Cyber Security Internship – Task 2

Operating System Security Fundamentals (Linux & Windows)

---

1. Introduction to OS Security

Operating System security focuses on protecting the OS from unauthorized access, misuse, and attacks. A secure OS ensures that users, processes, and files are properly controlled and monitored to reduce security risks.

---

2. User Accounts and Access Control

Operating systems use user accounts to control access.

- **Administrator / Root User:**
  Has full control over the system, including installing software and changing system settings.
- **Standard / Normal User:**
  Has limited permissions and cannot make critical system changes.

Using standard users for daily work improves security and reduces damage if an account is compromised.

---

3. File Permissions in Linux

Linux controls access to files using permissions.

Each file has:

- **Read (r)** – view file content
- **Write (w)** – modify file
- **Execute (x)** – run file

Permissions apply to:

- Owner
- Group
- Others

Common commands:

- ls -l → view permissions

- chmod → change permissions
- chown → change file owner

File permissions prevent unauthorized users from accessing sensitive files.

---

4. Administrator vs Normal User

- **Root/Administrator**
    - Full system access
    - Can modify system files
    - High risk if misused
- **Normal User**
    - Limited access
    - Safer for daily activities
    - Reduces accidental or malicious damage

---

5. Firewall Configuration

A firewall controls incoming and outgoing network traffic.

- **Linux:** UFW (Uncomplicated Firewall)
- **Windows:** Windows Defender Firewall

Firewalls block unauthorized connections and protect the system from network-based attacks.

---

6. Running Processes and Services

Operating systems run multiple processes and services in the background.

- Some services are required for system operation
- Others may be unnecessary and risky

Viewing running processes helps identify suspicious or unused services.

---

7. Disabling Unnecessary Services

Unnecessary services increase the attack surface.

Disabling them:

- Reduces security risks
- Improves system performance
- Limits entry points for attackers

---

8. OS Hardening Practices

OS hardening is the process of securing an operating system by reducing vulnerabilities.

Common hardening practices include:

- Keeping the OS updated
- Using strong passwords
- Enabling firewalls
- Disabling unnecessary services
- Applying least privilege principle
- Using antivirus and security tools

---

9. Summary

This task helped me understand operating system security fundamentals, including user permissions, file access control, firewall usage, and OS hardening practices. Securing the operating system is a critical step in protecting systems from cyber threats.