Cyber Security Internship – Task 2
Operating System Security Fundamentals (Linux & Windows)

Name: Charvi
Internship Domain: Cyber Security
Task Number: 2
Date: 16 / 01 / 2026

1. Install a Linux Virtual Machine using VirtualBox (Kali Linux)

Oracle VirtualBox is a virtualization software that allows us to run an additional operating system on the same computer. In this task, Oracle VirtualBox is already installed on the system, and Kali Linux is downloaded and used as the guest operating system. Kali Linux runs as a virtual machine inside VirtualBox, creating a separate and isolated environment from the main operating system.

Using a Linux virtual machine is important for learning operating system security because it provides a safe platform to study and test security concepts. Kali Linux is a security-focused operating system that is widely used in the cybersecurity field. It helps in understanding user account management, file permissions, access control mechanisms, firewall configuration, and system services.

The virtual machine environment ensures that any changes, misconfigurations, or security experiments performed inside Kali Linux do not affect the host system. This makes VirtualBox and Kali Linux a reliable and secure setup for learning operating system security fundamentals during the internship.

2. Explore User Accounts, Permissions, and Access Control Mechanisms

- **Operating System (OS) – Definition & Introduction**

  An **Operating System (OS)** is system software that acts as a bridge between the **user** and the **computer hardware**.
  It controls and manages all hardware resources such as CPU, memory, storage, and input/output devices, and allows users to run applications smoothly.

  Without an operating system, a computer cannot work because the user cannot directly communicate with the hardware.

Example of Operating System

- **Windows** – Used in personal computers and laptops

- **Linux** – Used in servers and cybersecurity environments

Example of Operating System

When a user turns on a computer and opens an application like Google Chrome, the Operating System starts working in the background.
The OS allocates RAM and CPU to the application so it can run smoothly.
It also allows the application to access files and connect to the internet securely.
If multiple applications are running, the OS manages them without conflict.
When the application is closed, the OS frees the memory and resources.
This shows how an operating system manages hardware and software efficiently.

- **User Accounts**

Definition of User Accounts

A **user account** is a unique identity created in an operating system for a person or program.
It allows the operating system to identify who is using the system and control access to resources.
Each user account has a username, password, and assigned permissions.
User accounts help manage different levels of access such as administrator and standard user.
They play an important role in protecting the system from unauthorized access.
User accounts are the foundation of operating system security.

Each user account includes:

- Username
- Password
- User ID (UID)
- Assigned permissions

User accounts are the foundation of operating system security because they control system access and user activities.

Types of User Accounts

Operating systems mainly have **two types of user accounts**:

1. Administrator (Root User)

An administrator has **full control over the system**.

- Can install and remove software
- Can change system settings
- Can create, modify, or delete user accounts

In Linux, this user is called the **root user**, and in Windows, it is called the **Administrator**.

---

2. Standard User

A standard user has **limited permissions**.

- Can use applications
- Can access allowed files and folders
- Cannot change critical system settings

Using standard user accounts for daily work improves system security.

Example of User Accounts

Consider a computer system used in an office environment.
The IT administrator logs in using an **administrator account** to manage system updates and software installations.
Employees are given **standard user accounts** so they can perform daily tasks without modifying system settings.
This separation helps prevent accidental changes and improves system security.

Importance of User Accounts

- ❖ Prevents unauthorized system access
- ❖ Controls user privileges
- ❖ Protects system from misuse
- ❖ Maintains accountability of user actions

❖ **Permissions**

Definition

Permissions are security rules defined by the operating system that control how users can access and use files, folders, and system resources.
They specify what actions a user is allowed to perform, such as reading, modifying, or executing a file.
Permissions help prevent unauthorized access, accidental deletion, and misuse of important system data.
They work together with user accounts to maintain system security and stability.

Types of Permissions

There are three main types of permissions used in operating systems, especially in Linux:

1. **Read (r):**
   Allows a user to open and view the contents of a file or list the contents of a folder.
2. **Write (w):**
   Allows a user to modify, edit, or delete a file or make changes inside a folder.
3. **Execute (x):**
   Allows a user to run a file as a program or script.

These permissions are applied to three categories of users: **Owner**, **Group**, and **Others**.

Example

Consider a file named data.txt.
If the owner has read and write permissions, they can open and edit the file.
If group users have only read permission, they can view the file but cannot change it.
If others have no permissions, they cannot access the file at all.
This permission structure ensures that only authorized users can access or modify files, keeping the system secure.

- **Access Control Mechanisms (In English)**

What are Access Control Mechanisms?

Access Control Mechanisms are security methods used by an operating system to decide **who can access system resources and what actions they are allowed to perform**.
They ensure that only **authorized users** can access files, folders, applications, and system settings.

Access control works together with **user accounts and permissions** to protect the operating system from unauthorized access.

Types of Access Control Mechanisms

1. Authentication

Authentication is the process of **verifying the identity of a user** before allowing access to the system.

Common authentication methods:

- Username and password
- PIN
- Biometric authentication (fingerprint, face recognition)

Example:
When a user enters a username and password while logging in, the operating system checks whether the credentials are correct before granting access.

---

2. Authorization

Authorization determines **what actions a user can perform after logging in**.

Example:
An administrator can install software and change system settings, while a standard user can only use applications and access allowed files.

---

3. Discretionary Access Control (DAC)

In DAC, the **owner of a file or resource decides who can access it** and what permissions they have.

Example:
A user can give read-only permission to another user for a file, preventing them from modifying it.

---

4. Mandatory Access Control (MAC)

In MAC, access rules are **strict and defined by the system**, and users cannot change them.

Example:
In government or military systems, classified files can only be accessed by users with proper security clearance.

Example of Access Control Mechanism

In an organization, when an employee logs into the system, the operating system first performs **authentication** by verifying the password.
After successful login, **authorization** checks what files and applications the employee is allowed to access.
Sensitive data is restricted to managers, while normal employees have limited access.
This ensures data security and controlled system usage.

Importance of Access Control Mechanisms

- Prevents unauthorized access
- Protects sensitive data
- Reduces security risks
- Strengthens overall operating system security

3 .Learn file permissions using chmod, chown, and ls -l.

- Introduction

Linux is a multi-user operating system where multiple users can access the system at the same time. To ensure security and controlled access to files and directories, Linux uses a file permission mechanism. File permissions define who can access a file and what type of actions they are allowed to perform. The commands ls -l, chmod, and chown are used to view and manage these permissions.

- Types of Users in Linux

Linux categorizes users into three classes:

- Owner (User)

The owner is the person who creates the file. The owner has the highest level of control over the file.

- Group

A group consists of multiple users who are given common access permissions to files.

- Others

Others refer to all remaining users on the system who are neither the owner nor part of the group.

❖ Types of File Permissions

Each file and directory in Linux has three basic permissions:

- Read (r)

Allows viewing the contents of a file.

- Write (w)

Allows modification or deletion of the file.

- Execute (x)

Allows running the file as a program or script.

Viewing File Permissions using ls -l

The ls -l command is used to display detailed information about files. It shows the file type, permission settings, owner, group, file size, and modification time. This command helps users understand the current access rights associated with a file or directory.

Permissions using chmod

The chmod command is used to modify file permissions. It allows the system administrator or file owner to control access by granting or revoking read, write, and execute permissions for the owner, group, and others. Permission changes can be applied using symbolic representation or numeric values. This command plays a crucial role in securing files and directories.

Permissions using chown

The chown command is used to change the ownership of a file or directory. It can modify the owner, the group, or both. Changing ownership is generally restricted to administrators to maintain system security and prevent unauthorized access.

- ❖ Importance of File Permissions

Ensures data security and privacy

Prevents unauthorized access to files

Supports safe file sharing among users

4. Understand Administrator vs Standard User Privileges

- Introduction

In an operating system, different users are given different levels of access to protect the system from misuse and security threats. These access levels are known as user privileges. The two most common types of user accounts are Administrator and Standard User. Each has specific rights and responsibilities.

- ❖ Administrator Privileges

An Administrator has full control over the operating system. This user can manage system-wide settings, install or remove software, create or delete user accounts, and change security configurations. Administrators can access and modify all system files and have the authority to override restrictions placed on standard users. Because of these powerful permissions, administrator access must be used carefully to avoid accidental damage or security risks.

- ❖ Standard User Privileges

A Standard User has limited access rights. This user can perform regular activities such as using applications, creating personal files, and changing basic personal settings. However, a standard user cannot modify system files, change system-wide settings, or manage other user accounts. These restrictions help protect the system from accidental errors and malicious actions.

- ❖ Key Differences Between Administrator and Standard User

Administrators have full system control, while standard users have limited access.

Administrators can manage system security and user accounts; standard users cannot.

Standard users help maintain system stability by reducing the risk of system damage.

Importance of Using Standard User Accounts

Using a standard user account for daily tasks improves system security. It minimizes the chances of malware gaining full system access and prevents accidental changes to critical system components.

5. Enable Firewall (UFW in Linux or Windows Firewall)

Introduction

A firewall is a security system that monitors and controls incoming and outgoing network traffic. It acts as a protective barrier between a computer and external networks such as the internet. Enabling a firewall helps prevent unauthorized access, hacking attempts, and malware attacks.

- ❖ Firewall in Linux (UFW)

In Linux systems, UFW (Uncomplicated Firewall) is a user-friendly firewall tool. It is designed to simplify the process of managing network security. UFW controls which services and connections are allowed or blocked. By enabling UFW, the system becomes protected from unwanted network access while still allowing trusted connections.

UFW (Linux Firewall) Example

On a Linux server, UFW is enabled to control network access. Only trusted services, such as web server or SSH, are allowed. All other ports are blocked to prevent hackers from exploiting them. This ensures sensitive server data is protected. The firewall acts as a security barrier for the Linux system.

- ❖ Windows Firewall

Windows Firewall is a built-in security feature of the Windows operating system. It filters network traffic based on predefined security rules. When enabled, it blocks suspicious connections and allows safe communication. Windows Firewall helps protect the system from viruses, hackers, and unauthorized data access.

Windows Firewall Example

In an office, Windows Firewall is enabled on all computers. It blocks any unauthorized access from the internet. Employees can still use approved applications like email or company intranet. Suspicious connections or malware attempts are automatically blocked. This helps keep the system and network secure.

Importance of Enabling a Firewall

Enabling a firewall increases system security by controlling network traffic. It helps prevent cyber attacks, protects personal data, and reduces the risk of system compromise. A firewall is an essential security component for both personal and professional systems

6. Identify Running Processes and Services

- Introduction

A computer operating system runs multiple programs simultaneously. These programs are called processes, and background programs that provide specific functionalities for the system are called services. Identifying running processes and services helps users monitor system performance, detect issues, and ensure the system is secure.

Purpose

- Monitoring CPU and memory usage
- Detecting unnecessary or suspicious programs
- Managing system resources efficiently
- Ensuring important services like network, security, or database servers are running

Example (Windows)

In Windows, a user can identify running processes such as chrome.exe or explorer.exe using Task Manager. Services like Windows Update or Print Spooler run in the background. By checking these, the user can detect if any unknown process is consuming excessive resources or if essential services are stopped.

7. Disable Unnecessary Services to Reduce Attack Surface

Introduction

Every operating system runs many services in the background to perform different tasks. For example, some services manage printing, networking, updates, or scheduled tasks. However, not all services are needed all the time. Every service that runs unnecessarily can become a weak point that hackers can exploit. To make the system safer, it is important to disable services that are not required. This reduces the “attack surface” of the system, meaning fewer points where attackers can try to gain access.

Purpose of Disabling Unnecessary Services

Improve Security – Fewer running services mean fewer opportunities for attackers to exploit.

Save System Resources – Stopping unused services reduces CPU and memory usage, making the system faster.

Better System Stability – Fewer running services reduce conflicts and errors.

Easier Monitoring – With only necessary services running, it is easier to detect unusual activity.

Example

Some Windows services like Fax, Remote Registry, or Print Spooler may not be needed on all computers. If these are left running, attackers could target them. By disabling such unnecessary services, only important services like Windows Update and Firewall continue running, keeping the system secure and stable.