

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

Introduction

This task focuses on understanding operating system level security in Linux and Windows. It covers user permissions, access control, firewalls, running services, and OS hardening practices.

1. Linux Virtual Machine / Windows Security

Linux Virtual Machines can be installed using VirtualBox. Windows provides built-in security features such as Windows Defender and Windows Firewall to protect the system from malware and network attacks.

2. User Accounts and Access Control

Operating systems use user accounts and access control to restrict unauthorized access. Permissions ensure that users can only access allowed files and system resources.

3. File Permissions in Linux

Linux file permissions define who can read, write, or execute files.

Commands used:

ls -l – View permissions

chmod – Change permissions

chown – Change file ownership

4. Administrator vs Standard User

Administrator (root) users have full control over the system. Standard users have limited permissions. Using standard users improves security and prevents accidental system damage.

5. Firewall Configuration

Firewalls control incoming and outgoing network traffic.

Linux: UFW (Uncomplicated Firewall)

Windows: Windows Firewall

Firewalls help block unauthorized network access.

6. Running Processes and Services

Processes and services are programs running in the background. Monitoring them helps detect suspicious activity and improves system security.

7. Disabling Unnecessary Services

Unused services should be disabled to reduce the system's attack surface and improve performance.

8. OS Hardening Best Practices

Apply regular updates and patches

Use strong passwords

Enable firewalls

Use least privilege principle

Disable unnecessary services

Monitor system logs

OS Security Checklist

Strong passwords enabled

System updated regularly

Standard user accounts used

Unnecessary services disabled

Least privilege followed

Interview Questions – Short Answers

What is OS hardening?

Securing an operating system by reducing vulnerabilities.

What are file permissions in Linux?

They control read, write, and execute access.

Why disable unnecessary services?

To reduce attack surface.

Difference between root and normal user?

Root has full access; normal user has limited access.

What is least privilege principle?

Giving users only the permissions required to do their work.

Prepared By:

SAFFIQ MOHAMMED S