Module 4: CS - Securing Web Applications
Services & Servers

1. Explain MAC spoofing and Email spoofing
   - ANS:MAC Spoofing: Changing the MAC address of a device to impersonate another device on the network.
   - Email Spoofing: Forging the sender's address in an email to deceive the recipient, often used in phishing attacks.

2. Perform practical of MITM tool and social engineering tool

ANS:Use tools like Ettercap for MITM and SET (Social-Engineer Toolkit) for phishing or credential harvesting.

3. Explain Kali Linux tool SYN Flooding Attack using Metasploit.

ANS: The SYN Flood attack in Metasploit sends a large number of SYN packets to a target, exhausting its resources and making it unavailable.

Command:

use auxiliary/dos/tcp/synflood
set RHOST <Target_IP>
run

4. Find online email encryption service

ANS :Services like ProtonMail, Tutanota, and Zoho Mail provide email encryption.

5. Types of Firewall .
   - ANS: Packet-Filtering Firewall
   - Stateful Inspection Firewall
   - Application Layer Firewall
   - NGFW (Next-Generation Firewall)
   - Proxy Firewall

6. Explain Evading Firewalls

ANS :Bypassing firewalls using techniques like encrypted tunnels (VPN), fragmenting packets, using proxies, or exploiting misconfigurations.

Web-Based Hacking

1. What is Session Hijacking? Explain with Techniques
   - **ANS** Stealing a user's active session to gain unauthorized access. Techniques:
   - Session ID Prediction
   - Session Fixation
   - XSS

- Man-in-the-Middle (MITM)

2. Find DoS/DDoS Attack Tools
ANS:Tools: LOIC, HOIC, HULK, Slowloris GoldenEye.

3. Explain SYN Flooding Attack with example
ANS:An attacker sends multiple SYN requests to a target but doesn't respond to the SYN-ACK, leaving the server overwhelmed. Example: Exploiting TCP's three-way handshake.

4. List of Web App Hacking Methodology
- ❖ Reconnaissance
- ❖ Vulnerability Scanning
- ❖ Exploitation (e.g., SQL Injection, XSS)
- ❖ Post-Exploitation
- ❖ Reporting

5. SQL Injection Methodology
ANS :- Input invalid SQL commands to manipulate database queries.
Steps:
Identify input point → Test payloads → Extract data.

6. Explain SQL Injection with any too
ANS :Tool: SQLmap
Command:
sqlmap -u <Target_URL> --dbs

7. Explain difference between VA and PT
ANS :- Vulnerability Assessment (VA): Identifies vulnerabilities in a system.
- Penetration Testing (PT): Exploits vulnerabilities to evaluate security.

8. How to write a Vulnerability Assessment Report
ANS :- Include: Executive Summary, Scope, Methodology, Findings, Risk Rating, and Recommendations.

9. Explain Zero-Day Attacks
ANS:An attack exploiting a vulnerability unknown to vendors or the public, leaving no time for mitigation. Example: Stuxnet worm.