Penetration Testing

Task:

Conduct penetration testing to identify and exploit vulnerabilities in systems and applications.

What is Penetration Testing?

Penetration testing (pentesting) is a cybersecurity practice where security professionals simulate real-world attacks to identify weaknesses in an organization's network, applications, or infrastructure. The goal is to discover vulnerabilities before malicious actors exploit them.

Steps to Conduct Penetration Testing

1. Planning and Reconnaissance

Define scope, objectives, and gather intelligence on the target system.

2. Scanning

Use tools like Nmap and Nessus to identify open ports and vulnerabilities.

3. Gaining Access

Exploit identified vulnerabilities using Metasploit or manual techniques.

4. Maintaining Access

Test persistence techniques to see if an attacker can remain undetected.

5. Analysis and Reporting

Document findings, impact assessment, and recommendations for mitigation.

6. Remediation and Reassessment

Fix vulnerabilities and conduct a retest to ensure they are resolved.

Penetration Testing Resources:

- OWASP Penetration Testing Guide: https://owasp.org/www-project-web-security-testing-guide/
- Kali Linux: https://www.kali.org/
- Metasploit Framework: https://www.metasploit.com/
- Nmap Security Scanner: https://nmap.org/
- Nessus Vulnerability Scanner: https://www.tenable.com/products/nessus