**EXPERIMENT -03**

**Aim: Arp spoofing attack & Mitm Attack using Bettercap Tool**

Theory: Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP addresses to machine MAC addresses. All network devices that need to communicate on the network broadcast ARP queries in the system to find out other machines’ MAC addresses. ARP Poisoning is also known as **ARP Spoofing**.

Here is how ARP works −

* When one machine needs to communicate with another, it looks up its ARP table.
* If the MAC address is not found in the table, the **ARP\_request** is broadcasted over the network.
* All machines on the network will compare this IP address to MAC address.
* If one of the machines in the network identifies this address, then it will respond to the **ARP\_request** with its IP and MAC address.
* The requesting computer will store the address pair in its ARP table and communication will take place.

**What is ARP Spoofing?**

ARP packets can be forged to send data to the attacker’s machine.

* ARP spoofing constructs a large number of forged ARP request and reply packets to overload the switch.
* The switch is set in **forwarding mode** and after the **ARP table** is flooded with spoofed ARP responses, the attackers can sniff all network packets.

Attackers flood a target computer ARP cache with forged entries, which is also known as **poisoning**. ARP poisoning uses Man-in-the-Middle access to poison the network.

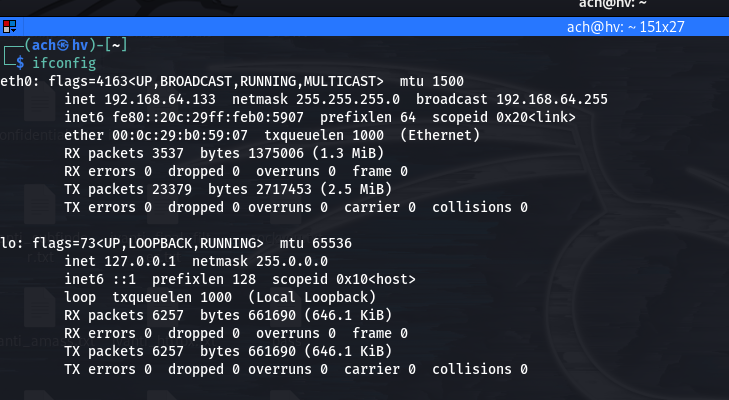
**What is MITM?**

The Man-in-the-Middle attack (abbreviated MITM, MitM, MIM, MiM, MITMA) implies an active attack where the adversary impersonates the user by creating a connection between the victims and sends messages between them. In this case, the victims think that they are communicating with each other, but in reality, the malicious actor controls the communication.

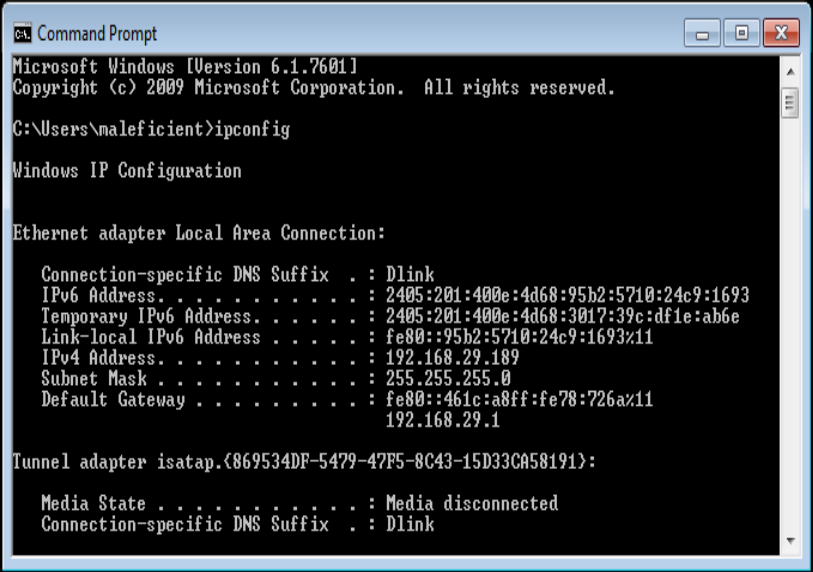
A third person exists to control and monitor the traffic of communication between two parties. Some protocols such as **SSL** serve to prevent this type of attack.

**Practical:**

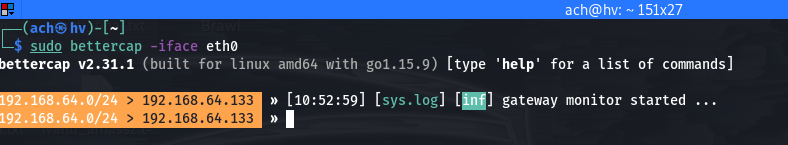
**Step1**: Check Attacker’s IP(Kali Linux) & MAC Address (ether)



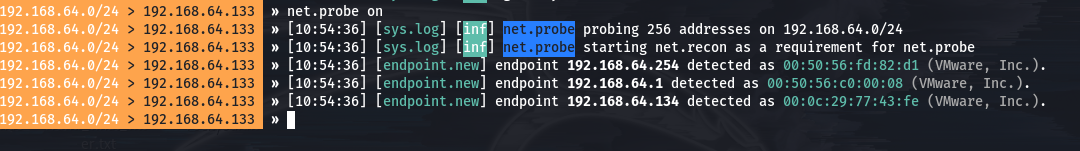
**Step2**: Check Victim’s IP (Windows 7)

****

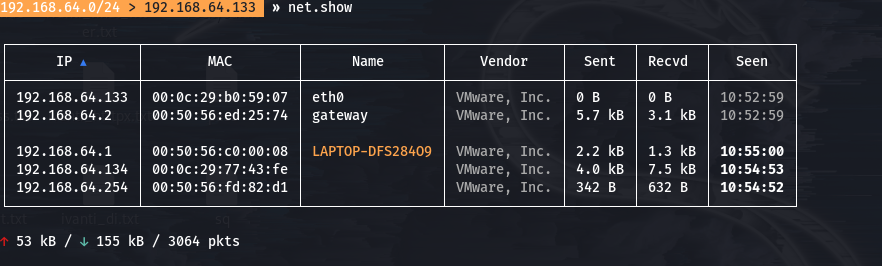
Step3: From attacker’s machine, run the tool (sudo bettercap -iface eth0). This command will execute the code of the bettercap tool and you just have to select your interface.



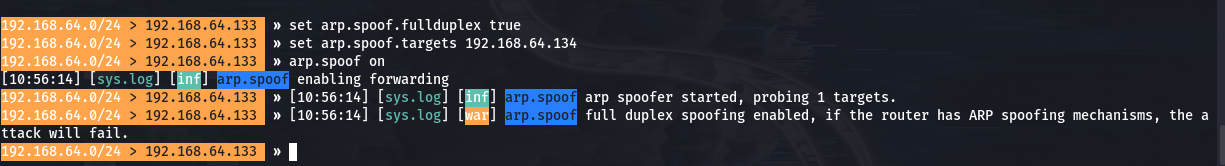
**Step4**: Now by the following command we are gathering information of the devices that are connected in our network.



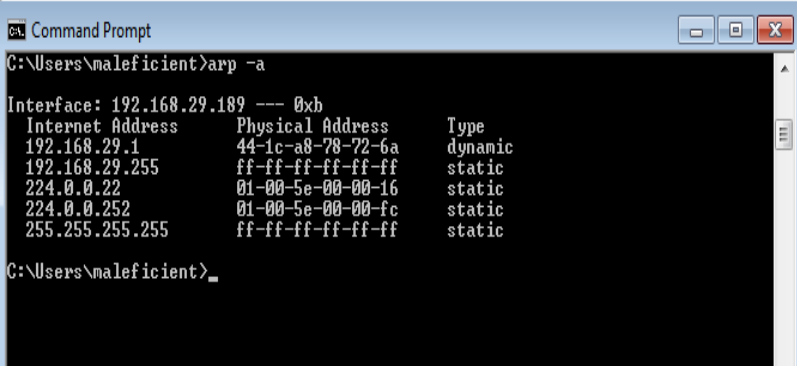
**Step5**: The following command will show the connected devices in that network in a tabular view. From here you can select the victim.



**Step6**: We have to turn the ful duplex mode on, so that we can intercept the traffic of our router and the victim at the same time. Also we select our target (192.168.64.134) or the list of targets to whom we want to attack. Finally turn on the arp spoofing to execute the attack.



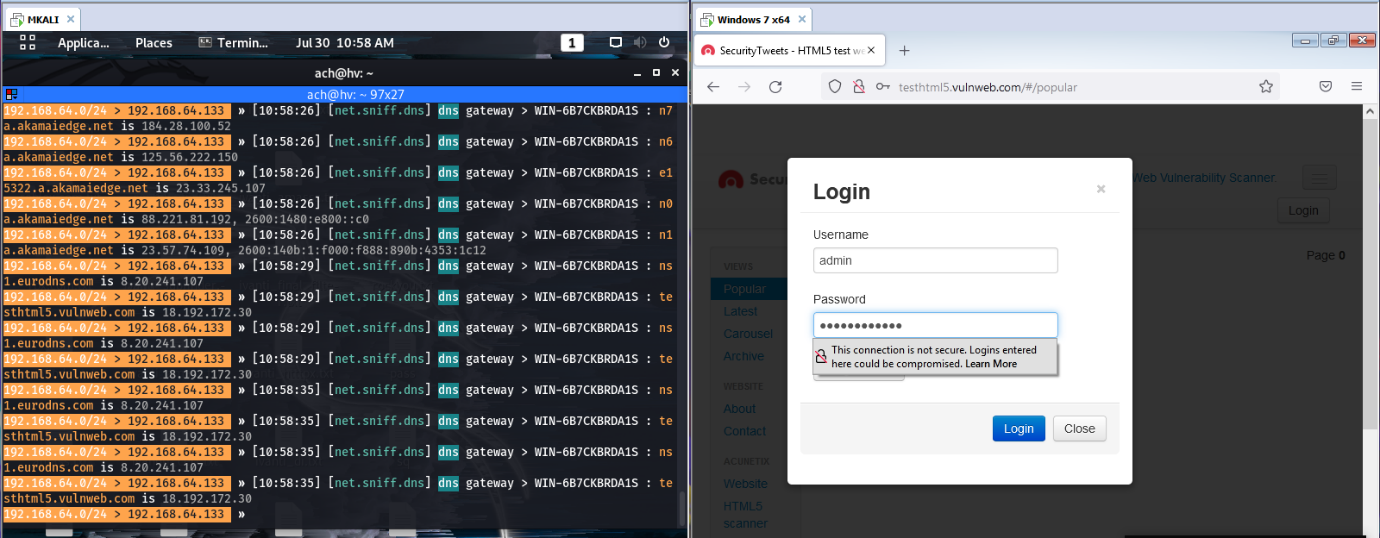
**Step7**: If we go and check the victim’s PC, we found that the mac address of the gateway/router(192.168.64.2) and the attacker(192.168.64.133) are same. It means arp spoofing successfully executed.



**Step8**: Now in this final step we only have to turn on the sniffer which will sniff packets of the victim and acts as a mitm (man in the middle ) attack.



**Step9**: Now if the victim enters his credentials in his browser that information also goes to attacker first then to the router.



**Step10**: Credentials intercepted as you can see the account and password of the victim in clear text format.

