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

Operating System security means protecting your computer from misuse, attacks, and unwanted access. Both Linux and Windows provide tools to do this. Let's understand step by step.

1. Using Linux VM or Windows Security
You can install Linux in VirtualBox to practice safely, or use your own Windows system.
A virtual machine is like a computer inside your computer. If something goes wrong, your main system is safe.

2. User Accounts and Permissions
Every OS has users.
Admin / Root user: Has full control over the system.
Standard user: Has limited access and is safer for daily work.
👉 Security rule:
Use admin only when needed, not all the time.

3. File Permissions in Linux
Linux controls who can:
Read (r) a file
Write (w) a file
Execute (x) a file

This shows file permissions.
Meaning:
Owner: read, write, execute
Group: read only
Others: read only
Commands:
chmod → change permissions
chown → change file owner
This prevents unauthorized access to files.

4. Administrator vs Standard User
Admin can install software, change system settings.
Standard user cannot damage the system easily.
Best practice: Always work as standard user.
Use admin rights only when required.

5. Firewall (System Protector)
A firewall blocks unwanted network traffic.
Linux:

Windows:
Windows Defender Firewall → Turn ON
Firewall helps stop hackers from connecting to your system.

6. Running Processes and Services
Processes are programs running in the background.
Linux:

Windows: Task Manager
Some services are not needed and can be risky.

7. Disable Unnecessary Services
If a service is not used, turn it off. This:
Reduces attack chances
Improves system performance
Less services = Less security risk.

8. OS Hardening Best Practices
OS Hardening means making the system stronger and safer.
Best practices:
-Keep OS updated
-Use strong passwords
-Disable unused services
-Use firewall
-Give minimum permissions
-Install software only from trusted sources

In short:
Your system becomes harder to hack and safer to use.

**Interview Questions**

1*. What is OS hardening*?
✓OS hardening means making the operating system more secure by reducing weak points.
This is done by:
-Turning off unused services
-Using strong passwords
-Applying updates
-Setting proper permissions
👉 Goal: Reduce chances of attack.

*2. What are file permissions in Linux?*
✓File permissions in Linux decide who can read, write, or run a file.
There are three permissions:
-Read (r) – view the file
-Write (w) – modify the file
-Execute (x) – run the file
And three user types:
-Owner
- Group
- Others
👉 This protects files from unauthorized access.

*3. Why should unnecessary services be disabled*?
✓Unnecessary services:
-Increase security risk
-Use system resources
-Can be targeted by attackers
-By disabling them:
-Attack surface is reduced
-System becomes faster and safer
👉 Less running services = better security.

*4. Difference between root and normal user?*
-Root User
-Normal User
-Full system access
-Limited access
-Can change system files
-Cannot change system files
-High risk if misused
-Safer for daily use
👉 Root is powerful but dangerous if used carelessly.

5. *What is the least privilege principle?*
Least privilege principle means giving only the minimum access needed to a user or program.
Example:
A student user should not have admin rights.
A program should access only required files.
👉 This limits damage if an account is compromised.