Task:-2 Operating system security fundamentals(Linux & Windows)

Project Breakdown :-

1. Environment Setup

Goal: Create a safe practice environment.

Install Linux VM (Ubuntu) using VirtualBox

OR use your existing Windows OS

Purpose: Avoid damaging your main system while learning security.

Outcome:

✔ Secure test environment ready

2. User Accounts & Access Control

Goal: Understand who can access what.

Linux:

View users:

cat /etc/passwd

Groups:

groups username

Create user:

sudo adduser testuser

Windows:

User Accounts → Standard vs Administrator

Local Users & Groups (lusrmgr.msc)

Concepts Learned:

Authentication

Authorization

Principle of Least Privilege

3. File Permissions (Linux Core Security)

Goal: Control access to files.

Commands:

ls -l → view permissions

chmod → change permissions

chown → change owner

Example:

Copy code

Bash

chmod 640 file.txt

chown user:group file.txt

Outcome:

✔ Understand Read (r), Write (w), Execute (x)

4. Admin vs Standard User Privileges

Goal: Prevent misuse & malware damage.

Linux: sudo vs normal user

Windows: Administrator vs Standard user

Security Benefit:

Malware running as standard user causes less damage.

5. Firewall Configuration

Goal: Control network traffic.

Linux (UFW):

Copy code

Bash

sudo ufw enable

sudo ufw status

sudo ufw allow ssh

Windows:

Windows Defender Firewall

Inbound & Outbound Rules

Outcome:

✔ Only trusted traffic allowed

6. Running Processes & Services

Goal: Detect suspicious activity.

Linux:

ps aux

top

systemctl list-units --type=service

Windows:

Task Manager

Services.msc

Security Angle:

Unknown processes = possible malware

7. Disable Unnecessary Services

Goal: Reduce attack surface.

Examples:

Disable unused services (FTP, Telnet, etc.)

Linux:

Copy code

Bash

sudo systemctl disable service_name

Outcome:

✔ **Fewer entry points for attackers**

8. OS Hardening Best Practices (Documentation)

Goal: Secure OS long-term.

Include:

Strong passwords & password policies

Automatic updates

Firewall enabled

Disable unused accounts

Antivirus / Defender enabled

Regular backups

Logging & monitoring

SUMMARY

This focuses on operating system security fundamentals using Linux and Windows. It covers user accounts, file permissions, administrator vs standard privileges, firewall configuration, process and service management, and disabling unnecessary services. The goal is to reduce the attack surface and apply basic OS hardening practices to improve system security.