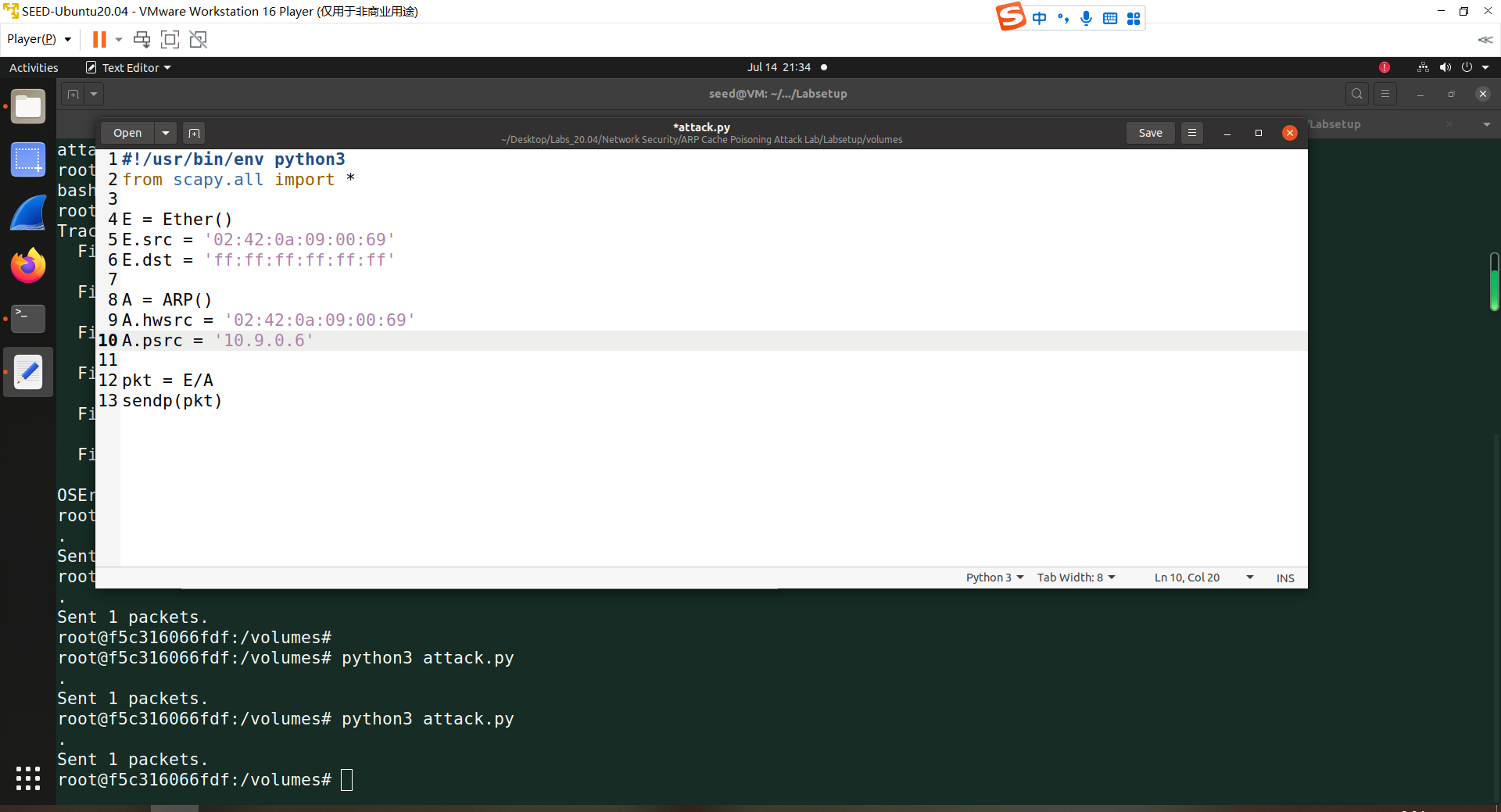
**ARP Cache Poisoning Attack Lab**

**57118215程文泽**

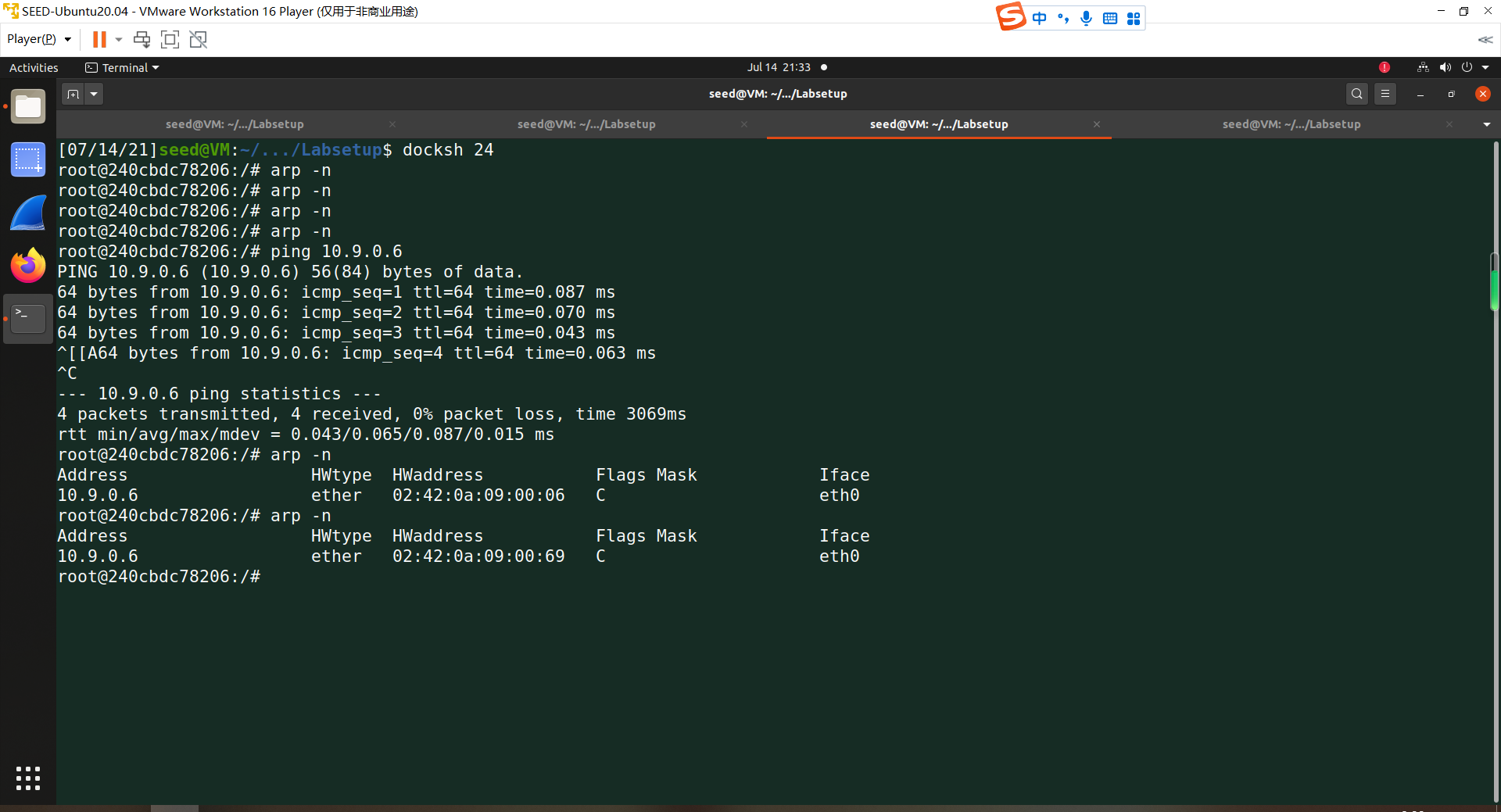
**Task 1: ARP Cache Poisoning**

**Task 1.A (using ARP request)**

构造ARP数据包脚本如下：

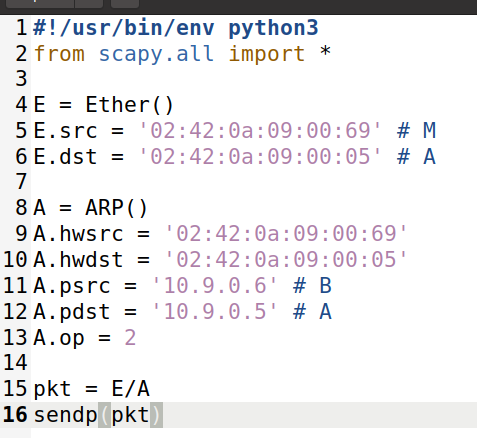


在进行攻击之前查看主机A中的ARP缓存，有来自主机B的MAC地址对B的IP地址的映射，随后运行脚本，再次查看主机A中的ARP缓存，可以看到主机M的MAC地址映射到B的IP地址上。



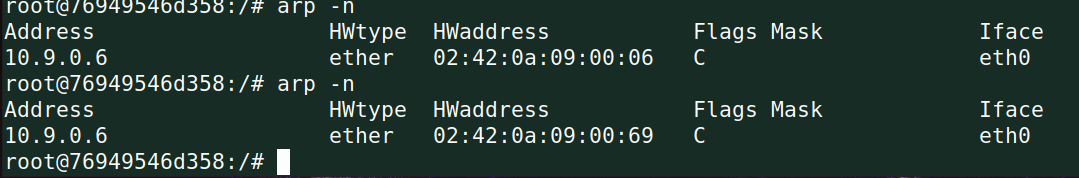
**Task 1.B (using ARP reply)**

构造ARP数据包脚本如下：



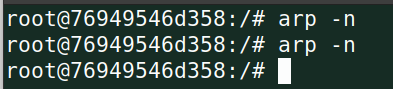
**Scenario 1: B’s IP is already in A’s cache**

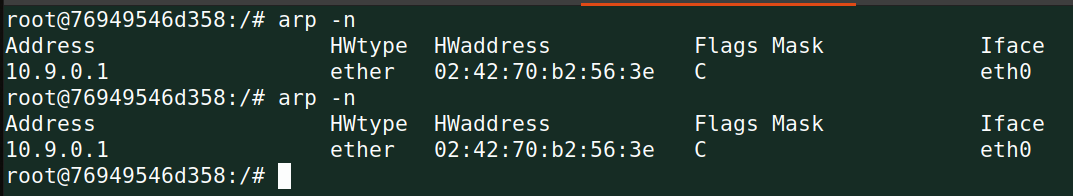
在进行攻击之前查看主机A中的ARP缓存，有来自主机B的MAC地址对B的IP地址的映射，随后运行脚本，再次查看主机A中的ARP缓存，可以看到主机M的MAC地址映射到B的IP地址上。



**Scenario 2: B’s IP is not in A’s cache**

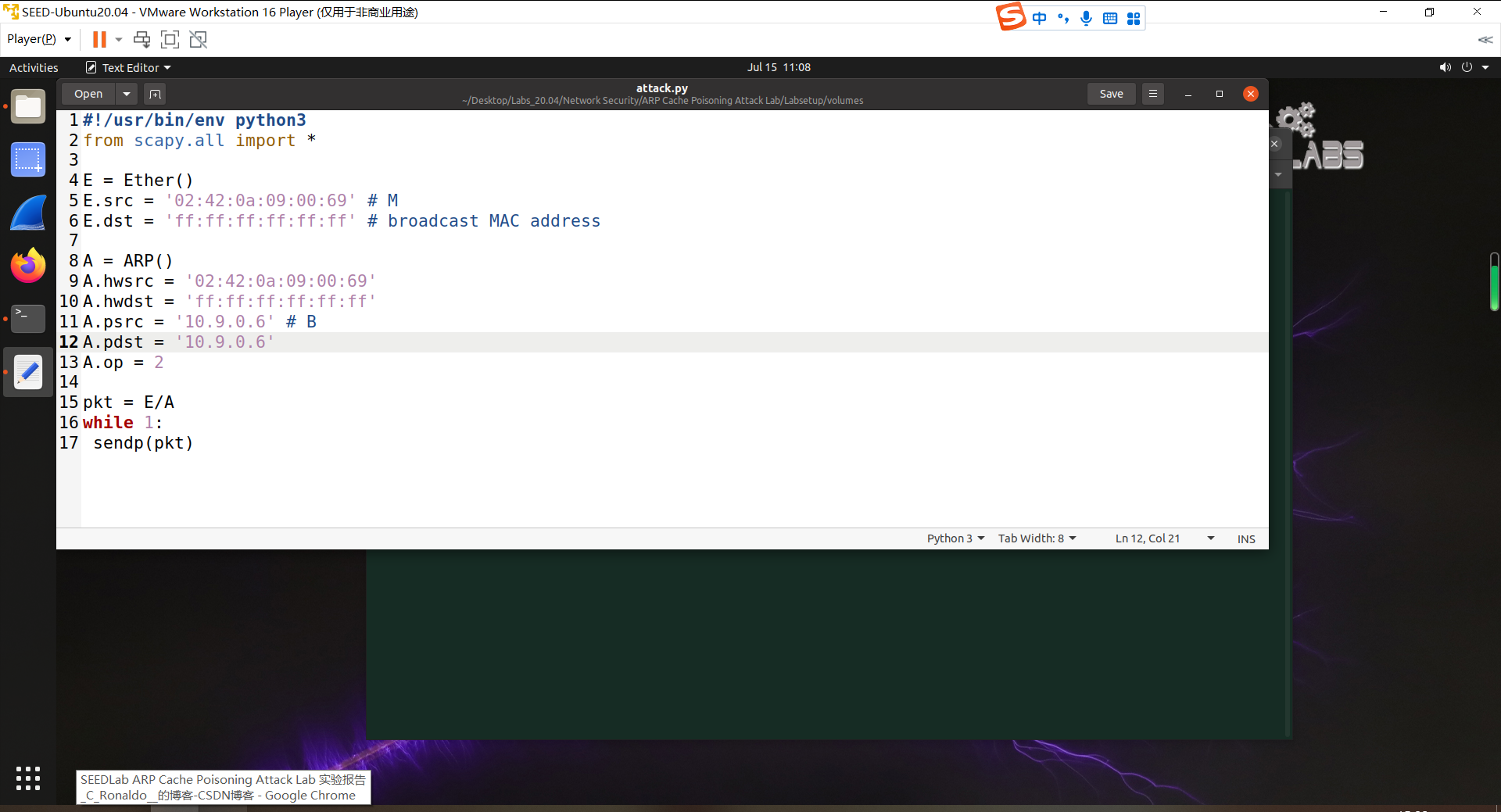
在进行攻击之前查看主机A中的ARP缓存，为空，随后运行脚本，再次查看主机A中的ARP缓存，仍然为空，攻击失败。如果主机A中的ARP缓存不为空，但不存在B的IP地址的MAC映射，结果仍然是失败。





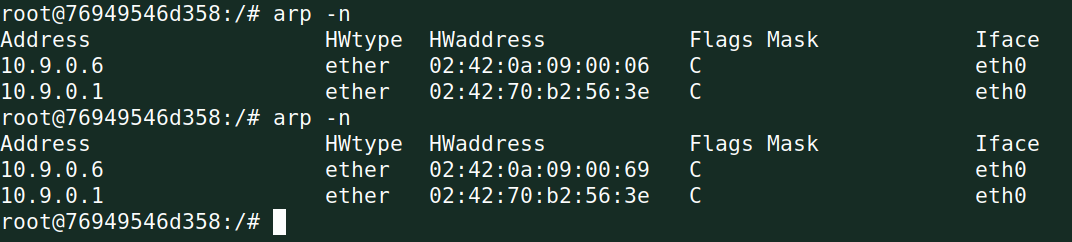
**Task 1C (using ARP gratuitous message)**

构造ARP数据包脚本如下：



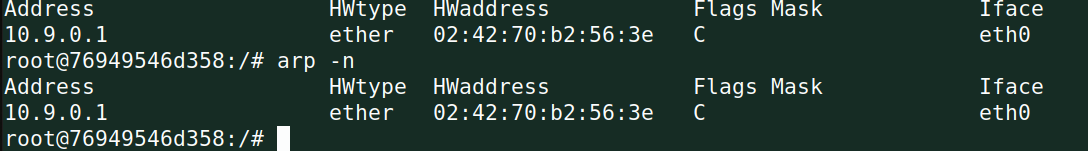
**Scenario 1: B’s IP is already in A’s cache**

在进行攻击之前查看主机A中的ARP缓存，有来自主机B的MAC地址对B的IP地址的映射，随后运行脚本，再次查看主机A中的ARP缓存，可以看到主机M的MAC地址映射到B的IP地址上。



**Scenario 2: B’s IP is not in A’s cache**

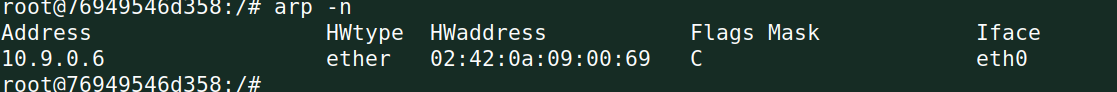
在进行攻击之前查看主机A中的ARP缓存，不存在B的IP地址的MAC映射，结果是攻击失败

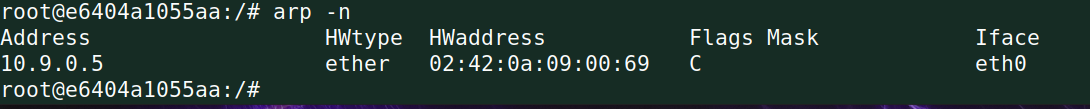


**Task 2: MITM Attack on Telnet using ARP Cache Poisoning**

**Step 1 (Launch the ARP cache poisoning attack)**

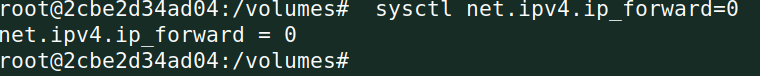
如下图，成功在A的ARP缓存中，把B的IP地址映射到M的MAC地址，以及在B的ARP缓存中，把A的IP地址也映射到M的MAC地址



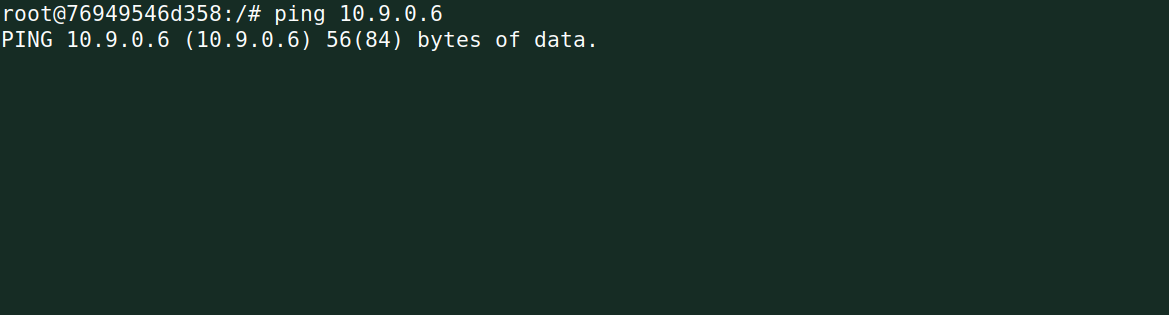


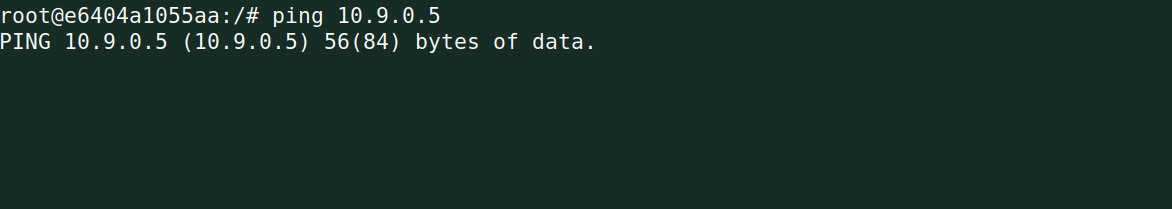
**Step 2 (Testing)**

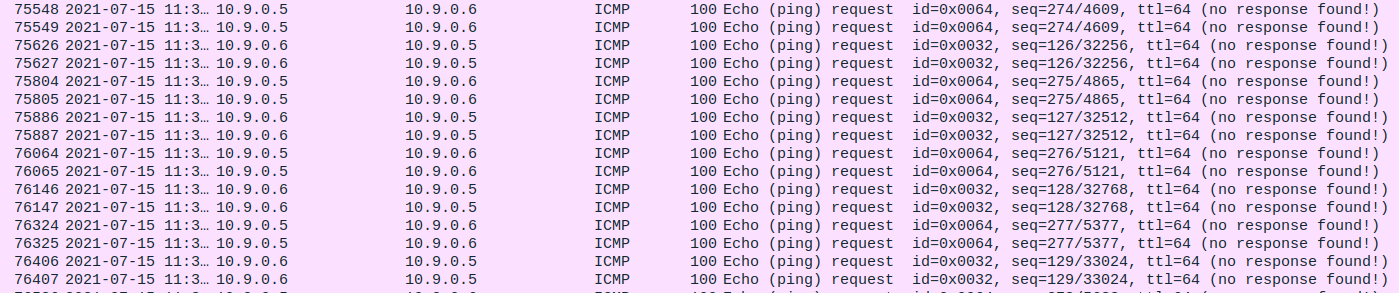
关闭主机M上的IP转发：



尝试在主机A上ping主机B，无反应，在主机B上ping主机A，也无反应，利用wireshark进行抓包，发现许多ICMP数据包无应答

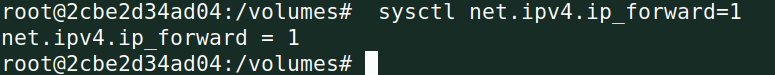




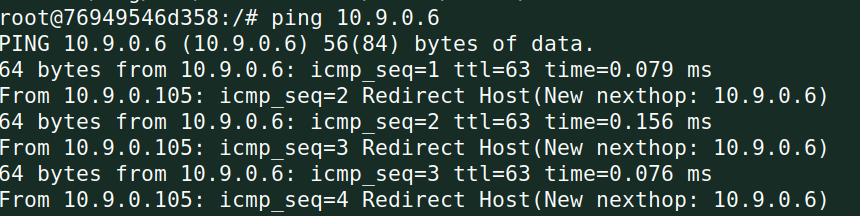


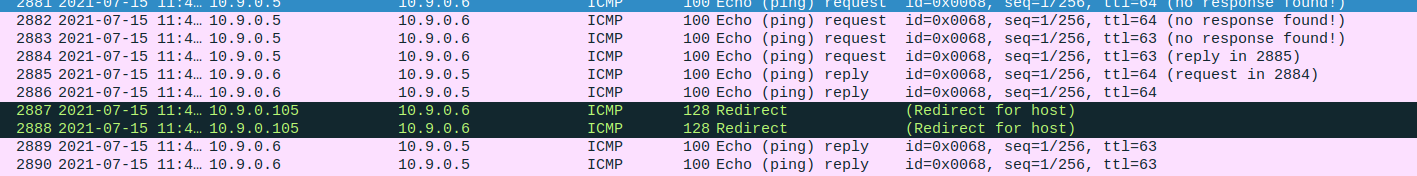
**Step 3 (Turn on IP forwarding)**

打开主机M上的IP转发：

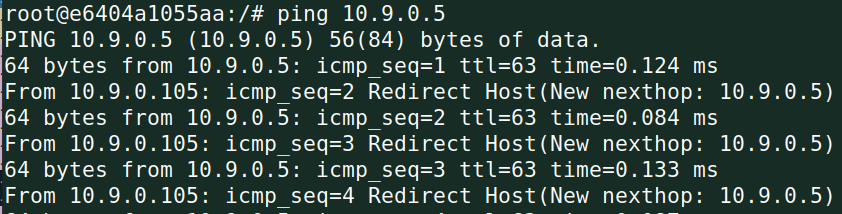


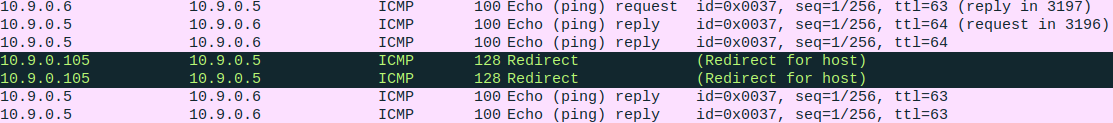
尝试在主机A上ping主机B，有应答，用wireshark进行抓包，发现了来自主机M的重定向报文，





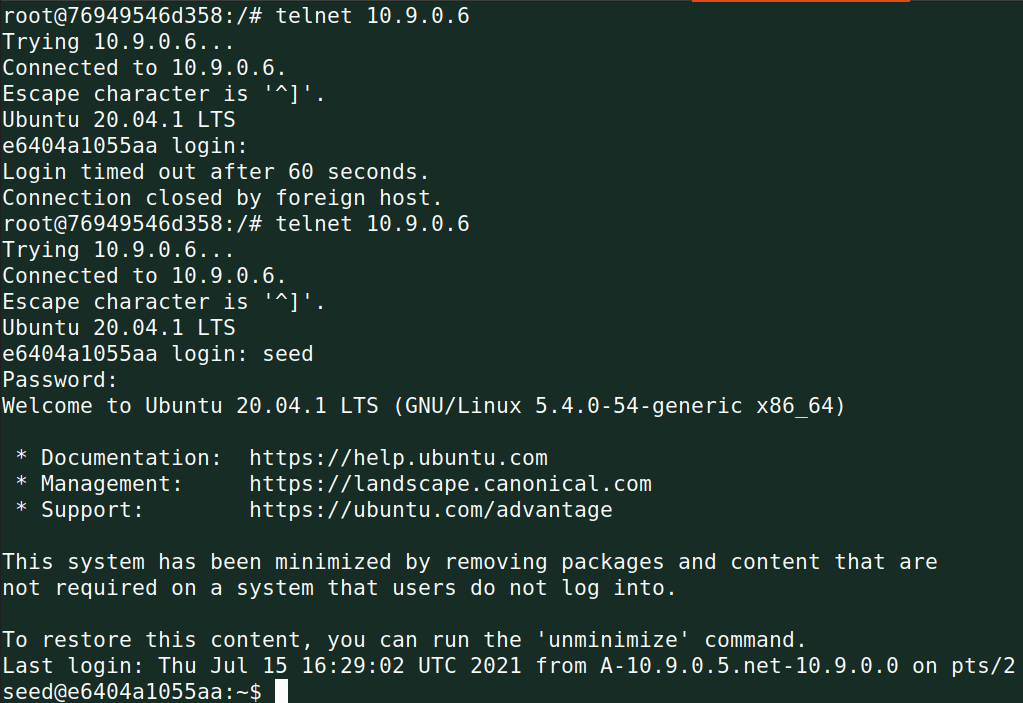
尝试在主机B上ping主机A，有应答，用wireshark进行抓包，也发现了来自主机M的重定向报文，



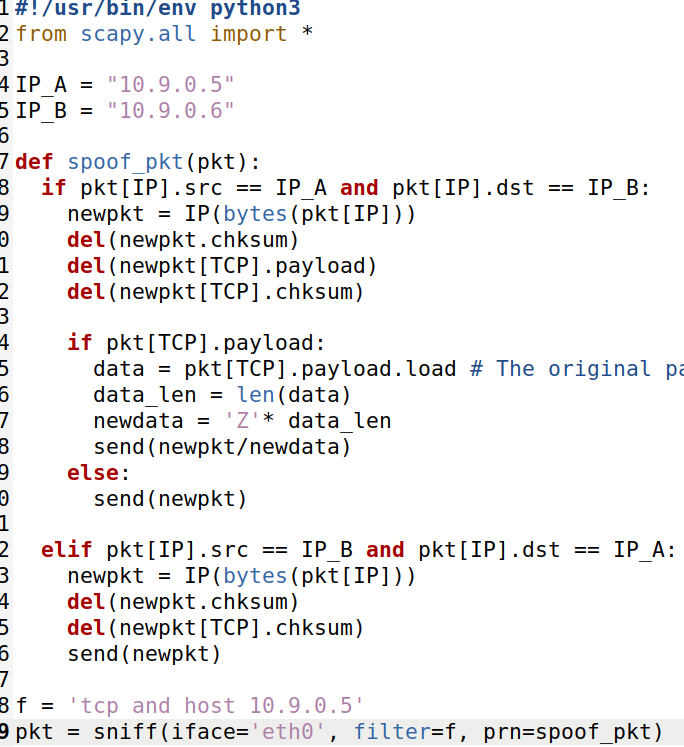


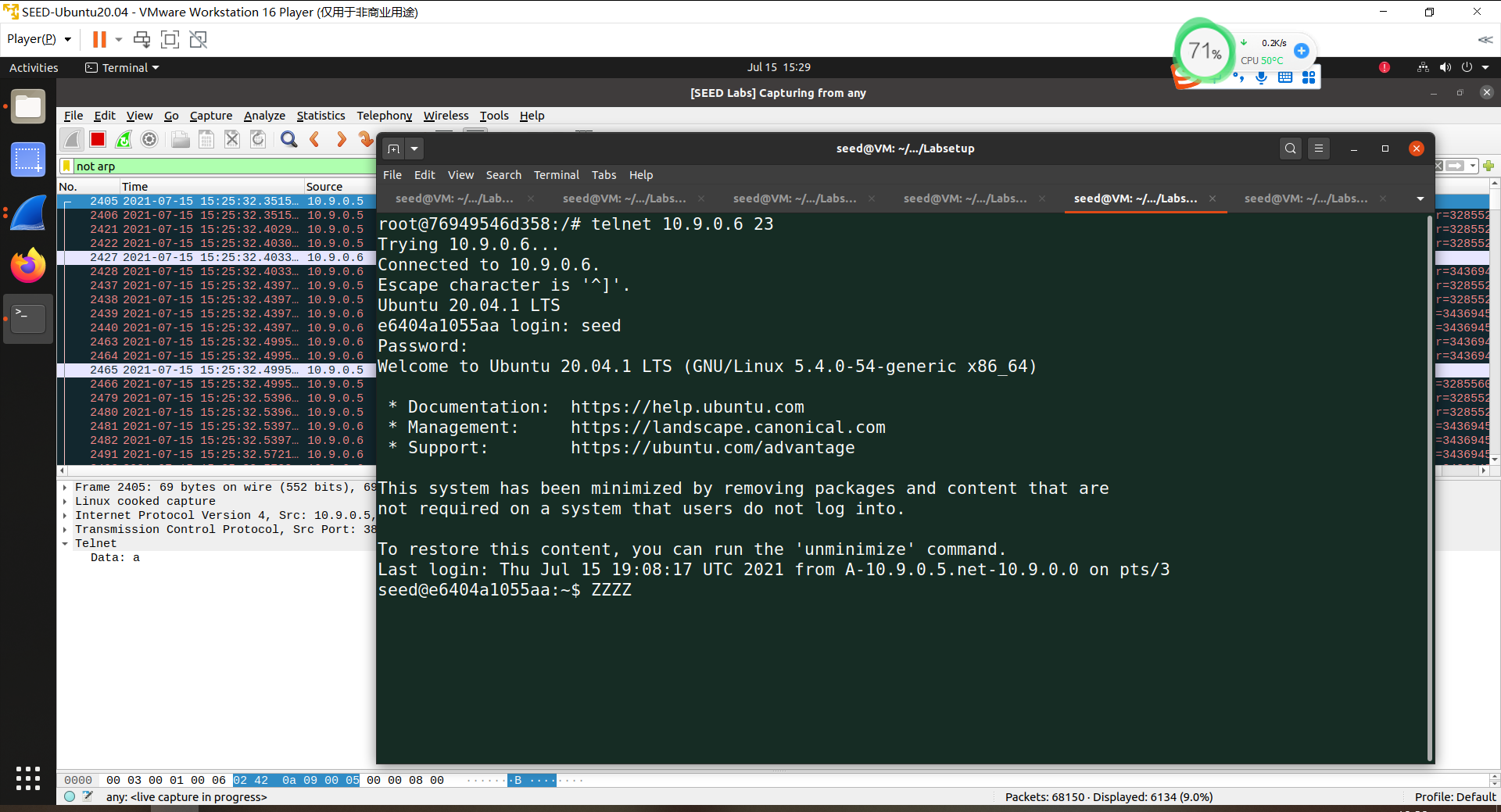
**Step 4 (Launch the MITM attack)**

在主机A上telnet远程登入到主机B上，然后关闭主机M上的IP转发，在主机A上进行键入，发现无响应，

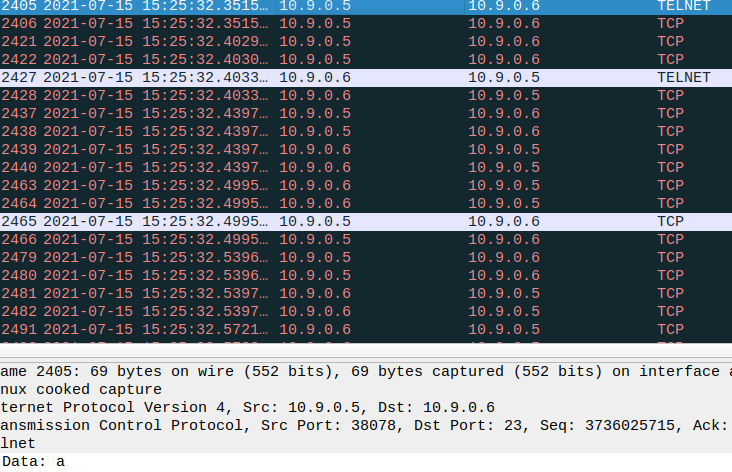


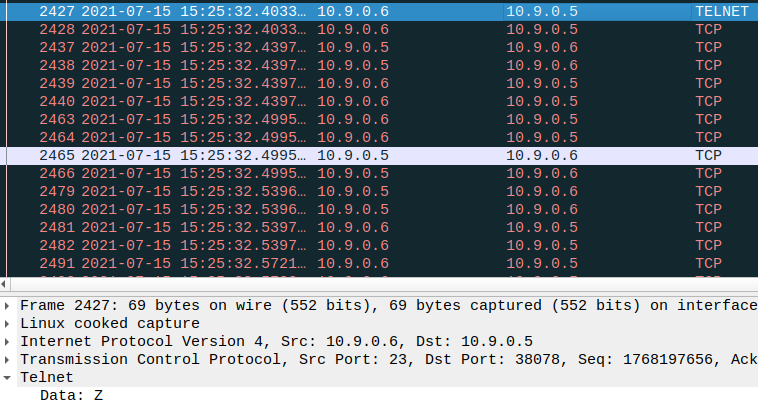
在主机M运行中间人攻击脚本，再在主机A上进行键入，输入a，返回了Z，





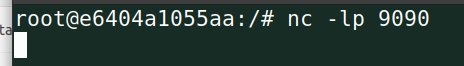
通过wireshark抓包如下，键入的是a，显示的是Z





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

主机A和B使用natcat进行通信

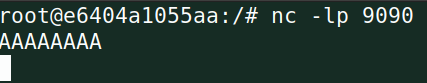




在主机M运行中间人攻击脚本，在主机A中键入seedlabs，可以在主机B中发现显示的是AAAAAAAA







通过wireshark进行抓包，可以看到发出的报文中seedlabs改成了AAAAAAAA

