ELEVATE LABS
TASK 2
Operating System Security Fundamentals (Linux & Windows)

1. What is operating System:-

An Operating System (OS) is system software that controls hardware resources and provides an interface between the user and the computer.
It manages processes, memory, files, and devices, enabling applications to run efficiently and securely.

2. What is virtual machine:-

A Virtual Machine (VM) is a software-based emulation of a physical computer that runs an entire operating system along with its applications on top of a host machine.
It uses a hypervisor (such as VMware, VirtualBox, or Hyper-V) to divide and manage physical resources like CPU, RAM, storage, and network, allowing multiple isolated operating systems to run simultaneously on the same hardware.
Virtual machines provide isolation, security, flexibility, and efficient resource utilization, and are widely used for testing, server virtualization, cloud computing, malware analysis, and cybersecurity labs.

3. What is Virtual Box:-

VirtualBox is an open-source virtualization software developed by Oracle that allows you to run multiple operating systems on a single physical computer,
It acts as a Type-2 hypervisor, enabling you to create and manage virtual machines where operating systems like Windows, Linux, or macOS run in isolation on a host system. VirtualBox is widely used for learning, testing, cybersecurity labs, and malware analysis because it is free, flexible, and easy to use.

Shaik Abdul Muneer

4. What is KALI LINUX :-

Kali Linux is a Debian-based, open-source Linux distribution developed and maintained by Offensive Security, specifically built for cybersecurity, penetration testing, and digital forensics.

It includes 600+ pre-installed security tools covering areas such as network penetration testing, web application testing, wireless attacks, password cracking, malware analysis, reverse engineering, and forensic investigation. Kali Linux supports live booting, virtual machines, cloud platforms, and ARM devices, making it highly flexible for labs and real-world security testing.

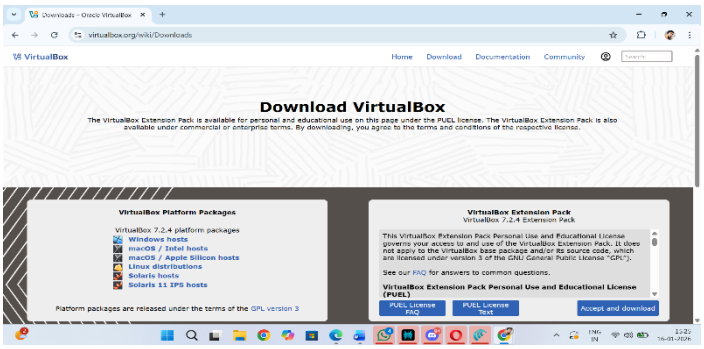
Kali follows a secure-by-default model, uses rolling updates, and is widely used by ethical hackers, red teams, blue teams, students, and researchers to identify, analyze, and help fix security vulnerabilities—always with proper authorization.

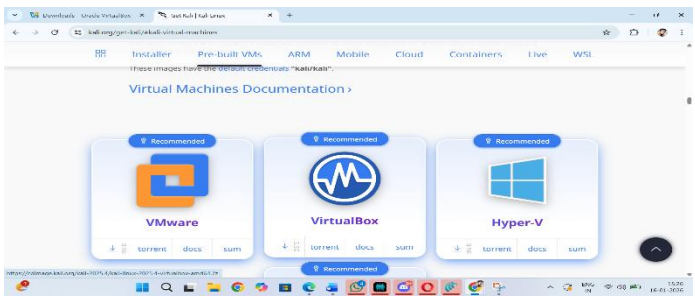
5. Installation of Kali linux:-

Kali Linux installation is the process of setting up the Kali operating system on a system so it can be used for cybersecurity, penetration testing, and digital forensics. Kali can be installed in multiple ways depending on the user's requirement and system capability.

Step1:-

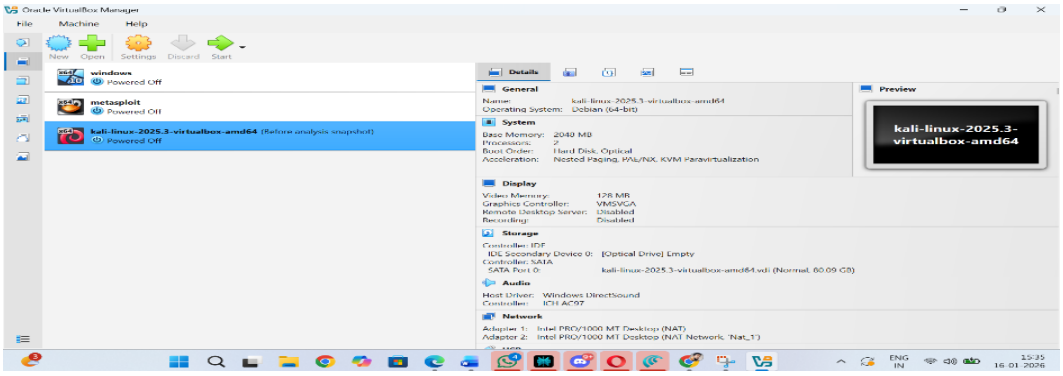
1. Download the Virtual Box
2. And install the kali file for virtual box

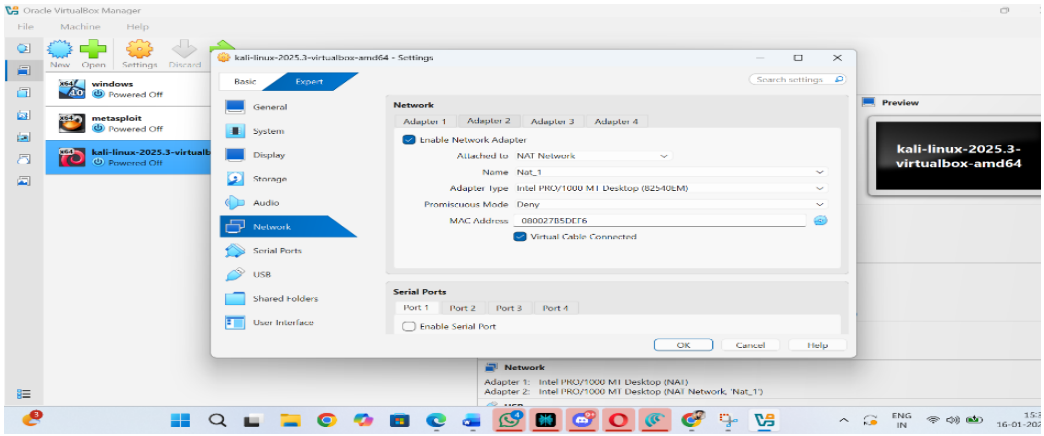


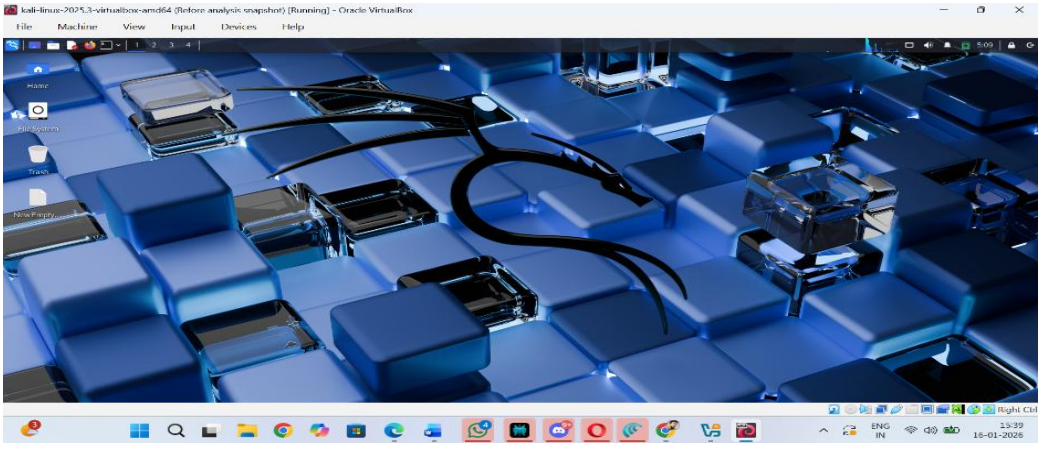


Step 2 :-

1. You can find the file in the file explorer
2. And open the virtual box
3. And select the desired options to install the kali in the virtual box
4. And allocate the necessary resources to the kali linux to run







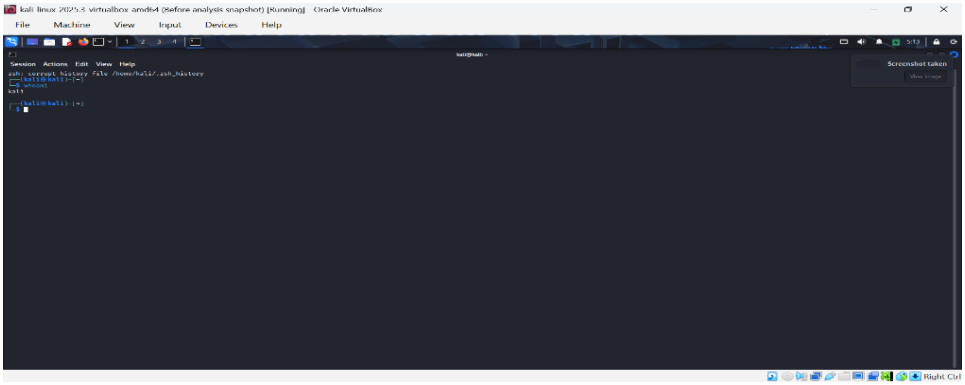
6. Understanding User Accounts, Permissions, and Access Control in Linux

In Linux, each individual who interacts with the system is recognized as a user account. Every user is assigned a unique identity, which helps the system control and track actions performed on files, processes, and system resources. This structured approach ensures that sensitive system components are protected from unauthorized access or unintentional modification.

Linux follows a strong access control mechanism, where permissions determine what actions a user can perform—such as reading, writing, or executing files. By enforcing these permissions, Linux maintains system stability and security while allowing users to work within defined boundaries.

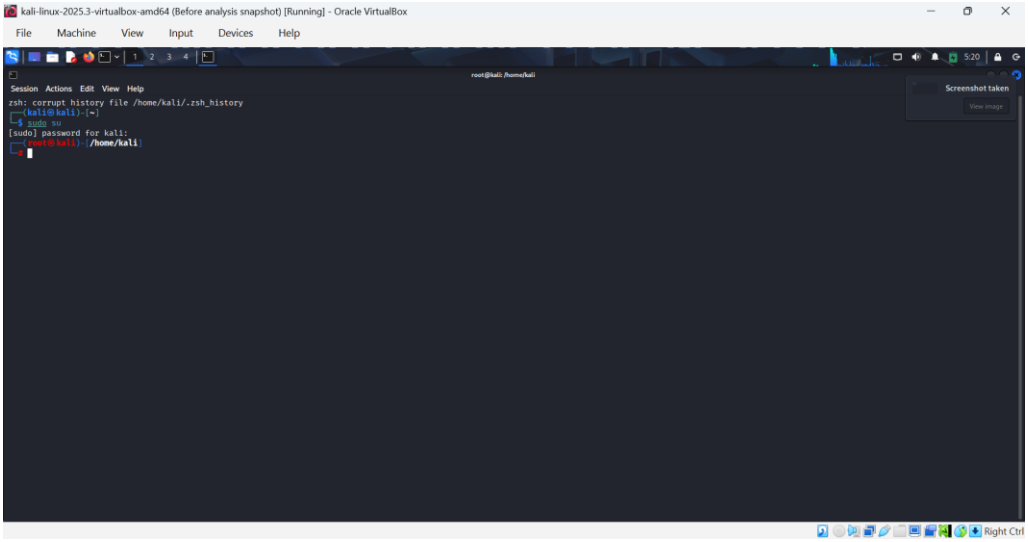
1. **To check the user**

   The command is who am i



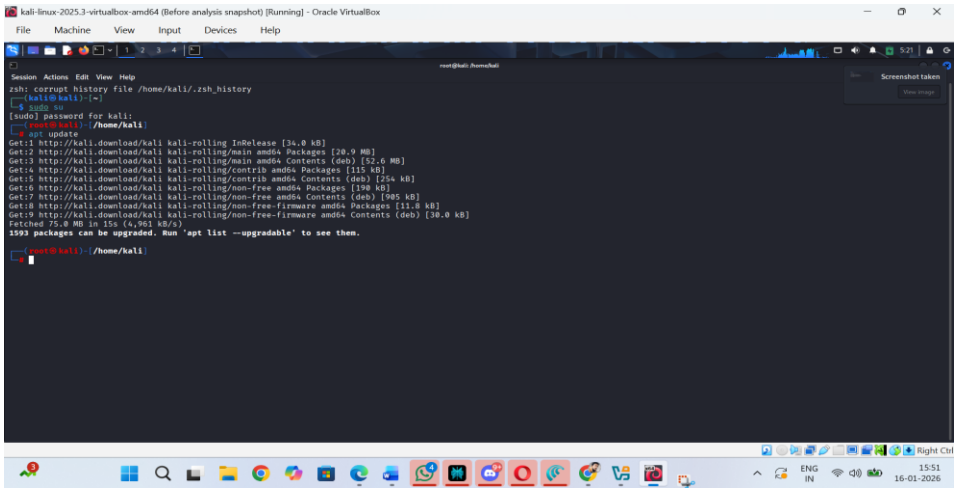
2. **To get root Access**

   The command is sudo su



3. **To try to access admin level**

   The command is apt update



7. File Permission Management and Control in Linux

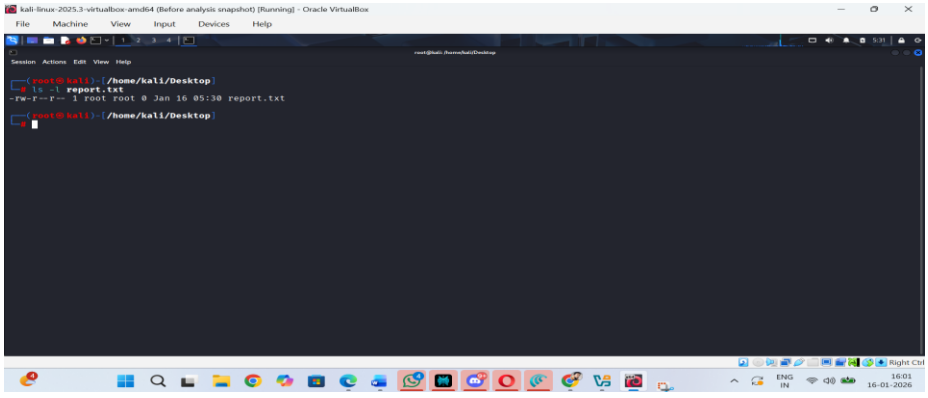
In Linux, every file and directory is protected by a permission system that defines what actions different users can perform. These permissions control who is allowed to view, modify, or execute a file, helping maintain system security and proper access control.

Permissions are assigned to three categories of users:

- The user who owns the file is called the owner
- A set of users who share common access rights is called group
- All remaining users on the system

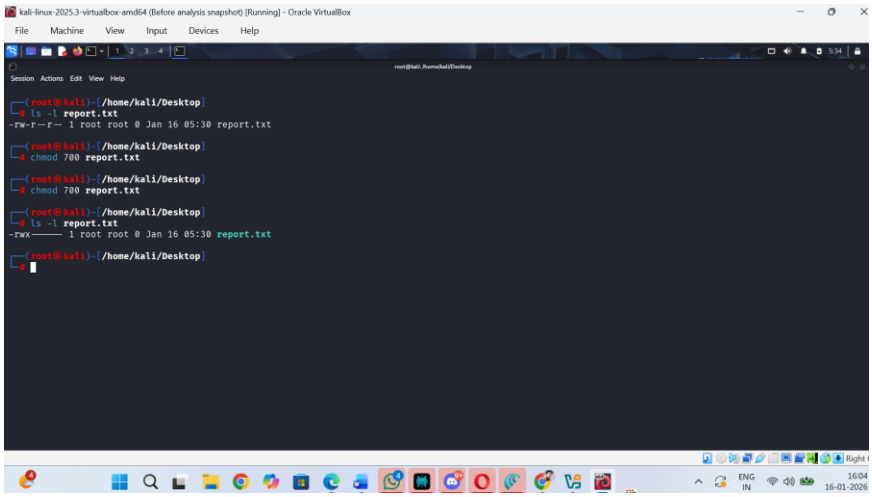
1. **To check the permissions for a text file:**

   The command is Ls -l text file name .txt



2. **Change file permissions using chmod:**

   The command is Chmod 700 text file name.txt



8. Difference Between Root and Standard User Roles in Linux

In Linux, user roles are divided to ensure system security and stability. The root user acts as the system administrator and has unrestricted access to all system resources. This includes installing or removing software, changing system configurations, accessing all files, and managing user accounts.

On the other hand, standard users operate with limited privileges. They are allowed to perform regular tasks such as creating files, running applications, and accessing permitted directories, but they cannot make critical system-level changes. This restriction is intentional and helps protect the system from accidental damage or malicious activity.

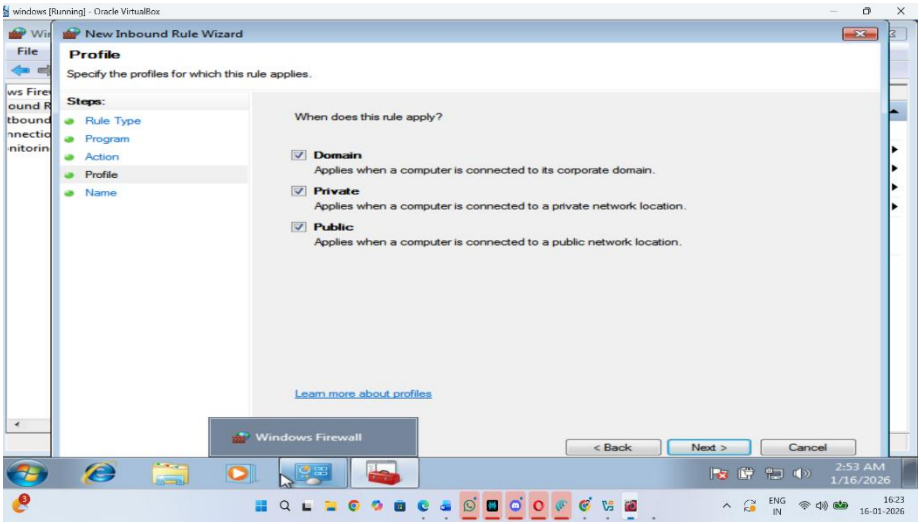
By separating administrative and standard user privileges, Linux reduces security risks. Even if a standard user account is compromised, the attacker's ability to control the entire system remains limited. Therefore, it is considered best practice to carry out everyday tasks using a standard user account and only use root privileges when absolutely necessary.

9. Configuring Network Protection Using Firewalls

A firewall is a critical security mechanism that controls how a system communicates with external networks. It works by filtering incoming and outgoing network traffic based on defined security rules, ensuring that only trusted connections are allowed.

In Linux systems, tools like UFW (Uncomplicated Firewall) provide a simple way to manage firewall rules, while Windows Firewall serves the same purpose on Windows systems. When enabled and properly configured, firewalls help block unauthorized access, detect suspicious activity, and protect against network-based threats.

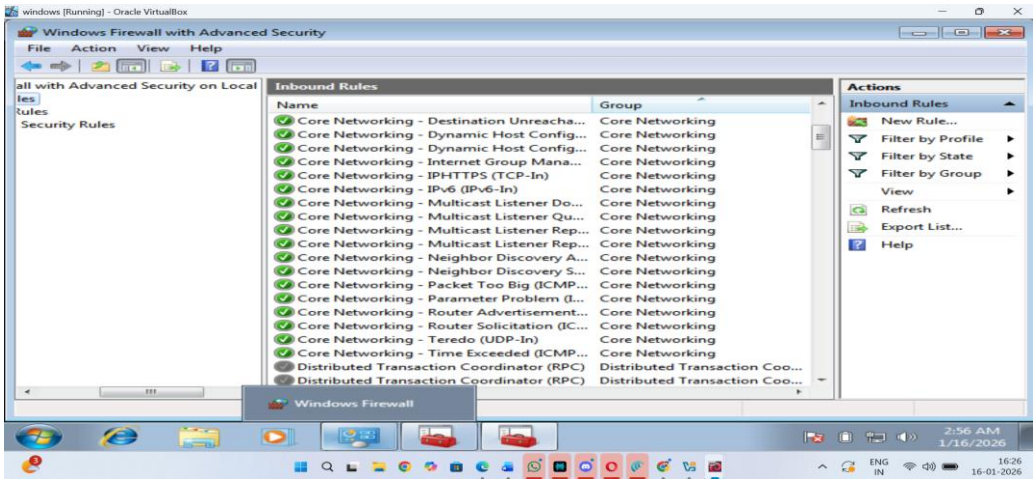
Using a firewall reduces the system's exposure to attacks without interrupting essential services. It plays a vital role in maintaining a secure environment by balancing protection and functionality.



10. Identify running processes and services:

Active processes and services are the programs and background operations currently executing on a system. Monitoring these running components allows users and administrators to understand how system resources are being used at any given time. Tools such as ps, top, and other system monitoring utilities provide real-time information about CPU usage, memory consumption, and active tasks.

Regularly reviewing running processes helps in identifying abnormal behavior, such as unfamiliar services or programs consuming excessive resources, which may indicate misconfiguration or potential security threats. A clear understanding of system processes also supports performance optimization and ensures that only legitimate and trusted applications are running, contributing to overall system stability and security.



11. **Establishing and Maintaining Operating System Security Standards**

Creating clear documentation for operating system security practices is essential for maintaining a secure and stable environment over time. Such documentation serves as a reference guide and security baseline, detailing standard procedures that help protect systems from threats. It ensures uniform implementation of security measures, supports audits, assists new administrators, and demonstrates compliance with security requirements.

Below are key areas that should be covered in a well-structured OS security standards document:

1. System Updates and Vulnerability Patching

Keeping the operating system up to date is a fundamental security requirement. Regular updates and patches address known vulnerabilities that could otherwise be exploited. Documenting update schedules and responsibilities ensures that systems are consistently protected against emerging threats.

2. User Account Lifecycle Management

Security documentation should define how user accounts are created, maintained, and removed. This includes enforcing strong authentication practices, removing inactive or unused accounts, and avoiding duplicate accounts. Proper account management minimizes unauthorized access and reduces insider risk.

3. Controlled Privilege Assignment

The documentation must emphasize restricting user privileges to only what is necessary for their role. Limiting access rights helps contain potential damage if an account is compromised and prevents misuse of system-level permissions.

4. Protection of Files and Directories

Clear guidelines should be provided for assigning permissions to files and directories, especially those containing sensitive or critical data. Well-defined access controls help prevent data leakage, unauthorized modifications, and accidental deletions.

5. Reducing the System Attack Surface

The hardening guide should identify unnecessary services, applications, and features that must be disabled or removed. Eliminating unused components reduces exposure to vulnerabilities and lowers the risk of exploitation.

6. Malware Defense and Endpoint Security

The use of antivirus or endpoint protection solutions should be formally documented, including update policies and scanning routines. This ensures consistent protection against malware, ransomware, and other malicious software.

7. Data Backup and System Recovery Measures

A secure system must also be recoverable. Documentation should include backup frequency, storage methods, and step-by-step recovery procedures. Regular backups ensure business continuity in the event of system failure, cyberattacks, or data loss.

12. SUMMARY:-

Linux security relies on user accounts, permissions, and access control. The root user has full system control, while standard users have limited privileges. File and directory permissions (read, write, execute) are managed with chmod, chown, and ls -l.

Monitoring processes and services helps detect unusual activity, and firewalls like UFW protect against unauthorized network access.

OS hardening includes regular updates, least privilege access, secure file permissions, disabling unnecessary services, antivirus use, and backup planning.

These practices ensure system security, stability, and protection from attacks.