Module 4: CS - Securing Web Applications Services & Servers

1. MAC (Media Access Control) spoofing refers to the practice of **changing** or **forging** the MAC address of a network interface card (NIC) to impersonate another device on a network.

Email spoofing is the act of **forging** the sender's address on an email to make it appear as though it was sent by someone else.

2. A SYN Flooding Attack is a type of Denial-of-Service (DoS) attack that targets the TCP handshake process, which is used to establish a connection between two devices.

Steps to Perform a SYN Flooding Attack Using Metasploit:

Set Up Kali Linux: Ensure you have Kali Linux installed on your machine. You can download the latest ISO image from the official Kali Linux .

Identify IP Addresses: Note down the IP addresses of both the attacker (your Kali Linux machine) and the victim (the target server).

Scan the Victim Machine: Use a tool like nmap to scan the victim machine and identify open ports.

Launch Metasploit: Open the terminal and type msfconsole to start the Metasploit Framework.

Search for SYN Flood Exploits: At the msf> prompt, type search syn to find SYN-based exploits. Refine the search by typing search syn flood.

Select the SYN Flood Module: Use the module auxiliary/dos/tcp/synflood by typing use auxiliary/dos/tcp/synflood.

Configure the Module: Set the target IP address and other necessary options.

Execute the Attack: Run the attack by typing run

3. Packet-Filtering Firewall

Stateful Inspection Firewall

Proxy Firewall (Application-Level Gateway)

Next-Generation Firewall (NGFW)

**Circuit-Level Gateway**

**4.** **Evading firewalls** refers to techniques or strategies used by attackers to bypass or circumvent the protective mechanisms of a firewall.

● Web Based Hacking

1. **Session hijacking** refers to the unauthorized act of taking over a valid user session to gain access to sensitive information or resources.

Techniques of Session Hijacking

Session Fixation

Session Sniffing (Man-in-the-Middle Attack)

Cross-Site Scripting (XSS)

Cookie Theft

Session Replay Attack

2. **Reconnaissance**

**Scanning and Enumeration**

Exploitation

Post-Exploitation

Reporting

3 **Information Gathering**

Detection

Exploitation

Post-Exploitation

**Reporting**

**4.** A **Vulnerability Assessment (VA)** is the process of identifying, quantifying, and prioritizing vulnerabilities in a system, network, or application.

**Penetration Testing (PT),** also known as ethical hacking, is the practice of simulating an attack on a system to identify and exploit vulnerabilities in a controlled manner.

5. A **Zero-Day Attack** refers to a type of cyberattack that targets a **vulnerability** in software or hardware that is **unknown to the vendor** or **developer** at the time of the attack.