Task 2: Operating System Security Fundamentals (Kali Linux)

Objective

To understand basic operating system security concepts and apply OS hardening techniques using Kali Linux.

Environment

- Operating System: Kali Linux
- Platform: Virtual Machine
- User Mode: Root (default Kali configuration)

1. User Accounts & Privileges

- Verified current user using whoami.
- Observed that Kali Linux runs as root by default.
- Understood the difference between root (administrator) and standard users.

2. File Permissions

- Viewed file permissions using ls -l.
- Modified permissions using chmod.
- Changed file ownership using chown.

Purpose: Enforce least privilege and protect sensitive files.

3. Firewall Configuration

- Installed and enabled UFW.
- Set default policy to deny incoming traffic.
- Verified firewall status.

Purpose: Reduce network-based attack surface.

4. Processes & Services

- Identified running processes using ps and top.
- Reviewed active services using systemctl.

5. Service Hardening

- Disabled unnecessary services.

Purpose: Minimize system attack surface.

6. System Updates

- Updated system using apt update and apt upgrade.

OS Hardening Best Practices

- Least privilege principle
- Secure file permissions
- Firewall enabled
- Unnecessary services disabled
- Regular system updates

Final Outcome

Understanding of OS-level security mechanisms and basic hardening techniques was achieved using Kali Linux.

Prepared by:

MOHAMMED JAVEETH M