# Operating System Security Fundamentals (Linux & Windows)

This document provides a detailed explanation of Operating System Security Fundamentals for both Linux and Windows environments. It is intended to be added to a GitHub repository as documentation for learning, reference, and demonstration purposes.

## 1. Virtual Machine & Environment Setup

Install Ubuntu Linux using VirtualBox or VMware. Virtual machines allow safe experimentation with system configurations without affecting the host OS. Windows users should explore Windows Security and Windows Defender settings.

## 2. User Accounts & Access Control

Operating systems use user accounts to control access to resources. Linux separates users using UID/GID, while Windows uses user accounts and groups. Least privilege is a core principle.

## 3. File Permissions (Linux)

Linux file permissions are managed using chmod, chown, and ls -l commands. Permissions define read, write, and execute access for owner, group, and others.

## 4. Administrator vs Standard User

Administrators have full system control, while standard users have limited permissions. Using standard accounts reduces risk from malware and accidental system changes.

## 5. Firewall Configuration

Firewalls control incoming and outgoing traffic. Linux commonly uses UFW, while Windows uses Windows Defender Firewall to enforce network security rules.

## 6. Processes & Services

Running processes and services can be viewed using tools like ps, top, systemctl (Linux), and Task Manager or Services.msc (Windows).

## 7. Disabling Unnecessary Services

Reducing running services minimizes the attack surface. Services not required for system functionality should be disabled or removed.

## 8. OS Hardening Best Practices

OS hardening includes regular updates, strong passwords, firewall usage, minimal services, secure configurations, and continuous monitoring.

## Conclusion

Understanding OS security fundamentals is essential for securing modern systems. This document serves as a foundational guide and can be extended with screenshots, commands, and configuration examples in a GitHub repository.