Operating System Security Fundamentals (Linux & Windows)

Linux Virtual Machine / Windows Security Setup:

Outcome:

Successfully understood the importance of isolating environments using Virtual Machines (VMs).

Learned how Ubuntu Linux can be deployed safely using VM Workstation for experimentation.

Understood that Windows Defender and built-in security settings provide baseline protection in Windows systems.

Key Learning: Virtual machines allow safe testing without affecting the host OS and are essential for cybersecurity practice.

User Accounts, Permissions & Access Control:

Outcome:

Learned how operating systems manage multiple users.

Understood how access control prevents unauthorized actions.

Identified how users are separated to reduce damage from compromised accounts.

Linux Insight:

Users and groups control access to files and services.

Windows Insight:

User Account Control (UAC) restricts unauthorized administrative actions.

Linux File Permissions (chmod, chown, ls -l)

Outcome:

Gained clear understanding of Read (r), Write (w), and Execute (x) permissions.

Learned permission levels for Owner, Group, and Others.

Understood how chmod modifies permissions and chown changes ownership.

Security Impact: Proper permissions prevent unauthorized file access and privilege escalation.

Administrator vs Standard User Privileges:

Outcome:

Understood why administrative access must be restricted.
Learned that admins/root users have full system control.
Standard users reduce risk by limiting actions.
Security Principle: Always operate as a standard user unless administrative access is required.

Firewall Configuration (UFW / Windows Firewall):

Outcome:

Learned the purpose of firewalls in blocking unauthorized network traffic.
Understood how UFW simplifies iptables management in Linux.
Learned Windows Firewall protects inbound and outbound traffic.
Security Benefit: Firewalls significantly reduce exposure to network-based attacks.

Identifying Running Processes & Services:

Outcome:

Learned how to view active processes in Linux and Windows.
Understood the difference between user processes and system services.
Identified potential security risks from unknown or unused services.
Security Insight: Monitoring processes helps detect malware and suspicious activity.

Disabling Unnecessary Services:

Outcome:

Understood how unused services increase the attack surface.
Learned that each running service may introduce vulnerabilities.
Gained awareness of service hardening best practices.

OS Hardening Best Practices:

Learned core OS hardening concepts:

Least privilege
Patch management
Strong authentication
Service minimization
Firewall enforcement

Understood how OS hardening strengthens system defence layers.

Summary:

This report covers the fundamentals of operating system security, including the use of virtual machines for safe testing, user accounts and access control, Linux file permissions, and the difference between administrator and standard users. It explains firewall usage, process and service monitoring, disabling unnecessary services, and core OS hardening practices, highlighting how these measures reduce attack surface and strengthen system security.