4th Assignment Ech - Web Based Hacking

1. Session Hijacking & Techniques

Session hijacking is when an attacker steals or takes over a valid session to gain unauthorized access to a system.

Techniques:

Session Fixation – Forcing a user to use a pre-set session ID.

Session Sidejacking – Capturing session tokens via network sniffing.

Cross-Site Scripted (XSS) Hijacking – Injecting scripts to steal session cookies.

Man-in-the-Middle (MITM) – Intercepting traffic to hijack sessions.

2. DoS/DDoS Attack Tools

LOIC (Low Orbit Ion Cannon) – Open-source DoS tool.

HOIC (High Orbit Ion Cannon) – More powerful than LOIC.

HULK (HTTP Unbearable Load King) – Generates heavy web traffic.

Slowloris – Sends partial HTTP requests to exhaust server resources.

Mirai Botnet – IoT-based botnet for massive DDoS attacks.

3. SYN Flooding Attack (Example)

A SYN flood is a DoS attack that sends excessive SYN (synchronization) requests to a server but never completes the handshake, overloading the system.

Example:

Attacker sends multiple SYN requests.

Server responds with SYN-ACK but never receives the ACK.

Server keeps resources open, leading to exhaustion and denial of service.

🛡 Mitigation: Rate limiting, SYN cookies, firewalls.

4. Web App Hacking Methodologies

Reconnaissance – Gathering info (Google Dorking, Whois, OSINT).

Scanning & Enumeration – Identifying vulnerabilities (Nmap, Nikto).

Exploitation – Using vulnerabilities (SQL Injection, XSS).

Privilege Escalation – Gaining admin access.

Covering Tracks – Hiding malicious activities.

5. SQL Injection Methodology

Identify Injection Points – Find input fields vulnerable to SQL injection.

Bypass Authentication – Inject ' OR '1'='1 to access restricted data.

Extract Data – Use UNION SELECT or LOAD_FILE() to retrieve sensitive data.

Modify Database – Use UPDATE or DELETE queries to manipulate data.

Maintain Access – Install a backdoor for persistence.

6. SQL Injection Using SQLmap (Tool Example)

SQLmap is an automated tool for detecting and exploiting SQL injections.

Example Usage:

```
sqlmap -u "http://example.com/login.php?id=1" --dbs
```

This command checks for SQL injection and retrieves database names.

🛡 Prevention: Use prepared statements, input validation, and WAF (Web Application Firewall).

7. Difference Between VA & PT

Feature	Vulnerability Assessment (VA)	Penetration Testing (PT)
Purpose	Identifies security flaws	Exploits vulnerabilities to test security
Approach	Automated scanning & reporting	Manual & automated exploitation
Depth	Broad, but no real attacks	Deep testing with attack simulations
Frequency	Regularly conducted	Periodic (Quarterly/Annually)

8. How to Write a Vulnerability Assessment Report

Executive Summary – Overview of findings.
Scope of Assessment – Define tested systems and networks.
Methodology Used – Describe scanning tools (e.g., Nessus, OpenVAS).
Identified Vulnerabilities – List issues with CVSS scores.
Impact Analysis – Explain risks associated with each vulnerability.
Recommendations – Provide fixes (patching, configuration changes).
Conclusion – Summary and next steps.

9. Zero-Day Attacks

A zero-day attack exploits unknown software vulnerabilities before a patch is available.

Examples:
Stuxnet – Targeted Iranian nuclear facilities.
EternalBlue – Used in WannaCry ransomware.
🛡 Mitigation:

Use behavior-based security tools (EDR, SIEM).
Apply patches and updates ASAP.
Implement zero-trust architecture