# Task 2: Operating System Security Fundamentals (Kali Linux)

## Objective:

To understand basic operating system security concepts using **Kali Linux**, including user accounts, file permissions, firewall configuration, process monitoring, service management, and OS hardening practices.

## Tools Used:

- **Operating System:** Kali Linux
- **Platform:** Oracle VirtualBox

## Step 1: Installation of Kali Linux Virtual Machine:

Kali Linux was installed as a virtual machine using Oracle VirtualBox.
The virtual machine provides an isolated environment to safely explore security settings without affecting the host system.

## Step 2: User Accounts and Access Control:

User accounts and access control mechanisms in Kali Linux were explored.
Linux uses users and groups to control access to files and system resources, ensuring only authorized users can perform sensitive operations.

## Step 3: File Permissions in Kali Linux:

File permissions were studied using Linux commands:

- ls -l to view file permissions
- chmod to change file permissions
- chown to change file ownership

These permissions define read, write, and execute access for users, groups, and others.

## Step 4: Administrator vs Standard User Privileges:

Kali Linux distinguishes between **root (administrator)** and **normal users**.
The root user has full control over the system, while standard users have limited permissions, improving system security.

## Step 5: Firewall Configuration:

The **UFW (Uncomplicated Firewall)** was enabled and configured in Kali Linux. The firewall helps control incoming and outgoing network traffic and protects the system from unauthorized access.

## Step 6: Identifying Running Processes and Services:

Running processes and services were identified to understand system activity. Monitoring processes helps detect unnecessary or suspicious services running in the background.

## Step 7: Disabling Unnecessary Services:

Unnecessary services were identified and disabled to reduce the system's attack surface. This step helps improve performance and enhances security.

## Step 8: OS Hardening Best Practices:

The following OS hardening practices were documented:

- Regular system updates
- Strong password policies
- Limited use of root privileges
- Enabling firewall protection
- Disabling unused services

## Conclusion:

This task helped in understanding operating system security fundamentals using Kali Linux. By managing users, permissions, firewall settings, and services, the system was hardened against common security threats.