CYBER SECURITY INTERNSHIP

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

Operating System security is one of the most important foundations of cybersecurity. In this task, I explored how both Linux and Windows operating systems handle security through user management, permissions, services, and system hardening techniques. The objective was to understand how attackers exploit weak OS configurations and how proper hardening can reduce security risks.

1. User Accounts and Access Control

Both Linux and Windows use user accounts to control access to system resources. I studied the difference between administrator (root) and standard user accounts. Administrative accounts have full control over the system, while standard users have limited permissions. Using standard accounts for daily activities helps prevent accidental or malicious system damage.

2. File Permissions in Linux

Linux uses a permission-based model to control access to files and directories. Using commands such as ls -l, chmod, and chown, I learned how read, write, and execute permissions are assigned to the owner, group, and others. Proper file permissions ensure that sensitive files are protected from unauthorized access.

3. Administrator vs Standard User

The root user in Linux or administrator in Windows has unrestricted access to the system. Normal users have restricted privileges. Running applications as root is risky because any exploited vulnerability can compromise the entire system. Therefore, administrative privileges should only be used when absolutely necessary.

4. Firewall Configuration

Firewalls act as a barrier between the system and external networks. I explored enabling UFW (Uncomplicated Firewall) in Linux and Windows Defender Firewall to control inbound and outbound traffic. Firewalls help block unauthorized connections and reduce exposure to network-based attacks.

5. Running Processes and Services

I identified running processes and background services using system monitoring tools. Unnecessary services increase the attack surface and can be exploited by attackers. Disabling unused services improves system performance and enhances security.

6. OS Hardening Best Practices

- Use strong passwords and enable account lockout policies.

- Follow the principle of least privilege.

- Disable unnecessary services and ports.
- Keep the operating system and software up to date.
- Enable firewall and security monitoring tools.
- Regularly audit user accounts and permissions.

Final Outcome

This task helped me understand operating system-level security concepts and practical hardening techniques. It improved my awareness of how proper configuration and access control can significantly reduce security risks in both Linux and Windows environments.