Module: Ech – Web Based Hacking

1. What is Session Hijacking Explain with Techniques?

Ans-> Session hijacking is a cyberattack where an attacker steals or compromises a user's active computer session. This allows the attacker to impersonate the legitimate user and gain unauthorized access to their data and activities.

* There are some Techniques of session Hijacking are as follow:-

1. Session Sniffing.
2. Cross-Site Scripting (XSS).
3. Session Fixation.
4. Man-in-the-Middle (MitM) Attacks.
5. Find DoS/DDoS Attack Tools.

Ans-> There are some Types of DoS/DDoS Attacks tools are as follow:-

1. Hping3.
2. LOIC (Low Orbit Ion Cannon).
3. HOIC (High Orbit Ion Cannon).
4. DDoS-Attack.
5. Metasploit
6. Explain SYN Flooding Attack with example.

Ans-> A SYN flood attack exploits the three-way handshake process used to establish a TCP connection. The attacker sends a large number of SYN packets (the first step in the handshake) to the target server, overwhelming it with connection requests. Example:- Imagine a restaurant with a limited number of tables. Customers (clients) arrive and request a table (SYN). The restaurant (server) acknowledges the request (SYN-ACK) and prepares a table.

1. List of Web App Hacking Methodology.

Ans-> There are some list of web App hacking Methodology are as follow:-

1. Reconnaissance
2. Scanning
3. Exploitation
4. Post-exploitation
5. SQL Injection Methodology.

Ans->

1.  Analyze website input fields (forms, search bars) for potential SQL injection points.
2. Inject malicious SQL queries into these fields to see if they execute on the server.
3. Common techniques include:
4. Using single quotes (') to break out of the original query.
5. Using UNION clauses to retrieve data from other tables.
6. Using comments (--) to bypass parts of the original query.
7. Explain sql injection with any tool.

Ans-> There are some points of sql injection are as follow:-

1. Install SQLmap
2. Target Selection
3. Command Execution
4. Data Retrieval
5. Explain deference between VA And PT.

Ans->  **Vulnerability Assessment (VA):**

* **Focus:** Identifies and assesses potential vulnerabilities in systems and networks.
* **Scope:** Broader, covering hardware, software, networks, and configurations.
* **Methodology:** Primarily automated scans and checks.
* **Output:** Detailed reports listing identified vulnerabilities and their potential impact.

**Penetration Testing (PT):**

* **Focus:** Exploits identified vulnerabilities to assess the actual impact and potential damage.
* **Scope:** More targeted, focusing on specific systems or applications.
* **Methodology:** Involves manual techniques and often requires advanced skills.
* **Output:** Detailed reports documenting the attack methodology, successful exploits, and recommendations for remediation.

1. How to write vulnerability assessment Report.

Ans-> There are some points of vulnerability assessment report are as follow:-

* 1.  **Executive Summary:** Briefly summarize the assessment's scope, methodology, and key findings.
  2.  **Introduction:** Provide background information on the organization and the systems assessed.
  3.  **Methodology:** Describe the tools and techniques used during the assessment.
  4.  **Findings:** Detail all identified vulnerabilities, including their severity, location, and potential impact.
  5.  **Recommendations:** Provide specific and actionable recommendations for mitigating the identified vulnerabilities.
  6.  **Conclusion:** Summarize the key findings and reiterate the importance of addressing the vulnerabilities.
  7.  **Appendices:** Include supporting documentation, such as scan results and detailed vulnerability descriptions.

1. Explain the Zero Day Attacks.

Ans-> Zero-day attacks exploit previously unknown vulnerabilities in software or hardware. A **zero-day attack** is a type of cyberattack that exploits a previously unknown vulnerability in software, hardware, or firmware. Since the vulnerability is unknown to the vendor or the public, there are no patches or fixes available at the time of the attack, making it highly dangerous.