Module : 31 Penetration Testing Basics

1) MAC Spoofing

- MAC spoofing is the act of changing the Media Access Control (MAC) address of a device's network interface card (NIC). The MAC address is a unique identifier assigned to the hardware, but attackers or users can alter it for various purposes.
- Email Spoofing
- Email spoofing is a technique where an attacker sends emails by forging the sender's address, making it appear as though the email comes from a trusted source.

2) 4 online email encryption service

- ProtonMail
- Preveil
- StartMail
- Tutanota

3) 8 Types of Firewall

- Packet-Filtering Firewalls
- Stateful Inspection Firewalls
- Proxy Firewalls (Application-Level Gateways)
- Next-Generation Firewalls (NGFWs)

- Circuit-Level Gateways
- Software Firewalls
- Hardware Firewalls
- Cloud Firewalls

4) Explain Evading Firewalls

- IP Fragmentation
- Encryption and Tunneling
- Port Manipulation
- Obfuscation
- Spoofing
- Time-Based Evasion

5) Session hijacking is a cyberattack where an attacker takes control of a user's active session with a web application or service. This is typically done by stealing or manipulating the session token, which is a unique identifier used to maintain the user's session.

- Techniques Used in Session Hijacking:
- Session Sniffing
- Cross-Site Scripting (XSS)
- Session Fixation
- Man-in-the-Middle (MITM) Attack
- Brute Force
- Trojan Attacks

6) SYN Flood Attack:

- The attacker sends a large number of SYN packets to the server, often using spoofed IP addresses.
- The server responds with SYN-ACK packets and waits for the final ACK packet to complete the handshake.
- Since the ACK packet never arrives, the server keeps these connections in a "half-open" state, consuming its resources.

7) List of Web App Hacking Methodology

- Information Gathering
- Mapping the Application
- Identifying Vulnerabilities
- Exploitation
- Post-Exploitation
- Reporting

8) SQL Injection Methodology

- Identify Input Points
- Test for Vulnerability
- Determine Database Type
- Extract Data
- Bypass Authentication
- Privilege Escalation

- Cover Tracks

9) Setup

- Install sqlmap on your system. It's available for free and supports multiple operating systems.
- Identify a vulnerable web application or URL where SQL Injection might be possible.
- Testing for Vulnerability:
- sqlmap -u "http://example.com/page?id=1"
- sqlmap will test the URL for SQL Injection vulnerabilities by injecting various payloads.
- Exploiting the Vulnerability:
- If the target is vulnerable, sqlmap can extract data from the database. For instance:
- sqlmap -u "http://example.com/page?id=1" --dump
- Advanced Features:
- sqlmap supports various SQL Injection techniques like boolean-based blind, time-based blind, error-based, and UNION query-based.
- It can also perform database fingerprinting, enumerate databases, tables, and columns, and even execute commands on the database server.
- Mitigation
- Use sqlmap responsibly for penetration testing to identify and fix vulnerabilities in your own applications.

10) Vulnerability Assessment (VA): Identifies, quantifies, and prioritizes vulnerabilities in systems, networks, and applications. The primary goal is to find potential weaknesses before they can be exploited.

- Penetration Testing (PT): Simulates real-world attacks to exploit vulnerabilities. The focus is on demonstrating the impact of vulnerabilities by attempting to breach the system.

11) Executive Summary:

- Write a brief overview for stakeholders (e.g., management) who may not be technical.
- Include the purpose of the assessment, scope, key findings, and a summary of recommendations.
- Introduction:
- Objective: State the goal of the assessment, such as identifying and mitigating vulnerabilities.
- Scope: Define the boundaries, including systems, applications, or networks assessed.
- Methodology: Explain the process used (e.g., automated scans, manual testing) and reference any frameworks like OWASP or NIST.
- Assessment Details
- Environment Details: Describe the technologies and infrastructure assessed.

- Tools Used: List tools like Nessus, OpenVAS, or Burp Suite used during the assessment.
- Testing Phases: Describe each phase, such as reconnaissance, scanning, and analysis.
- Findings:
- Vulnerability Name: State the issue (e.g., "SQL Injection").
- Description: Provide a brief explanation of the vulnerability.
- Affected Systems: Specify which systems or components are impacted.
- Severity: Assign a risk level (e.g., low, medium, high, critical).
- Evidence: Include screenshots, logs, or proof of concept where applicable.
- Impact Analysis
- Explain the potential risks, such as data breaches, unauthorized access, or system downtime.
- Assess business impact based on confidentiality, integrity, and availability.
- Recommendations
- Apply patches or updates.
- Use secure coding practices.
- Implement strong access controls.
- Perform regular security testing.
- Prioritize recommendations based on severity and impact.

12) A Zero-Day Attack is a type of cyberattack that exploits a previously unknown vulnerability in software, hardware, or firmware. The term "zero-day" refers to the fact that the vendor or developer has "zero days" to fix the flaw because it is discovered and exploited by attackers before a patch or solution is available.