Module 4: CS - Securing Web Applications Services & Servers

1. Explain MAC spoofing and Email spoofing

Ans:

1. **MAC Spoofing (Media Access Control Spoofing):**

- **What is it?**
  MAC spoofing is when someone **changes the MAC address** of their device to look like another device.
- **MAC address?**
  A MAC address is a **unique number** given to every device's network card (like a computer or phone) that connects to a network.
- **Why do people spoof it?**
  - To **bypass network filters** (e.g., Wi-Fi that allows only certain devices)
  - To **hide identity**
  - To **gain unauthorized access** to networks
- **Example:**
  If a school Wi-Fi only allows certain devices, someone could change their MAC address to match an allowed one and connect.

2. **Email Spoofing:**

- **What is it?**
  Email spoofing is when someone **sends an email that looks like it came from someone else's address**.
- **Why is it done?**
  - To **trick** the receiver (phishing)
  - To **spread malware**
  - To **steal personal info** (like passwords or bank details)
- **Example:**
  You get an email that **looks like it's from your bank**, asking you to click a link and enter your login info—but it's actually from a hacker.

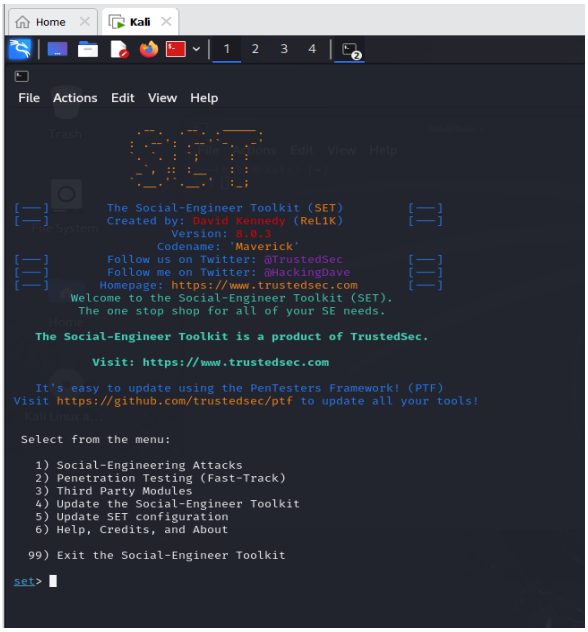
2. Perform practical of MITM tool and social engineering Tool

Ans:

1. MITM tool
   A **Man-in-the-Middle (MITM) attack** is when an attacker secretly intercepts and possibly alters communication between two parties without their knowledge.

2. social engineering Tool

- sudo setoolkit



- Enter your local IP address (e.g., 192.168.1.100)
- Enter the URL to clone (e.g., https://www.facebook.com)

3. Explain Kali linux tool SYN Flooding Attack using Metasploit

4. Find online email encryption service

Ans:

Service	Type of Encryption	Free Plan	Best For
ProtonMail	End-to-end, PGP	✅ Yes	Simple & secure private email
Tutanota	Full end-to-end (all data)	✅ Yes	Maximum privacy, open-source
Mailfence	PGP + Digital Signature	✅ Yes	Encrypted email + calendar/tools
Hushmail	PGP + password-protected	❌ No	Healthcare, legal, finance (HIPAA)
Virtru	Client-side for Gmail/Outlook	⚠️ Limited	Businesses using Gmail/Outlook
PreVeil	End-to-end with device keys	❌ No	Enterprises with strict security

Mailvelope	PGP via browser extension	☑ Yes	Encrypt Gmail/Outlook/Yahoo easily

Sender ✉ -> Encrypt with Recipient's Public Key 🔒 -> Encrypted Email Sent Over Internet ☁ -> Recipient Uses Private Key 🔑 to Decrypt -> Recipient Reads Secure Message ☑

- For **personal private email** → ProtonMail or Tutanota
- For **business/compliance** → Hushmail or Virtru
- For **using existing Gmail/Outlook** → Mailvelope or Virtru

5. Types of Firewall

Ans:

Based On Deployment	Description
Hardware Firewall	A physical device that filters traffic before it enters your network. Used in routers, enterprise setups.
Software Firewall	Installed on a computer/device. Filters traffic at the OS level (e.g., Windows Defender Firewall).
Cloud Firewall (FWaaS)	Firewall hosted in the cloud. Scalable and managed externally. Ideal for cloud apps and remote teams.

6. Explain Evading Firewalls

Ans: A **firewall** blocks or filters unwanted traffic.
Attackers try to "evade" firewalls by hiding or bypassing their malicious traffic so it looks normal.

Technique	Explanation (Easy)
Fragmentation	Break malicious data into small pieces (packets) so the firewall cannot detect the full attack.
Encryption / Tunneling	Hide attack traffic inside encrypted tunnels (e.g., SSH, VPN) so firewall can't inspect it.
Port Hopping	Send traffic through non-standard or random ports to confuse firewall rules.
Proxy / Anonymizers	Route traffic through proxy servers to mask the real source.
Protocol Obfuscation	Modify protocols slightly so firewall signatures don't match.
HTTP Tunneling	Send malicious traffic inside normal web traffic (HTTP/HTTPS), which firewalls usually allow.
Source Routing / IP Spoofing	Pretend to be a trusted system or change the IP path to bypass restrictions.

Web Based Hacking

1. What is Session Hijacking Explain with Techniques?

Ans:

When you log into a website (like Facebook), the website gives your browser a **session ID** — like a secret pass that tells the site, "This is you!"

Session hijacking is when a **hacker steals that session ID** and uses it to **pretend to be you** — without needing your password.

Example:

Imagine you log into your account at a coffee shop using public Wi-Fi.

- A hacker nearby **spies on the network**.
- They grab your **session ID**.

Technique	Simple Explanation
1. Packet Sniffing	Hacker uses tools to watch the network and steal your session ID. Often happens on public Wi-Fi.
2. Cross-site Scripting (XSS)	Hacker puts a fake script on a website. When you visit it, your session ID is sent to the hacker.
3. Session Fixation	Hacker tricks you into logging in with a session ID they already know.
4. Man-in-the-Middle (MITM)	Hacker stands between you and the website, watching what you send and receive.
5. Malware	Hacker uses a virus or keylogger to steal your session ID from your device.

2. Find DoS/DDoS Attack Tools

Ans:

Tool Name	Description
LOIC (Low Orbit Ion Cannon)	Easy-to-use tool for sending massive traffic to a target. Often used in DoS attacks.
HOIC (High Orbit Ion Cannon)	More powerful than LOIC; supports multi-threaded attacks and plugins.

Hping3	Command-line tool for TCP/IP packet crafting. Can be used for flooding attacks.
Slowloris	Sends partial HTTP requests to keep connections open, exhausting server resources.
Xerxes	A powerful DoS tool often used against web servers (used by Anonymous).
RUDY (R U Dead Yet)	Targets web applications by holding sessions open with slow HTTP POST requests.
GoldenEye	Python-based tool used for layer 7 (HTTP) DoS attacks.
UFONet	DDoS tool using botnets built via open redirect vulnerabilities.
Metasploit DoS modules	Metasploit includes some modules for DoS testing.
Botnets (e.g., Mirai)	Used in large-scale DDoS attacks by infecting IoT devices (extremely dangerous and illegal if used unethically).

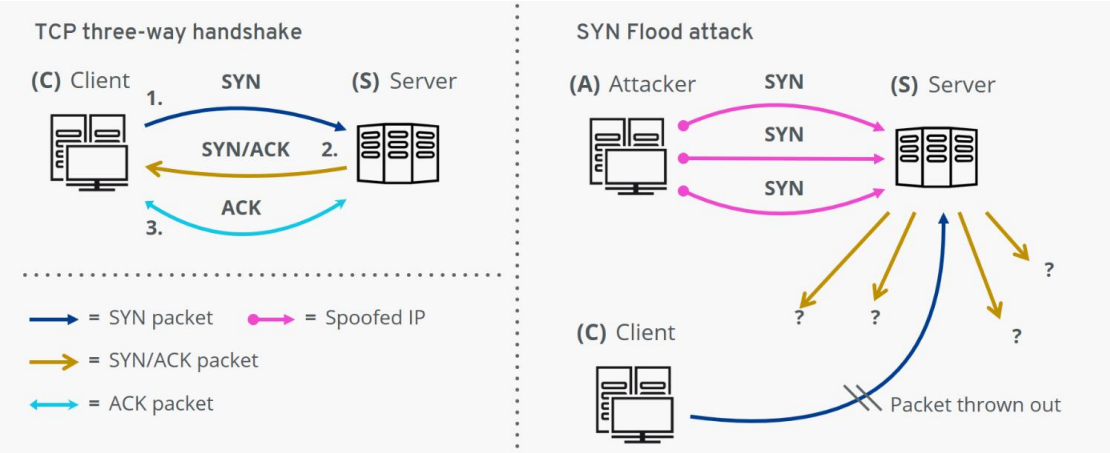
Defensive Tools for Testing:

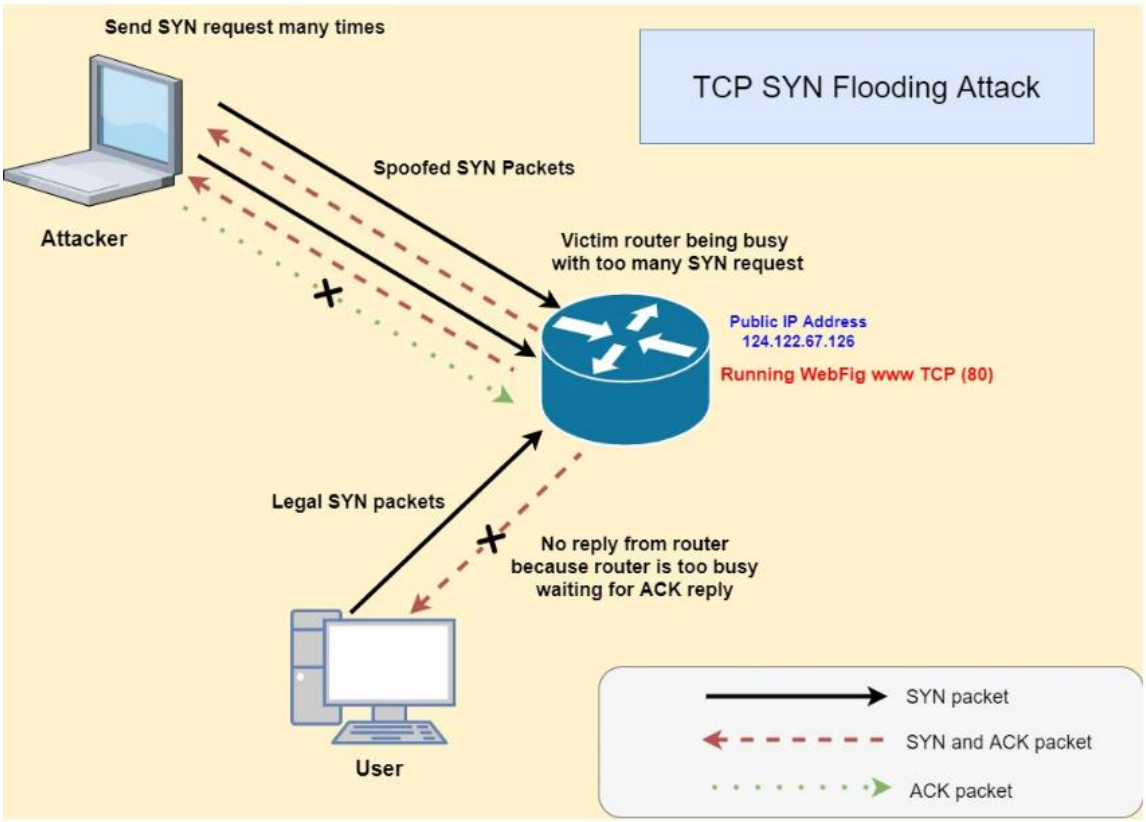
Tool/Service		Purpose
Wireshark	-	Analyze traffic and detect DoS/DDoS patterns.
Snort/Suricata	-	IDS/IPS systems to detect and block attacks.
Fail2ban	-	Blocks IPs with suspicious behavior.
Cloudflare	-	Protects websites from DDoS with WAF and mitigation services.

3. Explain SYN Flooding Attack with example

Ans:

A **SYN Flood** is a type of **cyberattack** where a hacker sends **lots of fake connection requests** to a server to **crash it or slow it down**.





Example:

Imagine a receptionist at a hotel:

- 100 fake people call and say, **"I want to book a room."**
- The receptionist replies, **"Okay, please confirm."**
- But no one ever confirms.
- While waiting, the receptionist can't talk to real guests.

The hotel (server) becomes **overloaded** and **real guests can't book rooms**.

4. List of Web App Hacking Methodology

Ans:

- **Information Gathering** – Collect details about the target (domain, IP, tech stack).
- **Reconnaissance** – Find hidden files, directories, and parameters.
- **Scanning & Enumeration** – Use tools to detect open ports, services, and vulnerabilities.
- **Vulnerability Analysis** – Identify weak points (SQLi, XSS, CSRF, etc.).
- **Exploitation** – Use the vulnerabilities to gain access or control.
- **Privilege Escalation** – Increase access rights if possible.
- **Post-Exploitation** – Extract data, maintain access, or create backdoors.
- **Covering Tracks** – Clear logs and traces to avoid detection.
- **Reporting** – Document findings and provide fixes.

5. SQL Injection Methodology

Ans: SQL Injection means tricking the database with smart inputs to get or change secret information.

The attacker **injects SQL code** into a vulnerable input → database executes it → attacker gets unauthorized access.

[User Input Field 📝]

⬇

[Attacker Inserts Malicious SQL Code 💉]

⬇

[Web App Sends Query to Database 💻]

⬇

[Database Executes Malicious Query 🗄️]

⬇

[Attacker Gains Access 🔑]

→ Extract Data (Usernames, Passwords)

→ Bypass Login

→ Modify/Delete Data

6. Explain sql injection with any tool

Ans: SQL Injection means **putting bad SQL code in a website input**.
sqlmap is a tool that does this automatically and shows the hidden data from the database.

- **Find a target** → A website with input like
  http://testphp.vulnweb.com/listproducts.php?cat=1

- **Use sqlmap tool** → Run command:
  sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" --dbs
- **sqlmap tests it** → It checks if the website is vulnerable to SQL Injection.
- **If vulnerable** → sqlmap shows the **database names**.
- **Extract data** → With more commands, attacker can see **tables, usernames, and passwords**.

7.Explain deference between VA And PT

Ans:

- **Vulnerability Assessment (VA)** is the process of scanning and finding all the weaknesses in a system. It tells you **what can go wrong**.
- **Penetration Testing (PT)** is when someone **actually tries to exploit** those weaknesses to see if they can break into the system. It shows **what really can happen if attacked**.

Aspect	Vulnerability Assessment (VA)	Penetration Testing (PT)
Purpose	To identify and list all security weaknesses in a system.	To exploit vulnerabilities to see how an attacker can gain access.
Depth	Focuses on discovering as many vulnerabilities as possible.	Focuses on exploiting selected vulnerabilities to measure real risk.
Approach	Mostly automated using scanning tools.	Manual and automated; simulates real attack scenarios.
Outcome	Provides a list of vulnerabilities with severity levels.	Provides proof of exploitability and the potential impact of attacks.
Frequency	Regular, often scheduled scans.	Less frequent, usually periodic or after major system changes.
Goal	Awareness and prevention.	Testing defenses and response to actual attacks.

- **VA:** (find problems)Finds weaknesses. ☑
- **PT:** (test problems)Exploits weaknesses to test security. ⚠

It’s like: **VA = spotting cracks, PT = trying to break in through cracks.**

8.How to write vulnerability assessment Report

Ans:

1. **Title Page** – Write the report title, company name, assessment date, and your name.
2. **Introduction** – Explain the purpose of the assessment and what systems were checked.
3. **Scope** – Mention which systems, applications, or network parts were included.
4. **Methodology** – Briefly describe how you scanned for vulnerabilities (tools or techniques used).
5. **Findings** – List all vulnerabilities found. For each one, include:

    - Name of vulnerability
    - Description
    - Severity (low, medium, high)
    - Location (system or application affected)

6. **Recommendations** – Suggest steps to fix or reduce each vulnerability.
7. **Conclusion** – Summarize the overall security posture and next steps.
8. **Appendix (Optional)** – Add screenshots, logs, or tool outputs for reference.

9.Explain the Zero Day Attacks

Ans: