What is ARP Spoofing_

ARP spoofing, also known as ARP poisoning, is a technique used to intercept network traffic by sending false ARP (Address Resolution Protocol) messages to a local area network. In the first step, an attacker associates their MAC address with the IP address of a legitimate device, such as a router, deceiving other devices on the network.

Once the attacker's MAC address is linked to the IP address of the legitimate device, all the data intended for that IP address is sent to the attacker's device instead. This allows the attacker to monitor, intercept, and potentially alter the data before forwarding it to its actual destination.

ARP spoofing can lead to serious security issues, including man-in-the-middle attacks, data theft, and session hijacking. It exploits the lack of authentication in ARP, making it a significant threat in unprotected networks. Network administrators use techniques like packet filtering, static ARP entries, and intrusion detection systems to mitigate ARP spoofing risks.

WHY to do ARP spoofing_

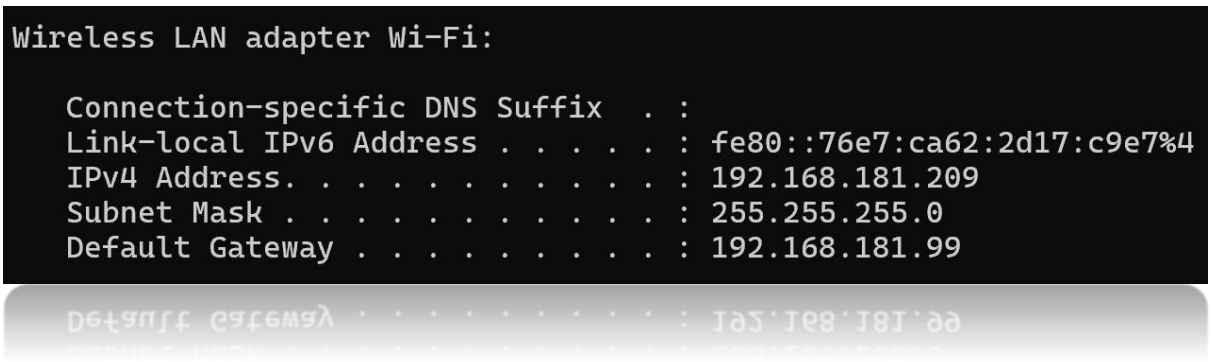
- **Man-in-the-Middle Attacks**: By intercepting communications between two devices, attackers can eavesdrop on or alter the data being transmitted.
- **Data Theft**: Attackers can capture sensitive information such as login credentials, personal information, and financial data.
- **Session Hijacking**: By intercepting session cookies or tokens, attackers can take over active user sessions, gaining unauthorized access to web accounts.
- **Network Traffic Analysis**: Attackers can monitor the network traffic to gather information about the network structure, active devices, and communication patterns.
- **Denial of Service (DoS)**: By disrupting the normal communication between devices, attackers can cause network outages or degrade the network performance.
- **IP Address Conflict**: Attackers can create IP address conflicts by associating their MAC address with an existing IP address, causing network disruptions.
- **Redirecting Traffic**: Attackers can redirect traffic to malicious websites or servers, facilitating phishing attacks or distributing malware.
- **Bypassing Network Security**: By masquerading as a legitimate device, attackers can bypass certain network security measures, gaining access to restricted areas of the network.

MAN IN THE MIDDLE_

To perform a man-in-the-middle attack using ARP spoofing, an attacker sends false ARP messages to a local network, associating their MAC address with the IP address of a target device, such as a router. This deceives other devices on the network, causing them to send their data to the attacker.

Once the attacker has intercepted the data, they can monitor, alter, or inject malicious content before forwarding it to the intended recipient. This allows the attacker to eavesdrop on private communications and potentially steal sensitive information.

MITM using BETTERCAP_



My target device is 192.168.181.209 and the default gateway is ***192.168.181.99***. Now when I will perform the ARP Spoof, I will pretend to be the router for the target machine and current MAC address for the router will be changed to my MAC address which is ***f8-16--------36-86.***

```
Internet Address      Physical Address      Type
192.168.181.67        f8-16-[redacted]-36-86     dynamic
192.168.181.99        d6-4b-[redacted]-db-9b     dynamic
192.168.181.217       f8-16-[redacted]-36-86     dynamic
```

As for now the gateway MAC address is ***d6-46------db-9d*** and the machine I am using for the attack is ***192.168.181.217***.

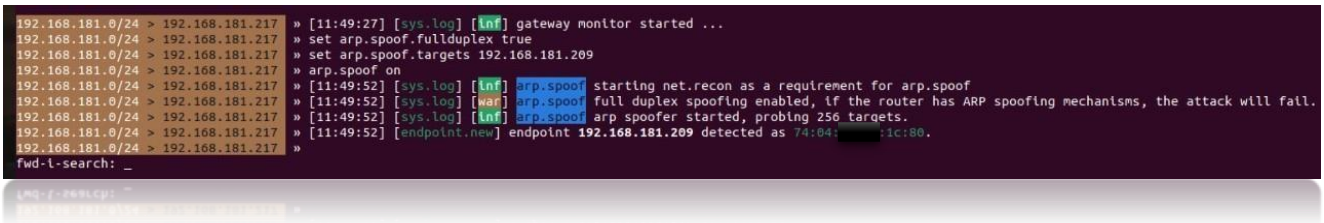
STEP 1:

First, we will fire up our tool, Bettercap. This powerful network utility allows us to perform a variety of different tasks. By exploring its features, we can see a range of options for network analysis and manipulation. For our purposes, we are going to specifically use the arp.spoof module. This module will enable us to execute ARP spoofing, allowing us to intercept and manipulate network traffic between devices, which is crucial for performing man-in-the-middle attacks.

STEP 2:

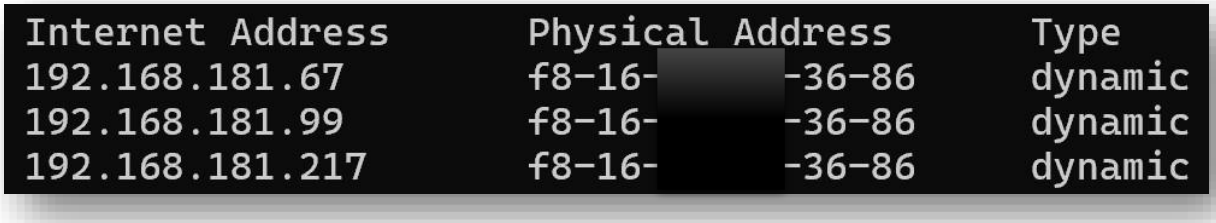
Now before setting arp.spoof to ON, we have to configure a couple of additional settings. First, we need to set arp.spoof.fullduplex to true, enabling full duplex communication. Next, we need to specify the target of the ARP spoofing by setting arp.spoof.targets, which in this case will be 192.168.181.209. This ensures that the spoofing attack is correctly directed at the intended device on the network.

Now we can set arp.spoof on.



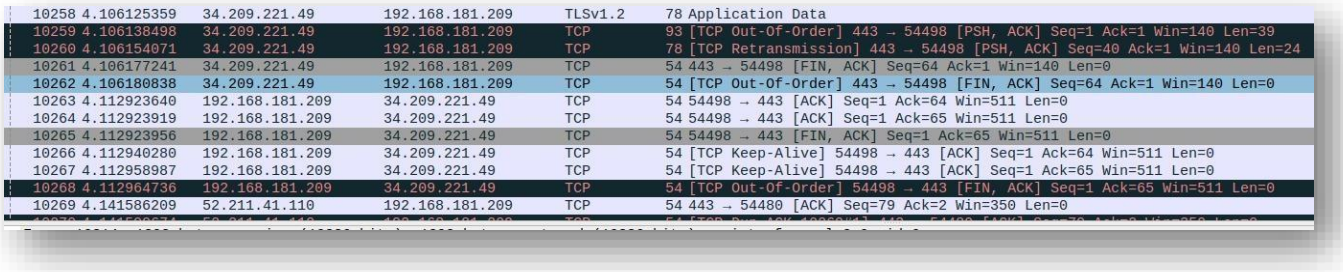
STEP 3:

Now we will check if the MAC address of the router has changed in our target machine or not and as you can see in the image below the MAC address of the gateway address (192.168.181.99) has been changed form ***d6-46------db-9d*** to ***f8-16--------36-86.***



STEP 4:

Now we will use Wireshark to capture the packets and let's check if can capture the packets coming for the target machine. And as you can see in the image, we have packets coming from the target machine (192.168.181.209).

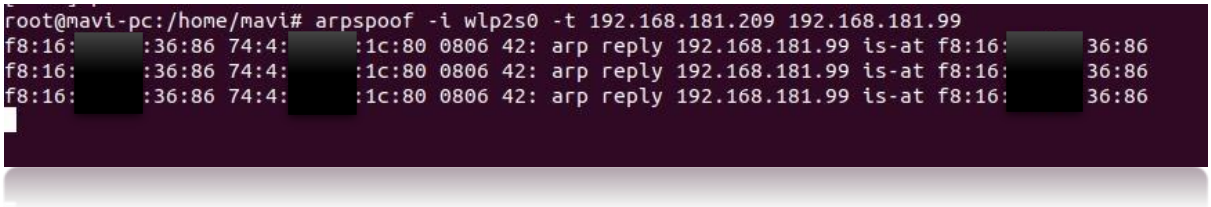


Now we have successfully implimended our Man In The Middle Attack. On our target and we can see and capture all the packets going and coming for the target.

MITM using Manual method_

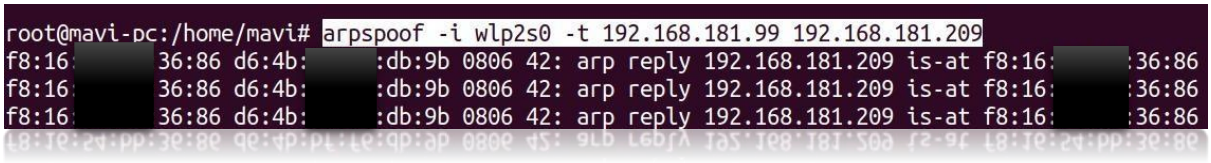
STEP 1:

We will need two terminal windows. In the first one, we will run arpspoof for our target machine to pretend to be a router in the eyes of the target device. This setup is crucial for intercepting and redirecting the network traffic intended for the router to the attacker's machine, setting up the man-in-the-middle attack effectively.



STEP 2:

Now, on the second terminal, we will run arpspoof for our router to pretend to be the target in the eyes of the router. This will enable the attacker to intercept and manipulate data packets between the target device and the router.



STEP 3:

Now, as you can see, our system is actively sending ARP packets to both the router and the target machine to ensure the successful implementation of our MITM attack.

Conclusion_

In this minor project, we were able to successfully implement the Man-in-the-Middle (MITM) attack on the target device using both manual methods and the tool BETTERCAP. By leveraging ARP spoofing techniques, we intercepted network

traffic, demonstrating the feasibility of MITM attacks. BETTERCAP provided an efficient and automated way to carry out the attack, while the manual method gave us a deeper understanding of the underlying processes. This comprehensive approach allowed us to effectively capture and analyze the data exchanged between devices on the network.