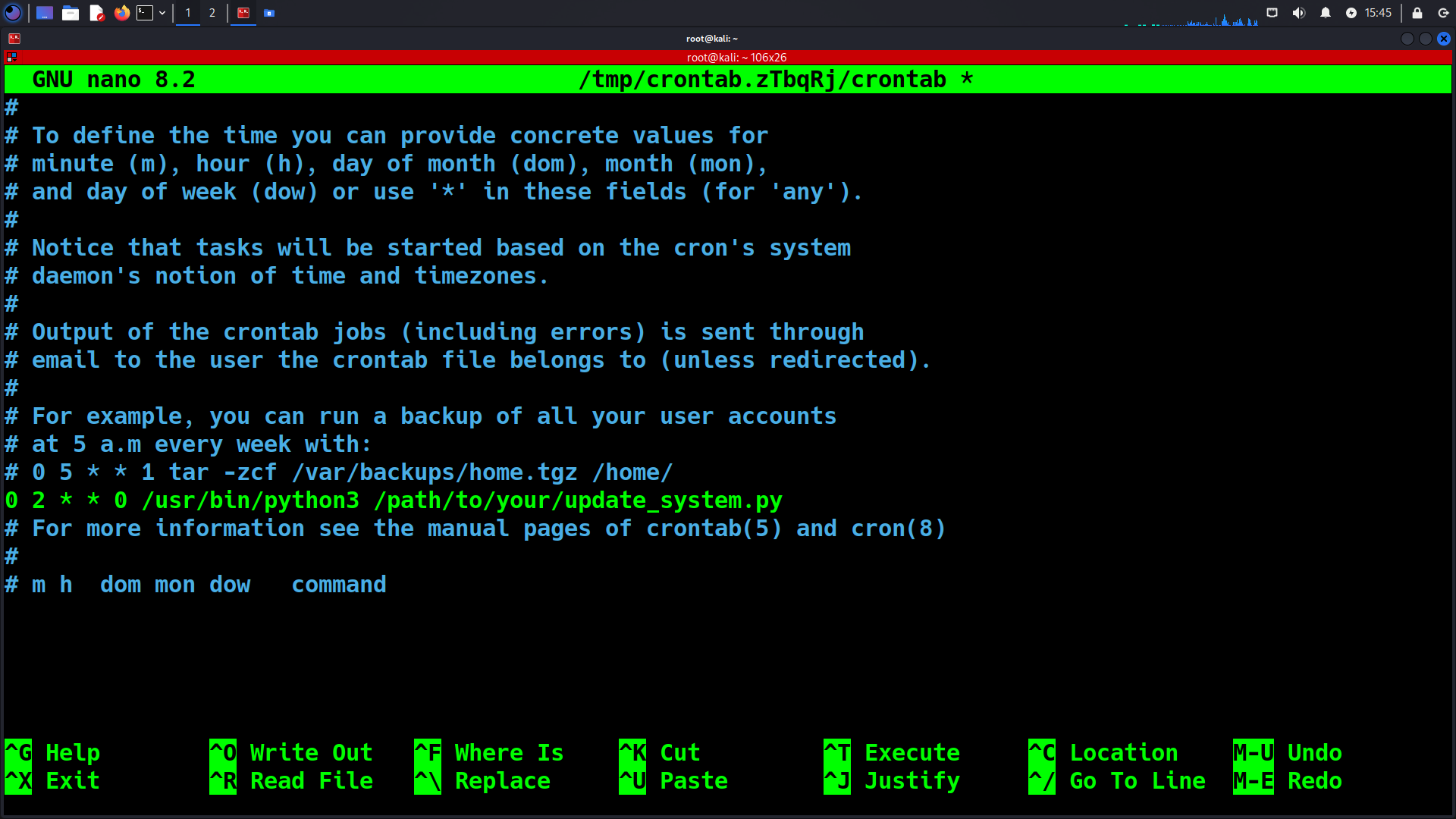
2. Type `sudo su` and press Enter

3. Type `passwd root` and/or `passwd kali` and Press Enter

4. Follow the prompts to set a new, strong password for either username.

5. Restart your computer and log in as root or kali with your new password

**2. Update the System**

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2024/11/Update-the-System.png)

Keeping your system up-to-date is crucial for security and performance. Kali Linux releases a lot of updates frequently.

You can create also an automated script in Python that can rapidly run the whole process of updating the OS operation.  To automate the process further, you can add this script to your cron jobs. This way, the system will update automatically without you needing to remember to run the process. Here’s how:

Automating the Update Process

1. Open the terminal

2. Type these commands one by one:

   – `apt update` (checks for updates)

   – `apt –list upgradable` (shows what can be upgraded)

   – `apt-get full-upgrade -y` (installs updates)

   – `apt dist-upgrade -y` (upgrades the distribution)

   – `apt autoremove -y` (removes unnecessary packages)

   – `apt autoclean -y` (cleans up the system)

Scheduling Automated Updates

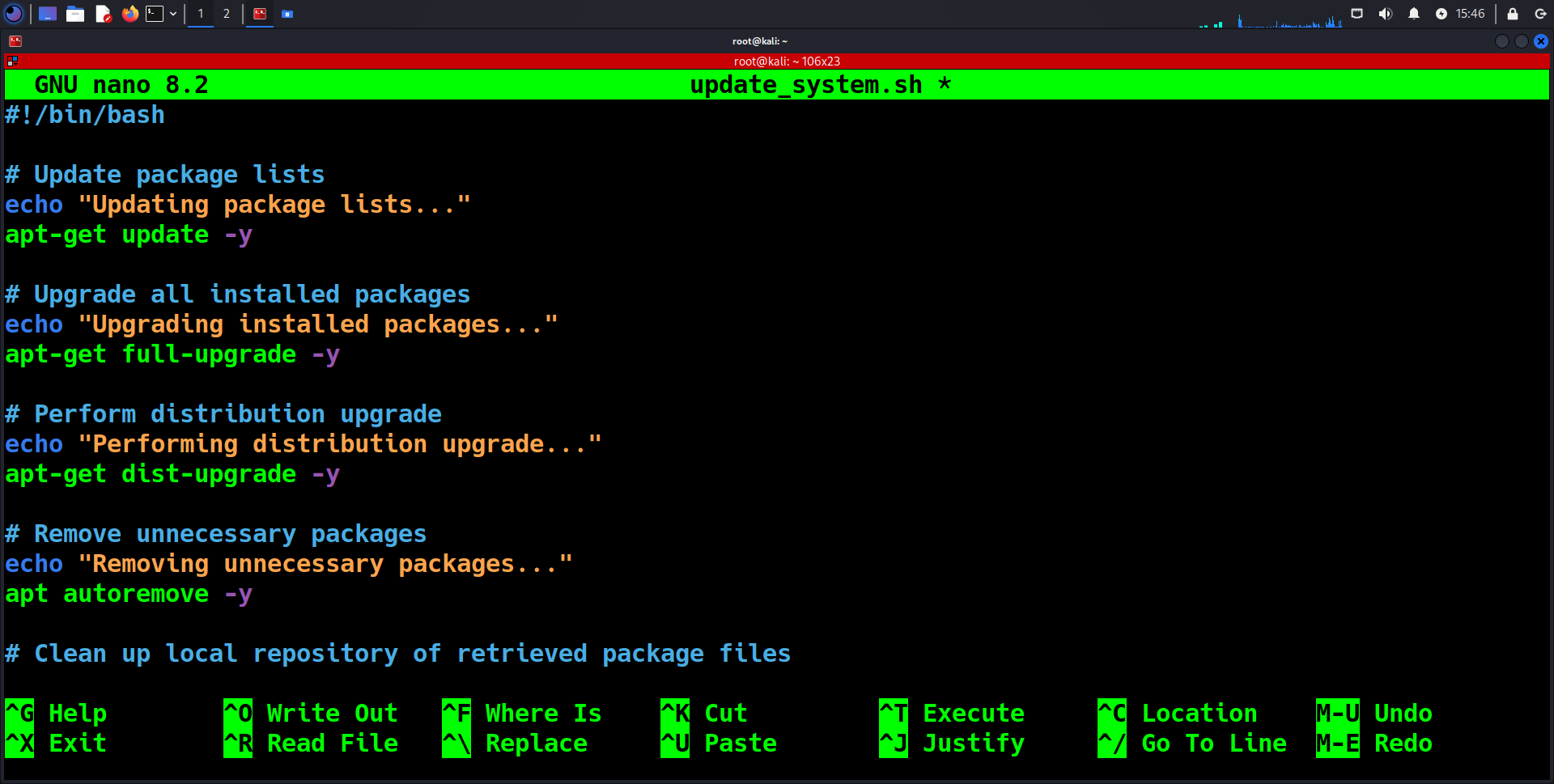
1. Open the crontab file

crontab -e

1. Add a line to run the script weekly for example every Sunday at 2 AM

0 2 \* \* 0 /usr/bin/python3 /path/to/your/update\_system.py

**Bonus Tip:**

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2024/11/Bonus-Tip.png)

Here is a one-liner that can also not just update your operating system, but perform cleaning and can be saved in a bash script for ease of use:

apt-get update -y && apt-get full-upgrade -y && apt-get dist-upgrade -y && apt autoremove -y && apt autoclean

**See Also:**[**Offensive Security Tool: TerminatorZ**](https://www.blackhatethicalhacking.com/tools/terminatorz/)

**3. Set Up SSH (If Needed)**

By default, SSH (Secure Shell) is turned off in Kali Linux to minimize potential security vulnerabilities, particularly when you have the default open port on 22, it can be exploited in various ways. However, if you need to enable SSH for remote access, file transfer, or other secure communications, you can easily configure and start the SSH service. Here’s a step-by-step guide:

1. Open the terminal

2. Type `nano /etc/ssh/sshd\_config` to edit the SSH config file

3. Make these changes:

   – Set `Port 7` (or any port you prefer)

   – Set `ListenAddress 0.0.0.0`

   – Set `MaxAuthTries 3`

   – Set `MaxSessions 7`

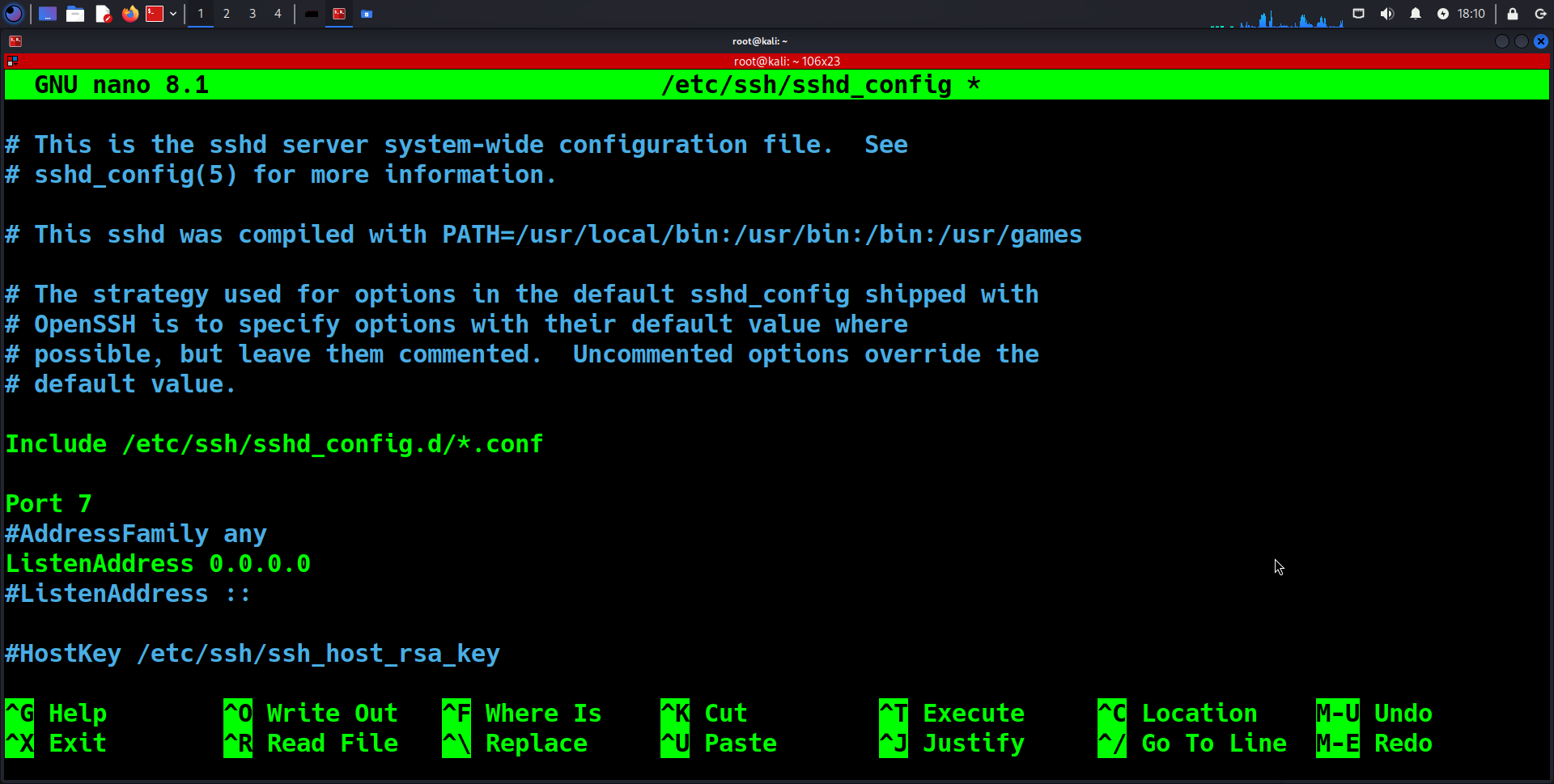
   – Set `PasswordAuthentication yes`

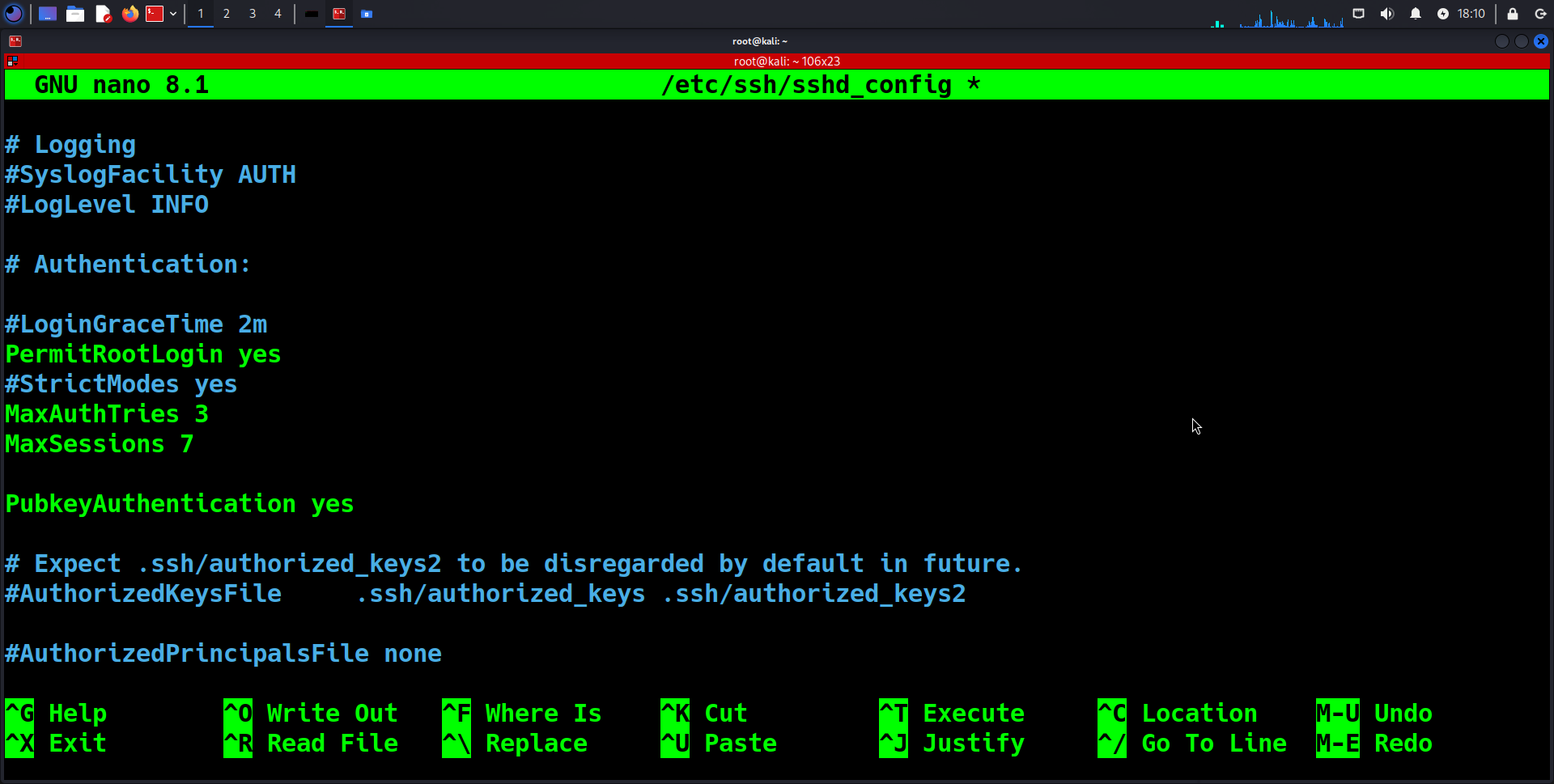
   – Set `PermitRootLogin yes`

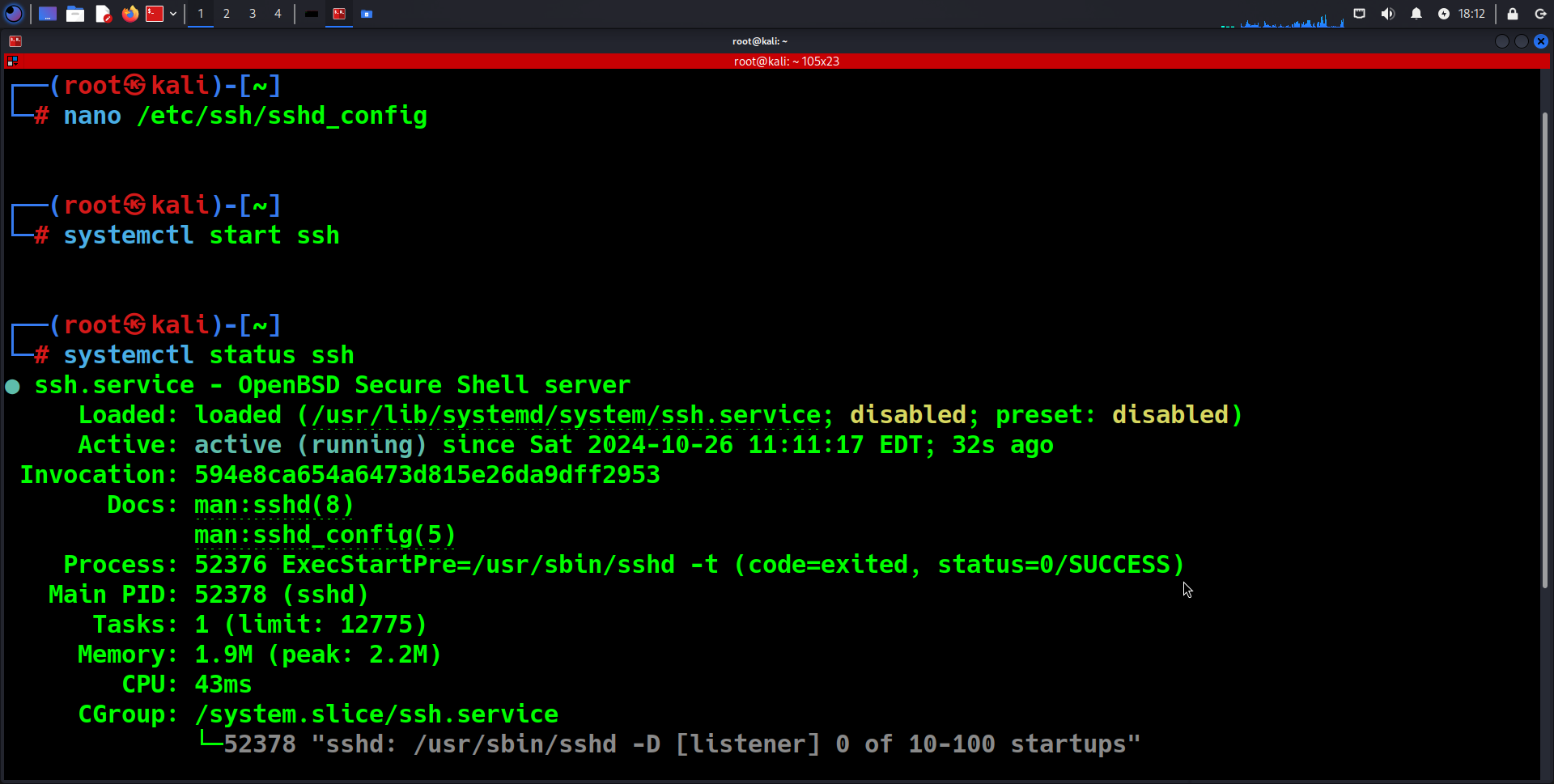
4. Save and exit the file

5. Type `systemctl start ssh` to start SSH

6. Type `systemctl status ssh` to check if it’s running

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2024/11/config_1.png)

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2024/11/config_2.png)

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2024/11/run.png)

**4. Install Additional Drivers**

After setting up SSH and ensuring secure remote access, you might find that some hardware components in your system, such as Wi-Fi cards, graphics cards, or other peripherals, require additional drivers to function properly. Kali Linux, being a specialized distribution, might not always come with all drivers pre-installed, especially for proprietary hardware.

1. Open the terminal

2. Type `apt install firmware-linux` to install additional firmware

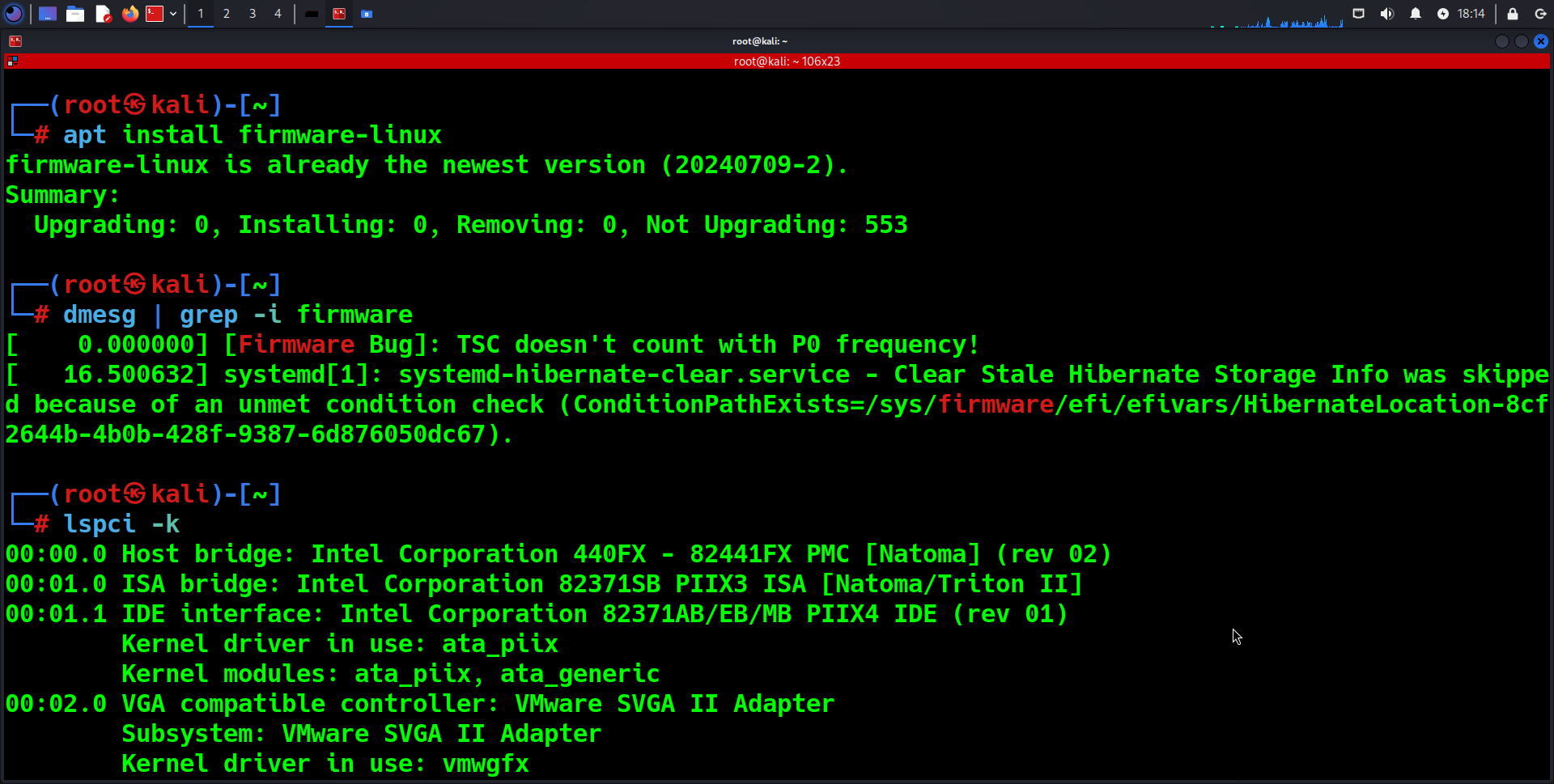
3. Use these commands to check your hardware:

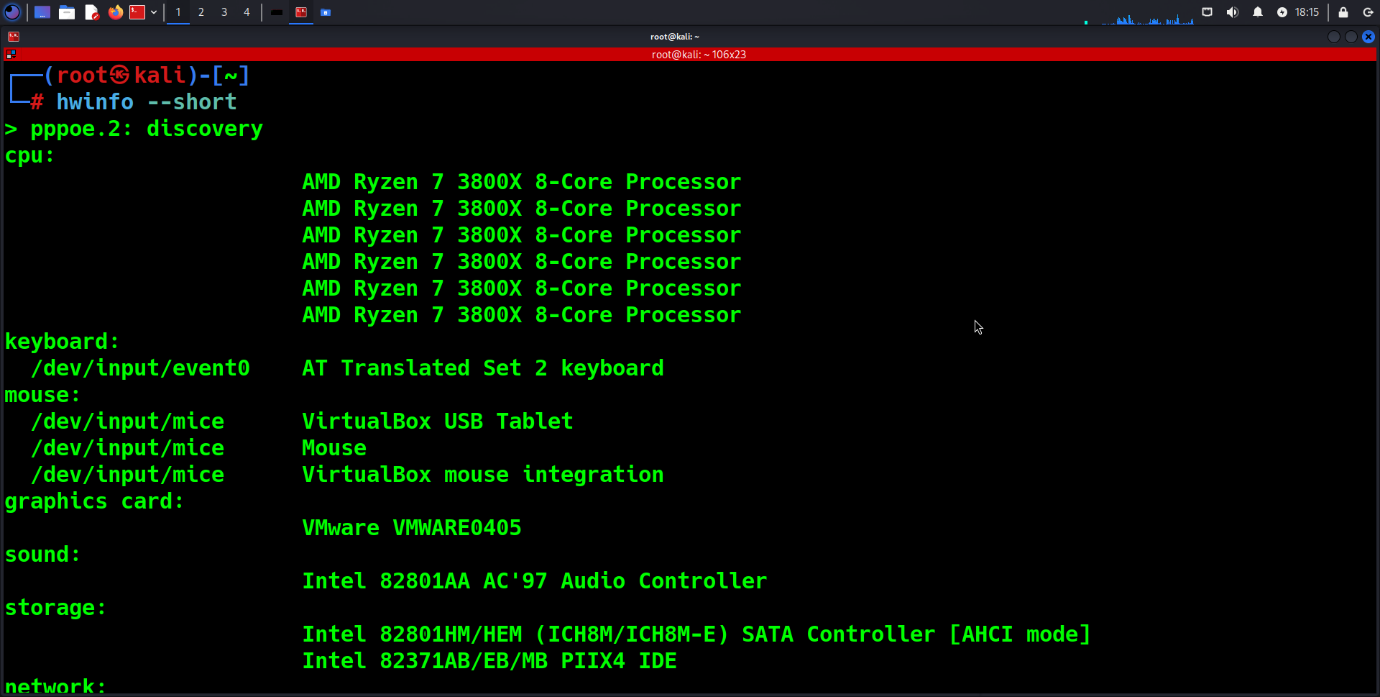
   – `dmesg | grep -i firmware`

   – `lspci -k`

   – `hwinfo –short`

   – `hwinfo bios`

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2024/11/Install-Additional-Drivers_1.png)

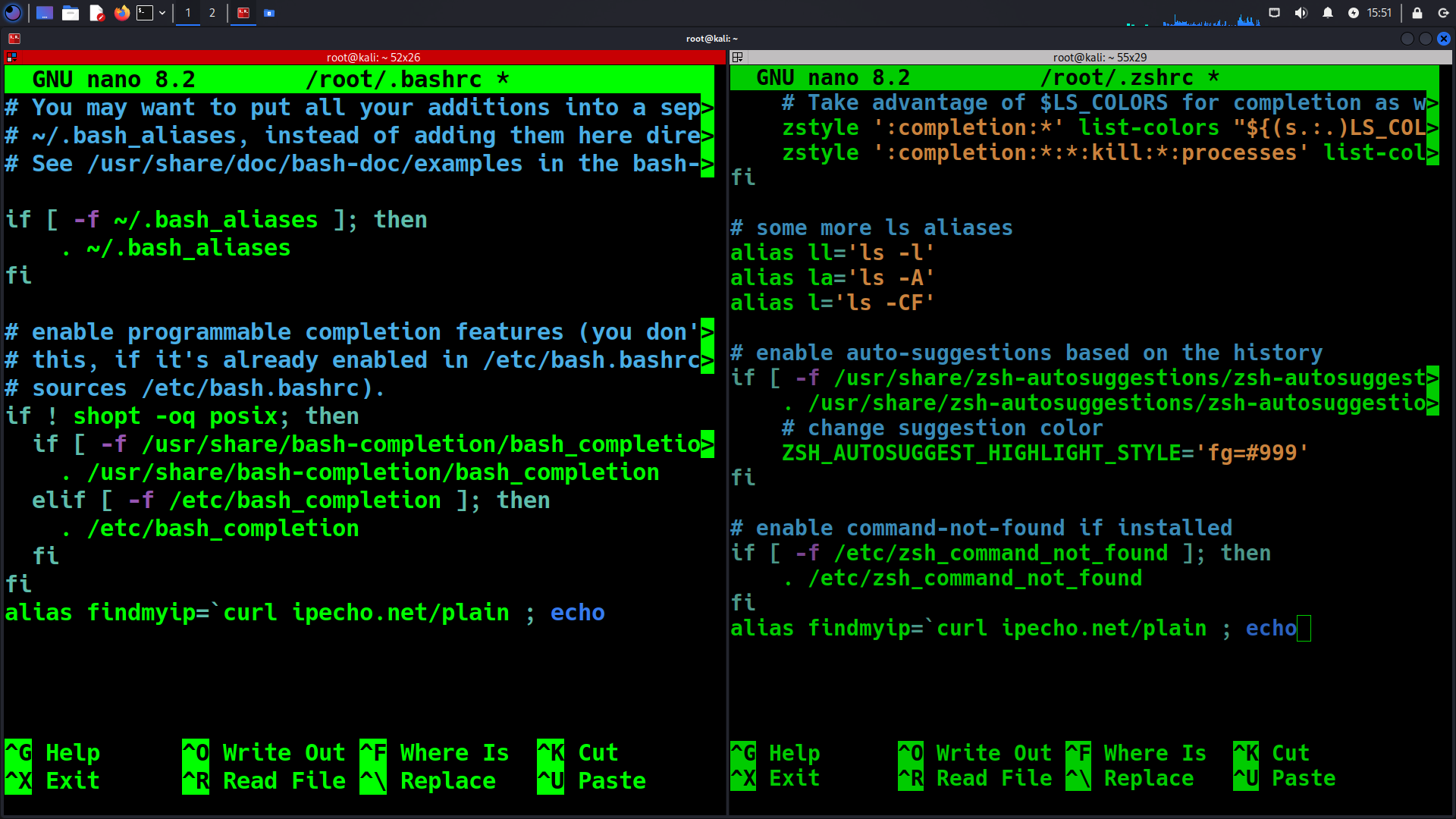
[](https://www.blackhatethicalhacking.com/wp-content/uploads/2024/11/Install-Additional-Drivers_2.png)

**5. Set Up Bash or ZSH Aliases**

Aliases are a great way to simplify and speed up your workflow by creating shortcuts for frequently used commands. On Kali Linux, you can set up aliases to save time and avoid typing long commands repeatedly.

1. Open the terminal
2. Type `nano ~/.bashrc` or `nano ~/.zshrc` to edit your bash or ZSH config
3. Add aliases like this: `alias findmyip=`curl ipecho.net/plain ; echo`
4. Save and exit the file
5. Type `source ~/.bashrc` or `source ~/.zshrc` to apply changes depending on the terminal you are using.

What this will do is whenever you type ‘findmyip, it will automatically display your external IP address.

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2024/11/Set-Up-Bash-or-ZSH-Aliases.png)

**6. How to List Available Metapackages**

Kali Linux metapackages are bundles of related tools that cater to specific purposes or tasks, making it easier to install all the tools you need with a single command. This is particularly useful for setting up a tailored penetration testing environment, as you can choose from various metapackages based on your needs. For Example, you can convert your Kali into a Digital Forensics only machine, or a Full edition with every single offensive security tool installed.

What Are Metapackages?

Metapackages are essentially “toolkits” grouped by category. When you install a metapackage, you’re installing all the tools and software associated with that category. For example, there are metapackages for wireless testing, forensics, or web application testing.

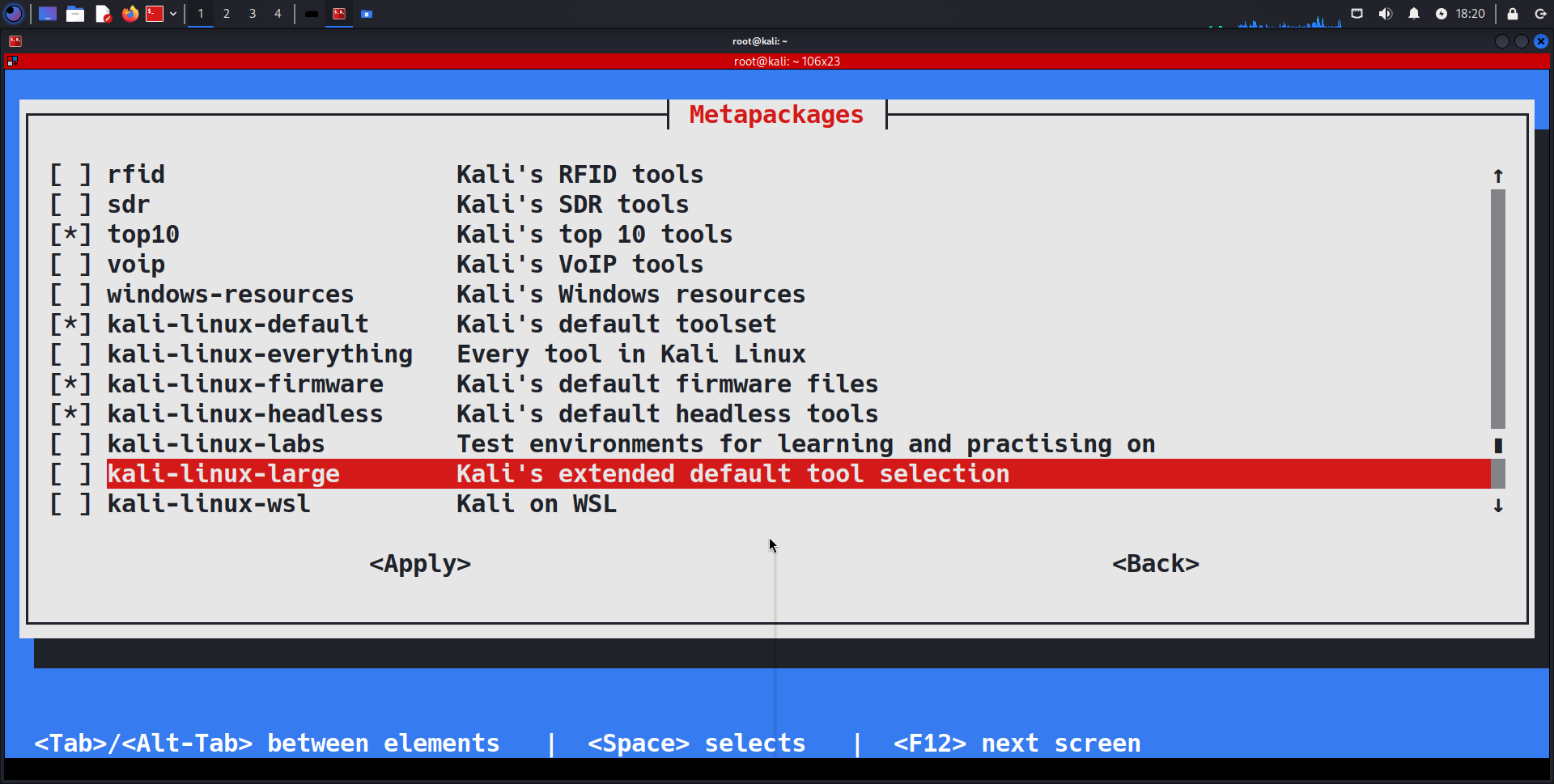
1. Open the terminal
2. Type these commands:

– `apt update`

– `apt full-upgrade -y`

– `apt install -y kali-linux-default`

1. Type `kali-tweaks` to open a menu for more customization options

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2024/11/Metapackages.png)

For more options, you can check them [here](https://www.kali.org/docs/general-use/metapackages/).

**See Also:**[**Exploit XSS Injections with a Powerful One-Line Technique**](https://www.blackhatethicalhacking.com/articles/exploit-xss-injections-with-a-powerful-one-line-technique/)

**7. Customize the Kali Linux Interface**

Customizing the Kali Linux interface can enhance your productivity and comfort, making your environment more suitable for your workflow. There are various ways to personalize the Kali interface, from tweaking the desktop environment to adding themes, changing icons, and setting up custom key bindings.

Make Kali look how you want:

1. Go to Menu > Settings > LightDM GTK Greeter settings
2. Change the background, icons, and other visual elements
3. To change the login screen background, go to `/usr/share/desktop-base/kali-theme/login` in the file manager

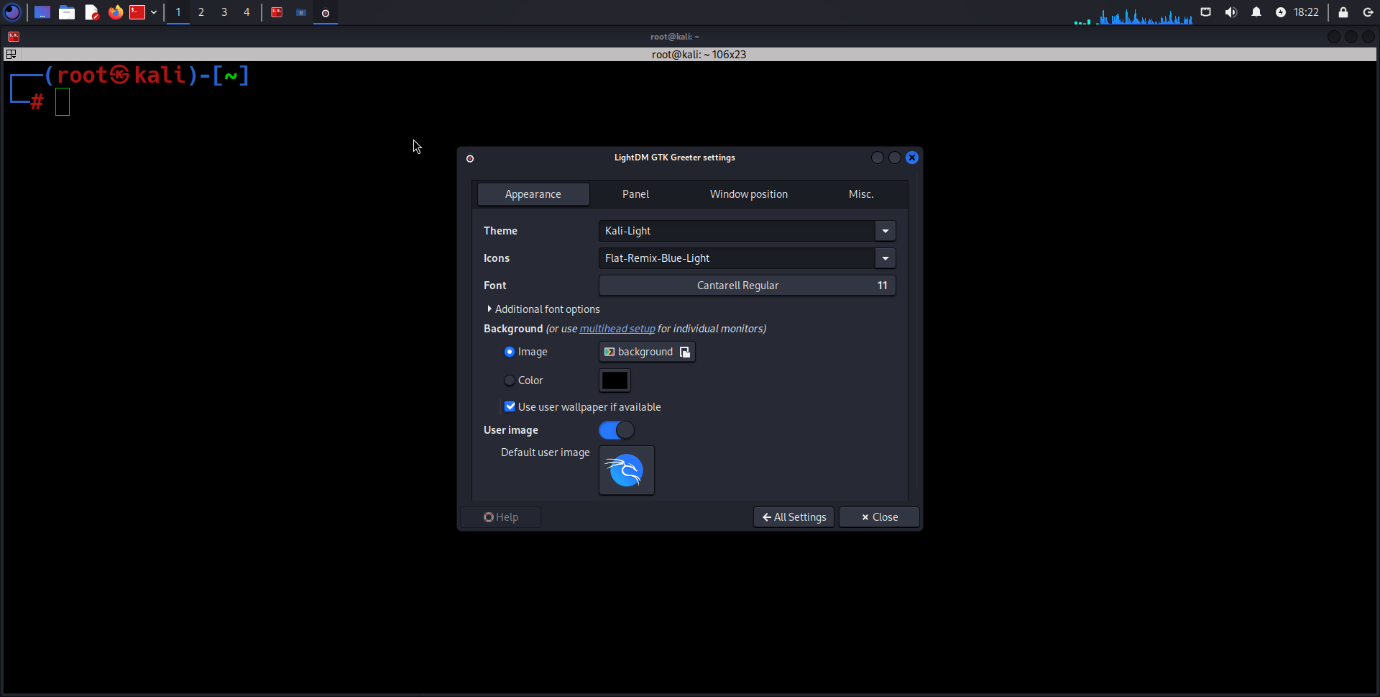
To change the default XFCE to a nicer and more rich interface you can install the KDE version.

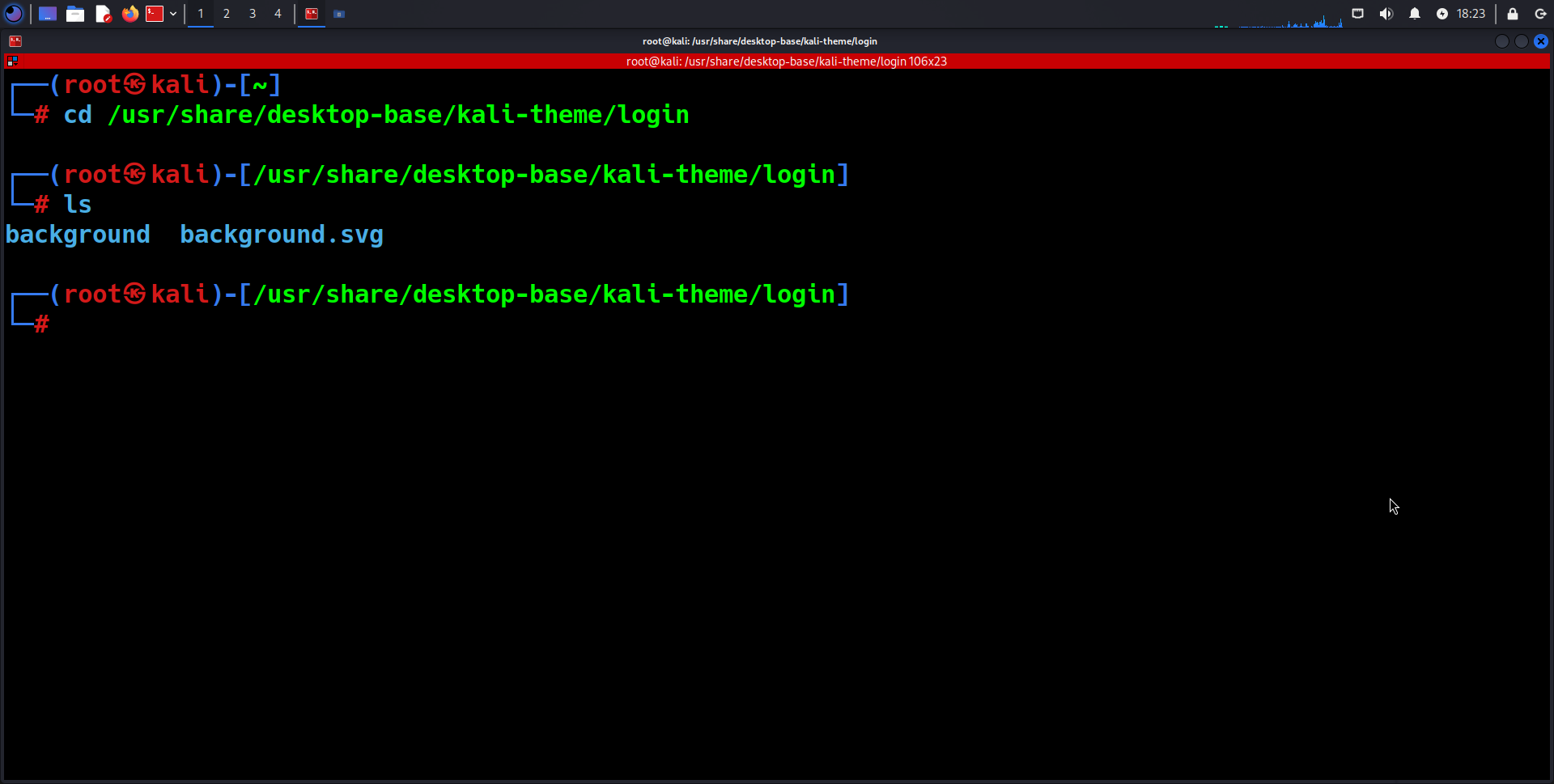
Open your terminal and type:

sudo apt install -y kali-desktop-kde

sudo update-alternatives –config x-session-manager

apt purge –autoremove kali-desktop-xfce

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2024/11/Customize-the-Kali-Linux-Interface_1.png)

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2024/11/Customize-the-Kali-Linux-Interface_2.png)

**8. Install Useful Terminal Tools**

Kali Linux provides a default terminal that is quite powerful, but sometimes you may need additional features or better functionality for more efficient workflow. Tools like **gueke** and **terminator** can enhance your terminal experience.

**Installing and Using gueke**

**gueke** is a terminal multiplexer similar to tmux that allows for splitting windows, running multiple terminal sessions within a single window, and creating panes and tabs. It is lightweight and very customizable.

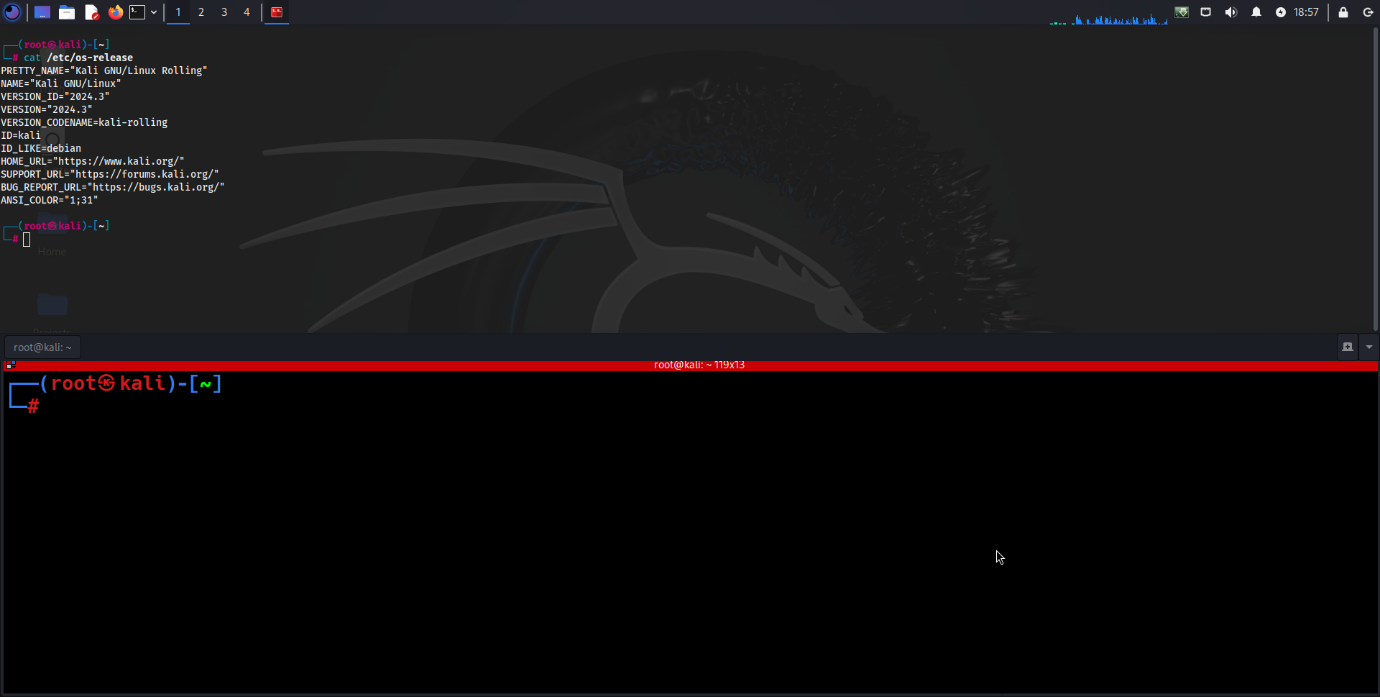
Some handy terminal tools to install:

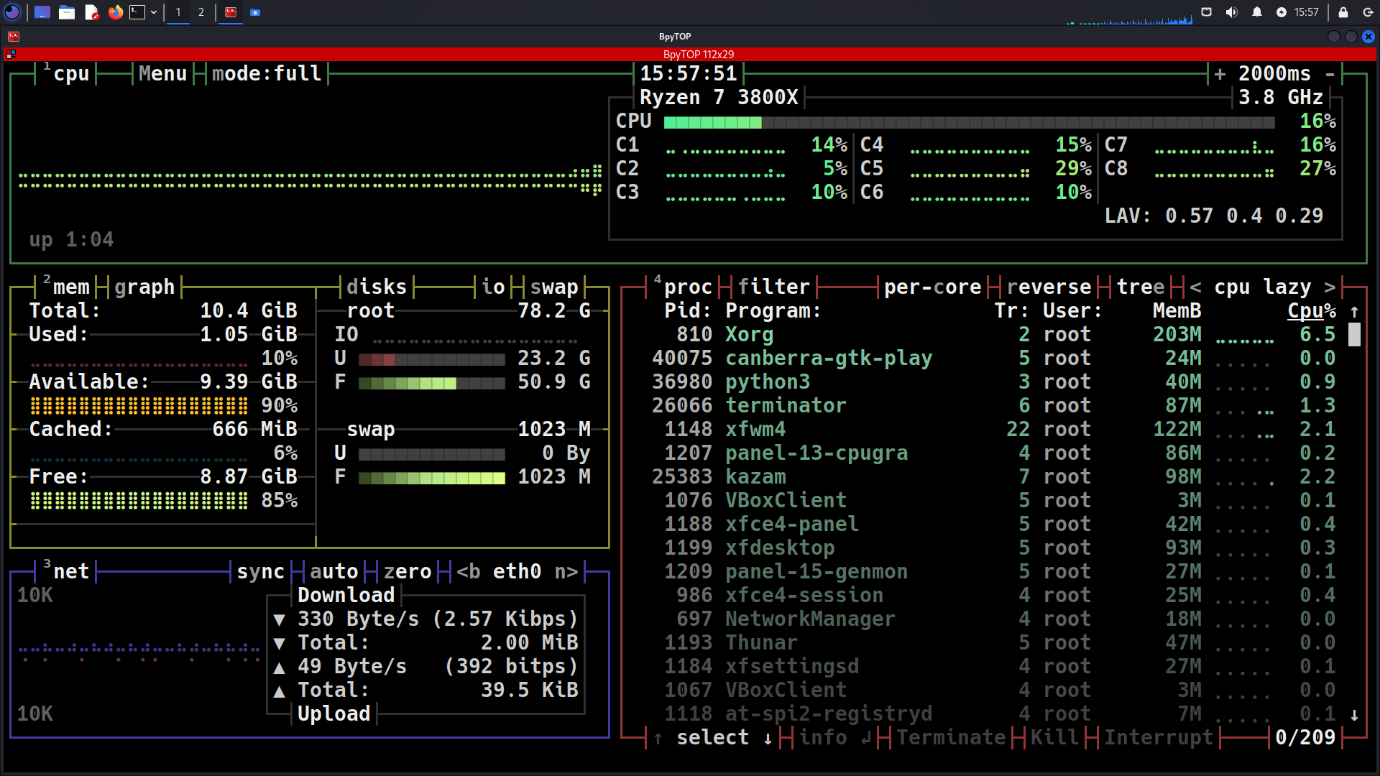
1. Open the terminal
2. Type these commands:

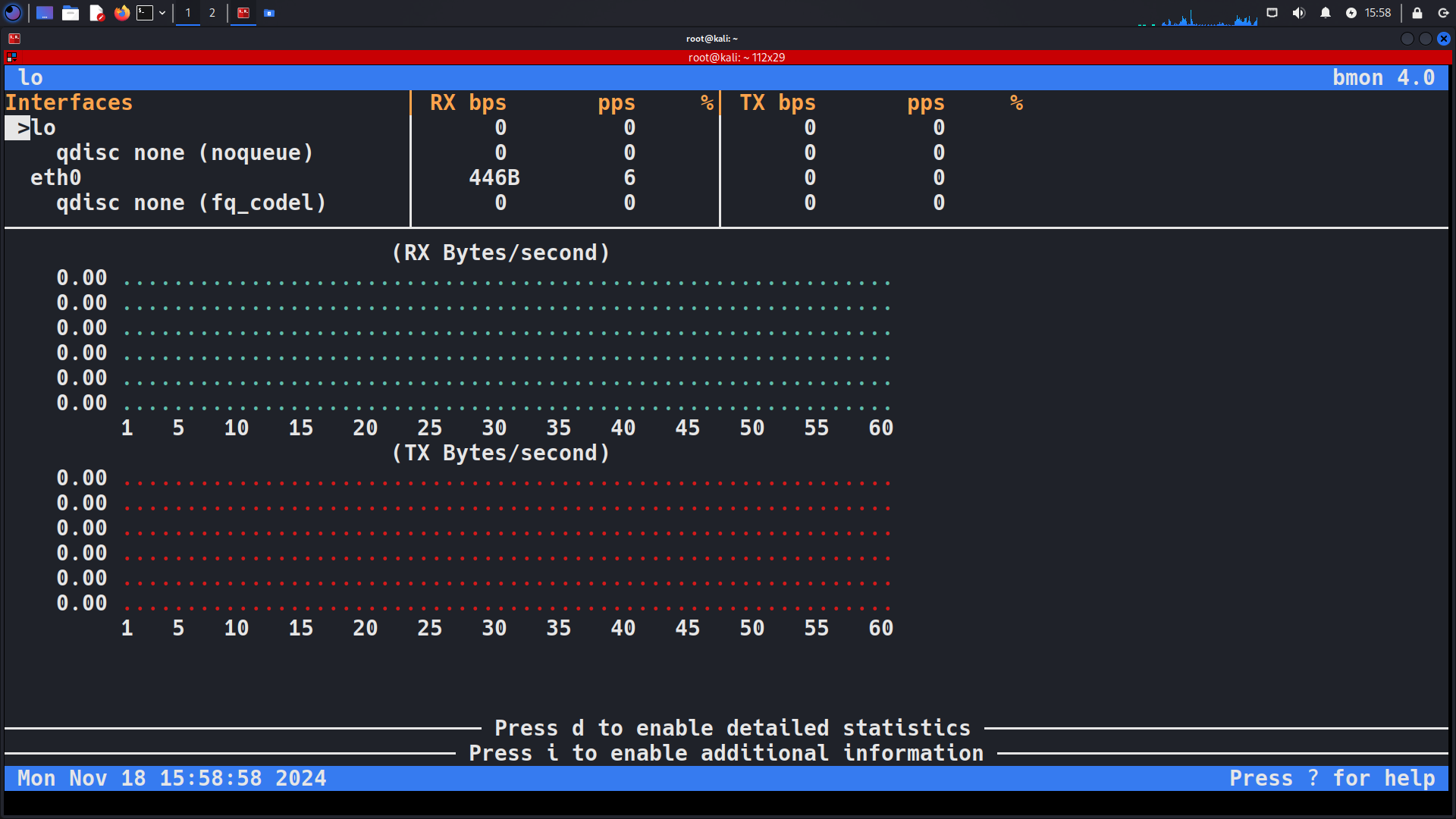
– `apt install guake` (for a drop-down terminal)

– `apt install terminator` (for multiple terminals in one window)

To monitor your network, you can also install tools for bandwidth monitoring, such as [bmon](https://github.com/tgraf/bmon), [bpytop,](https://github.com/aristocratos/bpytop) in the same way.

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2024/11/Customize-the-Kali-Linux-Interface_3.png)

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2024/11/Install-Useful-Terminal-Tools_1.png)

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2024/11/Install-Useful-Terminal-Tools_2.png)

**See Also:**[**The Importance of Expertise: Why Manual Pentesting Beats Automated Solutions**](https://www.blackhatethicalhacking.com/articles/the-importance-of-expertise-why-manual-pentesting-beats-automated-solutions/)

**9. Add Fun Terminal Customizations**

Customizing your terminal can make your daily work more enjoyable and personalized. There are a variety of fun and useful tools that can spice up your terminal experience in Kali Linux. Here are some tools to consider adding to your terminal setup.

Make your terminal more enjoyable with these fun tools:

1. Open the terminal
2. Type these commands:

– `apt install lolcat cowsay sl`

– `pip install lolcat`

– `apt install toilet`

1. Try them out by typing `cowsay Hello | lolcat` or just `sl`, or `toilet hello world | lolcat`

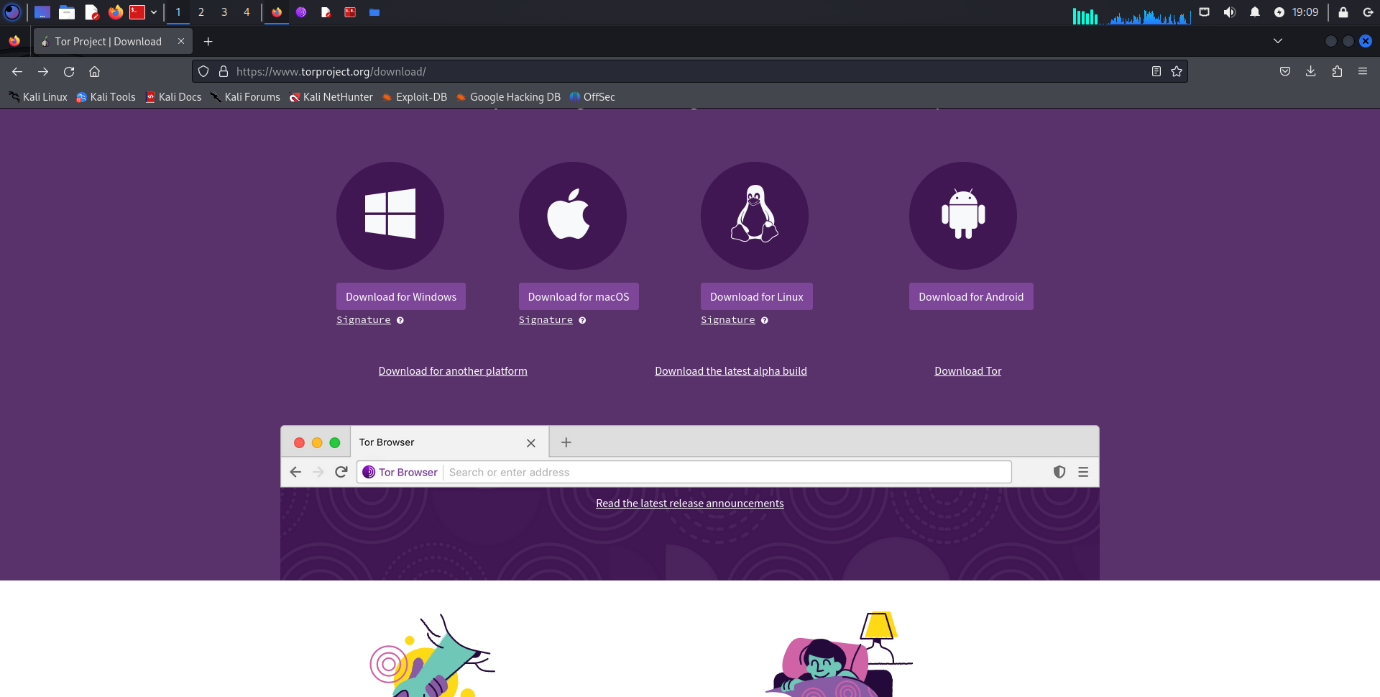
[](https://www.blackhatethicalhacking.com/wp-content/uploads/2024/11/Add-Fun-Terminal-Customizations.png)

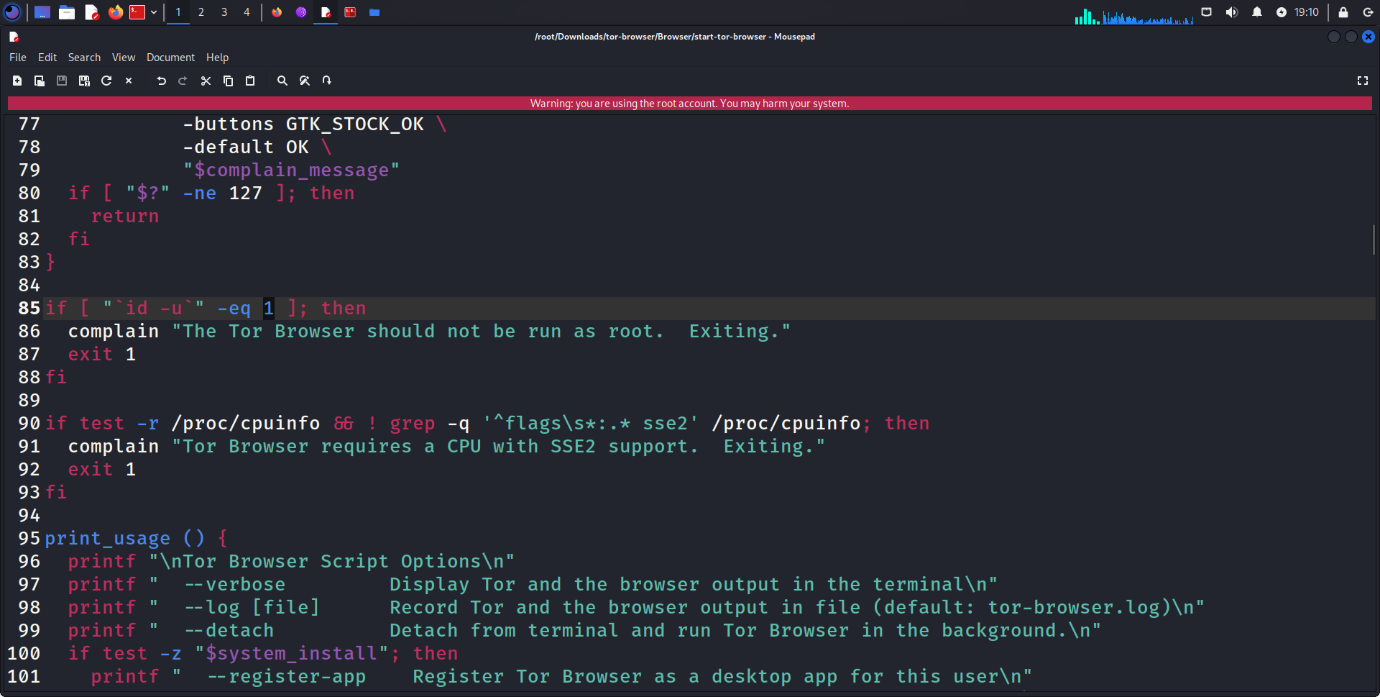
**10. Set Up Tor for Anonymous Browsing**

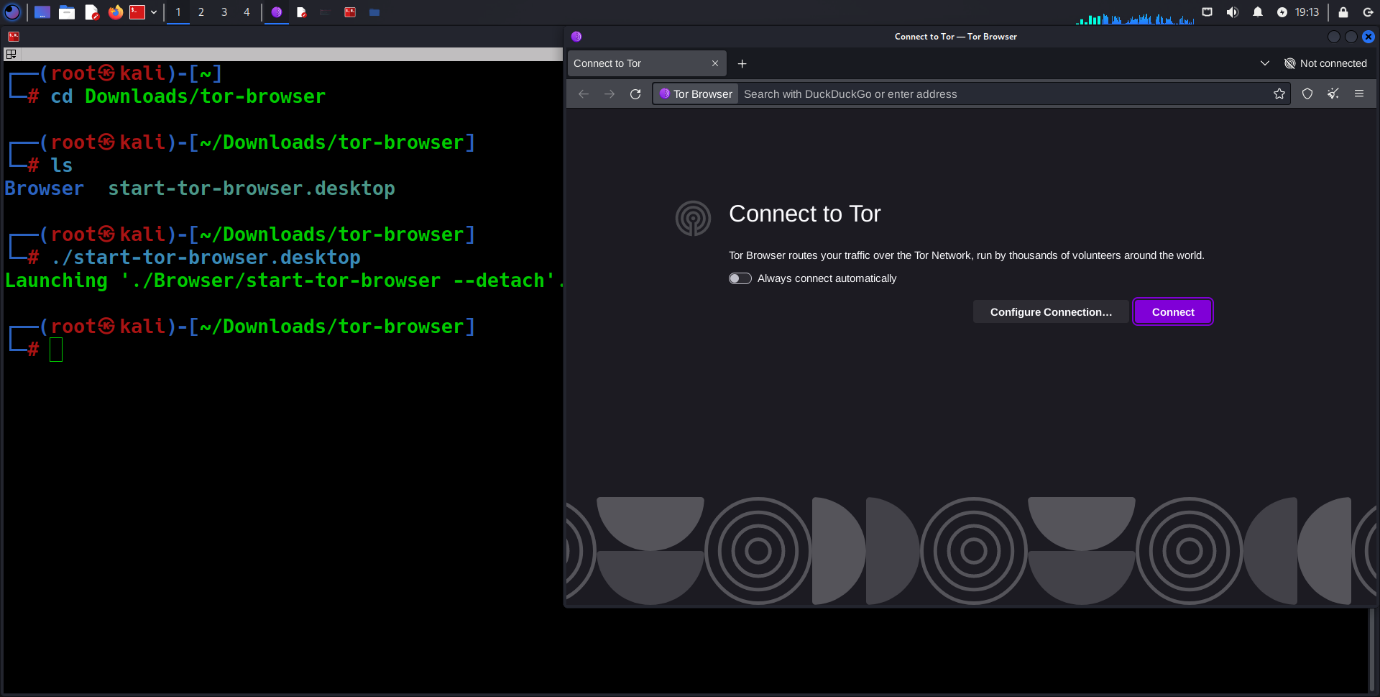
To enhance privacy and anonymity online, setting up **Tor** on your Kali Linux system is a great option. Tor routes your internet traffic through a network of volunteer-operated servers (nodes) to conceal your location and usage from anyone conducting network surveillance or traffic analysis using Socks5 an internet protocol used by Tor itself.

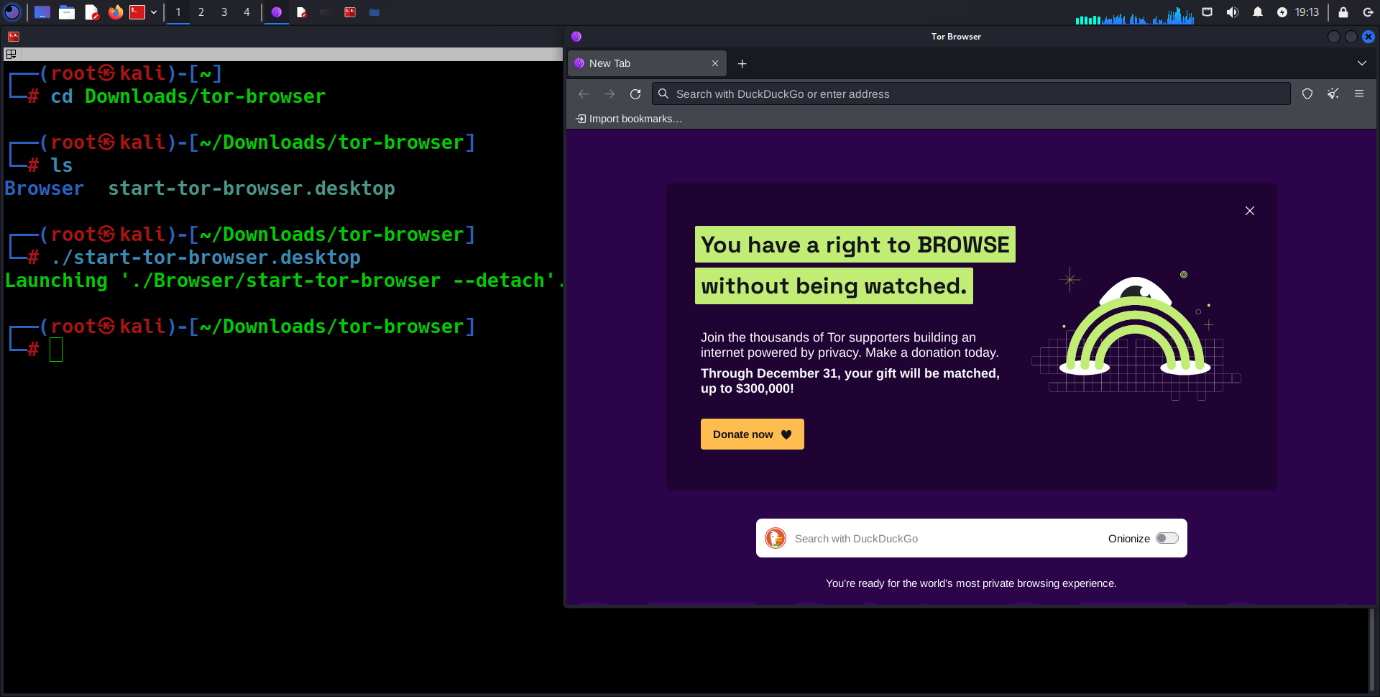
For more private browsing:

1. Open the terminal
2. Type `apt install tor torbrowser-launcher`
3. Once installed, you can launch Tor Browser from the application menu

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2024/11/Set-Up-Tor-for-Anonymous-Browsing_1.png)

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2024/11/Set-Up-Tor-for-Anonymous-Browsing_2.png)

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2024/11/Set-Up-Tor-for-Anonymous-Browsing_3.png)

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2024/11/Set-Up-Tor-for-Anonymous-Browsing_4.png)

To wrap up, the steps outlined in this guide are designed to help you establish a secure, efficient, and customized Kali Linux environment tailored to your needs as a cybersecurity enthusiast or professional. Remember, always use Kali Linux responsibly and ethically!

**Essential Skills Every Hacker Should Master**

*by | Oct 29, 2024 |*[*Articles*](https://www.blackhatethicalhacking.com/category/articles/)



**Post Views: 1,102**

**Join our**[**Patreon**](https://www.patreon.com/posts/how-to-use-to-2-58807517)**Channel and Gain access to 70+ Exclusive Walkthrough Videos.**

[](https://www.patreon.com/posts/perform-bug-and-94426120)

**Reading Time: 8 Minutes**

**Introduction**

With increased dependence on digital systems and the Internet, the surface of cyber threats and attacks expands. The high threat level further underscores the role played by hackers—not only as adversaries but as security defenders. Ethical hackers lead the charge in identifying and addressing vulnerabilities that can cause data breaches, financial losses, and even national security risks.

The objective of this article is to provide a comprehensive overview of the essential skills every hacker must master to excel in the field of offensive security. Whether you are an aspiring ethical hacker looking to enter the industry or an experienced professional seeking to sharpen your skills, understanding the core competencies required is crucial. By mastering these skills, you can effectively identify, analyze, and neutralize potential threats, thereby contributing to a safer and more secure digital world.

**See Also: So you want to be a hacker?**[**Offensive Security and Ethical Hacking Course**](https://www.blackhatethicalhacking.com/courses/offensive-security-and-ethical-hacking-course/)

**Scripting and Programming**

Proficiency in scripting and programming languages is a cornerstone for any hacker.

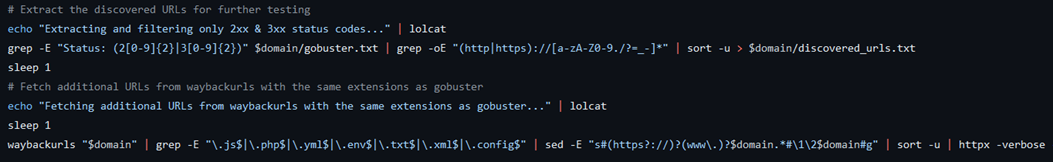
Here’s a closer look at the essential languages and why they are critical:

**Python**

* **Overview:** Bash is the default shell for Unix-based systems like Linux, which are widely used in hacking environments.
* **Practical use:** Bash scripting is vital for automating system tasks, managing files, and executing command sequences efficiently. It is particularly useful for creating scripts that automate repetitive tasks, thereby saving time and reducing errors.

**Bash**

* **Overview:** Bash is the default shell for Unix-based systems like Linux, which are widely used in hacking environments.
* **Practical use:** Bash scripting is vital for automating system tasks, managing files, and executing command sequences efficiently. It is particularly useful for creating scripts that automate repetitive tasks, thereby saving time and reducing errors.

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2024/10/SecretOpt1c.png)*Example of Bash Script, Snipped Code from BHEH tool*[*SecretOpt1c*](https://github.com/blackhatethicalhacking/SecretOpt1c/)

**JavaScript**

* **Overview:** JavaScript is the go-to language for web development, making it essential for understanding and exploiting web applications.
* **Practical use:** Proficiency in JavaScript allows hackers to manipulate web pages, identify and exploit client-side vulnerabilities such as Cross-Site Scripting (XSS), and craft sophisticated web attacks. Understanding JavaScript is also crucial for developing and debugging web-based payloads.

**SQL**

* **Overview:** SQL (Structured Query Language) is the standard language for interacting with databases, making it crucial for both web and data-driven hacking.
* **Practical use:** Knowledge of SQL is essential for identifying and exploiting SQL injection vulnerabilities, one of the most common and dangerous types of web application vulnerabilities. Hackers use SQL to manipulate database queries, extract sensitive information, and gain unauthorized access to databases. Mastery of SQL allows hackers to craft precise injection attacks, bypass authentication mechanisms, and even alter or delete data within a database.

**See Also:**[**Write up: Maximizing IDOR Detection with Burp Suite’s Autorize**](https://www.blackhatethicalhacking.com/articles/maximizing-idor-detection-with-burp-suites-autorize/)

**Networking**

**Understanding of Networking Protocols and Concepts**

A deep understanding of networking protocols and concepts is essential for any hacker. This includes a comprehensive grasp of TCP/IP, DNS, subnetting, packet analysis, and configuring firewalls and VPNs.

**TCP/IP (Transmission Control Protocol/Internet Protocol):**

* **Overview:** TCP/IP is the foundational suite of communication protocols used for the internet and other networks. Understanding how data is transmitted across networks, how connections are established and terminated, and the nuances of data encapsulation and packet structure is crucial.
* **Practical Use:** Knowledge of TCP/IP helps in analyzing and manipulating network traffic, identifying vulnerabilities in network protocols, and crafting custom packets for attacks such as TCP SYN flood and IP spoofing.

**UDP (User Datagram Protocol):**

* **Overview:** UDP is a simpler, connectionless protocol compared to TCP, used for applications where speed is critical and error correction is less important.
* **Practical Use:** Understanding UDP is important for analyzing network traffic in real-time applications like video streaming, gaming, and VoIP, and for exploiting vulnerabilities in protocols that use UDP.

**Identifying Internal and External IP Addresses:**

* **Overview:** IP addresses are critical identifiers used to locate devices on a network. Internal IP addresses (private) are used within a local network, while external IP addresses (public) are used on the broader internet. Understanding how to identify and differentiate between these IP addresses is fundamental for network configuration, reconnaissance, and planning attacks or defenses.

**Internal IP Addresses:**

* **Definition:** IP addresses are critical identifiers used to locate devices on a network. Internal IP addresses (private) are used within a local network, while external IP addresses (public) are used on the broader internet. Understanding how to identify and differentiate between these IP addresses is fundamental for network configuration, reconnaissance, and planning attacks or defenses.
* **Identification**: Internal IP addresses can be identified using tools like ipconfig on Windows, ifconfig or ip addr on Linux, or through router configurations. These IPs are assigned by DHCP servers within the local network.
* **Practical Use**: Knowing internal IPs helps hackers map out the network topology, identify potential targets within the network, and conduct lateral movement during an attack.

**External IP Addresses:**

* **Definition**: External IP addresses are routable on the internet and are assigned by ISPs. They are used to identify devices on a global scale.
* **Identification**: External IP addresses can be identified by querying online services like whatismyip.com, using the curl ifconfig.me command in a terminal, or checking the WAN status on a router’s web interface.
* **Practical Use**: Knowing external IPs helps hackers determine the entry points into a network from the internet, conduct reconnaissance, and plan attacks like DDoS or port scanning.

**DNS (Domain Name System)**

* **Overview:** DNS translates domain names to IP addresses, enabling users to access websites using human-readable names. Understanding DNS is critical for recognizing and exploiting vulnerabilities like DNS spoofing and DNS cache poisoning.
* **Practical Use:** Hackers use DNS knowledge to redirect traffic, intercept communications, and perform reconnaissance on targets.

**Subnetting**

* **Overview:** Subnetting involves dividing a network into smaller, manageable sub-networks. It is important for efficient IP address allocation and network management.
* **Practical Use:** Proficiency in subnetting allows hackers to understand network topologies, identify potential targets within a network, and avoid detection by staying within certain IP ranges.

**Packet Analysis**

* **Overview:** Packet analysis involves examining data packets transmitted over a network to diagnose network issues or detect malicious activity.
* **Practical Use:** Tools like Wireshark enable hackers to capture and analyze network traffic, identify suspicious packets, and uncover vulnerabilities in network protocols.

**Configuring Firewalls and VPNs**

* **Overview:** Firewalls control incoming and outgoing network traffic based on predetermined security rules, while VPNs (Virtual Private Networks) provide secure communication channels over the internet.
* **Practical Use:** Understanding how to configure and bypass firewalls and VPNs is essential for network security testing. Hackers often need to test firewall rules and VPN configurations to identify weaknesses and potential entry points.

**Web Protocols (HTTP/HTTPS):**

**HTTP Methods:**

* **Overview**: HTTP methods such as GET, POST, PUT, and DELETE are used to perform various actions on web servers. Each method serves a specific purpose in web communication.

**GET**: Used to retrieve data from a server.  
**POST**: Used to send data to a server to create or update resources.  
**PUT**: Used to update or create a resource on a server.  
**DELETE**: Used to delete a resource on a server.

* **Practical Use**: Understanding these methods is crucial for web application testing, including finding vulnerabilities such as insecure direct object references, parameter tampering, and cross-site scripting (XSS).

**Linux Proficiency**

**Operating Systems**

Mastery of Linux, particularly distributions tailored for security testing like Kali Linux and Parrot OS, is a fundamental skill for any hacker. These distributions are designed to provide a comprehensive suite of tools for penetration testing, digital forensics, and security research.

**Kali Linux:**



***Kali Linux OS Interface 2024***

* **Overview:** [Kali Linux](https://www.kali.org/) is a Debian-based distribution that comes pre-installed with hundreds of tools used for penetration testing and security research.
* **Key Features:** It includes tools for network analysis, web application testing, database assessment, password attacks, and more. Kali supports live booting from USB, which is useful for testing on different hardware without installation.

**Parrot OS:**

* **Overview:** [Parrot OS](https://parrotsec.org/) is another Debian-based distribution focused on security, privacy, and development.
* **Key Features:** It includes tools for penetration testing, digital forensics, reverse engineering, and anonymous web browsing. Parrot OS is known for its lightweight nature and ease of use.

**Command-Line Interfaces**

* **Overview:** The command line is the primary interface for interacting with Linux. Proficiency in using command-line interfaces (CLI) is crucial for efficiently managing and operating Linux systems.
* **Key Commands:** Important commands include ls, cd, cp, mv, rm, chmod, chown, ps, kill, grep, find, and tar. Mastery of these commands enables effective file management, process control, and system navigation.

**File Systems and Permissions**

* **Overview:** Understanding the Linux file system hierarchy, file types, and permissions is essential for system security and management.
* **Key Concepts:** This includes knowledge of directories like /etc, /usr, /var, /home, and /tmp, and file permission management using chmod, chown, and chgrp.

**Shell Scripting**

* **Overview:** Writing shell scripts in Linux automates tasks, manages system operations, and creates custom hacking tools.
* **Key Skills:** Knowledge of scripting languages like Bash and Python is crucial. Understanding how to write scripts that interact with system commands, handle user input, and perform automated tasks can significantly enhance productivity.

**See Also:**[**Offensive Security Tool: Upload\_Bypass**](https://www.blackhatethicalhacking.com/tools/upload_bypass/)

**Ethical Hacking Tools Proficiency**

Proficiency with a range of ethical hacking tools is essential for performing effective penetration testing and vulnerability assessments. These tools are designed to identify, exploit, and document security weaknesses in systems and applications.

Here’s an expanded look at some of the most critical tools and their applications:

**Metasploit**

Metasploit is one of the most widely used penetration testing frameworks. It provides a comprehensive suite of tools for discovering, exploiting, and validating vulnerabilities.

**Key Features:**

* **Exploitation Modules:** [Metasploit](https://www.metasploit.com/) includes hundreds of pre-built exploit modules for various vulnerabilities, making it easier to test and demonstrate security flaws.
* **Payloads:** It offers customizable payloads for delivering exploits and establishing control over compromised systems.
* **Auxiliary Modules:** These modules perform functions such as scanning, sniffing, and brute-force attacks.
* **Meterpreter:** A powerful payload that provides an interactive shell and numerous post-exploitation features.