CYBER SECURITY INTERNSHIP

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

1. Introduction

Operating System (OS) security is the foundation of cybersecurity. The OS manages hardware, software, user access, memory, and processes. If compromised, attackers can gain full system control, steal data, or disrupt services. This task focuses on understanding and implementing OS-level security mechanisms in Linux and Windows.

2. Objectives of the Task

• Understand OS-level security concepts
• Explore user accounts and access control
• Learn Linux file permissions and ownership
• Differentiate administrator/root and standard users
• Enable and configure firewalls
• Manage running processes and services
• Apply OS hardening best practices

3. Tools and Environment

Operating Systems Used:
• Ubuntu Linux (Virtual Machine)
• Windows 10/11

Tools:
• VirtualBox
• Linux Terminal
• UFW Firewall
• Windows Defender & Windows Firewall

4. User Accounts and Access Control

Linux uses user-based access control with unique user IDs and group memberships. Important files include /etc/passwd and /etc/shadow. Windows differentiates between Administrator and Standard user accounts to control system privileges.

5. File Permissions in Linux

Linux permissions control read (r), write (w), and execute (x) access for owner, group, and others. Commands such as ls -l, chmod, and chown are used to view and modify permissions and ownership.

6. Administrator vs Standard User

Root (Linux) and Administrator (Windows) accounts have full system privileges. Standard users operate with limited rights, reducing security risks and accidental damage.

7. Firewall Configuration

Firewalls filter network traffic. In Linux, UFW is used to allow or deny connections. Windows Firewall manages inbound and outbound rules to prevent unauthorized access.

8. Process and Service Management

Processes and services can be monitored using ps, top, and systemctl in Linux, and Task Manager and Services Manager in Windows.

9. Disabling Unnecessary Services

Unused services such as FTP or Telnet increase attack surface. Disabling them reduces vulnerabilities and improves system performance.

10. OS Hardening Best Practices

• Regular OS updates and patches
• Strong passwords and MFA
• Least privilege principle
• Firewall and antivirus enabled
• Disk encryption and backups

11. OS Security Checklist

• User accounts reviewed
• File permissions verified
• Firewall enabled
• Unnecessary services disabled
• System hardening documented

12. Interview Questions (Summary)

OS hardening secures systems by reducing vulnerabilities. Linux file permissions control access. Least privilege ensures minimal access to users and processes.

13. Final Outcome

This task provided hands-on exposure to OS-level security in Linux and Windows. It strengthened foundational knowledge required for SOC operations and cybersecurity roles.

14. Conclusion

Operating System security is a critical defense layer. Proper configuration, access control, and hardening significantly reduce cyber risks.