TRAINING DAY 9 REPORT

Understand Kali Linux , Command Line and file system in linux

Today, I learned some important concepts

Kali Linux

Kali Linux is a Debian-based Linux distribution designed for digital forensics, penetration testing, and cyber security research. It's widely used by ethical hackers, security professionals, and researchers due to its powerful collection of pre-installed tools and its support for customization.

Key Features of Kali Linux

- **Hundreds of pre-installed tools** for:
    - Penetration testing (e.g., Metasploit, Burp Suite)
    - Network analysis (e.g., Wireshark, Nmap)
    - Password cracking (e.g., John the Ripper, Hydra)
    - Wireless attacks (e.g., Aircrack-ng, Reaver)
- **Customizable ISO**: Create a tailored version of Kali with only the tools you need.
- **Live bootable environment**: Run Kali without installing it on your system.
- **ARM support**: Runs on devices like Raspberry Pi.
- **Rolling release model**: Regular updates and the latest versions of tools.
- **Rootless mode**: Better security by using a non-root default user.

Install Kali Linux

- On a **Virtual Machine** (recommended for beginners)
- As a **dual boot** with Windows/Linux
- On a **USB drive (Live USB)**
- On a **Raspberry Pi** or ARM device

Blackscreen Error

A **black screen error** when launching Kali Linux (especially in a virtual machine) is a common issue. Let's troubleshoot it step-by-step based on where you're seeing the black screen and what VM software you're using.

NAT (Network Address Translation)

- **Internet Access**: Yes
- **VM reachable from other devices on the network**: No
- **VM can reach the host**: Yes
- **Most secure for beginners**

Bridged Adapter

- **Internet Access**: Yes
- **VM reachable from other devices**: Yes
- **Can simulate real-world attacks on local devices**

Host-Only Adapter

- **Internet Access**: No (unless combined with NAT)
- **VM can communicate with host**
- **Other devices can’t see the VM**

DVWA (Damn Vulnerable Web Application)

DVWA is a PHP/MySQL web application intentionally full of security vulnerabilities, designed for **learning and testing web vulnerabilities** like:

- SQL Injection
- XSS (Cross-Site Scripting)
- CSRF (Cross-Site Request Forgery)

- Command Injection
- File Inclusion
- Brute Force attacks

Command Line

The **command line** (also called the **terminal**, **shell**, or **console**) is a text-based interface used to interact with your computer. Instead of clicking buttons, you type commands.On Kali Linux, you're usually using the **Bash shell** (`bash` stands for Bourne Again SHell*).*

Command shell basics

What Is a Shell?

A **shell** is a program that takes your commands and tells the operating system what to do.

- **Command Shell** = CLI interface (like bash, zsh, or `sh`)
- In Linux, most people use **Bash** (`/bin/bash`)

What Is a Kernel?

The **kernel** is the **core part of an operating system**. It's a bridge between your computer's hardware and the software (apps, commands, services) that you run. **The kernel controls everything** that happens on your computer — memory, CPU, devices, file access, etc.

Windows Command Line

The **Command Line (CMD)** is a text-based interface that lets you **control your computer by typing commands** instead of clicking. It's useful for:

- Navigating files and folders
- Running programs
- Automating tasks
- Troubleshooting

In Windows, you can open it by:

- Pressing `Win + R`, typing `cmd`, and hitting Enter
- Or searching for **"Command Prompt"** in the Start Menu

Linux Command Line

The **Linux command line** (a.k.a. **shell** or **terminal**) is a **text-based interface** where you can run commands to control your computer — create files, install software, manage systems, and more. Most Linux distributions use **Bash** as the default shell.

Linux File System

- A file system is basically a set of rules used to decide how data is stored and fetched in a storage device, be it a hard drive, flash drive, or something else.
- The entire Linux directory structure starting at the top (/) root directory.
- A specific type of data storage format, such as EXT3, EXT4, BTRFS, XFS, and so on
- Mounting: A mount point is simply a directory, like any other, that is created as part of the root file system.
- The Linux root file system is mounted on the root directory

NTFS vs FAT vs EXT

Feature	NTFS	FAT32 / exFAT	ext3 / ext4
Stands For	New Technology File System	File Allocation Table	Extended File System
Best For	Windows	USB drives / cross-platform	Linux (Kali, Ubuntu, etc.)
Max File Size	16 TB (theoretically)	FAT32: 4 GB / exFAT: 16 EB	ext4: 16 TB
Max Volume Size	256 TB	FAT32: 32 GB / exFAT: 128 PB	ext4: 1 EB
Permissions	Yes	No	Yes
Journaling	Yes	No	Yes (ext3, ext4)
OS Compatibility	Windows & Linux (read/write)	Windows, macOS, Linux	Linux only (Windows = read-only with tools)
Performance	Good on Windows	Fast but basic	Fast & optimized for Linux

Feature	NTFS	FAT32 / exFAT	ext3 / ext4
Drawbacks	Complex structure	No permissions, 4GB file limit (FAT32)	Not natively supported by Windows