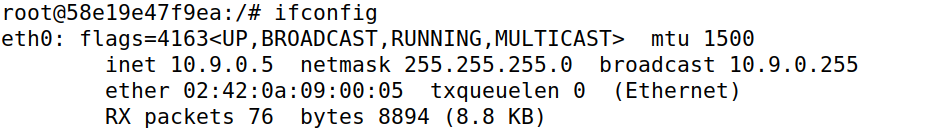
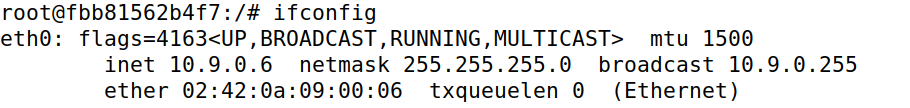
**ARP Cache Poisoning Attack Lab**57118112 王怡乐

**Task 1: ARP Cache Poisoning**

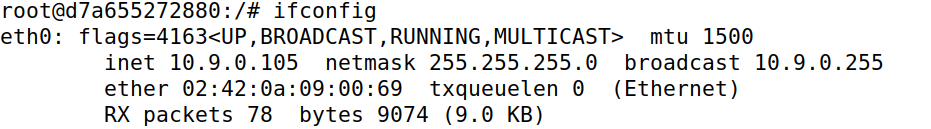
查看主机A的ip地址和mac地址



查看主机B的ip地址和mac地址



查看主机M的ip地址和mac地址

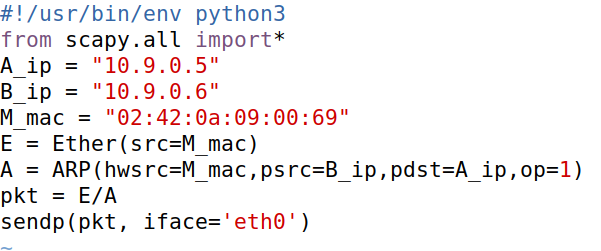


**• Task 1.A (using ARP request)**

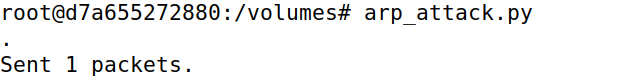
攻击前，在主机A上执行arp -n命令查看arp缓存，发现缓存为空



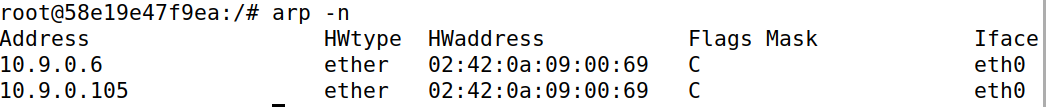
构造arp攻击报文如下，其中op为1表示是request报文。该报文是主机B发给主机A的 arp 请求包，用的是主机M也就是攻击主机的 mac地址



在主机M上执行攻击程序

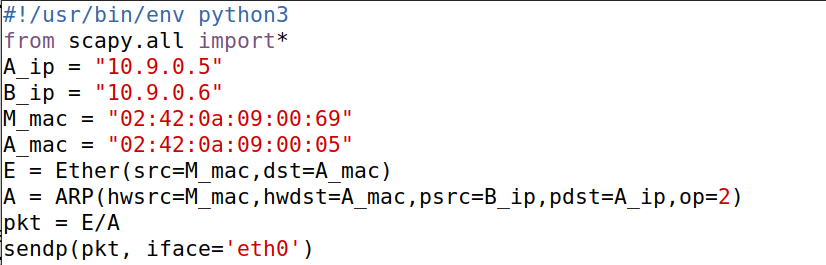


查看主机A的arp缓存，发现了主机B的ip对应主机M的mac地址，同时也有主机M的ip地址和mac地址的对应

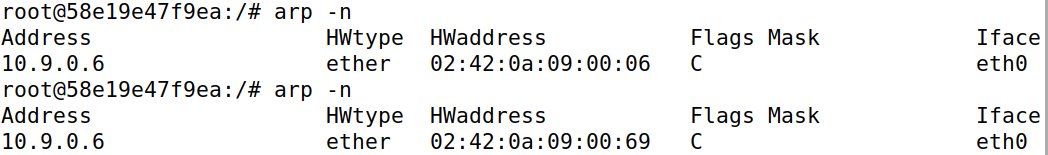


**• Task 1.B (using ARP reply)**

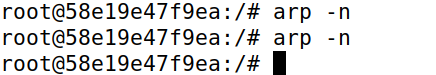
更改攻击程序如下



（1）B的ip在A的缓存中，执行攻击程序，主机B的ip地址映射到主机M的mac地址，攻击成功

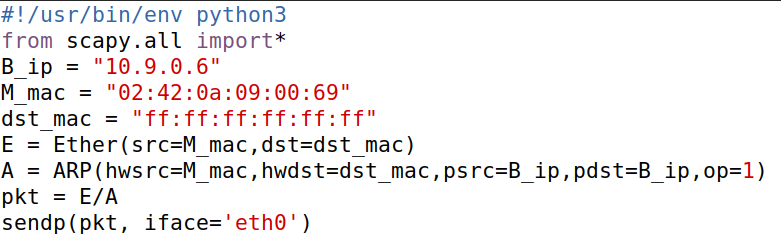


（2）B的ip不在A的缓存中，使用arp -d 10.9.0.6 删除相关缓存信息，执行攻击程序后发现仍然没有主机B的ip地址相关的缓存条目，攻击不成功

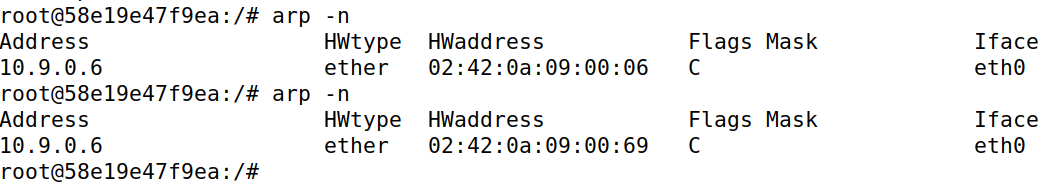


**• Task 1C (using ARP gratuitous message)**

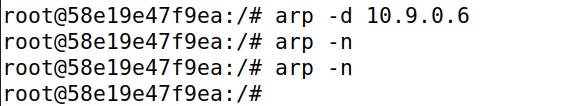
更改攻击程序如下



（1）B的ip在A的缓存中，执行攻击程序，主机B的ip地址映射到主机M的mac地址，攻击成功



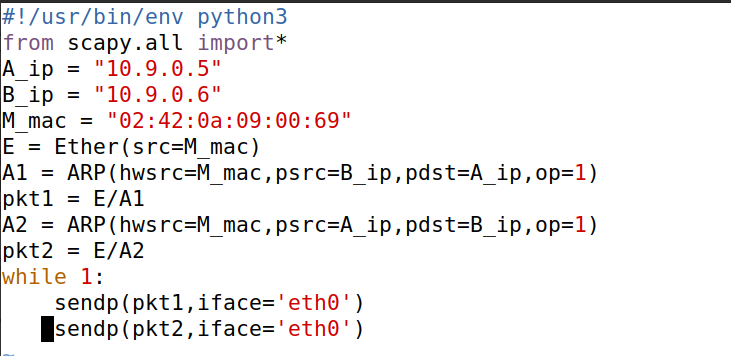
（2）B的ip不在A的缓存中，执行攻击程序后发现仍然没有主机B的ip地址相关的缓存条目，攻击不成功



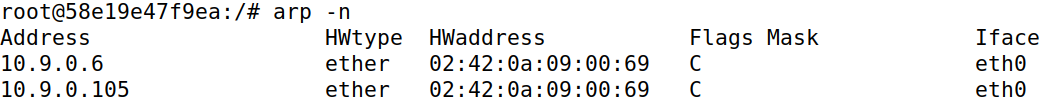
**Task 2: MITM Attack on Telnet using ARP Cache Poisoning**

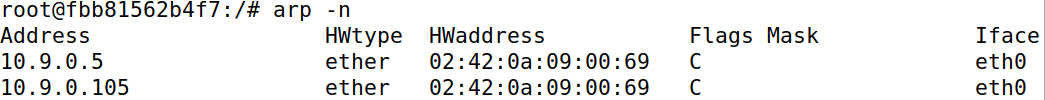
**Step 1 (Launch the ARP cache poisoning attack)**

对主机 A 和主机 B 都进行 arp 缓存中毒攻击，代码如下



执行攻击程序攻击后主机A、主机B arp 缓存分别如下



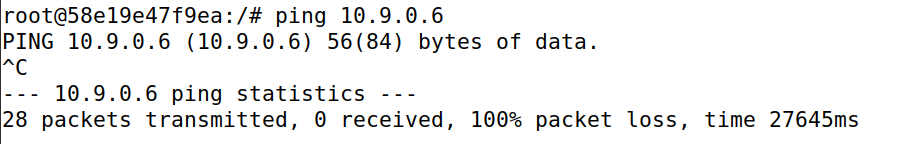


**Step 2 (Testing)**

关闭主机M的ip转发

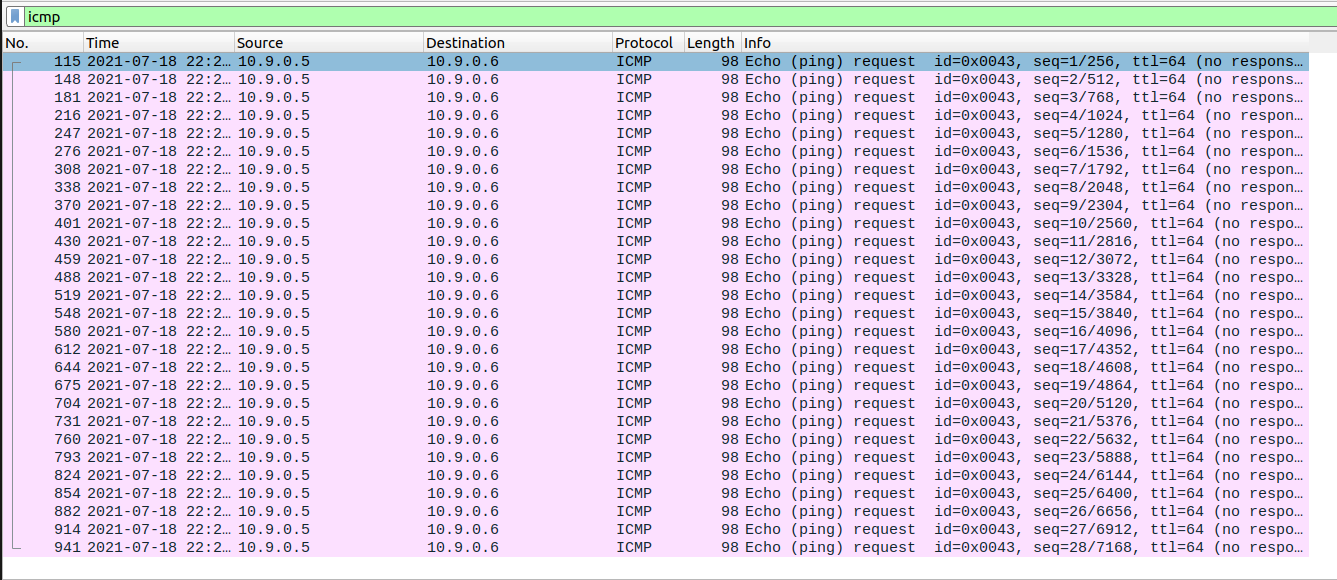


执行攻击程序，在主机A上ping主机B

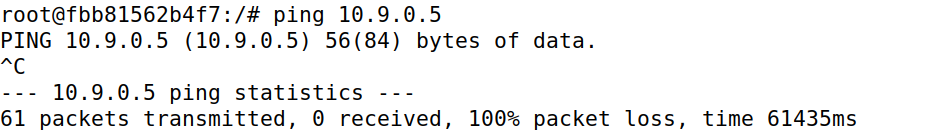


Ping不通，且丢包率为100%

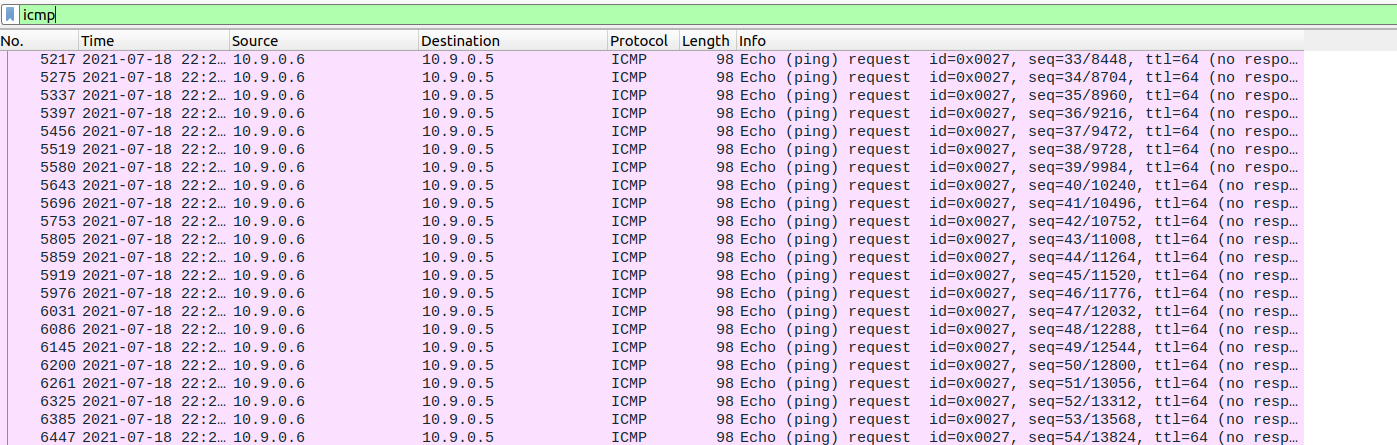
在wireshark中查看，发现只有icmp请求报文，没有回应，这是因为所有的报文都到了主机M，没有到主机B



同上，在主机B中ping主机A，ping不同，且丢包率为100%



在wireshark中查看，只有icmp请求报文，没有回复

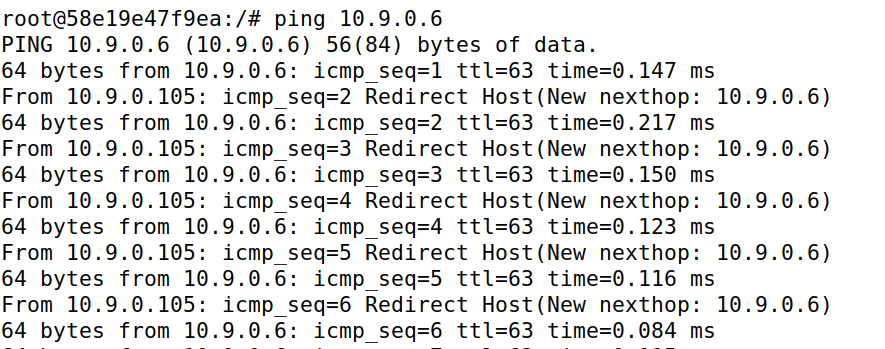


**Step 3 (Turn on IP forwarding)**

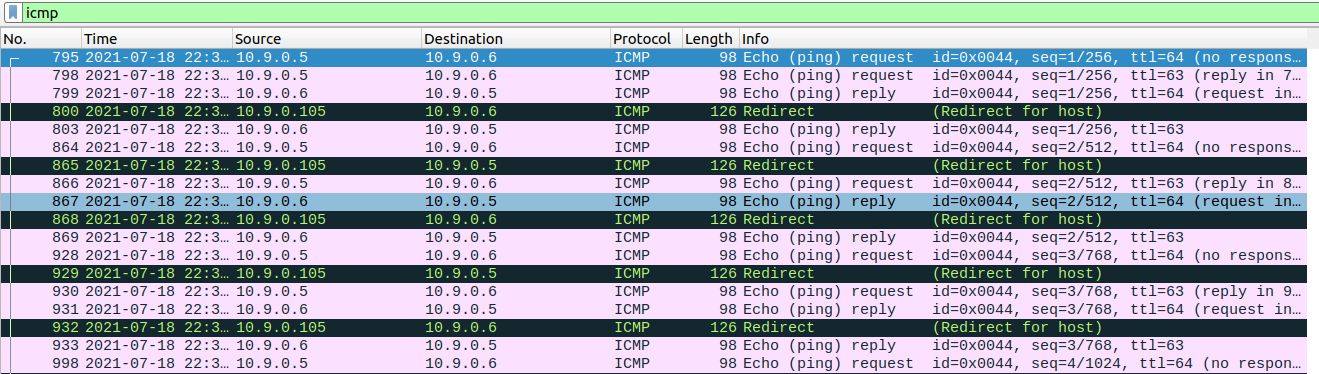
打开主机M的ip转发功能



重复step2过程，发现主机A可以ping通主机B

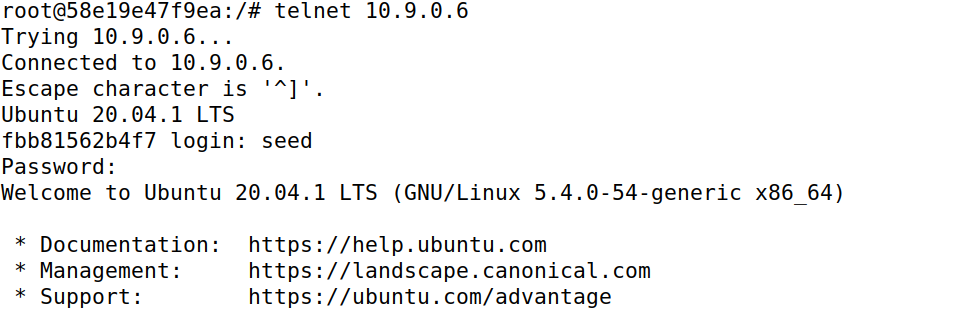


在wireshark中查看，发现icmp请求报文有相应，同时出现了一些重定向报文。可能是因为主机M收到报文后发现目标ip与自己的ip不同，所以发送重定向报文重新规划路由



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

在主机A上telnet主机B

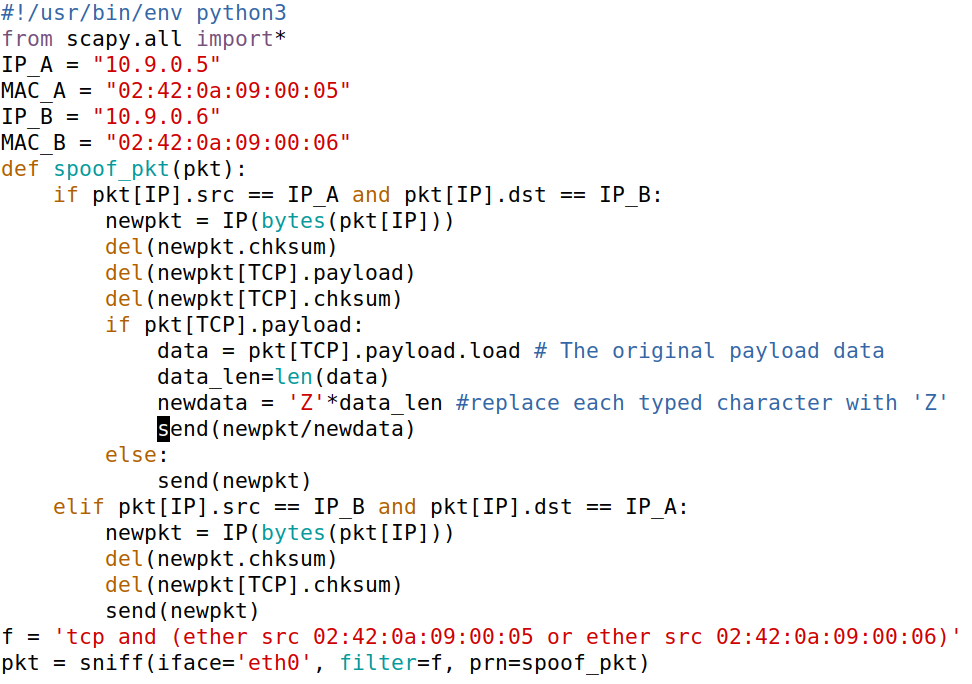


关闭主机M的ip转发

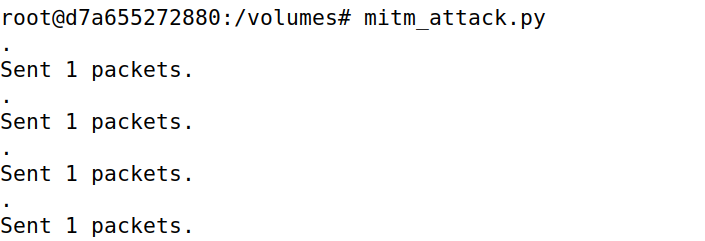


执行step1中的攻击代码，此时在主机A的telnet窗口无法键入字符

中间人攻击代码如下



执行中间人攻击程序

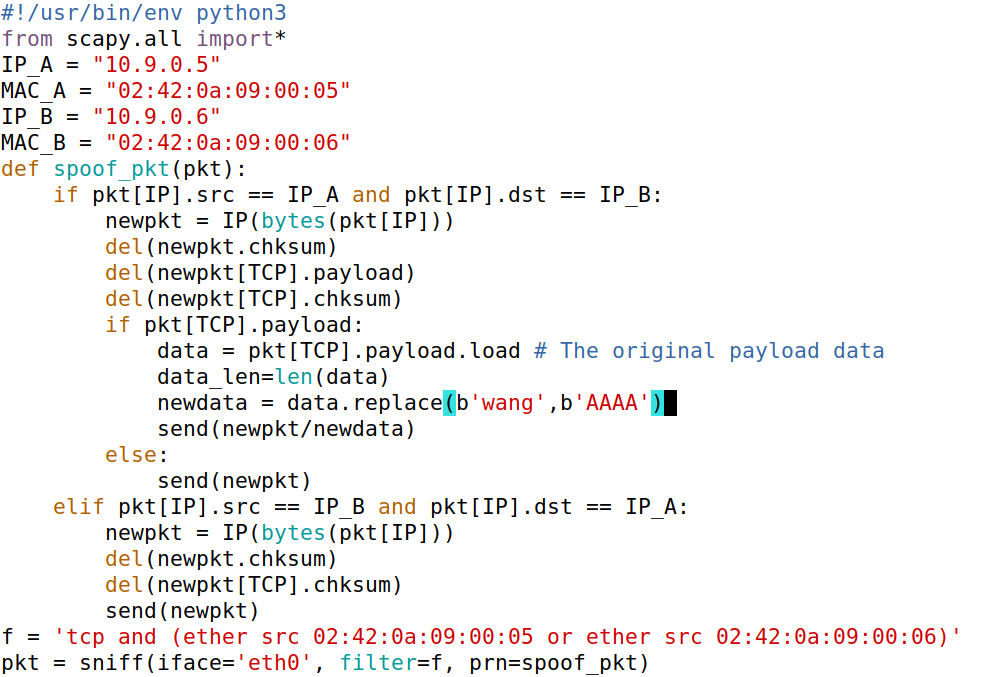


此时主机A中无论键入什么字符，最终显示的结果都是Z



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

将Task2代码中数据修改部分变为用“AAAA”替换“wang”



执行攻击程序，结果如下，攻击成功

