# What is the difference between active and passive MitM attacks?

**Passive MitM Attacks:**

* Characteristics: In passive MitM attacks, the intruder covertly monitors communication without actively manipulating the data.
* Methods: This is accomplished through techniques such as sniffing network traffic, utilizing tools like packet sniffers, or tapping into physical communication lines.
* Detection: Passive attacks pose a greater challenge for detection since the attacker refrains from directly altering the communication. Nevertheless, sophisticated intrusion detection systems may identify irregular patterns or behaviours.

**Active MitM Attacks:**

* Characteristics: In active MitM attacks, the assailant not only intercepts communication but also engages in the active modification of transmitted data between the parties.
* Methods: Common techniques encompass session hijacking, DNS spoofing, ARP spoofing, and SSL-stripping. The attacker may introduce malicious content, modify messages, or redirect traffic to nefarious sites.
* Detection: Active MitM attacks are comparatively more detectable, particularly with monitoring systems that can spot unexpected alterations in communication flow or when the targeted parties employ secure communication protocols.

# How to protect your network against ARP poisoning attacks?

Protecting a network against ARP poisoning attacks is crucial for ensuring the security of communications. Here are several strategies to safeguard your network:

**Utilize ARP Spoofing Detection Tools:**

* Employ tools and software designed to detect ARP spoofing. These tools can identify irregularities in ARP tables and promptly alert administrators to potential attacks. Examples include ARPWatch, XArp, and Wireshark.

**Implement Static ARP Entries:**

* Manually configure static ARP entries on critical devices like routers and servers. This practice ensures that ARP tables are less susceptible to manipulation, as statically configured entries take precedence over dynamically learned ones.

**Opt for Network Segmentation:**

* Divide your network into segments using VLANs or subnetting. This limits the impact of an ARP poisoning attack, confining the attacker's influence to a specific network segment.

**Deploy ARP Spoofing Prevention Techniques:**

* Deploy tools or mechanisms designed to actively prevent and mitigate ARP spoofing attacks. Some network security solutions offer features to thwart ARP spoofing attempts.

**Conduct Network Monitoring:**

* Regularly monitor network traffic for unusual patterns or behavior. Anomalies in ARP requests or responses may indicate ARP poisoning attempts. Network monitoring tools and intrusion detection systems can assist in identifying suspicious activities.

**Enable Port Security on Switches:**

* Strengthen security on switches by enabling port security features. This restricts the number of allowed MAC addresses on a specific port, making it more challenging for attackers to introduce unauthorized devices.

**Utilize ARP Spoofing Resistant Protocols:**

* Consider implementing protocols resistant to ARP spoofing, such as those utilizing cryptographic mechanisms to ensure communication integrity, like IPsec.

**Regularly Update and Patch Systems:**

* Keep all network devices and systems updated with the latest security patches. Vulnerabilities in operating systems or networking equipment can be exploited by attackers to carry out ARP poisoning attacks.

# Why it is important to use DNSSEC to prevent DNS spoofing attacks?

**DNSSEC** (Domain Name System Security Extensions) plays a crucial role in thwarting **DNS** (Domain Name System) spoofing attacks due to its reinforcement of DNS security and data integrity. DNS spoofing, also referred to as DNS cache poisoning, involves malicious entities providing false DNS responses, leading users to potentially harmful websites. Here's why the adoption of DNSSEC is pivotal in mitigating DNS spoofing attacks:

**Data Integrity Assurance:**

* DNSSEC introduces cryptographic signatures to DNS records, ensuring the preservation of data integrity. The inclusion of digital signatures verifies that the data received by a user aligns with the original information stored in the DNS server. Any tampering during data transit is detected through the failure of DNSSEC signature validation.

**Authentication Mechanism:**

* Providing a means of authenticating DNS responses, DNSSEC utilizes digital signatures to confirm that the received information originates from an authorized DNS server and has remained unaltered by malicious actors. This authentication layer prevents attackers from introducing false DNS data.

**Establishment of Chain of Trust:**

* DNSSEC establishes a robust chain of trust, extending from the root DNS server to the specific domain under inquiry. Each level in the DNS hierarchy signs the records for the domains beneath it, creating a secure chain that allows for the verification of DNS responses at each level. This process reduces the risk of receiving spoofed responses.

**Cache Poisoning Prevention:**

* A common tactic in DNS spoofing attacks, cache poisoning involves injecting malevolent data into the cache of a DNS resolver. DNSSEC guards against such instances by necessitating the validation of DNS responses using cryptographic signatures. Responses lacking valid signatures are rejected by the resolver.

**Contribution to Data Confidentiality:**

* While DNSSEC primarily focuses on integrity and authentication, it indirectly contributes to data confidentiality. By ensuring the unaltered state of DNS data during transit, DNSSEC helps prevent attackers from redirecting users to malicious websites.

**Elevated Security for DNS Queries:**

* DNSSEC enhances the security of DNS queries by allowing clients to verify the authenticity and integrity of received responses. This is particularly significant in scenarios where users may be engaging with sensitive services or sharing confidential information.

**Global Adoption and Standardization Impact:**

* As a widely adopted and standardized security protocol, DNSSEC contributes significantly to the global security of the DNS infrastructure. Its pervasive implementation reduces susceptibility to widespread DNS spoofing attacks. The broader the adoption of DNSSEC across domains and DNS servers, the more effective it becomes in securing the entire DNS ecosystem.

# What is monitor mode and how can you use it to eavesdrop network communication?

Monitor mode, also referred to as promiscuous mode, is a functionality found in network interface controllers (NICs) that enables them to capture and examine all network traffic passing through a given network segment. Unlike regular operation, where a NIC processes only the frames specifically addressed to its MAC address, monitor mode allows the NIC to intercept all traffic within its range.

**Operation of Monitor Mode:**

* Normal Mode:
  + Under normal circumstances, a network interface captures and handles frames addressed to its MAC address or broadcast/multicast frames.
* Monitor Mode:
  + When set to monitor mode, the NIC captures all frames on the network, irrespective of the destination MAC address, providing visibility into all traffic within its reach.

**Eavesdropping in Monitor Mode:**

* Packet Sniffing:
  + Employing packet sniffing tools like Wireshark or tcpdump, one can capture and scrutinize all network packets, including those not originally intended for the capturing device.
* Promiscuous Capture:
  + In monitor mode, the NIC becomes promiscuous, capturing all frames—data, control, and management frames—regardless of the addressed MAC. This includes potentially sensitive unencrypted data.
* Capture Unencrypted Data:
  + In scenarios where network communication lacks encryption, an individual in monitor mode can intercept and view the contents of unencrypted data packets. This could include sensitive information and login credentials.
* Analyze Network Traffic:
  + An entity with access to the captured data can analyze network traffic patterns, identify vulnerabilities, and potentially gain unauthorized access to sensitive information.

**Preventing Unauthorized Eavesdropping:**

* Encryption:
  + Employ robust encryption protocols (e.g., WPA2, WPA3 for Wi-Fi) to secure network communication. Encrypted traffic is significantly more resistant to deciphering, even if intercepted in monitor mode.
* Network Segmentation:
  + Implement network segmentation to confine the scope of monitor mode. This limits potential eavesdropping impact, as the capturing entity would only have visibility into traffic on the specific network segment.
* Intrusion Detection Systems (IDS):
  + Use intrusion detection systems capable of identifying abnormal patterns in network traffic, including potential eavesdropping activities.
* Regular Monitoring:
  + Routinely monitor and audit network activity to identify any unauthorized use of monitor mode. This may involve periodic checks of network configurations and the utilization of network monitoring tools.

# TASKS

KALI\_VM\_IP\_ADDRESS : 172.16.96.2

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated