**Module 3 : Wab Based Hacking**

**1. Explain MAC Spoofing and Email Spoofing**

* **MAC Spoofing:** Changing a device's MAC address to impersonate another device, bypassing access control measures like MAC filtering.
  + **Purpose:** Evading network restrictions or performing unauthorized activities.
* **Email Spoofing:** Faking the sender’s email address to deceive recipients.
  + **Purpose:** Used in phishing to trick users into providing sensitive information.

**2. Perform Practical of MITM Tool and Social Engineering Tool**

* **MITM Tools:** Use tools like **Ettercap**, **Bettercap**, or **Wireshark** to intercept and manipulate data between two parties.
  + Example: Intercepting HTTP traffic to extract credentials.
* **Social Engineering Tools:** Use tools like **SET (Social Engineering Toolkit)** for phishing simulations.
  + Example: Crafting a fake login page to collect user credentials.

**3. Explain Kali Linux Tool SYN Flooding Attack Using Metasploit**

* SYN Flooding: Overwhelms a target with SYN requests without completing the TCP handshake, causing resource exhaustion.
* **Steps with Metasploit:**
  1. Open Metasploit: msfconsole.
  2. Select module: use auxiliary/dos/tcp/synflood.
  3. Set target IP: set RHOST <target IP>.
  4. Execute: run.

**4. Find Online Email Encryption Service**

Examples of email encryption services:

* **ProtonMail**
* **Tutanota**
* **Hushmail**
* **StartMail**

**5. Types of Firewalls**

1. **Packet Filtering Firewall:** Examines packets and filters based on source/destination IP, port, and protocol.
2. **Stateful Inspection Firewall:** Tracks the state of active connections.
3. **Proxy Firewall:** Acts as an intermediary between users and the web.
4. **Next-Generation Firewall (NGFW):** Combines traditional firewalls with advanced features like DPI and IPS.
5. **Web Application Firewall (WAF):** Protects against web application attacks like SQL injection and XSS.

**6. Explain Evading Firewalls**

Evading firewalls involves bypassing their filtering mechanisms using techniques like:

1. **Tunneling Traffic:** Encapsulating prohibited traffic in allowed protocols (e.g., HTTP tunneling).
2. **Fragmentation:** Breaking malicious payloads into smaller packets to avoid detection.
3. **Using Anonymous Proxies or VPNs:** Masking the source IP address.

**Web-Based Hacking**

**1. What is Session Hijacking? Explain with Techniques**  
Session hijacking involves stealing a user’s session ID to impersonate them on a web application.

* **Techniques:**
  1. **Session Fixation:** Setting a session ID before the user logs in.
  2. **Cross-Site Scripting (XSS):** Injecting malicious scripts to steal cookies.
  3. **Packet Sniffing:** Capturing session IDs over unsecured networks.

**2. Find DoS/DDoS Attack Tools**  
Examples of tools:

* **LOIC (Low Orbit Ion Cannon)**
* **HOIC (High Orbit Ion Cannon)**
* **HULK (HTTP Unbearable Load King)**
* **GoldenEye**

**3. Explain SYN Flooding Attack with Example**  
SYN Flooding overwhelms a server by sending numerous SYN requests without completing the TCP handshake.

* **Example:**
  1. Attacker sends multiple SYN packets.
  2. Target allocates resources for each request but never receives the ACK to complete the handshake.
  3. Resources are exhausted, denying service to legitimate users.

**4. List of Web App Hacking Methodology**

1. Information Gathering.
2. Vulnerability Scanning.
3. Exploitation (e.g., SQL Injection, XSS).
4. Privilege Escalation.
5. Data Exfiltration.

**5. SQL Injection Methodology**

1. Identify vulnerable input fields.
2. Inject malicious SQL code to bypass authentication or retrieve data.
3. Exploit using tools like **sqlmap** or manually test payloads (' OR 1=1 --).

**6. Explain SQL Injection with Any Tool**  
Tool: **sqlmap**

* Steps:
  1. Identify the target URL with a vulnerable parameter.
  2. Run sqlmap -u "<target URL>".
  3. Extract data using options like --dump.

**7. Difference Between VA and PT**

* **Vulnerability Assessment:** Identifies potential vulnerabilities without exploiting them. Focuses on breadth.
* **Penetration Testing:** Actively exploits vulnerabilities to evaluate real-world impact. Focuses on depth.

**8. How to Write a Vulnerability Assessment Report**

1. **Executive Summary:** High-level overview for non-technical stakeholders.
2. **Scope and Methodology:** Describe what was tested and how.
3. **Findings:** List vulnerabilities with severity levels.
4. **Recommendations:** Provide actionable steps to fix issues.
5. **Conclusion:** Summarize overall security posture.

**9. Explain Zero-Day Attacks**  
A **Zero-Day Attack** exploits a vulnerability that is unknown to the vendor or public.

* **Examples:** Attacks exploiting vulnerabilities in software before a patch is released.
* **Prevention:** Implementing strong security measures like EDR (Endpoint Detection and Response) and regular system monitoring.