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

by: NROUPSINH GOHIL

Operating System Security Checklist (Windows)

Objective

The goal of this task is to understand and implement basic operating system security concepts in Windows, including user access control, file permissions, firewall protection, and OS hardening practices.

---

1. User Account Security

- Windows user accounts were reviewed.
- Difference between **Administrator** and **Standard User** was understood.
- Administrator accounts have full system control and can modify system settings.
- Standard users have limited permissions and are safer for daily usage.
- Using a standard user follows the **Least Privilege Principle**.

---

2. File & Folder Permissions

- Folder permissions were analyzed using **Properties → Security**.
- Permissions include:
    - Read
    - Write
    - Modify
    - Full Control
- Full control should only be given to trusted administrators.
- Limiting permissions helps reduce the impact of unauthorized access.

---

3. Firewall Protection

- Windows Defender Firewall was enabled.
- Firewall status was checked for both **Private** and **Public** networks.
- Inbound and outbound rules control network traffic.
- Firewall protects the system from unauthorized network access.

---

4. Running Processes & Services

- Active processes were reviewed using **Task Manager**.
- Background services were observed.
- Unnecessary services increase the system's attack surface.
- Reducing unused services improves security and performance.

---

5. OS Hardening Best Practices

- Keep the operating system updated.
- Use strong passwords.
- Avoid using administrator accounts for daily tasks.
- Enable firewall and antivirus protection.
- Disable unnecessary services and applications.
- Follow the least privilege principle.

Conclusion

This task helped in understanding how operating system–level security mechanisms protect systems and how proper configuration reduces security risks.