H M Mythreya
PES2UG20CS130
CNS LAB - 4

Task 1A: Launching ICMP Redirect Attack

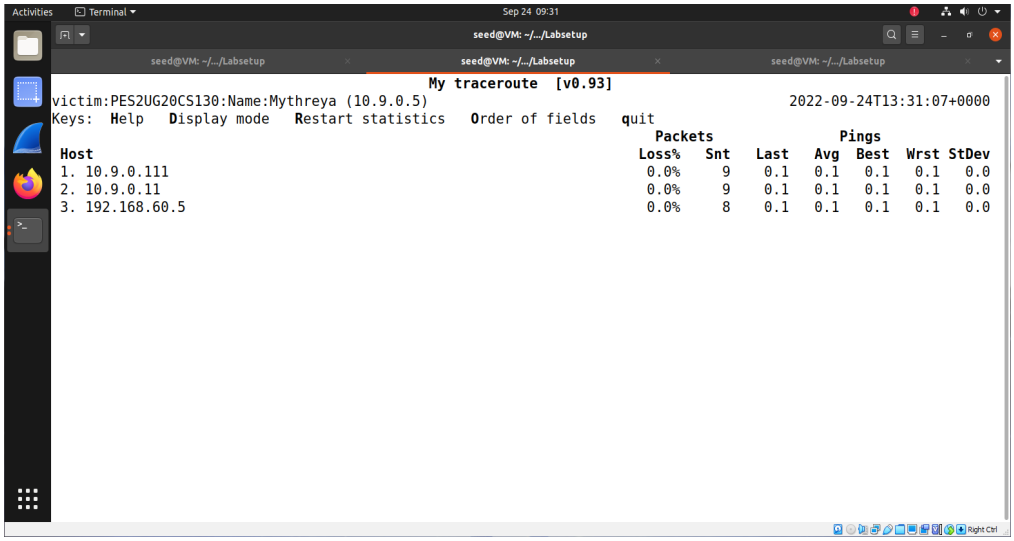
Victim, setting redirects to 1

```
root@victim:PES2UG20CS130:Name:Mythreya:/# ip route
default via 10.9.0.1 dev eth0
10.9.0.0/24 dev eth0 proto kernel scope link src 10.9.0.5
192.168.60.0/24 via 10.9.0.11 dev eth0
root@victim:PES2UG20CS130:Name:Mythreya:/# sysctl net.ipv4.conf.all.accept_redirects=1
net.ipv4.conf.all.accept_redirects = 1
root@victim:PES2UG20CS130:Name:Mythreya:/#
```

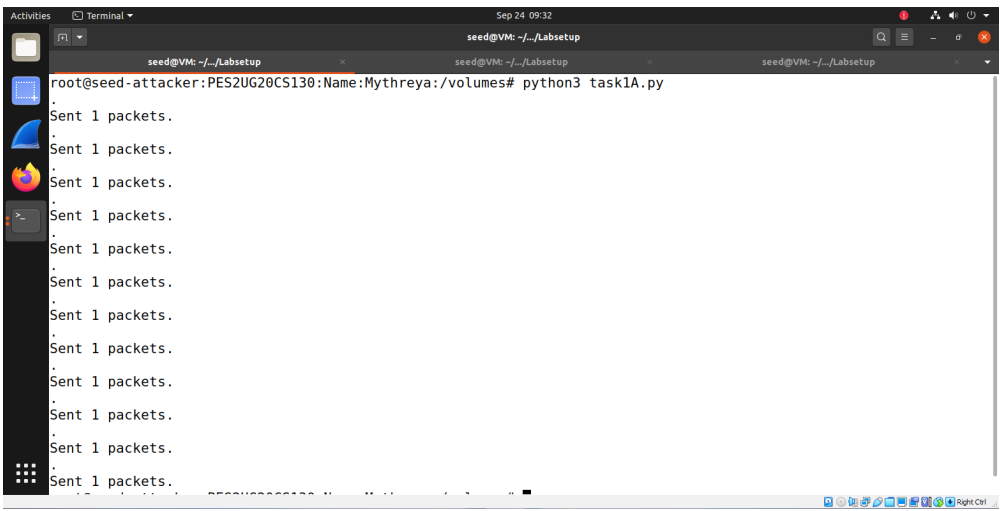
Pinging and checking route cache

```
10.9.0.0/24 dev eth0 proto kernel scope link src 10.9.0.5
192.168.60.0/24 via 10.9.0.11 dev eth0
root@victim:PES2UG20CS130:Name:Mythreya:/# sysctl net.ipv4.conf.all.accept_redirects=1
net.ipv4.conf.all.accept_redirects = 1
root@victim:PES2UG20CS130:Name:Mythreya:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=63 time=0.115 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.067 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.066 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.069 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.071 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.102 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.076 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.069 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.079 ms
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.080 ms
64 bytes from 192.168.60.5: icmp_seq=11 ttl=63 time=0.080 ms
^C
--- 192.168.60.5 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10191ms
rtt min/avg/max/mdev = 0.066/0.079/0.115/0.014 ms
root@victim:PES2UG20CS130:Name:Mythreya:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
    cache <redirected> expires 269sec
root@victim:PES2UG20CS130:Name:Mythreya:/#
```

Traceroute on victim machine

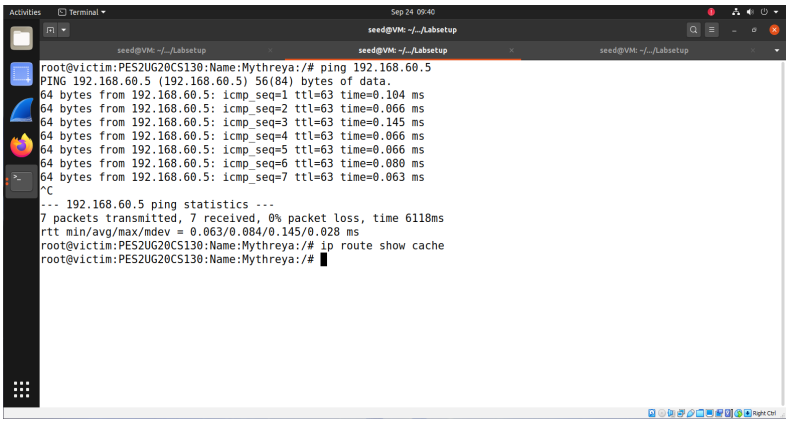


Attacker:

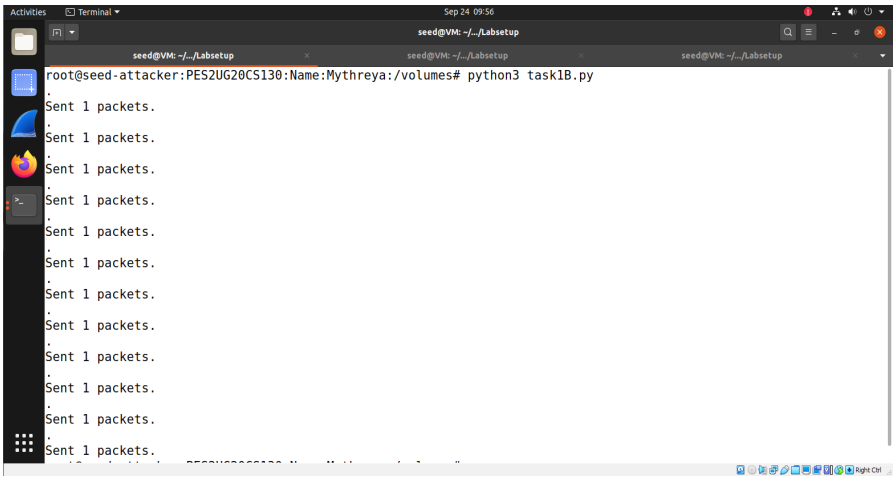


Task 1B

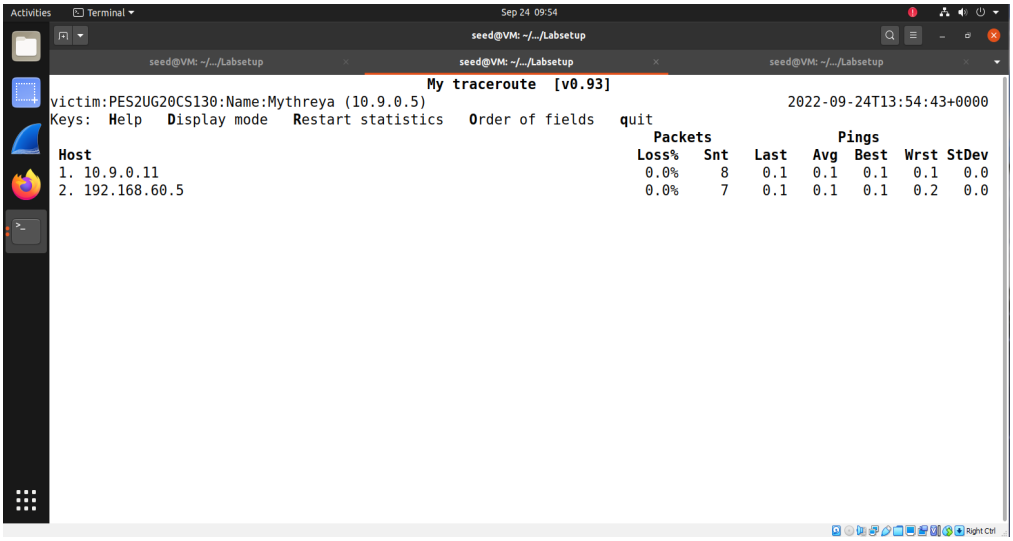
Victim's router cache



Attacker Machine

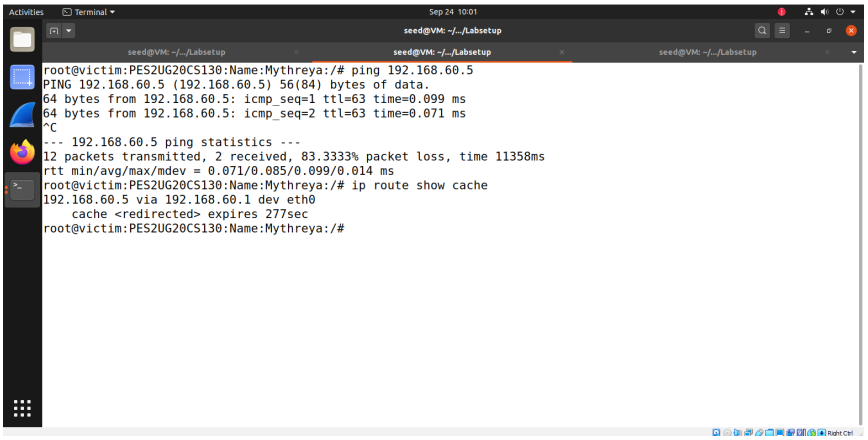


Traceroute on victim machine

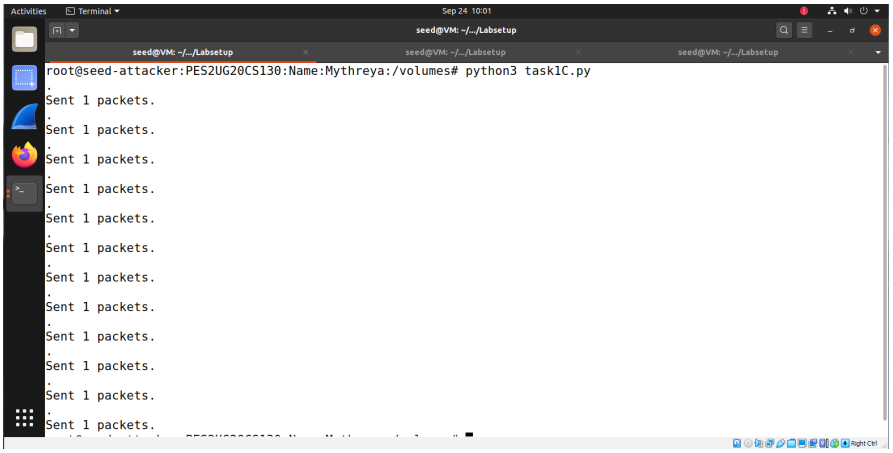


Task 1C

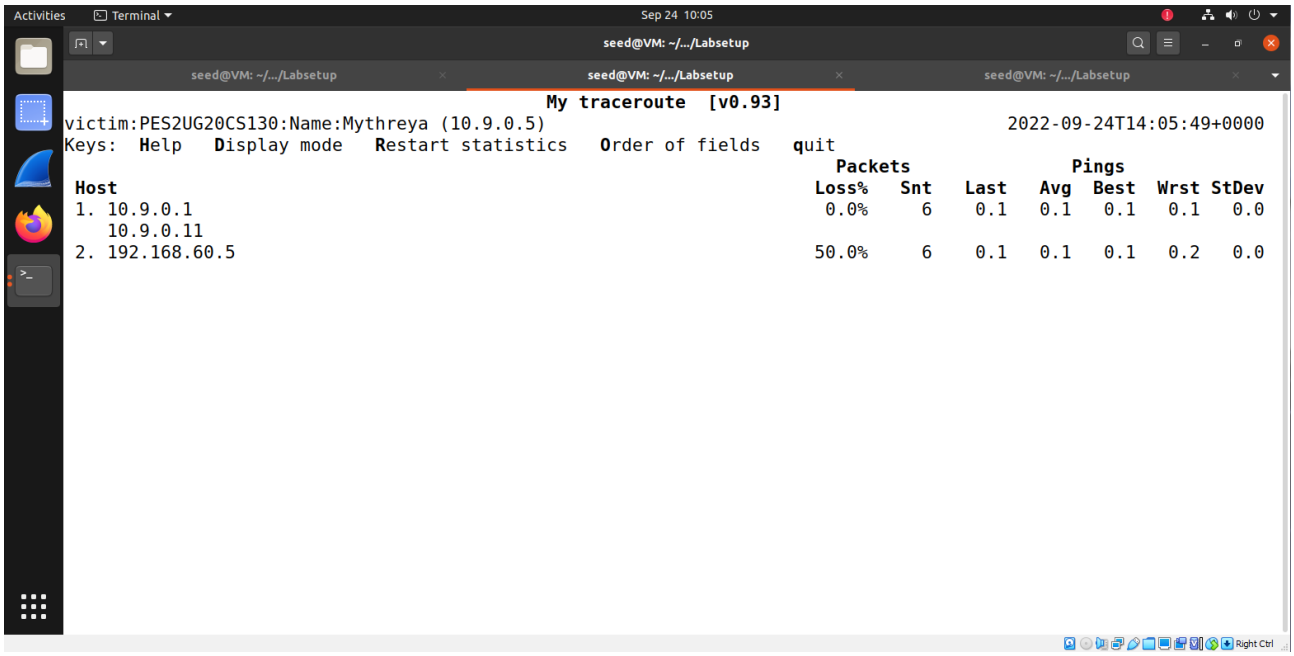
Victim



Attacker

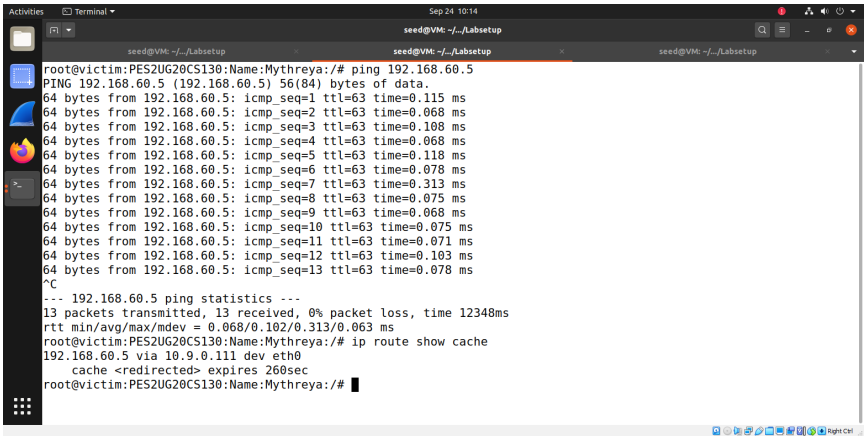


traceroute

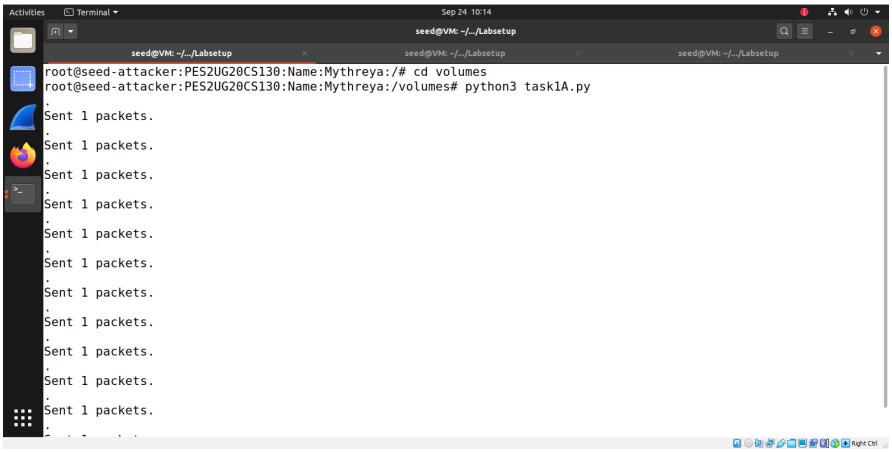


Task 1D

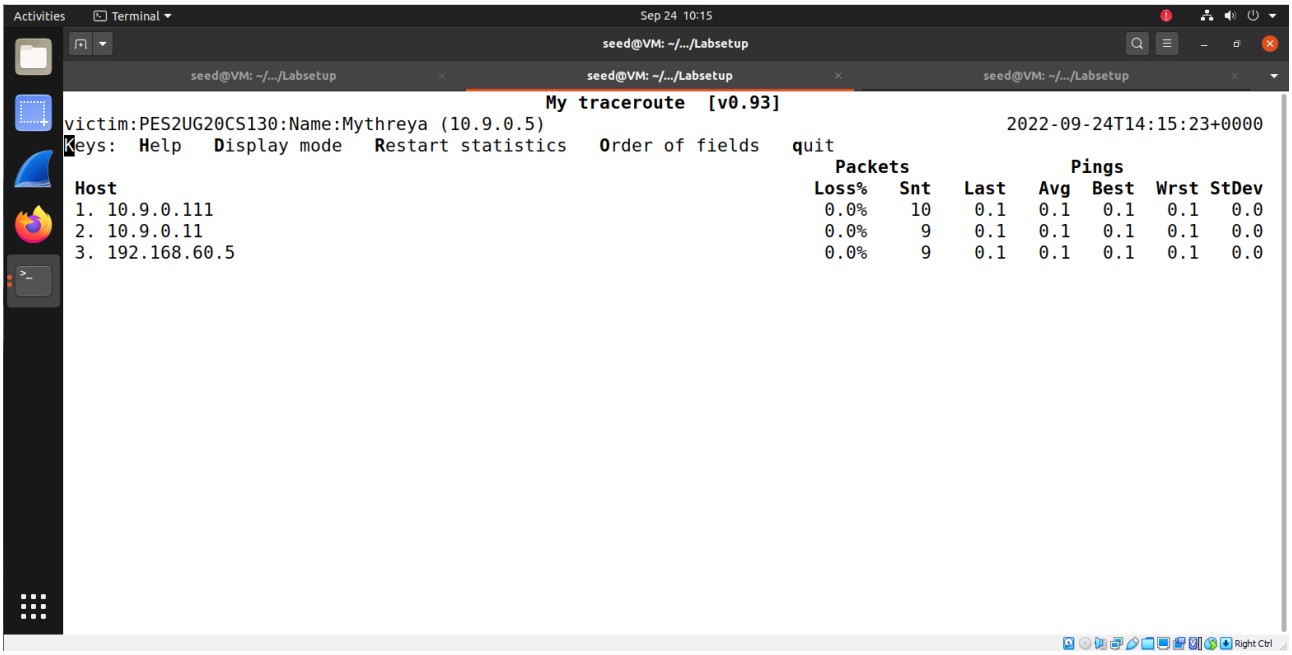
Victim



Attacker



traceroute



Task 2: Launching the MITM Attack

Establishing netcat between victim and host (192.168.60.6)

```
root@victim:PES2UG20CS130:Name:Mythreya:/# nc 192.168.60.5 9090
hi
this is victim machine
```

```
seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup
root@hostB1:PES2UG20CS130:Name:Mythreya:/# nc -lp 9090
hi
this is victim machine
```

Launching MITM attack from malicious router

```
seed@VM: ~/.../volumes    seed@VM: ~/.../volumes
root@malicious-router:PES2UG20CS130:Name:Mythreya:/volumes# python3 mitm.py
LAUNCHING MITM ATTACK.........
*** b'Mythreya\n', length: 9
```

Victim and Host have different messages:

```
seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup
root@victim:PES2UG20CS130:Name:Mythreya:/# nc 192.168.60.5 9090
hi
this is victim machine
Mythreya
```

```
seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup
root@hostB1:PES2UG20CS130:Name:Mythreya:/# nc -lp 9090
hi
this is victim machine
AAAAAAAA
```

Wireshark: