Web Based Hacking

1. What is Session Hijacking Explain with Techniques?

A: Session hijacking is when an attacker takes over a user's session to steal information. Methods include session fixation, sidejacking, cookie stealing, Man-in-the-Middle attacks, and session replay.

2. Find DoS/DDoS Attack Tools

A: LOIC, HOIC, Slowloris, Hping, Mirai

3. Explain SYN Flooding Attack with example

A: SYN Flooding is an attack where the attacker sends many fake connection requests to a server but never completes them. The server gets overwhelmed by waiting for responses, making it unable to handle real requests.

Example: The attacker sends fake requests to a web server, causing it to stop working for legitimate users.

4. List of Web App Hacking Methodology

A: Web application hacking methodologies include, injection attacks, XSS, CSRF, session hijacking, brute force attacks, file upload exploits, and privilege escalation.

5. Explain sql injection with any tool

A: SQL injection is when an attacker puts harmful SQL code into a form or URL, which lets them control a website's database. This can allow them to access or delete data. To prevent it, always use safe coding practices like prepared statements and input validation. Tools like SQLmap can help test for these vulnerabilities.

6. Explain deference between VA And PT

A: Vulnerability Assessment (VA) finds and lists potential security weaknesses in a system. It’s more about scanning for issues.

Penetration Testing (PT) goes a step further by actually trying to exploit those weaknesses to see how deep an attacker could go.

7. How to write vulnerability assessment Report

A:

Title Page: Report title, date, author.

Summary: Key findings and security status.

Findings: List vulnerabilities with severity and impact.

Recommendations: Fixes for each issue.

Conclusion: Highlight critical issues.

Appendices: Extra details if needed.