**Module 30**

**Web server and application base Attacks**

1. Explain MAC spoofing and Email spoofing

1. Ans: **MAC Spoofing**:
   * MAC spoofing, also known as MAC address spoofing, is the practice of changing or falsifying the Media Access Control (MAC) address of a network interface on a device.
   * The MAC address is a unique identifier assigned to a network interface controller (NIC) by the manufacturer and is used for communication within a local network.
   * MAC spoofing is often used for malicious purposes, such as bypassing MAC address filtering on a network, impersonating another device on the network, or conducting man-in-the-middle (MITM) attacks.
   * By spoofing a valid MAC address, an attacker can deceive network devices into accepting traffic from the attacker's device as if it were from the legitimate device with the spoofed MAC address.

**Email Spoofing**:

* Email spoofing is the forging of email headers to make an email message appear as if it originated from a different sender than the actual sender.
* Email spoofing does not require access to the sender's email account but instead manipulates the email's header information, including the "From" field, to mislead the recipient into believing that the email is from a trusted source.
* Email spoofing is often used in phishing attacks, where attackers send fraudulent emails pretending to be from reputable organizations in an attempt to trick recipients into revealing sensitive information or performing actions that benefit the attacker.

2. Perform practical of MITM tool and social engineering Tool

* Ans: Due to the potentially unethical and illegal nature of performing man-in-the-middle (MITM) attacks and social engineering attacks without proper authorization, it is important to emphasize responsible and ethical hacking practices.
* It is strongly recommended to obtain proper authorization and permission before conducting any security assessments, penetration testing, or ethical hacking activities on a network or system that you do not own or manage.
* Tools commonly used for MITM attacks include Ettercap, Wireshark, and Bettercap. These tools allow attackers to intercept, modify, and redirect traffic between two communicating parties.
* Social engineering tools such as SET (Social Engineering Toolkit) can be used to simulate phishing attacks, create malicious websites, and exploit human vulnerabilities to gain unauthorized access to systems or information.

3. Explain Kali Linux tool SYN Flooding Attack using Metasploit

* Ans: SYN flooding is a type of Denial-of-Service (DoS) attack where an attacker sends a large number of TCP SYN requests to a target server, overwhelming the server's resources and preventing it from responding to legitimate requests.
* In Kali Linux, the Metasploit Framework includes modules that can be used to conduct SYN flooding attacks.
* The specific module for conducting SYN flooding attacks using Metasploit is **auxiliary/dos/tcp/synflood**.
* To use this module, you would first start Metasploit by running the **msfconsole** command in the terminal, load the SYN flooding module, configure the target IP address and port, and then execute the attack.

4. Find online email encryption service

Ans: **Online Email Encryption Service**:

* There are several online email encryption services available, including:
  + ProtonMail
  + Tutanota
  + Hushmail
  + Virtru
  + Mailfence
* These services offer end-to-end encryption for email communication, ensuring that only the intended recipient can decrypt and read the encrypted emails.

5. Types of Firewalls

Ans: **Types of Firewalls**:

* There are several types of firewalls, including:
  + Network firewalls: These are traditional firewalls that filter traffic based on IP addresses, port numbers, and protocols.
  + Application layer firewalls: These firewalls operate at the application layer of the OSI model and can inspect and filter traffic based on application-specific data.
  + Proxy firewalls: Proxy firewalls act as intermediaries between internal and external networks, filtering and forwarding traffic on behalf of clients.
  + Next-generation firewalls (NGFWs): NGFWs combine traditional firewall functionality with advanced features such as intrusion prevention, application awareness, and deep packet inspection.
  + Stateful inspection firewalls: These firewalls maintain a state table of active connections and use this information to make filtering decisions, providing better security than traditional packet filtering firewalls.

6. Explain Evading Firewalls

Ans: **Evading Firewalls**:

* Evading firewalls involves techniques to bypass or circumvent firewall restrictions to gain unauthorized access to a network or system.
* Common methods of evading firewalls include:
  + Tunneling: Using protocols such as SSH or VPNs to encapsulate and encrypt traffic, making it difficult for firewalls to inspect.
  + Fragmentation: Breaking packets into smaller fragments to bypass packet inspection rules.
  + Protocol evasion: Exploiting weaknesses in protocol handling to pass through firewall filters undetected.
  + Application-layer evasion: Crafting packets or payloads to exploit vulnerabilities in application-layer protocols and bypass firewall filtering mechanisms.
* It's important for organizations to regularly update their firewall configurations and rulesets to mitigate the risk of firewall evasion techniques. Additionally, implementing intrusion detection and prevention systems (IDPS) can help
* **Web Based Hacking**

1. What is Session Hijacking Explain with Techniques?

**Ans: Session Hijacking**: Session hijacking is a type of attack where an attacker takes control of a legitimate user's session on a computer system or network service. The attacker can exploit vulnerabilities or weaknesses in the session management mechanism to impersonate the legitimate user and perform unauthorized actions. There are several techniques used in session hijacking:

* + **Session Fixation**: The attacker forces the victim to use a predetermined session identifier, which the attacker already knows. This can occur through various means, such as providing the victim with a malicious URL containing the session identifier or through social engineering techniques.
  + **Session Sniffing**: The attacker monitors network traffic to capture session cookies or tokens exchanged between the client and server. This can be accomplished using packet sniffing tools like Wireshark or by exploiting vulnerabilities in the network infrastructure.
  + **Session Sidejacking**: The attacker intercepts and steals the session identifier or authentication token from an insecure communication channel, such as unencrypted HTTP traffic. This can be achieved using tools like Firesheep or by exploiting vulnerabilities in web applications.
  + **Session Replay**: The attacker captures a legitimate user's session data and replays it to gain unauthorized access to the system. This can be mitigated by implementing mechanisms like session expiration and one-time tokens.
  + **Cross-site Scripting (XSS)**: In a cross-site scripting attack, the attacker injects malicious scripts into a web application, which are then executed in the context of the victim's session. This allows the attacker to steal session cookies or perform actions on behalf of the victim.

2. Find DoS/DDoS Attack Tools

**Ans: DoS/DDoS Attack Tools**: Some tools commonly used for conducting Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks include:

* + LOIC (Low Orbit Ion Cannon)
  + HOIC (High Orbit Ion Cannon)
  + XerXes
  + Slowloris
  + hping
  + RUDY (R-U-Dead-Yet)
  + GoldenEye
  + PyLoris

3. Explain SYN Flooding Attack with example

**Ans: SYN Flooding Attack**: SYN flooding is a type of DoS attack that exploits the three-way handshake mechanism in the TCP protocol. Here's how it works:

* + The attacker sends a large number of TCP SYN (synchronization) packets with spoofed source IP addresses to the target server.
  + The target server responds to each SYN packet with a SYN-ACK (synchronization-acknowledgment) packet and allocates resources to handle the connection.
  + However, because the source IP addresses in the SYN packets are spoofed, the target server never receives the expected ACK (acknowledgment) packets to complete the three-way handshake.
  + As a result, the target server's resources become exhausted as it waits for ACK packets that never arrive, leading to a denial of service for legitimate users.

4. List of Web App Hacking Methodology

**Ans: Web App Hacking Methodology**: A comprehensive web application hacking methodology typically includes the following steps:

* + Information Gathering
  + Configuration Management Testing
  + Identity Management Testing
  + Authentication Testing
  + Authorization Testing
  + Session Management Testing
  + Data Validation Testing
  + Cryptography Testing
  + Business Logic Testing
  + Client-Side Testing
  + Server-Side Testing
  + Business Logic Testing
  + Client-Side Testing
  + Server-Side Testing
  + Error Handling
  + API Testing

5. SQL Injection Methodology

**Ans: SQL Injection Methodology**: SQL injection is a type of attack where an attacker injects malicious SQL queries into input fields or parameters of a web application to manipulate the database or execute arbitrary SQL commands. The methodology for performing SQL injection includes:

* + Information Gathering
  + Identification of Injection Points
  + Exploitation of Injection Points
  + Extraction of Data
  + Post-exploitation Activities
  + Prevention and Remediation

6. Explain SQL injection with any tool

**Ans: SQL Injection with Tool**: SQLMap is a popular tool used for automating the detection and exploitation of SQL injection vulnerabilities in web applications. It allows testers to identify SQL injection vulnerabilities, extract database schema and data, and execute arbitrary SQL commands. To perform SQL injection using SQLMap, you would typically:

* + Identify a vulnerable input field or parameter in the target web application.
  + Use SQLMap to scan the target URL and identify SQL injection vulnerabilities.
  + Exploit the identified vulnerabilities to extract database schema and data or execute arbitrary SQL commands.
  + SQLMap provides various options and parameters to customize the scanning and exploitation process, allowing testers to perform comprehensive SQL injection testing.