Task 2: Operating System Security Fundamentals (Linux & Windows)

1. Install Linux or Use Windows Security
We can install Linux using VirtualBox.
Or we can use Windows built-in security settings.
Linux is often used for learning security because it gives more control.

2. User Accounts and Access Control
An operating system can have many users.
Each user has a username and password.
Access control decides who can use files or programs.
Linux:
Normal user → limited access
Root user → full access
Windows:
Standard user → limited access
Administrator → full access

3. File Permissions in Linux
Every file has permissions.
Permissions decide who can read, write, or run a file.
Commands:
ls -l → shows file permissions
chmod → changes file permissions
chown → changes file owner
Permission types:
r → read
w → write
x → execute

4. Administrator vs Standard User
Administrator can:
Install software
Change system settings
Standard user:
Can use the system
Cannot change important settings
Using a standard user is safer.

5. Firewall
Firewall protects the system from unauthorized network access.
Linux:
Uses UFW firewall
It blocks unwanted connections
Windows:
Uses Windows Defender Firewall
It protects the system automatically

6. Running Processes and Services
A process is a program that is running.

A service runs in the background.
Linux:
ps and top commands show running programs
Windows:
Task Manager shows running programs and services

7. Disable Unnecessary Services
Some services are not needed.
Unused services can be security risks.
Disabling them makes the system safer.

8. OS Hardening Best Practices
Use strong passwords
Enable firewall
Update the system regularly
Disable unused services
Use antivirus software
Give users only required permissions