Linux Basics and Operating System Report

Install a Virtual Machine on a Personal Computer and Install Kali Linux

Steps to Install Kali Linux on a Virtual Machine:

1. Download VirtualBox or VMware Player and install it.
2. Download Kali Linux ISO image from the official site.
3. Open VirtualBox/VMware and create a new virtual machine.
4. Allocate memory (RAM) and disk space as recommended.
5. Attach the Kali Linux ISO image to the VM's virtual CD/DVD drive.
6. Start the VM and follow the on-screen Kali Linux installation steps.
7. Complete the installation and reboot the VM.

Fig: Linux Desktop

What is Linux?

Linux is an open-source operating system created in 1991. It is fast, reliable, small, and highly customizable, requiring minimal hardware resources. Linux is maintained by a global community of programmers and runs on a wide range of devices from wristwatches to supercomputers. Unlike proprietary OSs like Windows or macOS, Linux source code is freely available for anyone to inspect, modify, and redistribute.

A **Linux distribution** (distro) bundles the Linux kernel with tools and software. Popular distros include Debian, Ubuntu, Red Hat, CentOS, and SUSE.

The Value of Linux

- **Open Source:** Anyone can use and customize Linux for free.
- **Powerful Command Line Interface (CLI):** Allows direct and remote system control.
- **Greater Control:** Root (superuser) access lets administrators modify everything.
- **Superior Network Control:** Linux is designed for robust networking and supports many network applications.

Linux Tools

Linux systems in Security Operations Centers (SOC) often include penetration testing tools like packet generators, port scanners, and exploits. Kali Linux is a distribution dedicated to pen-testing, bundling numerous security tools categorized by their functions.

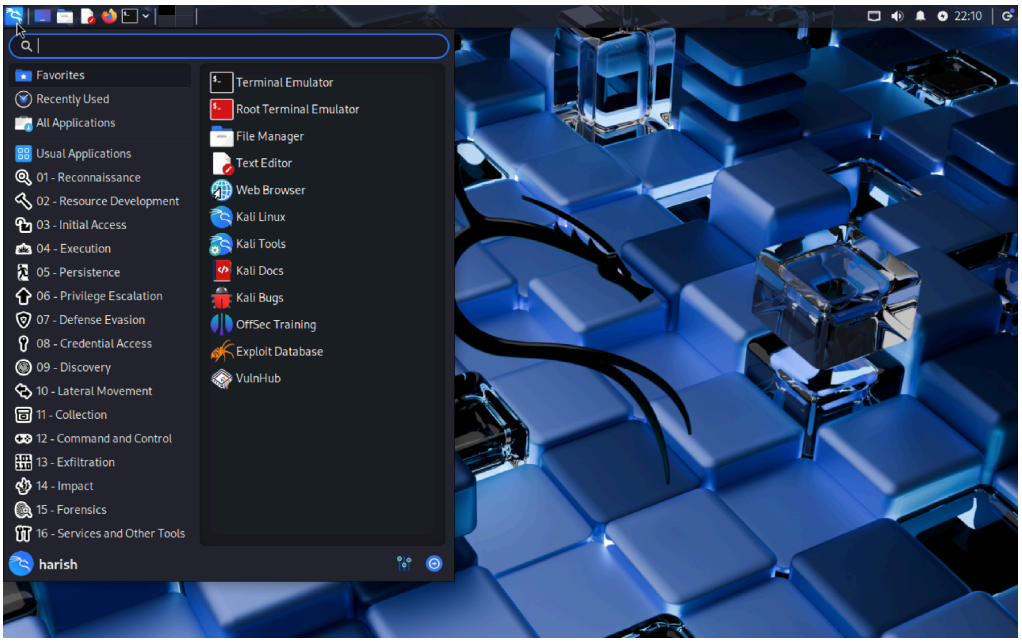

Fig: Pentesting Tools

Working in the Linux Shell

- Linux users interact via the CLI or GUI.
- The CLI is accessed through terminal emulators (e.g., `gnome-terminal`, `xterm`, `konsole`).
- The terms shell, console, CLI terminal, and terminal window often mean the same.

Basic Linux Commands

Command	Description
`ls`	Lists files and directories
`pwd`	Prints the current directory path
`cd`	Changes directory
`mkdir`	Creates a new directory
`rm`	Removes files or directories
`cp`	Copies files or directories
`mv`	Moves or renames files or directories

Note: Commands require proper permissions.

File and Directory Commands

Commands to navigate and manage files:

- `ls -l` : List with detailed info
- `stat filename` : Show file status and attributes
- `file filename` : Identify file type
- `find /path -name filename` : Search for files by name

Working with Text Files

Linux has many text editors:

- **Graphical editors:** Easy to use but require GUI.
- **Command-line editors:** Essential for remote management.

Common CLI text editors:

- **nano:** Easy to use; commands at bottom, e.g., `CTRL+O` to save, `CTRL+W` to search.
- **vim:** Powerful editor, steeper learning curve.

Example to open a file with nano:

nano /etc/hosts

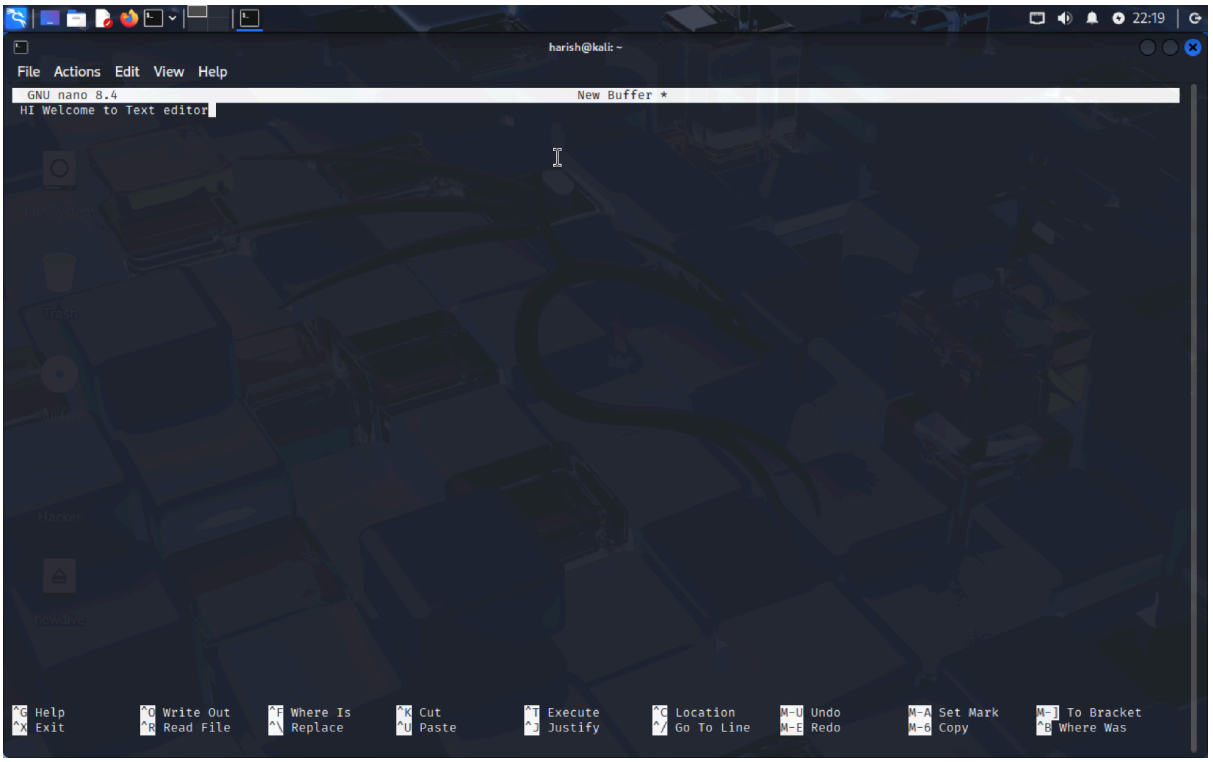

Fig: Text Editor (nano)

Linux Servers and Clients

- **Server:** A computer providing services like file sharing, email, or web hosting.
- **Client:** A computer or software that accesses server resources.

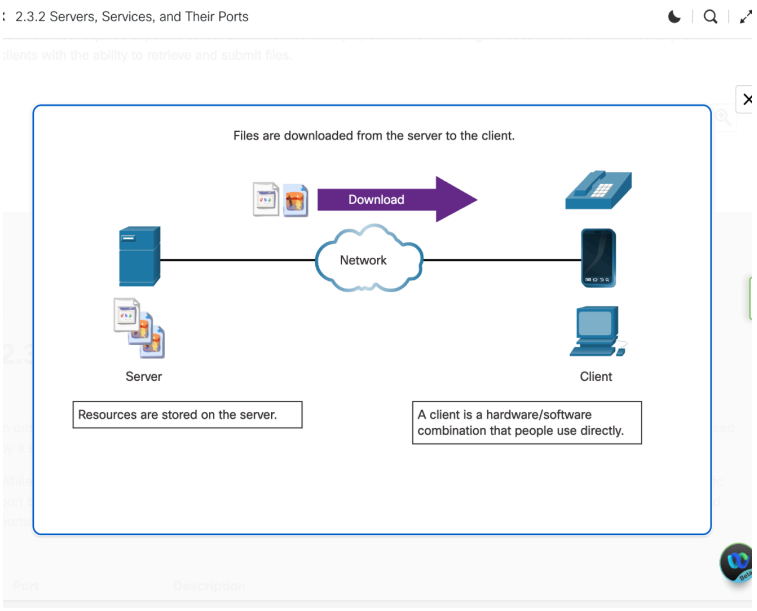

Fig: server to client

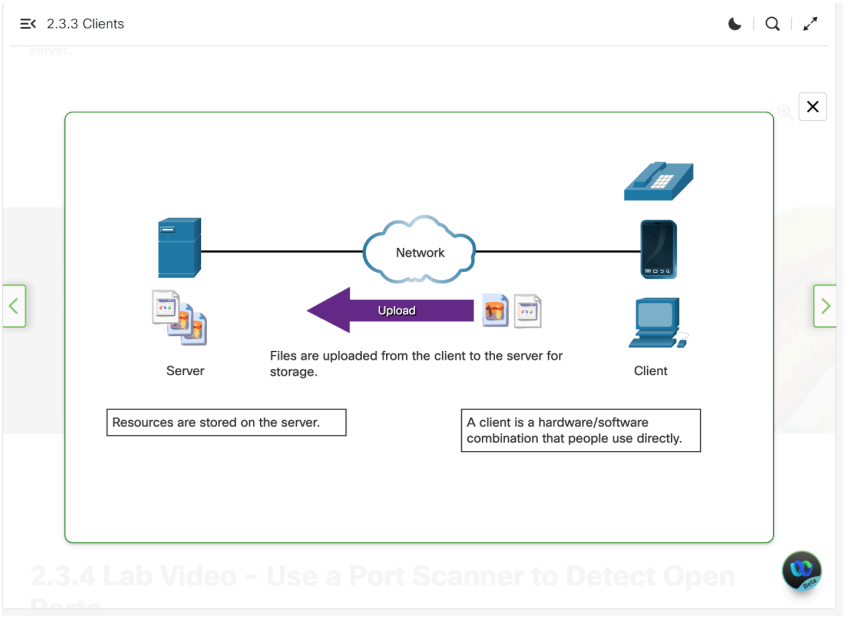

Fig: Client to Server

File System Types in Linux

Linux supports various file systems differing in speed, flexibility, and security.

---

ext2 (Second Extended File System)

- Default in many older Linux distros.
- No journaling (which increases speed but risks corruption).
- Preferred for flash storage to minimize writes.

---

ext3 (Third Extended File System)

- Adds journaling to ext2 for safer recovery.
- Maximum file size up to 32 TB.

---

ext4 (Fourth Extended File System)

- Successor to ext3 with better performance.
- Supports larger file sizes and volumes.
- Can run with or without journaling.

Installing and Running Applications on a Linux Host

Linux uses **package managers** to install and manage software.

- Debian/Ubuntu: `apt` and `dpkg`
- Arch Linux: `pacman`

Example commands for Debian-based systems:

```
sudo apt-get update    # Update package list
sudo apt-get upgrade   # Upgrade installed packages
sudo apt-get install package_name  # Install a package
```

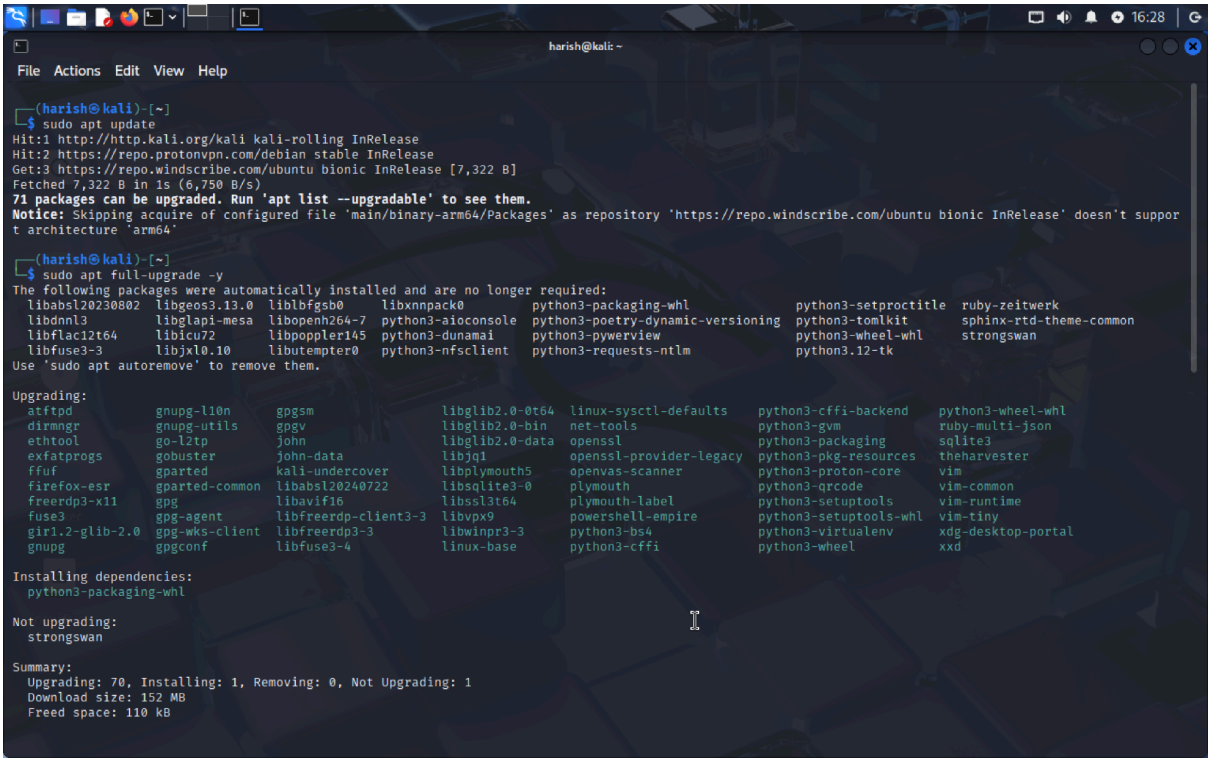

Fig: Update && Upgrade

Processes

- A **process** is an executing program.
- Useful commands:
    - `ps` : List running processes
    - `top` : Interactive process viewer
    - `kill PID` : Terminate a process by ID

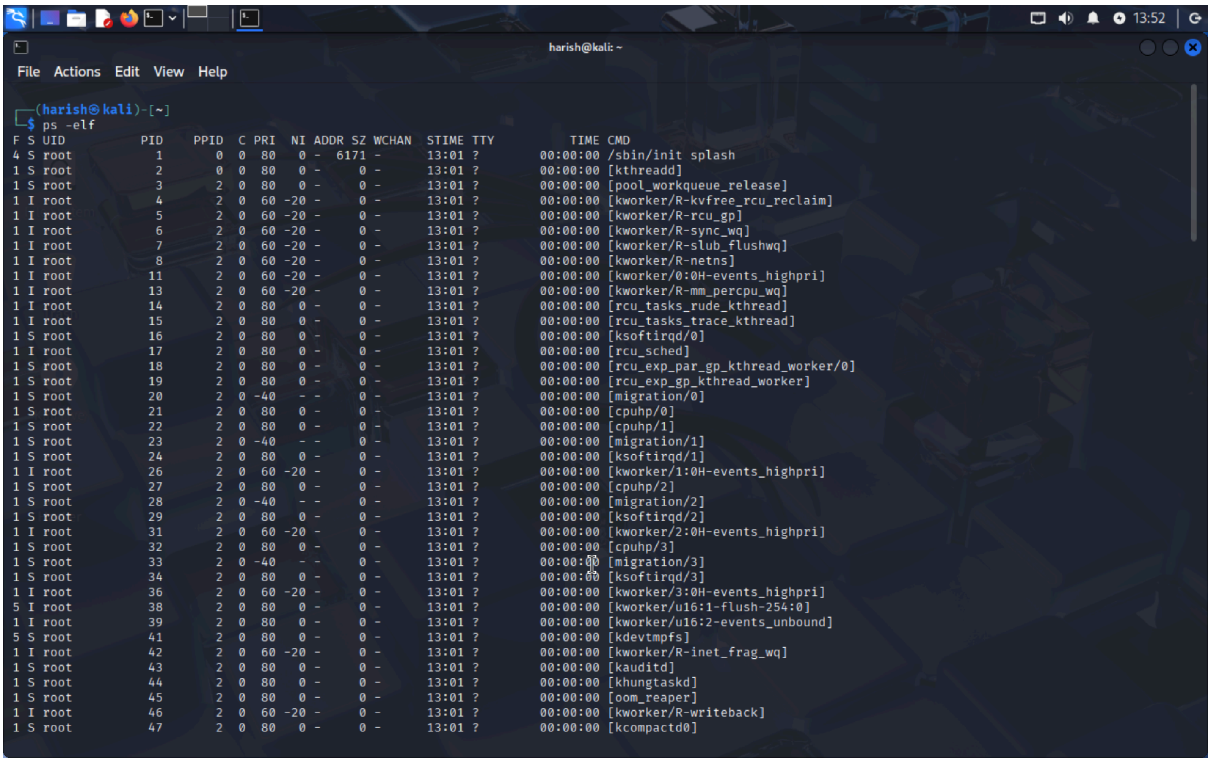

Fig: Processes (ps or ps aux)

Rootkit Check

A **rootkit** is malware that hides unauthorized access by modifying the OS kernel.

- Rootkits are hard to detect and remove.
- Detection often uses trusted media and specialized tools.

chkrootkit is a popular Linux tool to check for rootkits.

How to use chkrootkit:

Install:

sudo apt-get install chkrootkit

1. Run: sudo chkrootkit

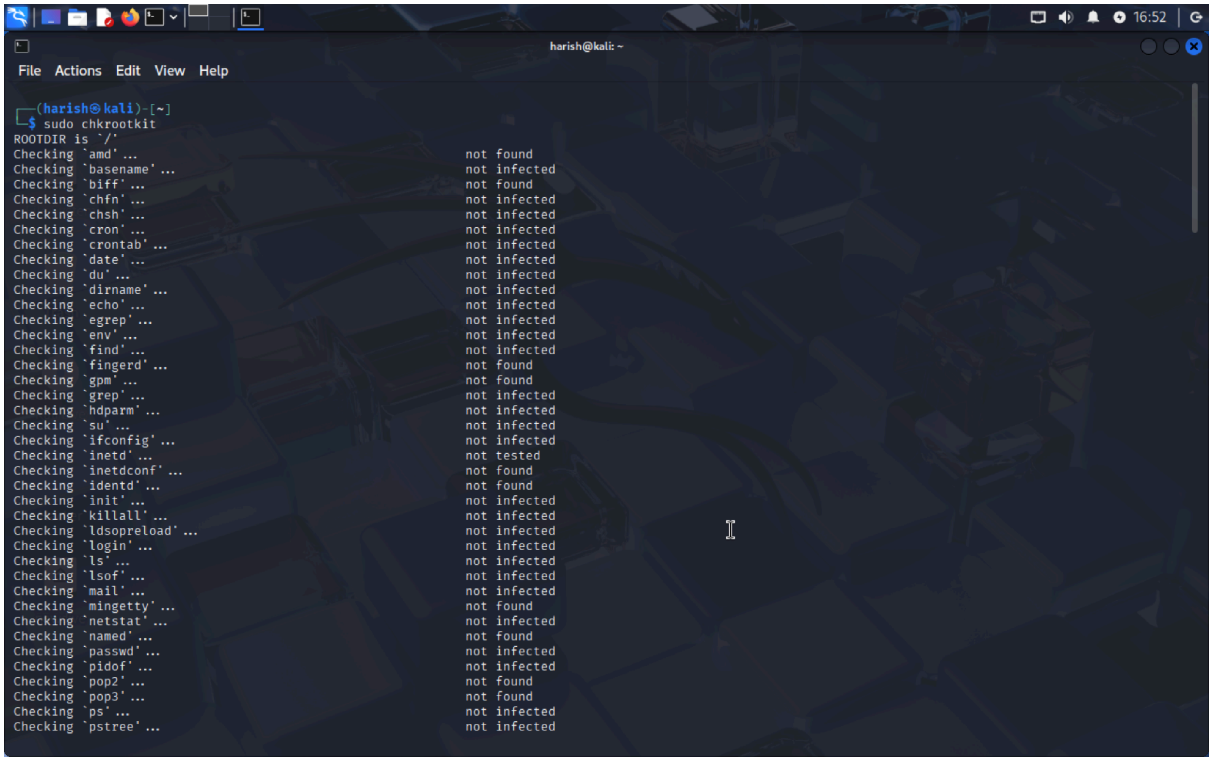

Fig: Checking RootKit

It scans the system for known rootkits but is not 100% reliable.

Conclusion

Linux is a powerful and versatile operating system widely used for security, networking, and server management. Understanding Linux basics, file systems, package management, processes, and security tools like rootkit detection are essential for effective administration and security. Tools such as Kali Linux enhance Linux's capabilities in penetration testing. Mastery of command-line tools and configuration files empowers users with precise control and flexibility.

Note: This report is based on material from Cisco Academy Operating Systems course in Information Technology.

Reference: https://www.netacad.com/courses/operating-systems-basics?courseLang=en-US