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

---

1. Install a Linux Virtual Machine or Use Windows Security Settings

A **virtual machine (VM)** allows you to run an operating system inside another operating system safely. Installing Linux in **VirtualBox** is useful because you can practice security concepts without risking your main system.

- VirtualBox lets you install Linux distributions such as **Ubuntu** or **Kali Linux**.
- A VM acts like a real computer but is isolated from your host system.
- If you cannot install Linux, you can still explore security features using **Windows Security Settings**, such as User Accounts, Firewall, and Device Security.

Security Benefit:
VMs allow safe experimentation and reduce the risk of damaging your main operating system.

---

2. Explore User Accounts, Permissions, and Access Control

Operating systems use **user accounts** to control who can access resources.

- Each user has a **username, password, and permissions**.
- Linux separates users clearly and enforces strict access control.
- Windows uses **User Accounts and Groups** (Administrators, Users, Guests).

Access control ensures users can only access files and settings they are authorized to use.

Security Benefit:
Prevents unauthorized users from accessing sensitive files or system settings.

---

3. Learn File Permissions (chmod, chown, ls -l)

Linux uses file permissions to control access.

- `ls -l` shows file permissions, owner, and group.
- Permissions are divided into:
  - **Read (r)** – view file contents
  - **Write (w)** – modify file
  - **Execute (x)** – run file as a program

Example:

```
-rwxr-xr--
```

- `chmod` changes permissions.
- `chown` changes file ownership.

Security Benefit:
Ensures only authorized users can read, modify, or execute files.

---

4. Understand Administrator vs Standard User Privileges

Operating systems separate **normal users** from **administrators**.

- **Administrator / Root**:
  - Full system control
  - Can install software, change system files
- **Standard User**:
  - Limited permissions
  - Cannot modify critical system settings

Linux uses `sudo` to temporarily grant admin rights.

Security Benefit:
Limits damage if a standard user account is compromised.

---

5. Enable Firewall (UFW or Windows Firewall)

A **firewall** controls incoming and outgoing network traffic.

- Linux uses **UFW (Uncomplicated Firewall)**:
  - Easy command-line firewall
  - Blocks unauthorized connections
- Windows has **Windows Defender Firewall**:
  - Protects against unwanted network access

Security Benefit:
Prevents attackers from accessing your system over the network.

---

6. Identify Running Processes and Services

Processes are programs currently running on the system.

- Linux commands:
  - `ps`
  - `top`
  - `htop`
- Windows tools:
  - Task Manager
  - Services Manager

Services often run in the background and may start automatically at boot.

Security Benefit:
Helps detect suspicious or unnecessary processes that could be malicious.

---

7. Disable Unnecessary Services

Some services are enabled by default but are not needed.

- Examples:
  - FTP servers
  - Remote desktop services
  - Print services on unused machines

Disabling unused services reduces system exposure.

Security Benefit:
Reduces the **attack surface**, making it harder for attackers to exploit vulnerabilities.

---

8. Document Best OS Hardening Practices

OS hardening means securing an operating system by reducing weaknesses.

Best practices include:

- Use strong passwords
- Keep the system updated
- Disable unused services
- Enable firewalls

- Use least privilege principle
- Monitor logs and processes

Documenting these practices ensures consistency and helps with audits or troubleshooting.

Security Benefit:
Creates a secure and well-maintained operating system environment.
