Cyber Security Internship – Task 2

Operating System Security Fundamentals (Linux & Windows)

What is Operating System Security?

Operating System (OS) security focuses on protecting the core system that controls hardware, software, users, and processes. A secure OS prevents unauthorized access, malware infections, and system misuse.

What is OS Hardening?

OS hardening is the process of securing an operating system by reducing its attack surface. This is done by disabling unnecessary services, applying updates, and enforcing strong security policies.

User Accounts and Access Control

- Each user is given a specific account with limited permissions.
- Access control ensures users can only access resources they are authorized for.
- Strong passwords and user separation improve system security.

Administrator vs Standard User

- Administrator/Root user has full system control.
- Standard user has limited permissions.
- Daily work should be done using standard user accounts.

Linux File Permissions

Linux uses file permissions to control who can read, write, or execute a file. These permissions protect files from unauthorized access.

- Read (r): Allows viewing file content.
- Write (w): Allows modifying file content.
- Execute (x): Allows running the file.

Least Privilege Principle

The principle of least privilege means giving users and programs only the permissions they need. This limits damage if an account is compromised.

Firewall Configuration

- Linux uses UFW to manage firewall rules.
- Windows uses Windows Defender Firewall.
- Firewalls block unauthorized network access.

Processes and Services

Processes and services run in the background to support system functions. Some services are not required and can be security risks.

- Identify running services regularly.
- Disable unnecessary services.
- Fewer services mean fewer attack points.

Why Disable Unnecessary Services?

Unnecessary services increase the attack surface of the system. Disabling them improves performance and security.

OS Security Checklist

- Keep the OS updated.
- Use strong passwords.
- Enable firewall.
- Limit administrator access.
- Monitor processes and logs.

Final Summary

Operating system security is a critical part of cyber security. By applying OS hardening techniques, managing users, configuring firewalls, and disabling unnecessary services, systems can be protected from common attacks.