Task 2 Report: Operating System Security Fundamentals

Operating System: Kali Linux (Oracle VirtualBox)

1. Introduction

Operating system security plays a crucial role in protecting applications, data, and network resources. This report summarizes the practical implementation of OS security fundamentals performed on Kali Linux as part of Task 2 of the Cyber Security Internship.

2. Environment Setup

A Kali Linux virtual machine was installed using Oracle VirtualBox. Using a virtualized environment provides isolation from the host system and allows safe experimentation with security configurations and administrative controls.

3. User Accounts and Access Control

User identity and group memberships were reviewed to understand access control mechanisms. Administrative privileges were managed using sudo, ensuring that elevated permissions were only used when required. This approach aligns with the principle of least privilege.

4. File Permissions and Ownership

Linux file permissions and ownership were analyzed to control access to system resources. Proper permission management prevents unauthorized reading, writing, or execution of files, thereby protecting system integrity.

5. Firewall and Network Security

Network-level protection was implemented by enabling the Uncomplicated Firewall (UFW). The firewall helps regulate incoming and outgoing traffic, reducing exposure to network-based attacks.

6. Processes and Services Management

Running processes and services were monitored to identify active system components. Regular monitoring helps detect suspicious activity and supports the identification of unnecessary services that could increase the system attack surface.

7. OS Hardening Practices

- Use strong authentication mechanisms
- Apply the principle of least privilege
- Avoid direct root login
- Enable and configure firewall protection
- Disable unnecessary services
- Perform regular system updates
- Monitor system processes and logs

8. Conclusion

Through this task, a foundational understanding of operating system security was achieved. Applying proper access controls, permission management, firewall protection, and monitoring practices significantly enhances the security posture of an operating system.