Task 2: Operating System Security – Detailed Explanation of 7 Steps

Operating System Used: Kali Linux (Oracle VirtualBox)

Introduction

This document explains the seven fundamental operating system security steps performed in Task 2. For each step, the concept, its importance, and the method of implementation are described. These steps collectively help in hardening an operating system and reducing its attack surface.

Step 1: User Identification and Privilege Verification

What it is: Identifying the currently logged-in user and their group memberships.
Why it is used: To confirm whether actions are being performed by a normal user or a privileged user.
Why it is important: Running daily tasks as a non-root user reduces the risk of accidental or malicious system damage.
How to do it: Use commands like **whoami** and **id** to display user identity and groups.

Step 2: Sudo Privileges and Access Control

What it is: Checking whether a user can execute administrative commands using sudo.
Why it is used: To allow controlled administrative access without permanent root login.
Why it is important: It enforces accountability and minimizes security risks associated with full-time root access.
How to do it: Run **sudo -l** to view permitted administrative commands.

Step 3: Understanding Linux Users and System Accounts

What it is: Reviewing all user accounts present on the system.
Why it is used: To distinguish between system accounts and human users.
Why it is important: System accounts are restricted for security; understanding them helps prevent privilege misuse.
How to do it: Examine the **/etc/passwd** file using **cat /etc/passwd**.

Step 4: File Permissions and Ownership Management

What it is: Controlling access to files using permissions and ownership.
Why it is used: To restrict who can read, write, or execute files.
Why it is important: Prevents unauthorized data access, modification, or execution of malicious files.
How to do it: Use **ls -l** to view permissions, **chmod** to change permissions, and **chown** to change ownership.

Step 5: Root User vs Normal User

What it is: Understanding the difference between root and normal users.
Why it is used: To perform administrative tasks when required.

Why it is important: Root has unrestricted power; misuse can compromise the entire system.
How to do it: Use **sudo su** to switch to root and **exit** to return to normal user mode.

Step 6: Firewall Configuration (UFW)

What it is: Enabling a firewall to control network traffic.
Why it is used: To block unauthorized incoming and outgoing connections.
Why it is important: Firewalls reduce exposure to network-based attacks.
How to do it: Install UFW using **apt install ufw**, enable it with **ufw enable**, and verify using **ufw status**.

Step 7: Monitoring Processes and Services

What it is: Observing active system processes and services.
Why it is used: To detect unnecessary or suspicious activities.
Why it is important: Fewer running services reduce the attack surface and improve system stability.
How to do it: Use commands like **top** or **ps aux** to monitor running processes.

Conclusion

These seven steps together form the foundation of operating system security. By implementing proper user controls, permission management, firewall protection, and monitoring, the operating system becomes significantly more resilient to attacks.