**ARP SPOOFING**

**USING ARPSPOOF**

There are a number of tools that can be used to run an ARP Spoofing attack, you can even build your own tool

**We are going to use simple yet reliable tool called:**

**arpspoof**

Later we will use a tool called **BetterCAP** because it has more features

**arpspoof** is also ported to many operating systems including iOS and Android

You can only use this tool to redirect the flow of data and make it flow through your computer and then you will have to use another tool like a packet sniffer like **Wireshark** to analyze this data and do more stuff with it

**Using arpspoof is very simple:**

**First one to fool the victim**

**Second one to fool the router**

arpspoof -i eth0 -t 10.0.2.7 10.0.2.1

(tool)

(-i to specify the interface that is connected to the target network)

(-t to specify the target(his IP))

(IP of the gateway)

**! split screen action !**

arpspoof -i eth0 -t 10.0.2.1 10.0.2.7

(tool)

(-i to specify the interface that is connected to the target network)

(-t to specify the IP of the gateway)

(the victim's IP)

You can check the result in the arp -a in the Windows VM(The MAC Addresses will be changed)

Our computer is not a router so when it gets requests, its actually going to stop them from flowing and going to the router, this is a security feature in Linux

So you need to enable port forwarding so that our computer would allow packets to flow through it just like a router

**To enable port forwarding, we are going to do:**

echo 1 > /proc/sys/net/ipv4/ip\_forward

Now the victim would still have internet access but all these requests are not going directly to the router but they are going to our computer first and then our computer is forwarding them to the router and then when the responses come back, they are going to go to our computer first and then go to the victim

Simple tool allowing us to redirect the flow of data, allowing us to become the man in the middle and once done we can inject code in the browser of the target, we can steal usernames, passwords, see all the info that the person sends and receives, replace downloaded files with Trojans and much much more