**MITM ATTACKS**

**Man In The Middle Attacks**

**These are attacks that we can launch only if we are able to intercept the communication between two devices**

**Normal communication == where the device is directly communicating with the entity that they want to communicate with**

In MITM, the hacker would be able to place themselves in the middle of the connection allowing them to intercept and see anything that is being transferred between the two devices

**There are number of ways to achieve this, the first method is using an:**

**ARP spoofing attack**

**ARP spoofing allow us to redirect the flow of packets**

Instead of the victim sending requests to the access point and getting responses, it will send requests to the hacker, the hacker will send them to the access point, the hacker will receive responses and then send those responses to the victim

**This means that any messages, any websites, any images, any usernames, any passwords entered by the target will have to flow through my computer**

**This allows us to read this info, modify it or drop it**

**This is very serious and very powerful attack and the reason why it is possible is because ARP is not very secure**

**ARP = Address Resolution Protocol**

**- Simple protocol used to map IP Address of a machine to its MAC Address**

**Since devices in networks dont communicate with their IPs, they communicate with their MAC Addresses**

**If one client wants to communicate with other client, it needs to use ARP protocol**

That means it sends a broadcast message - it sends an ARP request to all the clients on the network saying: Who has 10.0.2.6(IP) ?

All devices will ignore this packet except the one that has this IP Address(10.0.2.6)

So the device with that IP will send ARP responce back to the asking device

In the responce the device will say: I have 10.0.2.6 and my MAC Address is this ....

That way the asking device will have the MAC Address of the device and now it will be able to communicate with it and do whatever task it wanted to do initially

**So all of this communication is facilitated using the ARP protocol**

**! The whole point of it is so we can link IP Addresses to MAC Addresses or translate IP Addresses to MAC Addresses !**

**Each computer have an ARP table which links IP Addresses on the same network to their MAC Addresses**

**If any computer wanted to send a request, it will go directly to the router**

**What we can do is we can exploit the ARP protocol and send two ARP responses - one to the gateway and one to the victim**

We are going to tell the gateway that im the IP of the victim so the access point will update its ARP table and it will associate the IP of the target with our MAC Address

We will do the same with the victim so we will send it an ARP response and think that we are the router

**Why ARP Spoofing is possible ?**

**1 Clients accept responses even if they did not send a request**

**2 Clients trust response without any form of verification**