Week 03:

**SNIFFERS** / network sniffer / packet sniffer / network analyser.

- An application or device designed to capture, or "sniff," network traffic as it moves across the network - analysing network traffic, troubleshooting.

- Capable of capturing various types of information - email passwords, FTP credentials, email contents, and transferred files.

- Works by putting a network adapter into **promiscuous mode** (also called monitor mode), allowing it to capture all traffic it can hear, regardless of the destination address.

In **normal mode**, a network adapter drops or ignores any packet not intended for it.

**SNIFFERS THREATS TO PROTOCOLS**

1. Telnet: Keystrokes transmitted over Telnet; can be easily sniffed; does not encrypt the data being transmitted, making it vulnerable to interruption.

2. Hypertext Transfer Protocol (HTTP): Designed to send information in plain text; without encryption, HTTP is susceptible to sniffing attacks as the data transmitted over HTTP can be easily intercepted and read by sniffers.

3. Simple Mail Transfer Protocol (SMTP): SMTP is commonly used for transferring email messages, but it does not include protection against sniffing.

4. Post Office Protocol (POP): POP is designed to retrieve email from servers, but it also lacks protection against sniffing.

5. File Transfer Protocol (FTP): FTP is used for transferring files, and all transmissions are sent in clear text without encryption.

**PASSIVE SNIFFING**

* Eavesdropping on / monitoring transmission
* Make use of the info but not affect system.
* Difficult to detect.
* Done very easily.
* Internal network

**ACTIVE SNIFFING**

* Send packets to targets to extract sensitive data.
* Involves injecting malicious code into target system.
* To take control or steal sensitive information.

**PASSIVE ATTACKS-HTTP BASIC AUTHENTICATION**

- A simple challenge and response mechanism used by servers to request authentication information (such as a username and password) from clients.

- The client passes the authentication information to the server in an Authorization header.

- Insecure because the full credentials (username and password) are transmitted over the network in plain text, making them susceptible to interception by attackers.

**DNS ATTACKS-DNS PHARMING** - An attacker attempts to change the IP associated with a server maliciously.

**DNS ATTACKS-DNS CACHE POISONING**

DNS cache poisoning is a malicious attack where false DNS records are inserted into the cache of a DNS resolver.

Here are the **main methods** of DNS cache poisoning:

1. Redirecting the attacker's domain nameserver to the target domain's nameserver and assigning a fake IP address to the target nameserver.

2. Redirecting the nameserver of an unrelated domain to a fake nameserver controlled by the attacker.

3. "Racing" the real nameserver to provide false information to the resolver before the legitimate response arrives.

DNS cache poisoning **can occur** when a nameserver:

- Disregards identifiers - allowing attackers to inject false responses without proper validation.

- Has predictable ids - making it easier for attackers to guess and spoof responses.

- Accepts unsolicited DNS records - allowing attackers to send forged DNS responses without a corresponding request.

**SESSION HIJACKING**

* Session hijacking is a type of attack that exploits vulnerabilities in network communication.
* Builds on sniffing the network.
* The attacker's goal is to not only monitor ongoing sessions but also to take over a session that has authenticated access to a resource.
* Occurs when attackers exploit a valid session to gain unauthorized access to a system, information, or service.
* Attackers target the authentication process, which typically occurs at the beginning of a session, allowing session hijacking to occur after authentication.
* Relies on a basic understanding of how messages and their packets flow over the Internet.

\*\* A security analyst is investigating an attack. An intruder managed to take over the identity of a user who was legitimately logged in to Gwen's company's website by manipulating Hypertext Transfer Protocol (HTTP) headers. Which type of attack likely took place? Session hijacking

In a session hijacking attack, an attacker takes control of or modifies any communications between two hosts by:

- Placing themselves between Party A and Party B.

- Monitoring the flow of packets using sniffing techniques.

- Analysing and predicting the sequence number of the packets.

- Sever the connection between the two parties.

- Seizing control of the session.

- Performing packet injection into the network.

To identify an active session:

1. Attacker must locate and identify a suitable session for hijacking.
2. Guess the sequence numbers to hijack a session.

**SEQUENCE NUMBER PREDICTION** is a crucial aspect of session hijacking:

- When a client initiates a connection with a server by sending a SYN packet, the server responds with a SYN/ACK packet.

- The client then sends an ACK packet to acknowledge the SYN/ACK packet and complete the three-way handshake.

- During this handshake, the starting sequence number for the session is assigned by the server using a random method, if supported by the operating system.

If the sequence number generation algorithm is predictable or if the attacker can accurately guess the sequence numbers, they can initiate a connection to the server with a legitimate address. Subsequently, the attacker can open a second connection from a forged address, allowing them to hijack the session successfully.

To maintain control over the session and prevent the legitimate client from sending new data that could shift sequence numbers forward, the attacker needs to disrupt or delay the client's communication. This could involve launching a denial-of-service (dos) attack against the client or sending packets to the server before the client does, effectively "holding down" the client.

Session hijacking exploits the lack of ongoing session security.

Attacks categorized into: Man-in-the-Middle, Blind Hijack, Session Theft. - These attacks compromise data integrity and user privacy.

**MAN IN THE MIDDLE ATTACK (MITM)**

1. Attacker ***intercepts all communications*** between two hosts.

2. Attacker positions themselves to manipulate the communication between client and server to flow.

3. Which also allows them to modify the communication

4. Target protocols often ***rely on public key exchange*** to protect communication (e.g., ARP (Address Resolution Protocol) and DNS (Domain Name System)).

**BLIND HIJACK ATTACK**

1. Attacker ***injects data***, including malicious commands, into communications.

2. Named "blind" because attacker ***can't see responses to injected data***.

3. Attacker's effectiveness relies on successful injection despite lack of response visibility.

4. ***Still very effective***

**SESSION REPLAY ATTACK / SESSION THEFT ATTACK**

1. Attacker ***neither intercepts nor injects data into existing communications***.

2. Attacker ***creates new sessions or utilizes old ones***.

3. Involves repeating sessions.

4. Common at the application level, like in web applications.

**PORT SCANNING**

Port scanning is a network reconnaissance technique used to discover open ports on a target system.

1. Ping Scan: **Sends ICMP** echo request to destination device to check device availability. Returns ICMP echo reply if active.

2. Connect Scan: Fully connected to target IP and port in TCP handshake. **Reliable but noisy.**

3. SYN Scan / half-open: sends SYN requests to gather info about open ports without completing TCP handshake. **Resets handshake upon identification**.

4. FIN Scan: Sends FIN packet to target. No response if port not listening. **Error response** received if listening.

**PORT KNOCKING**

Act of attempting to make connections to blocked ports in a certain order to open a port.

Very susceptible to replay attacks. Recorded knocking attempts can be repeated to open the port again.

Secure against brute force attacks since there are 65536k combinations, where k is the number of ports knocked.

Time-dependent knock sequences can help protect against replay attacks by introducing time-based elements into the sequence.

**NETWORK LAYER ATTACKS.**

**IP VULNERABILITIES**

1. Unencrypted Transmission: Eavesdropping possible during routing due to lack of encryption.

2. No Source Authentication: Sender can spoof source address, making packet tracing difficult.

3. No Integrity Checking: Packets can be modified en-route, enabling content forgeries and man-in-the-middle attacks.

4. No Bandwidth Constraints: Large number of packets can be injected to launch denial-of-service attacks.

**IP SPOOFING ATTACKS -** Intruder sends packets from one IP address that appear to originate from another.

Server might behave maliciously, thinking it's receiving messages from the real source after authenticating a session.

Types of IP Spoofing:

- Blind Spoofing: Spoof IP address without essentially knowing the ACK sequence pattern.

- Non-Blind Spoofing: Spoof IP address after identifying correct ACK sequence.

The spoofed IP cannot exist with another user on the network.

Successful IP spoofing requires the spoofed IP to not exist on the network. In non-blind IP spoofing, attackers often conduct a Denial-of-Service attack on the genuine client, rendering them unavailable.

For non-blind spoofing, the attacker would:

* Analyse the network packets using a packet sniffer,
* Determine the ACK sequence pattern.
* Spoof the IP of an actual client and send packets with the correct sequenced acknowledgment number.

Using forged source addresses is known as **Source address spoofing.**

For an attacker to hijack a TCP session, they need to –

* Inject data into the session before the client sends its next packet.
* Spoof the client's IP address.
* Determine the correct sequence number the server is expecting from the client.

**DATA LINK LAYER ATTACKS**

**MAC FLOODING -** To flood the switch with fake MAC addresses to all ports.

Overwhelms the switch's Content Addressable Memory (CAM), causing it to switch failing.

It is used to build a lookup table. Tracks which MAC addresses are present on which ports on the switch. Facilitates correct traffic routing to ports and hosts.

MAC flooding is considered an active sniffing attack.

**MAC FILTERING -** The network administrator can create a **block** or **allow** lists of MAC addresses to certain network. This is called MAC Filtering. Wireless networks use MAC filtering to only permit certain devices to connect.

**MAC SPOOFING -** Impersonates another machine's MAC address.

Steps:

Find MAC address of target machine using a packet sniffer.

Reconfigure MAC address of rogue machine.

Turn off or unplug target machine.

MAC filtering is easily bypassed by spoofing MAC addresses, rendering it ineffective.

**ARP SPOOFING -** ARP spoofing, also known as ARP poisoning, is a type of cyber-attack where an attacker sends falsified Address Resolution Protocol (ARP) messages over a local area network.

ARP table is updated whenever an ARP response is received.

Requests are not tracked.

ARP announcements are not authenticated.

Machines trust each other.

A rogue machine can spoof other machines.

**ARP POISONING -** A method of bypassing a switch where sniffing is performed on an IPv4 network. Attacker attaches itself to the network with a valid IP address and a spoofed MAC address from the switch's ARP table stored in the Content Addressable Memory (CAM).

ARP poisoning is an active sniffing attack on IPv4 networks.

ARP cache updates whenever it receives an ARP reply, regardless of sending an ARP request.

Attacker may inject data and hope it's received before the client can send new data or launch a Denial of Service (DoS) attack on the client.

**Denial of Service attacks -** Most common types of attacks. It prevents legitimate users from accessing the system.

A form of attack on the availability of some service.

aimed to consume resources but may also involve actual disruption of a service or server.

overwhelms a network connection from a single source.

The idea is that computers have physical limitations.

* Number of users
* Size of files
* Speed of transmission
* Amount of data stored.

**DISTRIBUTED DENIAL OF SERVICE ATTACK**

A DoS attack aims to disrupt access to network resources for legitimate users.

In a distributed denial of service (DDoS) attack, this goal is amplified by utilizing multiple compromised hosts.

DDoS attack employs numerous intermediary hosts to generate sufficient traffic to disrupt targeted servers or entire network segments.

Detecting DDoS attacks poses challenges due to the traffic originating from multiple IP addresses, making it harder to identify until significant disruption has already occurred.

Top of Form

Bottom of Form

**CHARACTERISTICS OF DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS:**

- Utilizes hundreds or thousands of systems to carry out the attack, - coordinated through botnets or networks of compromised devices.

- Involves primary and secondary victims of the DDoS attack, with the primary victim being the target and secondary victims being devices unwittingly used to strengthen the attack.

- Tracking the source of a DDoS attack can be challenging or even impossible due to the distributed nature of the attack and the use of compromised systems.

- Defending against DDoS attacks is difficult, and the impact is typically higher than that of a traditional Denial of Service (DoS) attack due to the sheer number of attackers involved.

**DOS/DDOS ATTACKS: EXPLOITATION OF PROGRAMMING DEFECTS**

- The Ping of Death (PoD):

Unable to handle oversized packets.

Some systems are unable to handle such large packets, and when they attempt to reassemble the fragmented packets, they may crash due to buffer overflow vulnerabilities. [maximum size (65,536 bytes) ]

- Teardrop Attack: Sends malformed packets with adjusted offset values, causing overlaps when reconstructed by the victim system.

This can lead to crashes or system locks, especially on systems unable to handle such issues.

- Land DoS: Sends packets with the same source and destination address and port to the victim's system. Systems incapable of processing this may crash when receiving such packets.

**DOS/DDOS ATTACKS: CONSUMPTION OF RESOURCES**

**SYN FOOD**

* Uses forged packets with the SYN flag set.
* attacker sends many TCP connection requests (SYN packets) to the victim's system but does not complete the handshake process.
* the victim's system becomes overwhelmed with half-open connections, exhausting its resources and making it unable to handle legitimate requests.

**ICMP FLOOD:**

- This type of attack involves flooding the victim's system with a large volume of ICMP (Internet Control Message Protocol) packets.

There are two variants:

- **Smurf Attack:** The attacker sends ICMP echo request packets (pings) to the broadcast address of a network, with the victim's IP address spoofed as the source address. This causes all hosts on the network to respond to the victim, overwhelming its resources.

- **Ping Flood:** Like a Smurf attack, but instead of targeting the broadcast address, the attacker sends ICMP echo request packets directly to the victim's IP address, causing it to become overwhelmed with responses. Simple attack.

**REFLECTED ATTACK:**

- The attacker spoofs or forges the source address of packets or requests and sends them to numerous systems.

- These systems, believing the requests are legitimate, respond to them, flooding the target system with responses.

- This attack is like a ping flood attack but on a larger scale.

**DHCP STARVATION:**

- This attack aims to exhaust the address space allocated by DHCP (Dynamic Host Configuration Protocol) servers.

- The attacker floods the network with DHCP request packets, causing the DHCP servers to allocate all available IP addresses.

- As a result, legitimate devices on the network are unable to obtain IP addresses, effectively denying them network access.

- "The Gobbler" is likely an example of a tool - will do this for the attacker to easily commit this type of attack.

**HTTP FLOOD:**

- In an HTTP flood attack, the attacker bombards a web server with a large volume of HTTP requests.

- This consumes considerable server resources, such as CPU and memory, and can overload the server's capacity to handle connections.

- **SLOWLORIS** is a variant of this attack that aims to monopolize server resources by sending HTTP requests that never complete, tying up server connections indefinitely.

- These attacks often utilize legitimate HTTP traffic, making them harder to detect and mitigate.

**BOTNETS** are networks of compromised computers and devices, primarily consisting of Internet of Things (IoT) devices, that are infected with malicious software.

Botnets are frequently used to launch distributed denial of service (DDoS) attacks, overwhelming target systems or networks with a flood of traffic.

**Click Fraud**: Attackers may infect many devices with the intention of using them to generate fraudulent clicks on online advertisements, thereby generating revenue for the attackers.

**Stealing information** - Attacks have also been carried out with botnets to steal information from unsuspecting users’ systems.