Sniffing Module 8

by Durgesh Thakare

Introduction to Sniffing

Sniffing refers to the process of intercepting and capturing network traffic for analysis. It's a crucial technique in ethical hacking to understand and evaluate the security of a network.

Types of Sniffing

Passive Sniffing

- **Description:** Passive sniffing involves monitoring network traffic without actively injecting any packets. It's a non-intrusive method that helps in understanding the communication patterns.

Active Sniffing

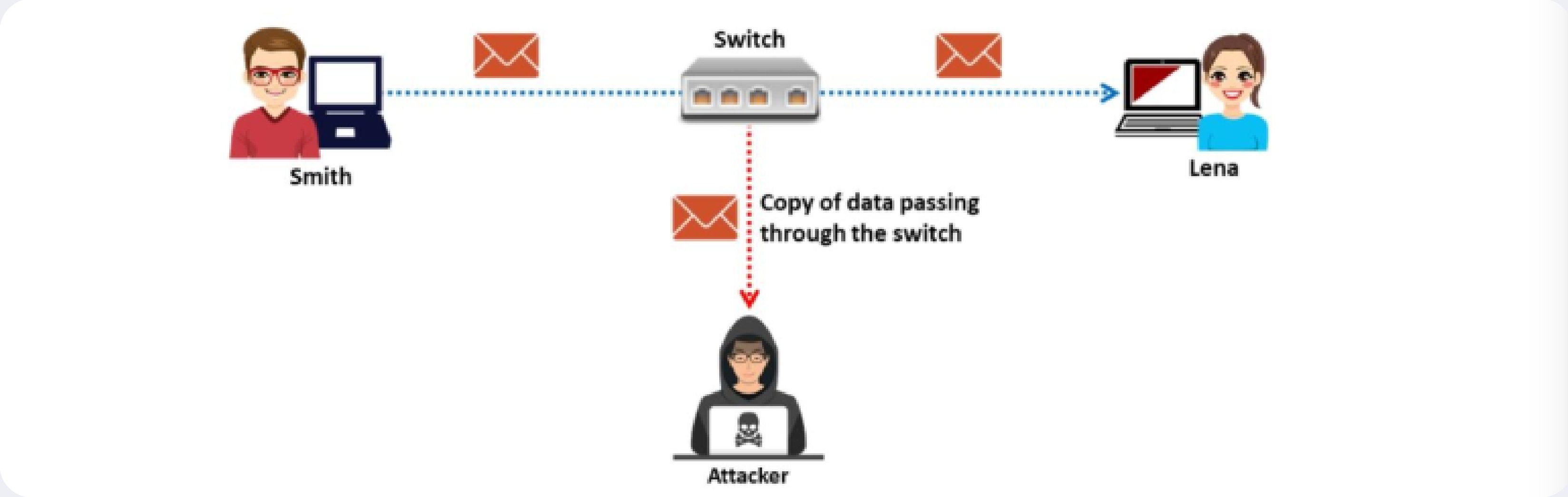
- **Description:** Active sniffing includes injecting packets into the network to capture responses. This method is more intrusive and allows for a more comprehensive analysis of network behavior.

Packet Sniffing

Packet sniffing is the process of intercepting and inspecting data packets as they traverse a network. This technique is employed for various purposes, including network troubleshooting, security analysis, and unfortunately, for malicious activities.

It allows an attacker to observe and access the entire network traffic from a given point

Packet sniffing allows an attacker to gather sensitive information such as Telnet passwords, email traffic, syslog traffic, router configuration, web traffic, DNS traffic, FTP passwords, chat sessions, and account information



ARP Spoofing

ARP (Address Resolution Protocol) Spoofing is a type of attack where an attacker sends falsified ARP messages over a local area network. The goal is to link the attacker's MAC address with the IP address of a legitimate network node, leading to the interception of data intended for that node.

How ARP Spoofing Works

- **ARP Protocol:** ARP is used to map an IP address to a MAC address in a local network. In ARP spoofing, the attacker sends ARP messages with false MAC-IP mappings, tricking other devices on the network.
- **Man-in-the-Middle (MitM):** ARP spoofing creates a Man-in-the-Middle situation, allowing the attacker to intercept, modify, or block data between two communicating parties.

MAC Flooding

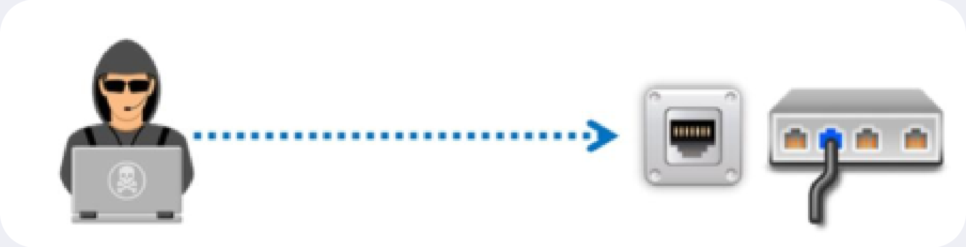
MAC Flooding is a network attack where an attacker floods the switch's MAC address table with fake MAC addresses, causing the switch to enter into a state where it operates as a hub, allowing the attacker to capture traffic.

How MAC Flooding Works

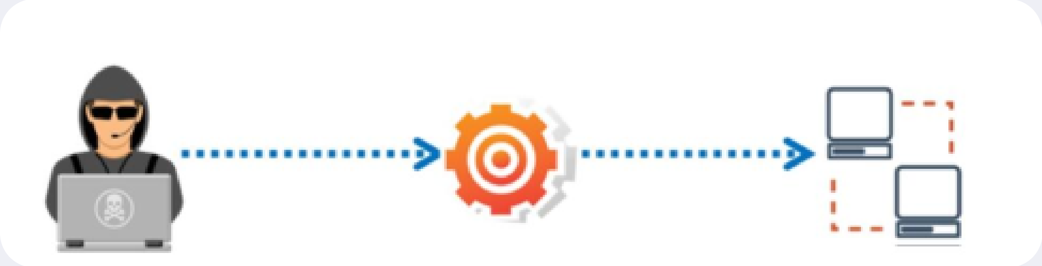
- **Switch MAC Table:** Switches use MAC address tables to forward data to the correct port. MAC flooding overwhelms the table, forcing the switch to broadcast traffic to all ports.
- **Capture Opportunity:** The attacker can then capture sensitive information by intercepting the broadcasted traffic

How Attacker Hacks The Network Using Sniffing

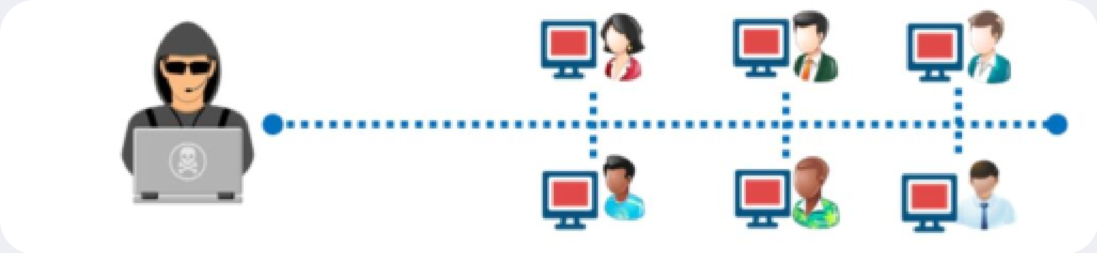
Step 1: An attacker who decides to hack a network first discovers the appropriate switch to access the network and connects a system or laptop to one of the ports on the switch.



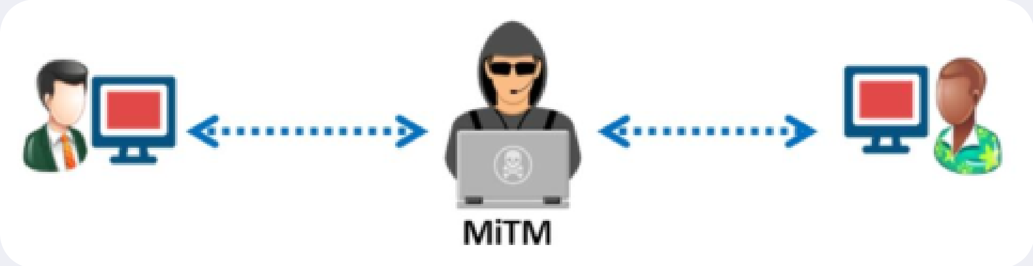
Step 2: An attacker who succeeds in connecting to the network tries to determine network information such as the topology of the network by using network discovery tools



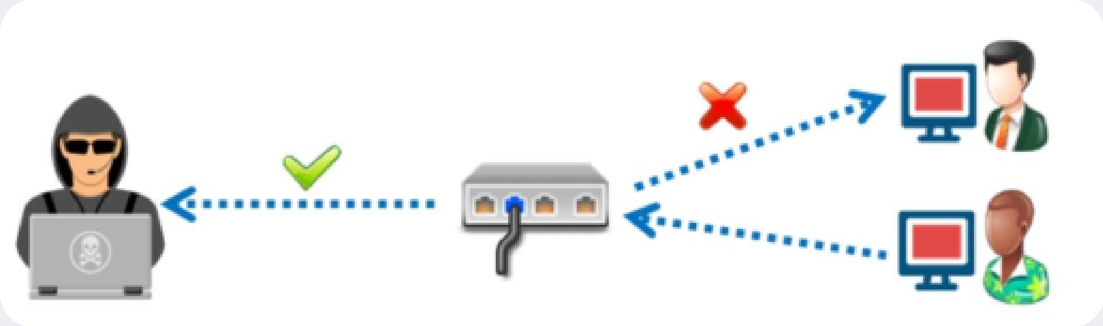
Step 3: By analyzing the network topology, the attacker identifies the victim's machine to target his/her attacks.



Step 4: An attacker who identifies a target machine uses ARP spoofing techniques to send fake (spoofed) Address Resolution Protocol (ARP) messages



Step 5: The previous step helps the attacker to divert all the traffic from the victim's computer to the attacker's computer. This is a typical man-in-the-middle (MITM) type of attack.



Step 6: Now, the attacker can see all the data packets sent and received by the victim. The attacker can now extract sensitive information from the packets, such as passwords, usernames, credit card details, and PINS.

Top Protocols Vulnerable to Sniffing

Telnet and Rlogin Telnet is a protocol used for communicating with a remote host (via port 23) on a network using a command-line terminal. rlogin enables an attacker to log into a network machine remotely via a TCP connection. Neither of these protocols provides encryption; therefore, data traveling between clients connected through any of these protocols are in plaintext and vulnerable to sniffing. Attackers can sniff keystrokes, including usernames and passwords.

HTTP Due to vulnerabilities in the default version of HTTP, websites implementing HTTP transfer user data across the network in plaintext, which attackers can read to steal user credentials.

SNMP Simple Network Management Protocol (SNMP) is a TCP/IP-based protocol used for exchanging management information between devices connected on a network. The first version of SNMP (SNMPv1 and SNMPv2) does not offer strong security, which leads to the transfer of data in a cleartext format. Attackers exploit the vulnerabilities in this version to acquire passwords in plaintext

SMTP Simple Mail Transfer Protocol (SMTP) is used for transmitting email messages over the Internet. In most implementations, SMTP messages are transmitted in cleartext, which enables attackers to capture plaintext passwords. Further, SMTP does not provide any protection against sniffing attacks.

NNTP Network News Transfer Protocol (NNTP) distributes, inquires into, retrieves, and posts news articles using a reliable stream-based transmission of news among the ARPA- Internet community. However, this protocol fails to encrypt the data, which allows attackers to sniff sensitive information.

POP Post Office Protocol (POP) allows a user's workstation to access mail from a mailbox server. A user can send mail from the workstation to the mailbox server via SMTP. Attackers can easily sniff the data flowing across a POP network in cleartext because of the protocol's weak security implementations.

FTP File Transfer Protocol (FTP) enables clients to share files between computers in a network. This protocol fails to provide encryption; therefore, attackers can sniff data, including user credentials, by running tools such as Cain & Abel.

IMAP Internet Message Access Protocol (IMAP) allows a client to access and manipulate electronic mail messages on a server. This protocol offers inadequate security, which allows attackers to obtain data and user credentials in cleartext.

Wiretapping

Wiretapping: Wiretapping refers to the unauthorized interception of telephone or internet communications, typically through the tapping or monitoring of the communication lines.

Methods of Wiretapping

Physical Wiretapping

- **Procedure:** Physically tapping into communication lines, often requiring direct access to cables or communication infrastructure.

Electronic Wiretapping

- **Procedure:** Intercepting communication signals electronically, often involving the use of specialized equipment or software to capture and analyze data.

Uses of Wiretapping

Law Enforcement

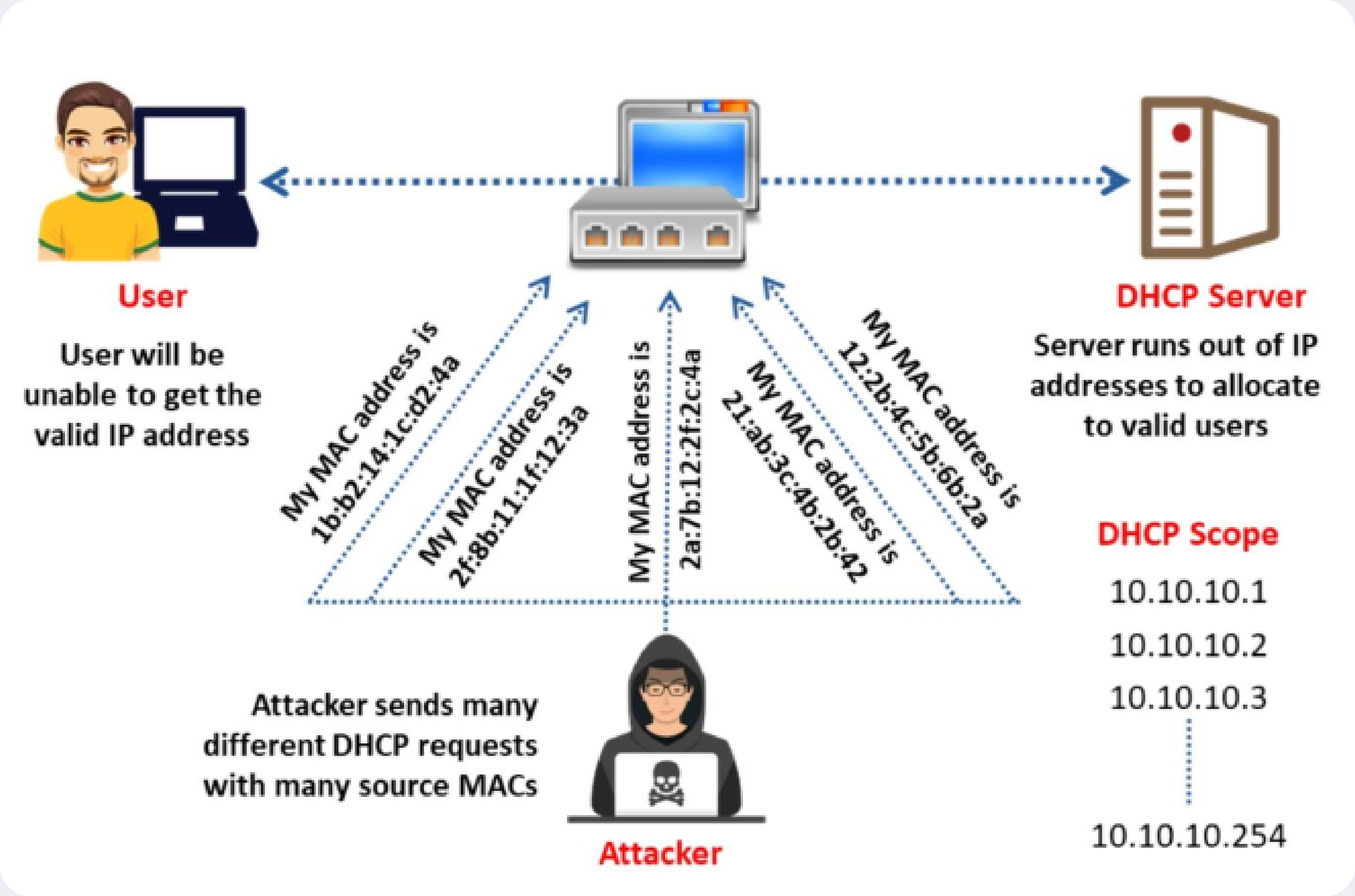
- **Investigations:** Law enforcement agencies may use wiretapping as a tool for investigating and gathering evidence in criminal cases.

National Security

- **Surveillance:** Government agencies may employ wiretapping for national security purposes, monitoring potential threats to public safety.

DHCP Starvation Attack

This is a denial-of-service (DoS) attack on the DHCP servers where the attacker broadcasts forged DHCP requests and tries to lease all the DHCP addresses available in the DHCP scope Therefore, the legitimate user is unable to obtain or renew an IP address requested via DHCP, and fails to get access to the network


User
User will be unable to get the valid IP address
DHCP Server
Server runs out of IP addresses to allocate to valid users
My MAC address is 1b:b2:14:1c:d2:4a
My MAC address is 2f:8b:11:1f:12:3a
My MAC address is 2a:7b:12:2f:2c:4a
My MAC address is 21:ab:3c:4b:2b:42
My MAC address is 12:2b:4c:5b:6b:2a
DHCP Scope
10.10.10.1
10.10.10.2
10.10.10.3
10.10.10.254
Attacker sends many different DHCP requests with many source MACs
Attacker

TOOLS FOR DHCP STARVATION ATTACK

Yersinia

DhcpStarvation

Dhcpstarv

Gobbler

Dhcpig

Threats of ARP Poisoning

Packet Sniffing: Sniffs traffic over a network or a part of the network.

Session Hijacking: Steals valid session information and uses it to gain unauthorized access to an application.

VoIP Call Tapping: Uses port mirroring, which allows the VoIP call tapping unit to monitor all network traffic, and picks only the VoIP traffic to record by MAC address.

Manipulating Data: ARP spoofing allows attackers to capture and modify data, or stops the flow of traffic.

Man-in-the-Middle Attack: An attacker performs a MITM attack where they reside between the victim and server.

Data Interception: Intercepts IP addresses, MAC addresses, and VLANs connected to the switch in a network.

Connection Hijacking: In a network, the hardware addresses are supposed to be unique and fixed, but a host may move when its hostname changes and use another protocol. In connection hijacking, an attacker can manipulate a client's connection to take complete control.

Stealing Passwords: An attacker uses forged ARP replies and tricks target hosts into sending sensitive information such as usernames and passwords.