TRAINING DAY 6 REPORT

Understand Linux Operating System

Today, I learned some important concepts

➢ Linux Operating System

Basic Overview

- Open-source, Unix-like operating system
- Developed by Linus Torvalds in 1991
- Known for stability, flexibility, and security
- Kernel-based architecture

Key Features

- Multitasking and multiuser capabilities
- Open-source and customizable
- Strong permission and access control system
- Built-in networking tools and protocols
- Shell support (Bash, Zsh, etc.)
- Package management (apt, yum, dnf, etc.)

Common Linux Distributions

- **Ubuntu** – User-friendly, popular for desktops and servers
- **Debian** – Stable, widely used as a base for other distros
- **CentOS / Rocky Linux / AlmaLinux** – Enterprise use (RHEL-based)
- **Kali Linux** – For penetration testing and ethical hacking
- **Arch Linux** – Rolling release, for advanced users
- **Fedora** – Cutting-edge features, upstream of RHEL

Basic Components

- **Kernel** – Core of the OS
- **Shell** – Command-line interpreter
- **File System** – Hierarchical structure starting from /
- **Services/Daemons** – Background processes (e.g., systemd)
- **Package Manager** – Installs, updates, removes software

Basic Linux Commands

- ls, cd, pwd, mkdir, rm – File management
- sudo, chmod, chown – Permissions and access
- ps, top, kill – Process control
- apt, yum, dnf – Package management
- scp, ssh, ping, netstat – Networking tools

➢ Evolution of Linux

UNIX project started at 1969 at Bell Laboratories, in C language

Used in large organizations which later developed their own dialects of UNIX

Wasn't open source and collaborative, so failed to gain popularity

In 1991, Torvalds thought to write his own UNIX and make it freely available

From 1992. Linux is under GNUGPL License and not available for commercial use

Programmers have modified and released many flavors of Linux over the years

➢ Advantages of Linux

- **Open Source** – Free to use, modify, and distribute
- **Secure** – Strong user permissions and low malware risk
- **Stable and Reliable** – Rarely crashes; excellent uptime
- **Lightweight** – Can run on older or low-resource hardware
- **Customizable** – Full control over appearance and functionality
- **Active Community Support** – Large forums, documentation, and updates
- **Multitasking and Multiuser Support** – Efficient handling of tasks and users
- **Regular Updates** – Frequent security patches and enhancements
- **Powerful Command Line Interface (CLI)** – Advanced control for users and admins
- **Wide Range of Distributions** – Tailored for different needs (e.g., Ubuntu, Kali, CentOS)
- **Ideal for Developers** – Great environment for programming and scripting

- **Better Resource Management** – Efficient use of RAM and CPU

➢ Linux for Penetration Testing

Why Linux is Preferred for Penetration Testing

- Open-source and customizable
- Built-in networking and security tools
- Access to powerful command-line utilities
- Lightweight and runs well in VMs
- Large community and support
- Preferred OS by ethical hackers and security pros

Best Linux Distros for Penetration Testing

1. **Kali Linux**

- Most popular pentesting distro
- Comes with 600+ tools (e.g., Nmap, Metasploit, Burp Suite)
- Maintained by Offensive Security

2. **Parrot Security OS**

- Lightweight alternative to Kali
- Includes development and privacy tools
- Suitable for both pentesting and daily use

3. BlackArch

- Arch Linux-based
- Over 2,800 pentesting tools
- Suited for advanced users

4. BackBox

- Ubuntu-based with a focus on security testing
- Simple UI and fast performance

Common Tools in Pentesting Linux Distros

- **Nmap** – Network scanning
- **Metasploit Framework** – Exploitation
- **Wireshark** – Packet analysis
- **Aircrack-ng** – Wi-Fi hacking
- **Hydra** – Brute-force attacks
- **John the Ripper** – Password cracking
- **Burp Suite** – Web app testing
- **Nikto** – Web server scanner