# CYBER SECURITY INTERNSHIP
# Task 2: Operating System Security Fundamentals (Linux & Windows)

## 1. Introduction

Operating System (OS) security is a critical aspect of cyber security that focuses on protecting the operating system from threats, unauthorized access, and misuse. Since the OS manages hardware, software resources, and user interactions, compromising it can give attackers complete control over a system.

## 2. User Accounts and Access Control

Operating systems support multiple user accounts with different privilege levels. Access control ensures users can only perform authorized actions.

## 3. Administrator vs Standard User

Administrators (root in Linux, Administrator in Windows) have full system control. Standard users have limited privileges to improve security.

## 4. File Permissions in Linux

Linux uses read, write, and execute permissions for owner, group, and others. Commands such as chmod, chown, and ls -l are used to manage permissions.

## 5. Process and Service Management

Processes and services run in the background to support OS functionality. Monitoring them helps detect suspicious activity.

## 6. Disabling Unnecessary Services

Disabling unused services reduces the attack surface and improves system security.

## 7. Firewall Configuration

Firewalls such as UFW (Linux) and Windows Defender Firewall control network traffic and help block unauthorized access.

## 8. OS Hardening Practices

OS hardening includes updates, strong passwords, firewall usage, disabling services, and applying the least privilege principle.

## 9. Interview Questions – Explained

OS hardening secures systems by minimizing vulnerabilities. File permissions control access. Unnecessary services increase attack surface. Root has full access; normal users do not. Least privilege limits access rights.

## 10. Conclusion

This task strengthened understanding of operating system security and hardening techniques in both Linux and Windows environments.