**FAZAL E WADOOD HARIS - 205179 CYBER 6TH**

**MAN IN THE MIDDLE (MITM) USING BETTERCAP**

**BETTERCAP:**

Better Cap is a powerful, easily extensible and portable framework written in Go which aims to offer to security researchers, red teamers and reverse engineers an easy to use, all-in-one solution with all the features they might possibly need for performing reconnaissance and attacking Wi-Fi networks, Bluetooth Low Energy devices, wireless HID devices and Ethernet networks.

**Main features include:**

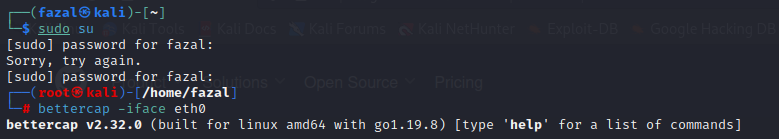
Address Resolution Protocol ARP Spoofing, DNS poisoning and for MITM attacks on IPv4 and IPv6 based networks.

Here, our goal is to perform and demonstrate Man in The Middle attack using this tool in KALI Linux.

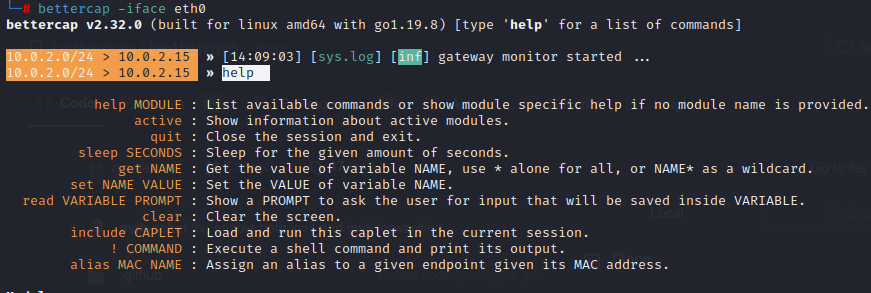
First download Better Cap form git-hub using ‘**sudo apt-get bettercap** ’ command in CLI KALI.

**SCREENSHOTS:**

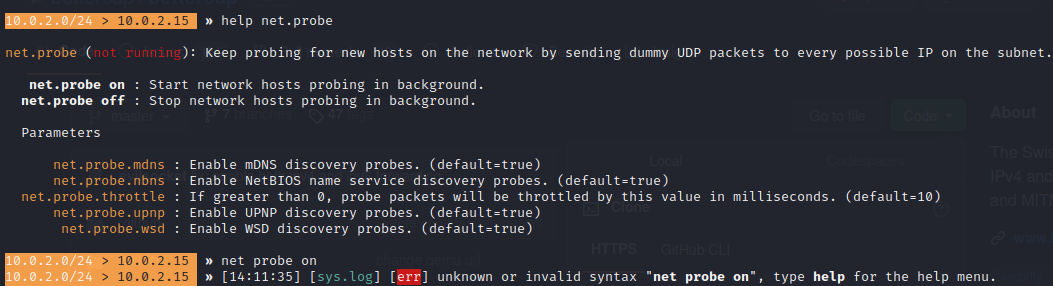
here **i face is for intrface** and **eth0** is interface's name for my PC



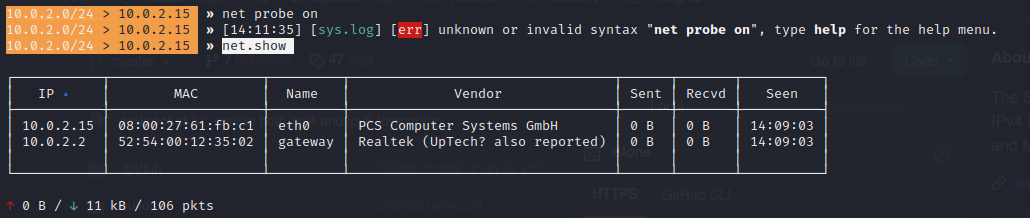
Enter **help** as shown below



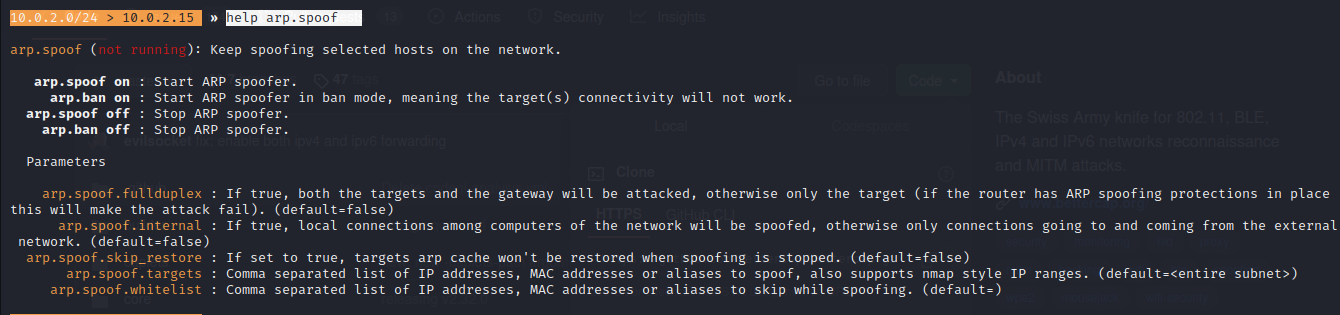
Then enter **help net.probe** command which refers to the process of actively scanning or testing a network to gather information about its devices, services, and vulnerabilities.



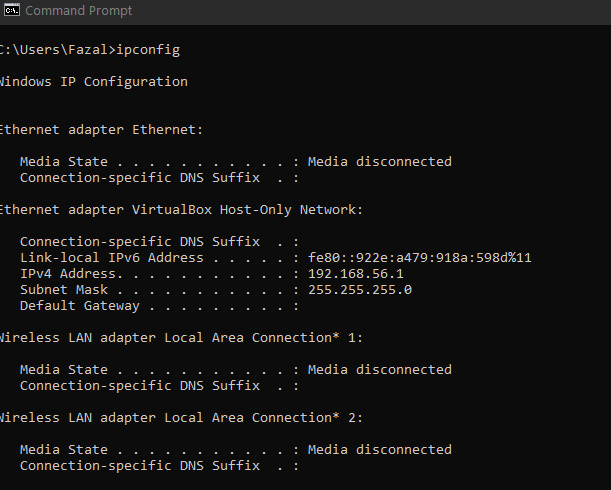
Then **enter net.show** command to check the ip in table image



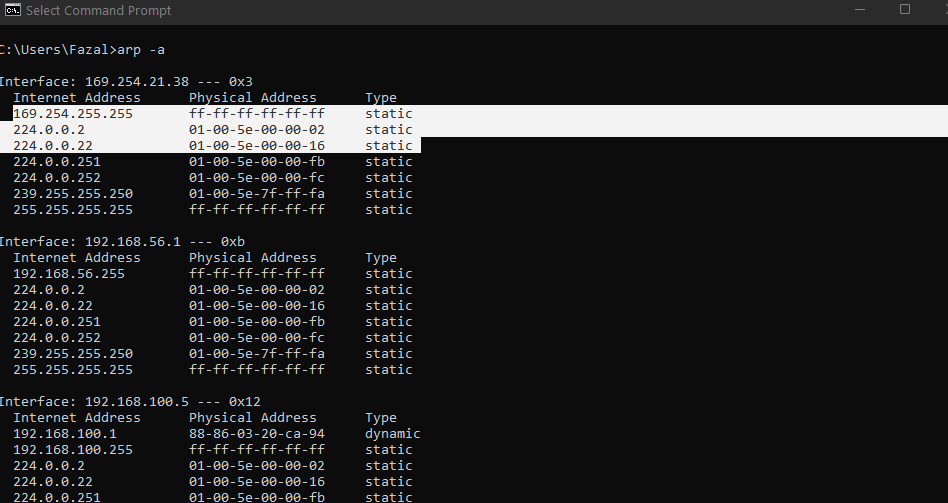
I spoofed the MAC address to capture the packets from target machine using **ARP spoofing command**.



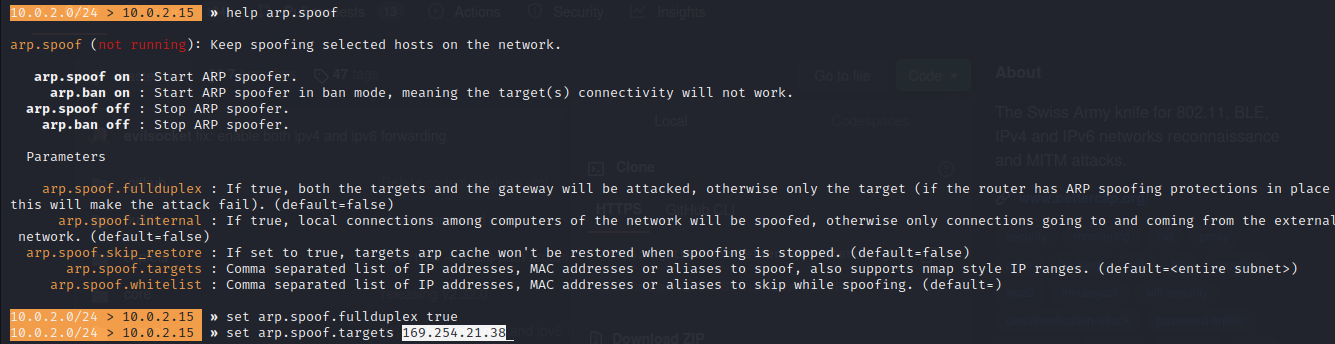
Then check your ip, default gateway in CMD windows as I did



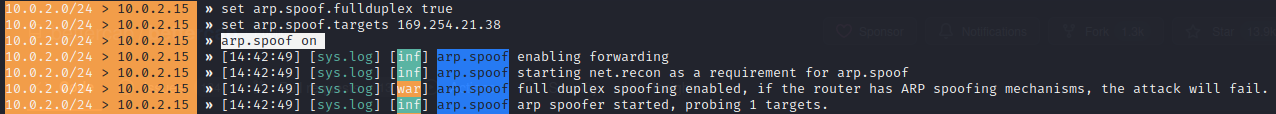
I used arp-a command



Enter targets ip which is my own laptop in this attack therefore,



Next, I used the **arp spoof on** command to start arp spoofing



This very **attack is performed on the same network and** this technique will only work **on HTTP website** **for HTTPS you will need to perform some other method**.

Since I had spoofed the packets successfully next thing, I will **do is start capturing the packets and monitor it.**

I used **sniff command** to capture plus monitor packets, for this purpose I browsed something on my target machine and then monitor/read it (the packets).

