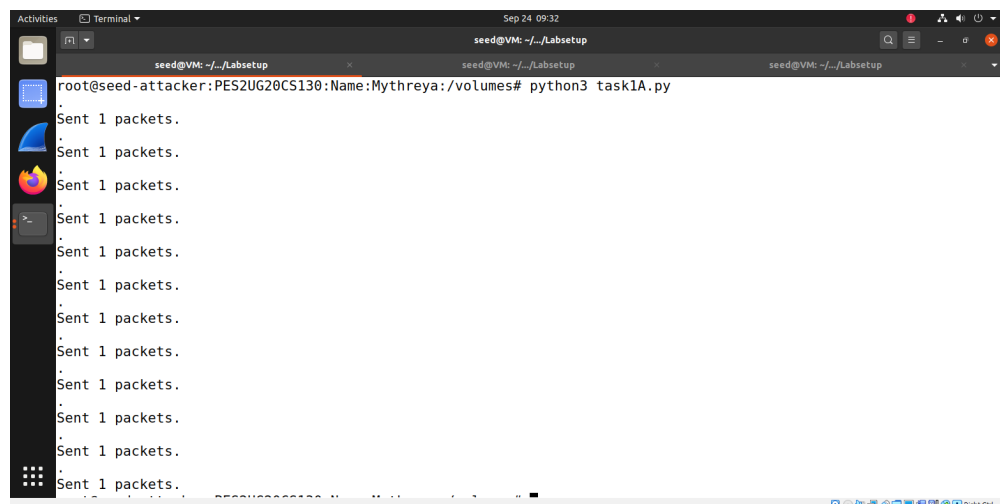


Task 1A: Launching ICMP Redirect Attack

Pinging and checking route cache



Task 1B

Victim's router cache

```
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=0.104 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.066 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.145 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.066 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.066 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.080 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.063 ms
^C
--- 192.168.60.5 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6118ms
rtt min/avg/max/mdev = 0.063/0.084/0.145/0.028 ms
root@victim:PES2UG20CS130:Name:Mythreya:/# ip route show cache
root@victim:PES2UG20CS130:Name:Mythreya:/#
```

Attacker Machine

```
root@seed-attacker:PES2UG20CS130:Name:Mythreya:/volumes# python3 task1B.py
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
```

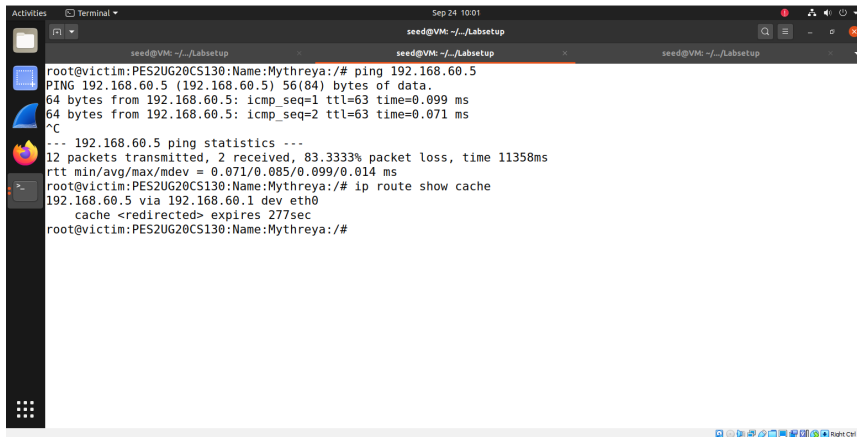
Traceroute on victim machine

```
victim:PES2UG20CS130:Name:Mythreya (10.9.0.5)
Keys: Help Display mode Restart statistics Order of fields quit
My traceroute [v0.93] 2022-09-24T13:54:43+0000

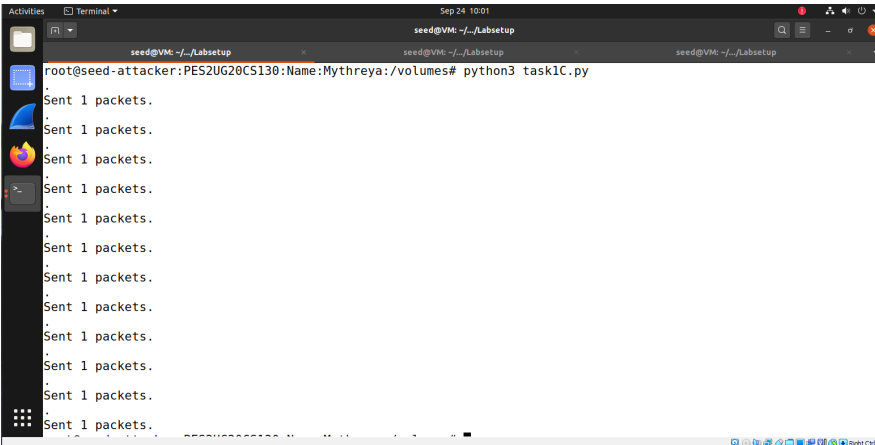
Host      Packets      Pings
Loss%  Snt  Last  Avg  Best  Wrst  StDev
1. 10.9.0.11 0.0%    8   0.1   0.1   0.1   0.1   0.0
2. 192.168.60.5 0.0%    7   0.1   0.1   0.1   0.2   0.0
```

Task 1C

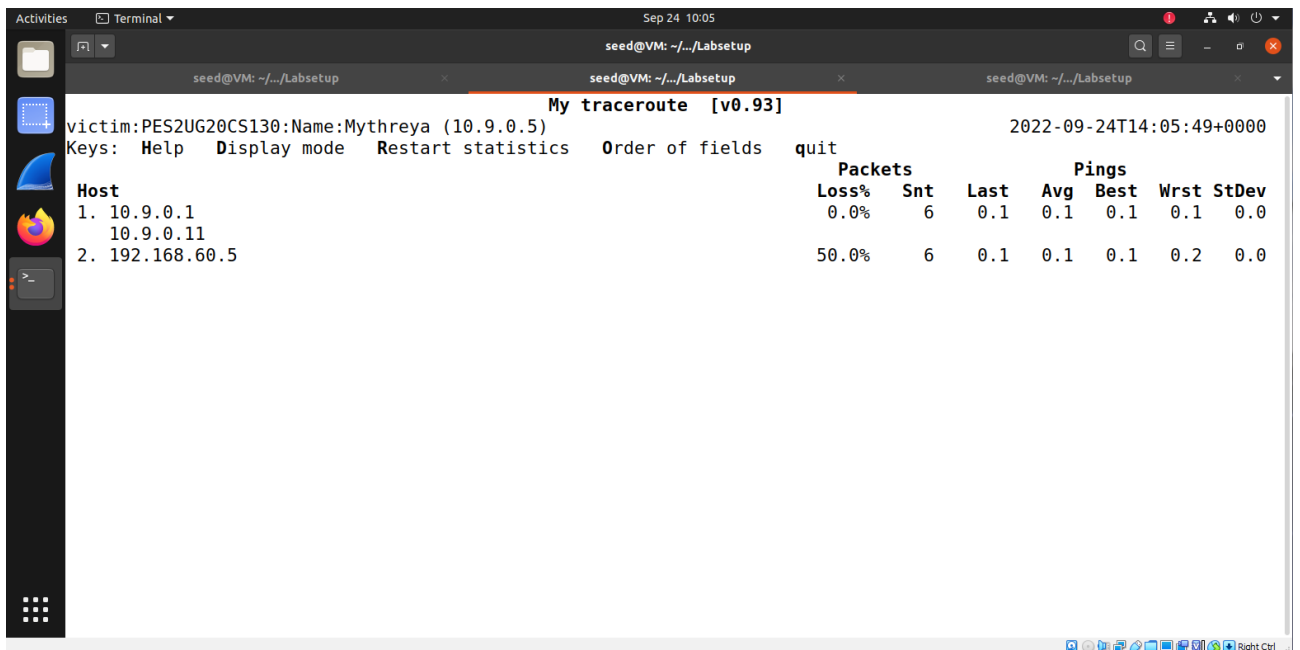
Victim



Attacker

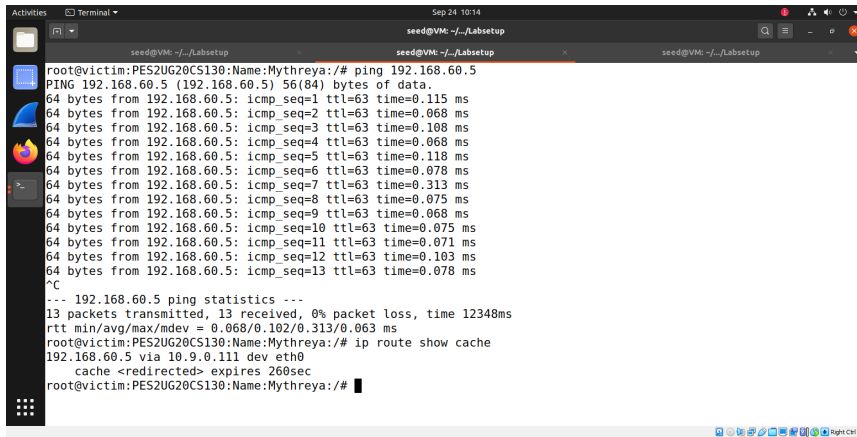


traceroute

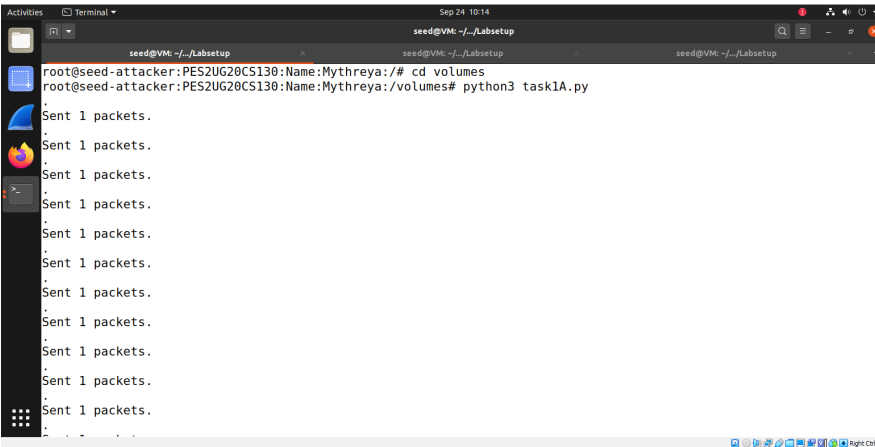


Task 1D

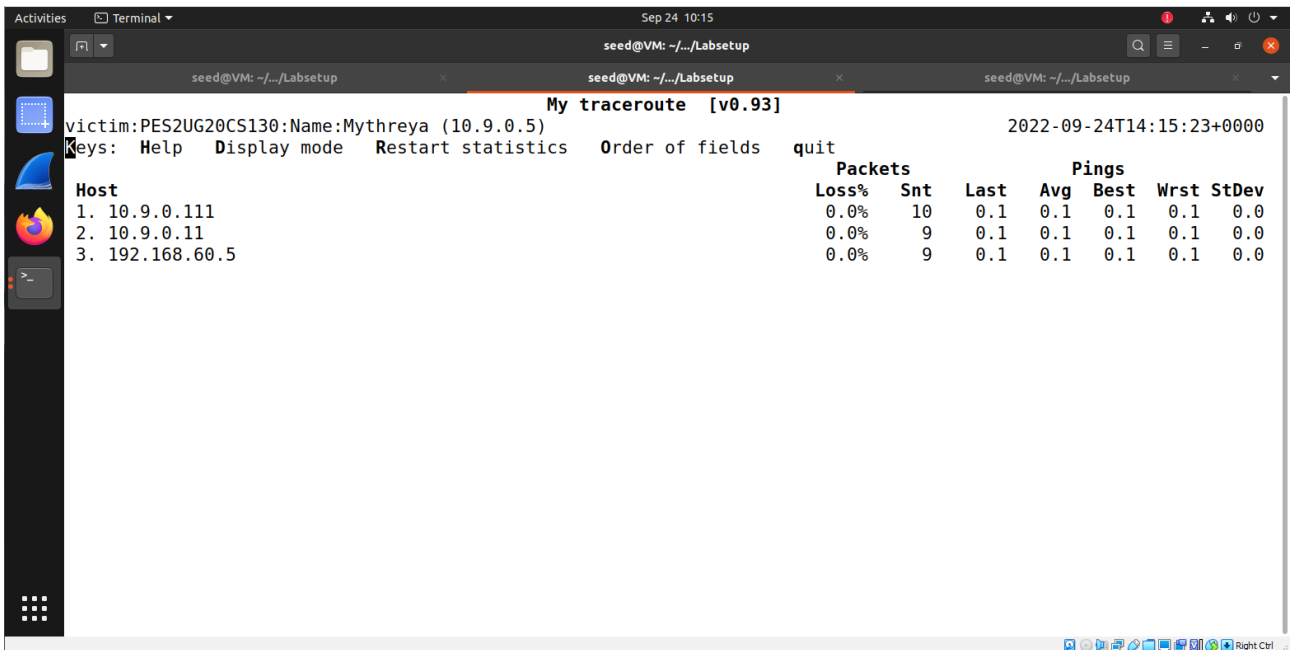
Victim



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

Launching MITM attack from malicious router

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

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

Wireshark:

ip.addr == 192.168.60.5

No.	Time	Source	Destination	Protocol	Length	Info
1134	2022-09-27 10:4...	10.9.0.5	192.168.60.5	TCP	77	[TCP Spurious Retran
1135	2022-09-27 10:4...	10.9.0.5	192.168.60.5	TCP	77	[TCP Spurious Retran
1136	2022-09-27 10:4...	10.9.0.5	192.168.60.5	TCP	77	[TCP Spurious Retran
1137	2022-09-27 10:4...	192.168.60.5	10.9.0.5	TCP	80	[TCP Dup ACK 5#564]
1138	2022-09-27 10:4...	192.168.60.5	10.9.0.5	TCP	80	[TCP Dup ACK 5#565]
1139	2022-09-27 10:4...	192.168.60.5	10.9.0.5	TCP	80	[TCP Dup ACK 5#566]
1140	2022-09-27 10:4...	192.168.60.5	10.9.0.5	TCP	80	[TCP Dup ACK 5#567]
1141	2022-09-27 10:4...	10.9.0.5	192.168.60.5	TCP	77	[TCP Spurious Retran
1142	2022-09-27 10:4...	10.9.0.5	192.168.60.5	TCP	77	[TCP Spurious Retran
1143	2022-09-27 10:4...	10.9.0.5	192.168.60.5	TCP	77	[TCP Spurious Retran
1144	2022-09-27 10:4...	10.9.0.5	192.168.60.5	TCP	77	[TCP Spurious Retran
1145	2022-09-27 10:4...	192.168.60.5	10.9.0.5	TCP	80	[TCP Dup ACK 5#568]
1146	2022-09-27 10:4...	192.168.60.5	10.9.0.5	TCP	80	[TCP Dup ACK 5#569]
1147	2022-09-27 10:4...	192.168.60.5	10.9.0.5	TCP	80	[TCP Dup ACK 5#570]
1148	2022-09-27 10:4...	192.168.60.5	10.9.0.5	TCP	80	[TCP Dup ACK 5#571]

Frame 54: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface any, id 0

- Linux cooked capture
- Internet Protocol Version 4, Src: 192.168.60.5, Dst: 10.9.0.5
- Transmission Control Protocol, Src Port: 9090, Dst Port: 39478, Seq: 2957177025, Ack: 866816314, Len: 80

0000 00 04 00 01 00 06 02 42 c0 a8 3c 05 00 00 08 00B .<.....
0010 45 00 00 40 03 00 40 00 40 06 30 fd c0 a8 3c 05 E...@...@.0...<.