**Module 30:**

**Web server and application base Attacks**

* 1. Explain MAC spoofing and Email spoofing

MAC spoofing and email spoofing are two different types of cyber attacks that involve disguising one's identity to gain unauthorized access or deceive a recipient.

MAC spoofing involves changing the Media Access Control (MAC) address of a device, which is a unique identifier assigned to each network interface. By changing the MAC address, an attacker can make it appear as if their device is actually a different device on the network, allowing them to bypass access controls and security measures that are based on MAC addresses. This can be particularly dangerous if the attacker gains access to a network that contains sensitive information or resources.

Email spoofing, on the other hand, involves sending an email that appears to come from a different sender than the actual sender. This is often done by altering the email header information, such as the From address, to make it look like the email came from a trusted source. Email spoofing can be used to launch phishing attacks, where the attacker tries to trick the recipient into divulging sensitive information or clicking on a malicious link.

Both MAC spoofing and email spoofing can be used to gain unauthorized access, steal information, or launch other types of attacks. It is important to be aware of these threats and take steps to protect against them, such as using strong authentication mechanisms and verifying the authenticity of emails before responding to them.

* 1. Perform practical of MITM tool and social engineering Tool

A Man-In-The-Middle (MITM) attack involves intercepting communication between two parties and altering the data exchanged between them. This type of attack can be carried out using various tools, such as Ettercap, Cain and Abel, or Wireshark, which can capture and analyze network traffic, and even modify it in real-time. MITM attacks can be used to steal sensitive information, such as login credentials, banking details, or personal data, or to inject malware or other malicious code into the target system.

Social engineering is a tactic that involves manipulating people into divulging sensitive information or taking an action that benefits the attacker. Social engineering attacks can be carried out using various tools and techniques, such as phishing emails, phone calls, or messages, pretexting, baiting, or impersonation. Some common social engineering tools include SET (Social Engineering Toolkit), BeEF (Browser Exploitation Framework), or Maltego, which can automate and streamline the process of creating and delivering social engineering attacks.

It is important to note that the use of MITM and social engineering tools for malicious purposes is illegal and unethical. Such tools should only be used for legitimate and authorized testing and security purposes, with proper permissions and precautions.

* 1. Explain Kali linux tool SYN Flooding Attack using Metasploit

Kali Linux is a popular distribution of the Linux operating system that is commonly used for penetration testing and security auditing. It comes pre-installed with a variety of security tools, including Metasploit, which is a powerful framework for developing and executing exploits against vulnerable systems.

SYN flooding is a type of Denial-of-Service (DoS) attack that targets the TCP/IP handshake process by overwhelming the target system with a flood of SYN packets. The attacker sends a large number of SYN packets to the target system, each with a spoofed source IP address, and without completing the full three-way handshake process. This can cause the target system to run out of resources trying to keep track of all the incomplete connections, leading to degraded performance or complete failure.

Metasploit includes several modules that can be used to launch SYN flooding attacks against vulnerable systems. One such module is the "auxiliary/dos/tcp/synflood" module, which sends a large number of SYN packets to a target system. This module allows the attacker to specify the target IP address, the source IP address, and other parameters, such as the number of packets to send and the interval between packets.

To launch a SYN flooding attack using Metasploit, the attacker would first open the Metasploit console and select the "auxiliary/dos/tcp/synflood" module. They would then set the target IP address and other parameters as needed and run the module. The module would then send a flood of SYN packets to the target system, potentially causing it to become unresponsive.

It is important to note that SYN flooding attacks are illegal and unethical unless they are carried out with proper authorization and consent for legitimate security testing purposes. It is also important to take appropriate precautions to prevent unintended harm or disruption to innocent parties or systems.

* 1. Find online email encryption service

There are several online email encryption services available, some of which include:

ProtonMail - A popular email service that offers end-to-end encryption and allows users to send encrypted messages to non-ProtonMail users as well.

Tutanota - Another secure email service that provides end-to-end encryption and supports sending encrypted messages to non-Tutanota users.

Hushmail - A secure email service that offers end-to-end encryption and provides HIPAA-compliant email for healthcare professionals.

Mailfence - A secure and private email service that offers end-to-end encryption, digital signing, and supports OpenPGP encryption.

StartMail - An email service that offers end-to-end encryption, two-factor authentication, and supports sending encrypted messages to non-StartMail users.

It is important to note that while these services can provide secure email encryption, the recipient must also be using a compatible encryption system to receive and read the encrypted message.There are several online email encryption services available, some of which include:

ProtonMail - A popular email service that offers end-to-end encryption and allows users to send encrypted messages to non-ProtonMail users as well.

Tutanota - Another secure email service that provides end-to-end encryption and supports sending encrypted messages to non-Tutanota users.

Hushmail - A secure email service that offers end-to-end encryption and provides HIPAA-compliant email for healthcare professionals.

Mailfence - A secure and private email service that offers end-to-end encryption, digital signing, and supports OpenPGP encryption.

StartMail - An email service that offers end-to-end encryption, two-factor authentication, and supports sending encrypted messages to non-StartMail users.

It is important to note that while these services can provide secure email encryption, the recipient must also be using a compatible encryption system to receive and read the encrypted message.There are several online email encryption services available, some of which include:

ProtonMail - A popular email service that offers end-to-end encryption and allows users to send encrypted messages to non-ProtonMail users as well.

Tutanota - Another secure email service that provides end-to-end encryption and supports sending encrypted messages to non-Tutanota users.

Hushmail - A secure email service that offers end-to-end encryption and provides HIPAA-compliant email for healthcare professionals.

Mailfence - A secure and private email service that offers end-to-end encryption, digital signing, and supports OpenPGP encryption.

StartMail - An email service that offers end-to-end encryption, two-factor authentication, and supports sending encrypted messages to non-StartMail users.

* 1. Types of Firewall

Firewalls are network security systems that monitor and control incoming and outgoing traffic based on a set of predefined security rules. There are several types of firewalls, including:

Packet-filtering Firewall: This type of firewall filters traffic based on the source and destination addresses, port numbers, and protocols of individual packets. It can be configured to allow or block packets based on specific criteria.

Circuit-level Firewall: This type of firewall operates at the session layer of the OSI model and monitors the establishment of TCP connections. It does not inspect the packet contents, but rather determines whether a connection should be allowed based on the source and destination addresses and port numbers.

Stateful Firewall: A stateful firewall operates at the network layer of the OSI model and keeps track of the state of network connections. It can differentiate between legitimate and unauthorized traffic by analyzing the packet contents and matching them against known state information.

Application-level Firewall: An application-level firewall, also known as a proxy firewall, operates at the application layer of the OSI model and can filter traffic based on the application protocol. It can inspect and filter traffic at the application layer, providing more granular control over network traffic.

Next-Generation Firewall: A next-generation firewall combines traditional firewall capabilities with additional security features, such as intrusion prevention, deep packet inspection, and advanced threat protection. It can provide more comprehensive protection against modern threats and attacks.

* 1. Explain Evading Firewalls

Evading firewalls is a technique used to bypass or circumvent network security systems such as firewalls, intrusion detection and prevention systems (IDPS), and other security measures. The goal of evading firewalls is to gain unauthorized access to a network or system, exfiltrate sensitive data, or launch an attack.

There are several techniques that can be used to evade firewalls, including:

Protocol Obfuscation: This technique involves altering the characteristics of network traffic to make it more difficult for firewalls to identify and block. This can be done by using non-standard ports, modifying packet headers, or using encryption to hide the contents of network traffic.

Traffic Fragmentation: Traffic fragmentation involves breaking up large packets into smaller ones to evade deep packet inspection (DPI) by firewalls. This can be done by sending data in small fragments or using tools that automatically fragment traffic.

IP Spoofing: IP spoofing involves modifying the source IP address of packets to make them appear to come from a trusted source or a legitimate internal IP address. This can be used to bypass firewall rules that are based on IP address filtering.

Tunneling: Tunneling involves encapsulating network traffic within another protocol to bypass firewall filtering. This can be done by using VPNs, SSH tunnels, or other tunneling protocols.

Covert Channels: Covert channels are hidden communication channels that can be used to transmit data undetected by firewalls or other security systems. This can be done by hiding data within seemingly innocuous network traffic, such as DNS requests or HTTP headers.

* Web Based Hacking

1. What is Session Hijacking Explain with Techniques?

Session hijacking is a type of network attack in which an attacker takes control of a valid user session in order to gain unauthorized access to a system or application. Session hijacking attacks typically involve intercepting and stealing session tokens or cookies, which are used to authenticate and maintain a user's session on a web application.

There are several techniques used in session hijacking attacks, including:

Packet Sniffing: An attacker can use packet sniffing tools to intercept and capture network traffic between the client and server. By analyzing the captured packets, the attacker can extract session tokens or cookies used to authenticate the user and use them to impersonate the user.

Cross-Site Scripting (XSS): XSS attacks involve injecting malicious scripts into a website that are executed when a user visits the website. By exploiting vulnerabilities in the website's code, the attacker can steal session tokens or cookies from the user's browser.

Man-in-the-Middle (MITM) Attacks: In MITM attacks, an attacker intercepts traffic between the client and server and can modify or steal session tokens or cookies to hijack the user's session.

Session Fixation: In a session fixation attack, the attacker sets a valid session ID for the user before they log in to the web application. The attacker then waits for the user to log in and use the application, at which point they can use the pre-set session ID to hijack the user's session.

Session Sidejacking: In session sidejacking, the attacker uses a packet sniffer or other tool to intercept session tokens or cookies transmitted over an unencrypted Wi-Fi network or other insecure network. By stealing the session token or cookie, the attacker can hijack the user's session.

To protect against session hijacking attacks, it is important to use secure authentication mechanisms, such as multi-factor authentication and HTTPS encryption, and to regularly monitor and audit network traffic for suspicious activity. Web application developers should also follow best practices for secure coding, such as using frameworks that automatically handle session management and avoiding the use of session tokens in URLs.

1. Find DoS/DDoS Attack Tools

[Denial-of-service](https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/) (DoS) and [distributed denial-of-service](https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/) (DDoS) attacks are malicious attempts to disrupt the normal operations of a targeted server, service, or network by overwhelming it with a flood of Internet traffic.

DoS attacks accomplish this disruption by sending malicious traffic from a single machine — typically a computer. They can be very simple; a basic [ping flood attack](https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/) can be accomplished by sending more [ICMP (ping) requests](https://www.cloudflare.com/learning/ddos/glossary/internet-control-message-protocol-icmp/) to a targeted server than it is able to process and respond to efficiently.

DDoS attacks, meanwhile, use more than one machine to send malicious traffic to their target. Often, these machines are part of a [botnet](https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/) — a collection of computers or other devices that have been infected with [malware](https://www.cloudflare.com/learning/ddos/glossary/malware/) and can thus be controlled remotely by an individual attacker. In other circumstances, multiple individual attackers launch DDoS attacks by working together to send traffic from their individual computers.

DDoS attacks are more prevalent and damaging in the modern Internet for two reasons. First, modern security tools have evolved to stop some ordinary DoS attacks. Second, DDoS attack tools have become relatively cheap and easy to operate.

1. Explain SYN Flooding Attack with example

A SYN flooding attack is a type of denial of service (DoS) attack in which an attacker floods a target server with a large number of spoofed TCP SYN packets, overwhelming the server's ability to respond to legitimate requests. This can cause the server to crash or become unresponsive, effectively denying service to legitimate users.

Here is an example of how a SYN flooding attack might be executed:

The attacker sends a large number of spoofed TCP SYN packets to the target server, each containing a fake source IP address.

The server responds to each SYN packet with a SYN-ACK packet, which is intended to establish a connection with the client.

However, because the source IP address of the SYN packets is spoofed, the server is unable to establish a connection and waits for the client to respond with an ACK packet.

Since the attacker does not respond with an ACK packet, the server keeps the half-open connection in its memory, waiting for the ACK packet to arrive. As the number of half-open connections increases, the server's memory and processing resources become overwhelmed.

Eventually, the server is unable to accept any new legitimate connection requests, and legitimate users are unable to access the server's resources.

To protect against SYN flooding attacks, network administrators can implement measures such as SYN cookies, which are used to mitigate the impact of SYN flooding attacks by sending a cookie to the client instead of keeping the half-open connection in memory. Additionally, network administrators can implement rate limiting or traffic filtering to block suspicious traffic and reduce the impact of such attacks.

1. List of Web App Hacking Methodology

Web application hacking methodology typically involves the following steps:

Information Gathering: Collecting information about the target application, such as the operating system, web server, application server, programming languages used, and any known vulnerabilities.

Configuration Management Testing: Testing the target application's configuration, such as the presence of default or weak passwords, open ports, and unsecured directories.

Authentication Testing: Testing the target application's authentication mechanism, such as password policies, cookie manipulation, and session hijacking.

Session Management Testing: Testing the target application's session management mechanism, such as session fixation, session hijacking, and cookie tampering.

Authorization Testing: Testing the target application's authorization mechanism, such as directory traversal, privilege escalation, and access control testing.

Input Validation Testing: Testing the target application's input validation mechanism, such as SQL injection, cross-site scripting (XSS), and command injection.

Error Handling Testing: Testing the target application's error handling mechanism, such as error message leakage, stack trace disclosures, and error code enumeration.

Cryptography Testing: Testing the target application's cryptographic mechanisms, such as encryption, decryption, key management, and secure communication channels.

Business Logic Testing: Testing the target application's business logic, such as logic flaws, race conditions, and code injection.

Client-Side Testing: Testing the target application's client-side mechanisms, such as JavaScript code, client-side validation, and DOM manipulation.

Overall, web application hacking methodology involves a comprehensive approach to identifying and exploiting vulnerabilities in web applications, which requires a combination of technical skills, experience, and knowledge of common web application vulnerabilities and attack techniques. It is important to always use this knowledge ethically and responsibly and to obtain proper legal permission before performing any security testing or hacking.

1. SQL Injection Methodology

SQL injection is a type of web application vulnerability that occurs when an attacker is able to inject malicious SQL statements into a web application's database. This can allow the attacker to access sensitive information, modify or delete data, or even take control of the web application.

The SQL injection methodology typically involves the following steps:

Information Gathering: The attacker gathers information about the target web application, such as the underlying database technology and the structure of the database.

Identification of Injection Points: The attacker identifies potential injection points in the target application, such as input fields, cookies, or URL parameters.

Injection of Malicious Code: The attacker injects malicious SQL statements into the injection points identified in step 2. This can include UNION SELECT statements, which allow the attacker to extract data from the database, or DROP TABLE statements, which allow the attacker to delete data.

Exploitation of Vulnerabilities: Once the attacker has successfully injected malicious SQL code, they can begin to exploit vulnerabilities in the web application, such as extracting sensitive information, modifying or deleting data, or even taking control of the web application.

Covering Tracks: Finally, the attacker may attempt to cover their tracks by deleting log files or other evidence of their activities.

To protect against SQL injection attacks, web application developers and administrators can implement measures such as input validation, parameterized queries, and access control. Additionally, web application scanners can be used to automatically identify potential SQL injection vulnerabilities and provide guidance on how to remediate them.

1. Explain sql injection with any tool

SQL injection is a type of web application vulnerability that occurs when an attacker is able to inject malicious SQL statements into a web application's database. This can allow the attacker to access sensitive information, modify or delete data, or even take control of the web application.

One tool that can be used to demonstrate SQL injection is SQLMap. SQLMap is a powerful and user-friendly tool that automates the process of detecting and exploiting SQL injection vulnerabilities in web applications.

To demonstrate SQL injection using SQLMap, follow these steps:

Download and install SQLMap from the official website.

Identify a target web application that is vulnerable to SQL injection. This can be done using manual testing or automated scanning tools such as Burp Suite.

Once a vulnerable target has been identified, launch SQLMap and specify the target URL as the input.

SQLMap will automatically detect any SQL injection vulnerabilities and provide options for exploiting them. For example, SQLMap may offer to extract data from the database, modify or delete data, or even take control of the web application.

Select the desired option and follow the prompts provided by SQLMap to carry out the attack.

It is important to note that SQL injection attacks can be illegal if performed without proper authorization. Always obtain legal permission before performing any security testing or hacking.