CYBERSECURITY TRAINING
(WEEK 3 - Day 3)

1.1 Phases of Penetration testing

1. Planning and Reconnaissance

Objective: Understand the scope and gather initial information about the target.

- Define goals and rules of engagement.

- Identify the target systems and testing methods (black box, white box, gray box).

2. Scanning

Objective: Discover open ports, services, and vulnerabilities.

- Network Scanning: Identify live hosts and open ports (e.g., using Nmap).
- Use tools like Nessus or OpenVAS to detect known vulnerabilities.

3. Gaining Access

Objective: Exploit vulnerabilities to gain unauthorized access.

- Use exploitation techniques such as:
  Buffer overflow
  SQL injection
  Credential brute-forcing

4. Maintaining Access

Objective: Create a persistent backdoor to access the system later.

- Install malware, create new user accounts, or modify startup scripts.

- Tools: Metasploit's Meterpreter, Netcat, Reverse Shells, etc.

5. Covering Tracks / Reporting

Objective: Erase traces of the attack and prepare a report.

- Covering Tracks:
  Clear logs, delete tools/scripts used during the test.
  Avoid detection (anti-forensics).

1.2 Tools used in Penetration testing

nslookup :queries DNS records to map IPs and domains.

whois : retrieves domain ownership and registration information.

shadon :search engine for internet connected devices and services.

nmap:network scanner to detect live hosts ,open port.

metasploit: A powerful network for developing and executing exploits.

SQLMap:Automated detection and exploitation of SQL injection vulnerabilities.