Task 2

Operating System Security Fundamentals (Linux & Windows)

1) Introduction

Operating system security focuses on protecting the system from unauthorized access, misuse, and attacks. A secure operating system ensures that users, files, and system resources are properly protected.

2) User Accounts and Access Control

Operating systems use user accounts to control who can access the system and its resources. Each user is assigned specific permissions based on their role. Access control ensures that users can perform only the actions they are allowed to, which helps prevent misuse and unauthorized access.

3) File Permissions in Linux

Linux uses file permissions to control access to files and directories. These permissions decide who can read, write, or execute a file.

Viewing File Permissions :

The `ls -l` command is used to view file permissions.

Permissions are :

- **r** – read
- **w** – write
- **x** – execute

Permissions will be applied to:

- Owner
- Group
- Others

For Changing Permissions :

- `chmod` is used to change file permissions.
- `chown` is used to change file ownership.

These commands help restrict file access to authorized users only.

4) Administrator vs Standard User Privileges

An administrator (root user in Linux) has full control over the operating system and can make system-level changes. A standard user has limited permissions and cannot modify critical system settings. Using a standard user for daily activities improves system security by reducing the risk of accidental or malicious changes.

5) Firewall Configuration

A firewall helps protect the system by controlling network traffic. It allows only authorized connections and blocks unwanted access.

- In Linux, UFW (Uncomplicated Firewall) is used to manage firewall rules.
- In Windows, Windows Firewall provides built-in network protection.

Enabling a firewall is an important step in securing the operating system.

6) Running Processes and Services

Operating systems run many processes and background services to perform tasks. Some services are essential for system operation, while others may not be required. Identifying running processes and services helps administrators understand what is active on the system.

7) Disabling Unnecessary Services

Unnecessary services increase the system’s attack surface. If unused services are running, attackers may exploit them to gain access. Disabling unnecessary services improves system security and performance by reducing potential entry points.

8) Best OS Hardening Practices

OS hardening is the process of securing the operating system by minimizing vulnerabilities. Common hardening practices are :

- Using strong passwords.
- Applying regular system updates.
- Limiting user permissions.
- Disabling unused services.
- Enabling firewalls.

- Monitoring system activities.

These practices help protect the system from common attacks.

9) Conclusion

Operating system security is essential for protecting systems from unauthorized access and attacks. User accounts and access control help limit what users are allowed to do on the system. Linux file permissions ensure that only authorized users can access files. Using standard users instead of administrators for daily tasks improves security. Firewalls protect the system from network threats, and disabling unnecessary services reduces the attack surface. By following OS hardening best practices, both Linux and Windows systems can be made more secure and reliable.