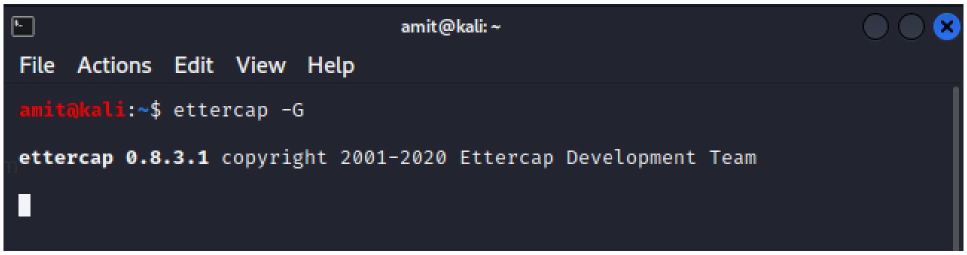
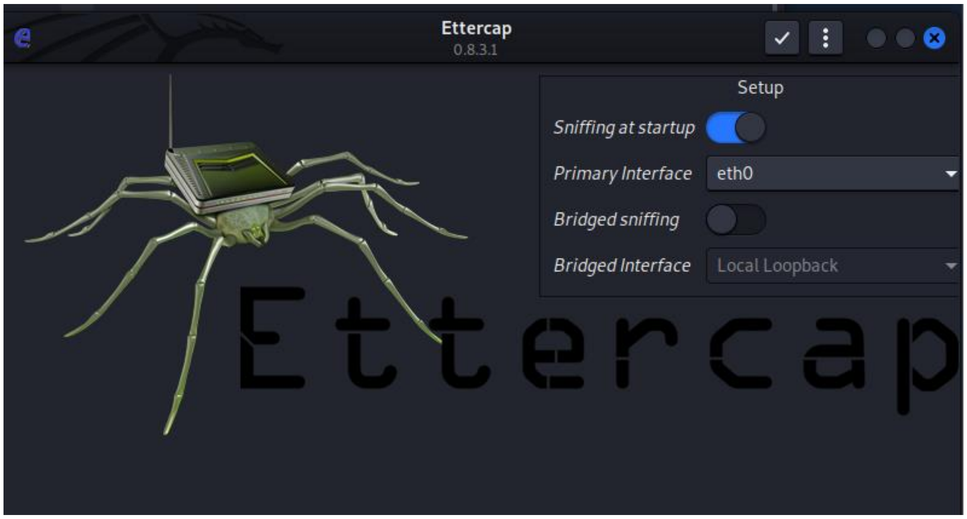
Practical 8 : Man In The Middle Attack

1. Open Terminal and "type ettercap –G"



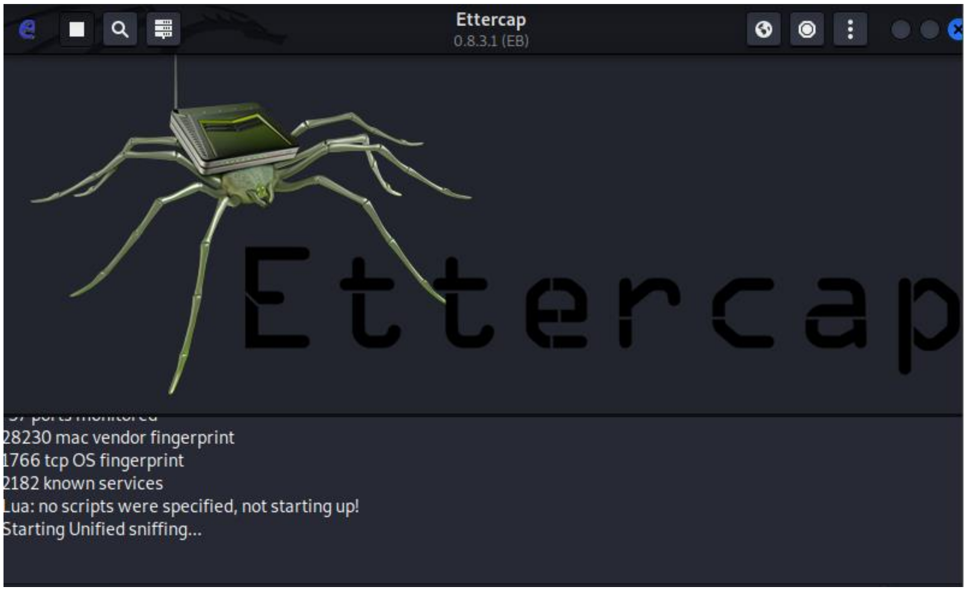
```
amit@kali:~$ ettercap -G

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

```

2. Ettercap GUI will open after entering the command



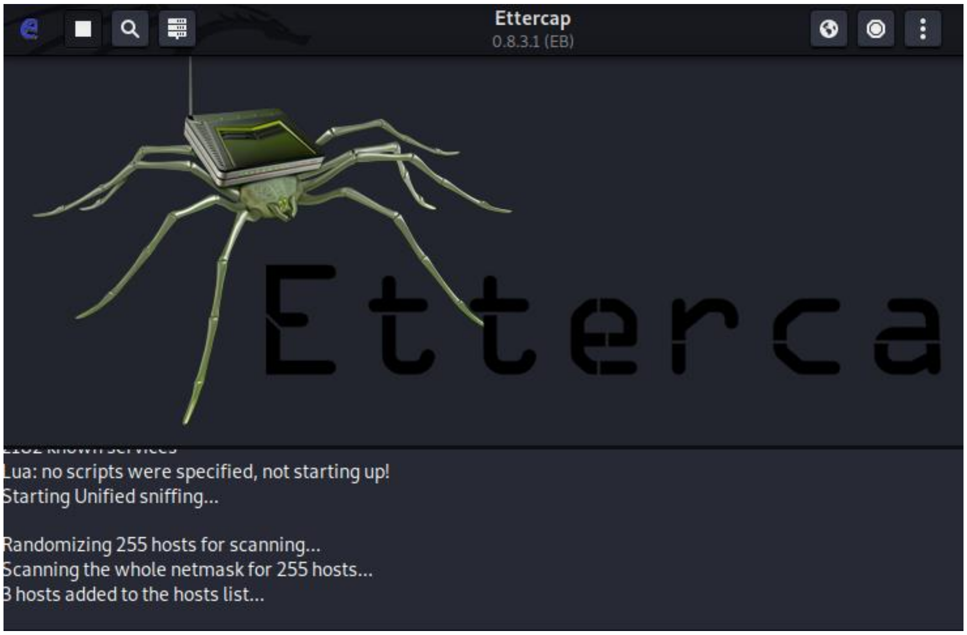
Sniffing at startup: on
Primary Interface: eth0
Bridged sniffing: off
Bridged Interface: Local Loopback

3. Click on the Tick ✓ icon to start sniffing.



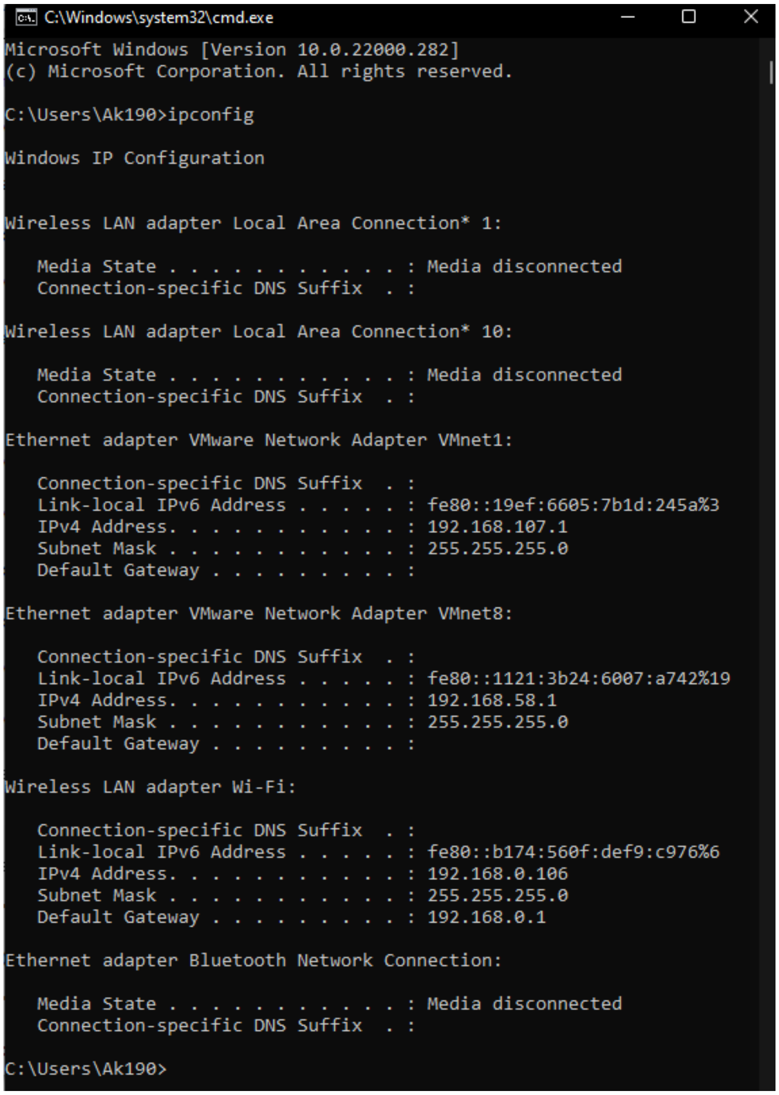
```
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```

4. Click on Search 🔍 Icon to search for host.



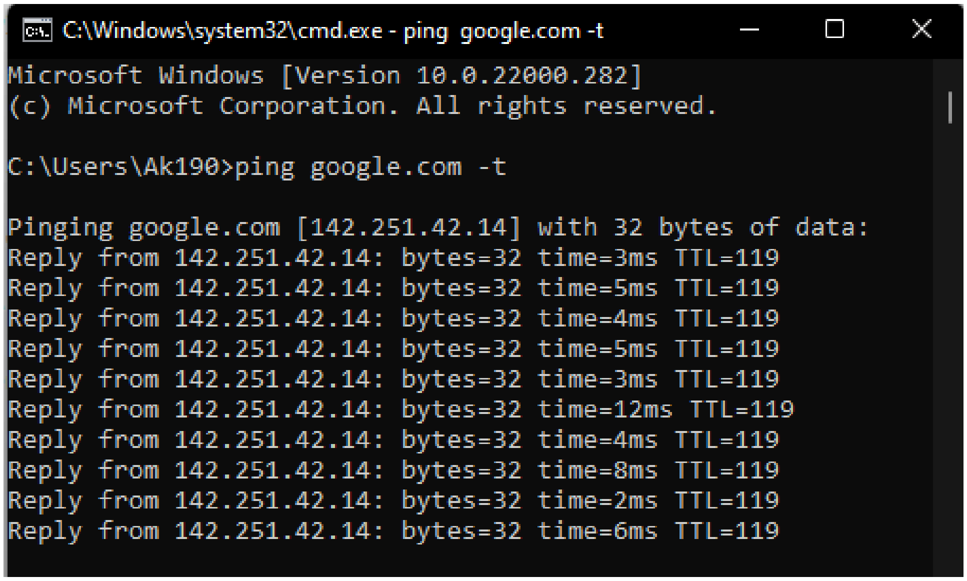
```
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
```

5. Open CMD on windows and type ipconfig and note down the IP Address and Gateway.



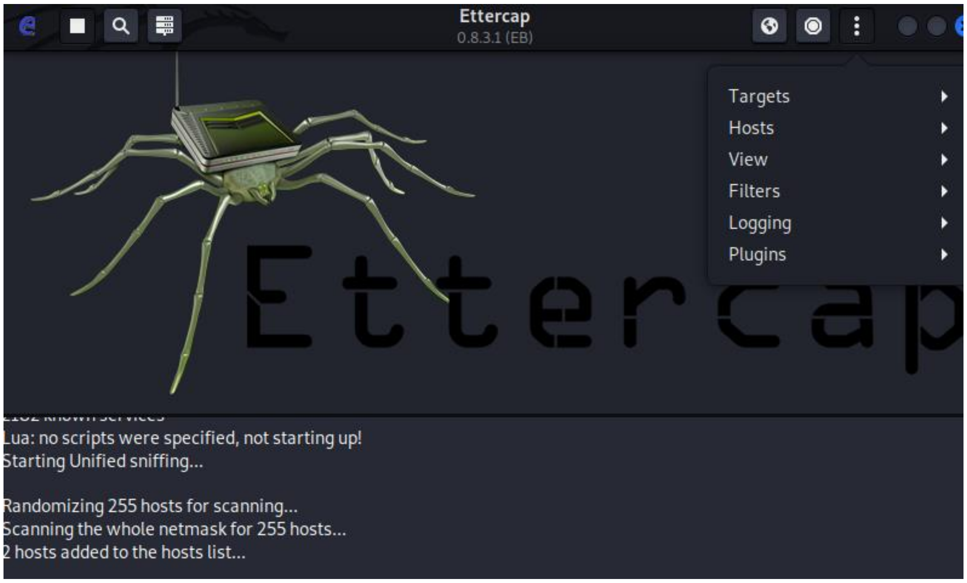
```
Microsoft Windows [Version 10.0.22000.282]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Ak190>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::19ef:6605:7b1d:245a%3
   IPv4 Address. . . . . . . . . . . : 192.168.107.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1121:3b24:6007:a742%19
   IPv4 Address. . . . . . . . . . . : 192.168.58.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b174:560f:def9:c976%6
   IPv4 Address. . . . . . . . . . . : 192.168.0.106
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Ak190>
```

6. Write ping www.google.com -t (to check if our sniffing is successful or not, we ping Facebook to check the packet loss after arp spoofing).

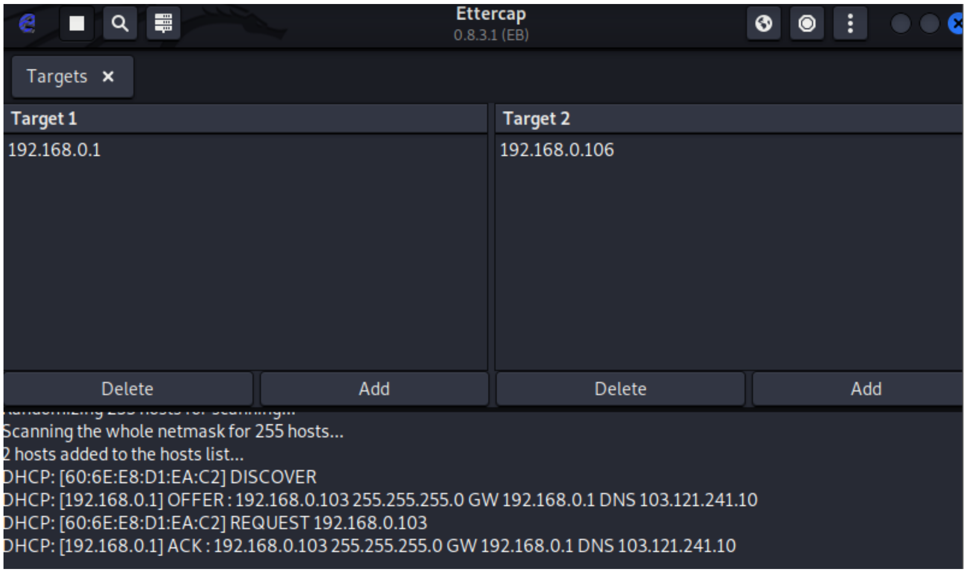


```
Microsoft Windows [Version 10.0.22000.282]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Ak190>ping google.com -t

Pinging google.com [142.251.42.14] with 32 bytes of data:
Reply from 142.251.42.14: bytes=32 time=3ms TTL=119
Reply from 142.251.42.14: bytes=32 time=5ms TTL=119
Reply from 142.251.42.14: bytes=32 time=4ms TTL=119
Reply from 142.251.42.14: bytes=32 time=5ms TTL=119
Reply from 142.251.42.14: bytes=32 time=3ms TTL=119
Reply from 142.251.42.14: bytes=32 time=12ms TTL=119
Reply from 142.251.42.14: bytes=32 time=4ms TTL=119
Reply from 142.251.42.14: bytes=32 time=8ms TTL=119
Reply from 142.251.42.14: bytes=32 time=2ms TTL=119
Reply from 142.251.42.14: bytes=32 time=6ms TTL=119
```

7. Click on targets and add click on add targets, in target 1 add the gateway and in target 2 add your computers ip.



```
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
2 hosts added to the hosts list...
```

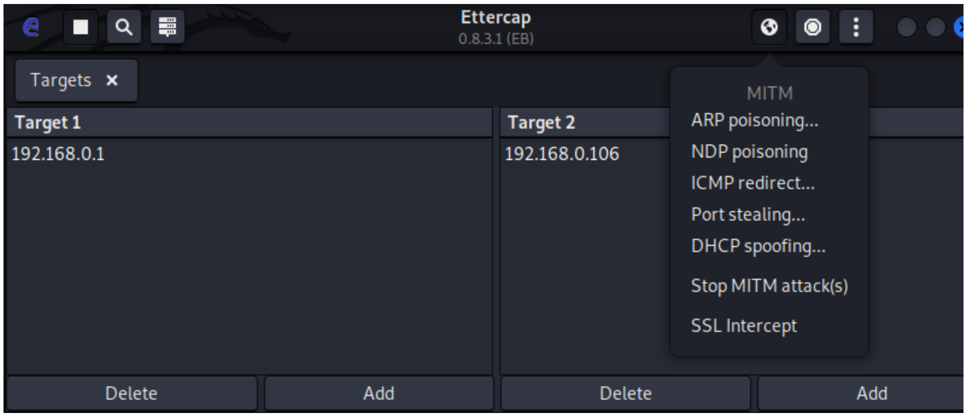


Target 1: 192.168.0.1

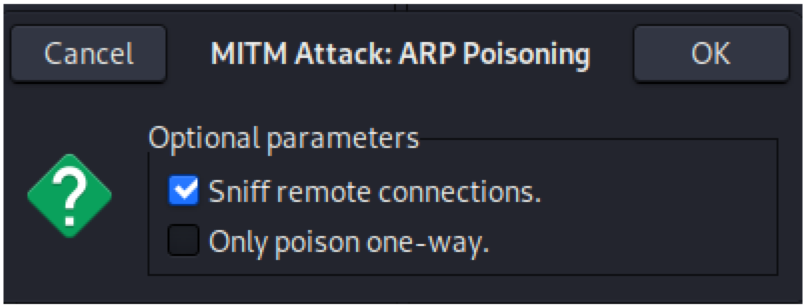
Target 2: 192.168.0.106

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
2 hosts added to the hosts list...
DHCP: [60:6E:E8:D1:EA:C2] DISCOVER
DHCP: [192.168.0.1] OFFER : 192.168.0.103 255.255.255.0 GW 192.168.0.1 DNS 103.121.241.10
DHCP: [60:6E:E8:D1:EA:C2] REQUEST 192.168.0.103
DHCP: [192.168.0.1] ACK : 192.168.0.103 255.255.255.0 GW 192.168.0.1 DNS 103.121.241.10
```

8. Click on MITM and select ARP poisoning.



9. Click on sniff remote connections.

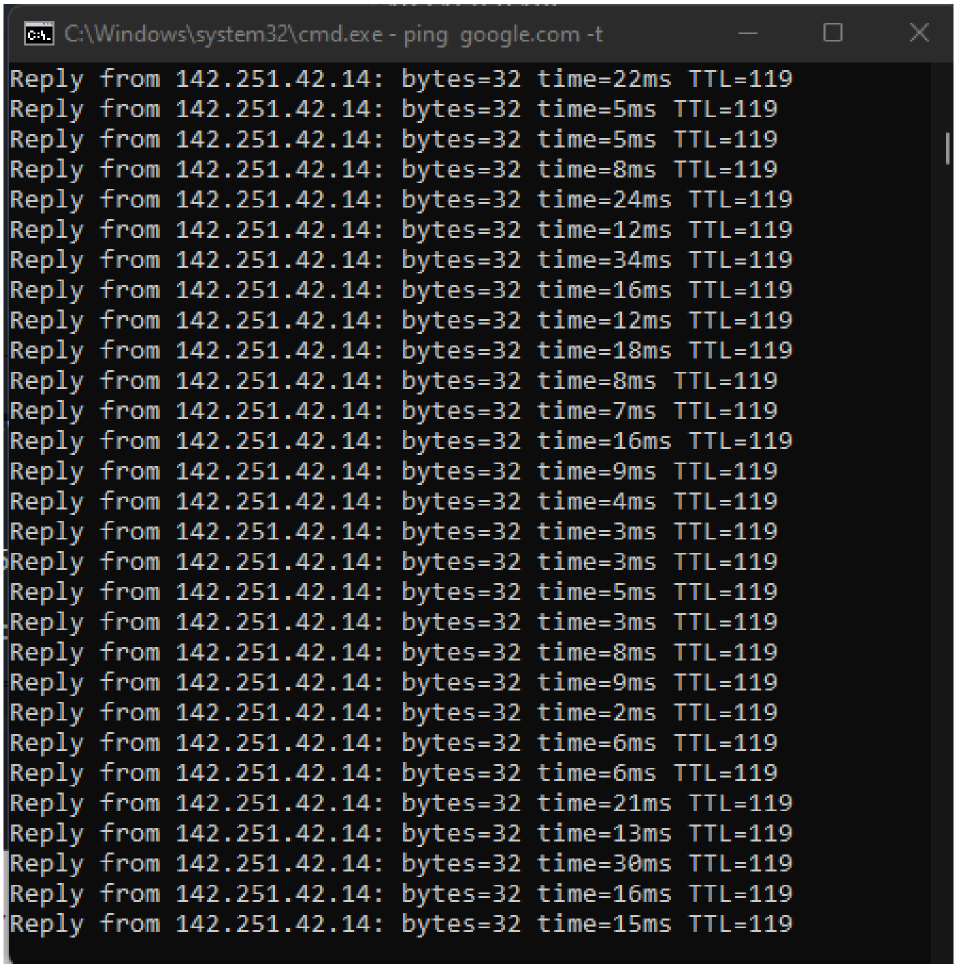


Optional parameters

☑ Sniff remote connections.

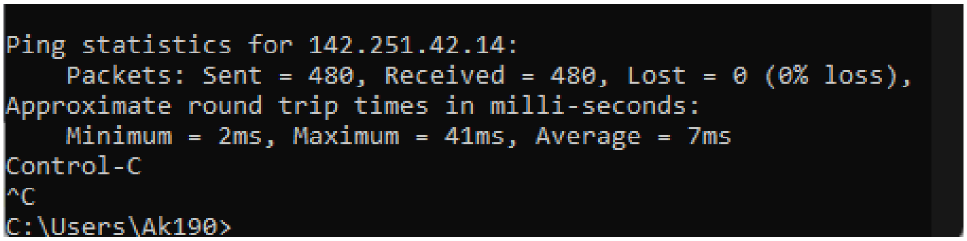
□ Only poison one-way.

10. Open cmd and see that ping command it will show request timeout or ms will go up.



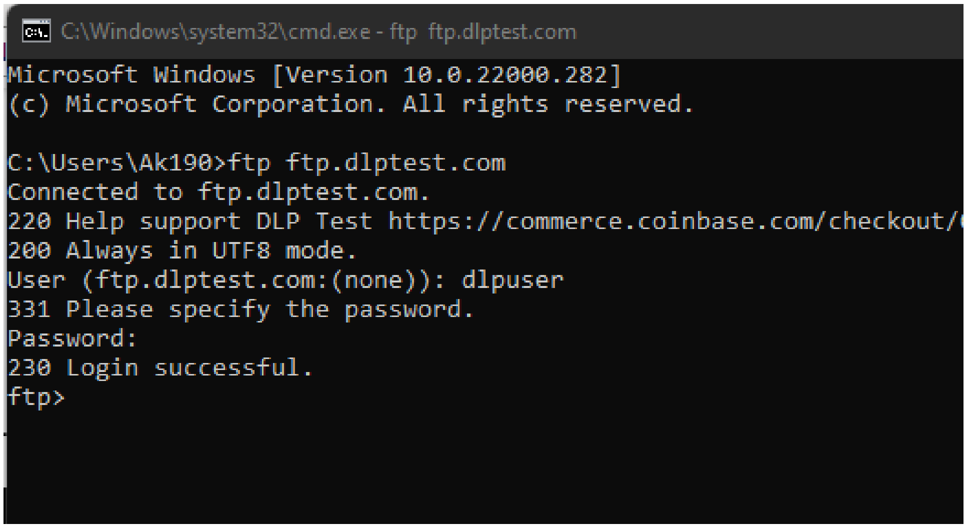
```
Reply from 142.251.42.14: bytes=32 time=22ms TTL=119
Reply from 142.251.42.14: bytes=32 time=5ms TTL=119
Reply from 142.251.42.14: bytes=32 time=5ms TTL=119
Reply from 142.251.42.14: bytes=32 time=8ms TTL=119
Reply from 142.251.42.14: bytes=32 time=24ms TTL=119
Reply from 142.251.42.14: bytes=32 time=12ms TTL=119
Reply from 142.251.42.14: bytes=32 time=34ms TTL=119
Reply from 142.251.42.14: bytes=32 time=16ms TTL=119
Reply from 142.251.42.14: bytes=32 time=12ms TTL=119
Reply from 142.251.42.14: bytes=32 time=18ms TTL=119
Reply from 142.251.42.14: bytes=32 time=8ms TTL=119
Reply from 142.251.42.14: bytes=32 time=7ms TTL=119
Reply from 142.251.42.14: bytes=32 time=16ms TTL=119
Reply from 142.251.42.14: bytes=32 time=9ms TTL=119
Reply from 142.251.42.14: bytes=32 time=4ms TTL=119
Reply from 142.251.42.14: bytes=32 time=3ms TTL=119
Reply from 142.251.42.14: bytes=32 time=3ms TTL=119
Reply from 142.251.42.14: bytes=32 time=5ms TTL=119
Reply from 142.251.42.14: bytes=32 time=3ms TTL=119
Reply from 142.251.42.14: bytes=32 time=8ms TTL=119
Reply from 142.251.42.14: bytes=32 time=9ms TTL=119
Reply from 142.251.42.14: bytes=32 time=2ms TTL=119
Reply from 142.251.42.14: bytes=32 time=6ms TTL=119
Reply from 142.251.42.14: bytes=32 time=6ms TTL=119
Reply from 142.251.42.14: bytes=32 time=21ms TTL=119
Reply from 142.251.42.14: bytes=32 time=13ms TTL=119
Reply from 142.251.42.14: bytes=32 time=30ms TTL=119
Reply from 142.251.42.14: bytes=32 time=16ms TTL=119
Reply from 142.251.42.14: bytes=32 time=15ms TTL=119
```

11.Press control c and stop the ping command there will loss shown in percentage.



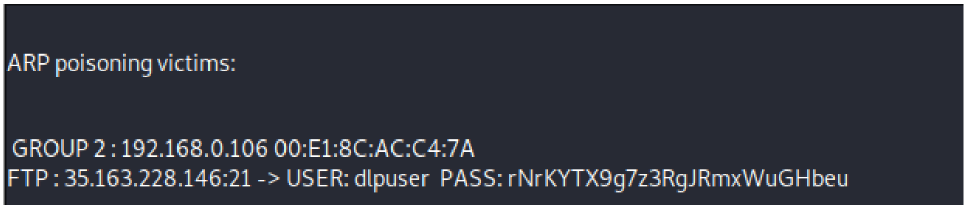
```
Ping statistics for 142.251.42.14:
    Packets: Sent = 480, Received = 480, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 41ms, Average = 7ms
Control-C
^C
C:\Users\Ak190>
```

12. In cmd type “ftp ftp.dlptest.com” or any other free ftp server. for username enter dlpuser and for password enter “rNrKYTX9g7z3RgJRmxWuGHbeu”



```
C:\Windows\system32\cmd.exe - ftp  ftp.dlptest.com
Microsoft Windows [Version 10.0.22000.282]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Ak190>ftp ftp.dlptest.com
Connected to ftp.dlptest.com.
220 Help support DLP Test https://commerce.coinbase.com/checkout/
200 Always in UTF8 mode.
User (ftp.dlptest.com:(none)): dlpuser
331 Please specify the password.
Password:
230 Login successful.
ftp>
```

13. Now go back to the Ettercap the username and password entered in windows command line will be shown in ettercap in linux.



```
ARP poisoning victims:


 GROUP 2 : 192.168.0.106 00:E1:8C:AC:C4:7A
FTP : 35.163.228.146:21 -> USER: dlpuser  PASS: rNrKYTX9g7z3RgJRmxWuGHbeu
```