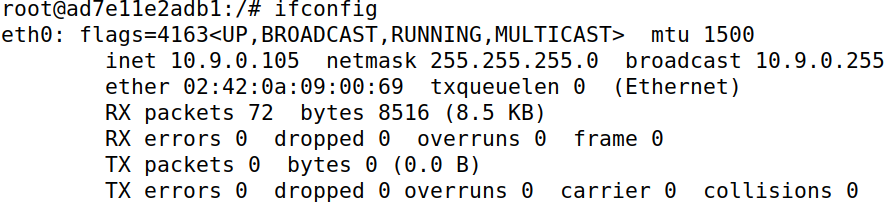
**57118110 杨紫瑄**

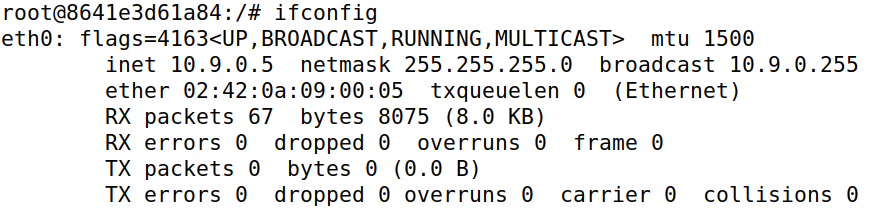
**Task 1: ARP Cache Poisoning**

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

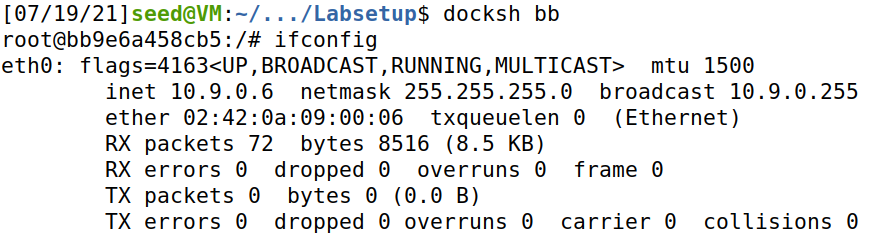
主机M的ip和mac地址：



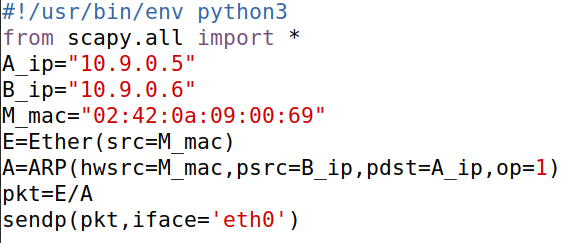
主机A的ip和mac地址：



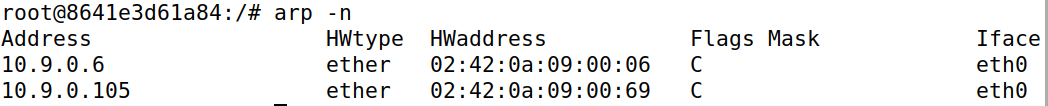
主机B的ip和mac地址：



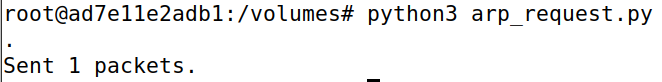
构造攻击代码如下：

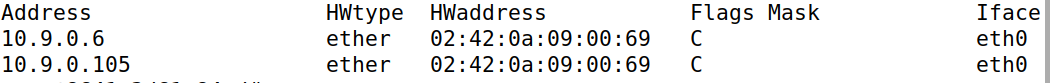


其中，op=1代表ARP request包，IP地址分别为两端主机地址，mac地址为主机M的mac地址



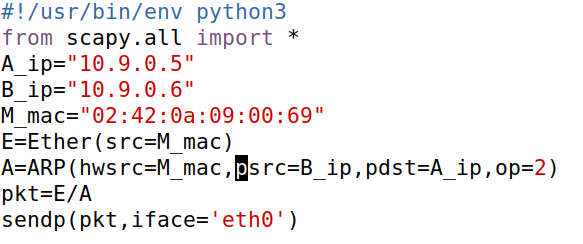
运行代码前，分别在主机A中ping主机B与主机M的地址，将地址加入cache





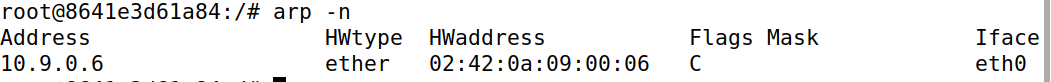
运行攻击代码后，主机M发送一个数据包，此时在主机A中再次查看ARP缓存，发现两者MAC地址由之前的不同改为相同，也就是成功将主机M的mac地址映射到主机B的ip地址上

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

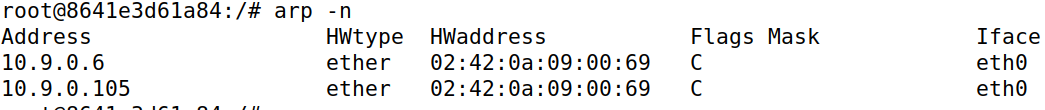


将攻击代码中的op改为2，表示ARP reply

1. B的ip已经在A的缓存中

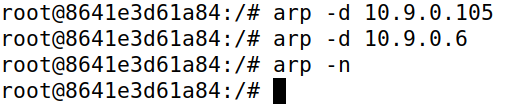


未运行攻击代码前，A的ARP缓存如上图

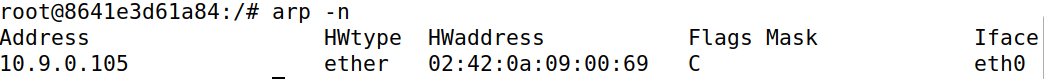


运行代码后发现主机B的ip地址成功映射到主机M的mac地址上，攻击成功

1. B的ip不在A的缓存中

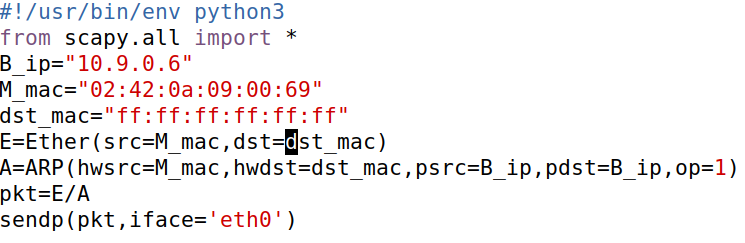


使用arp -d ip命令删除主机M和主机B的ARP缓存，此时主机B的ip不在A的缓存中



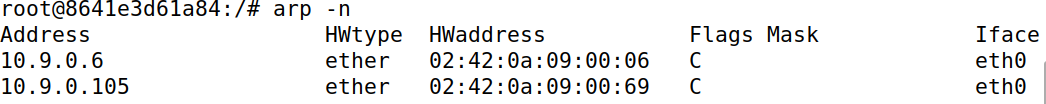
运行攻击程序后发现只有主机M的地址，没有主机M的mac地址到B的ip地址的映射，攻击失败，这是因为reply包只能更新arp缓存条目而不能增加，所以当B的ip地址在A的缓存中时攻击可以成功，不在时则攻击失败

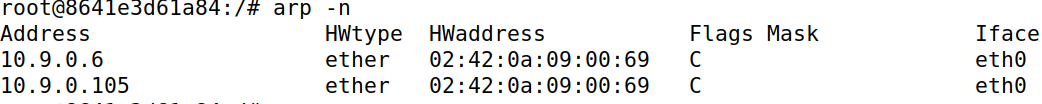
**Task 1C (using ARP gratuitous message).**



构造攻击代码如上，其中，该报文的mac地址为ff:ff:ff:ff:ff:ff，源地址和目的地址都为主机B的ip地址

1. B的ip在A的缓存中



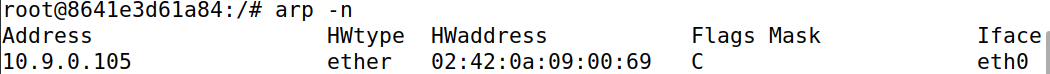


显然攻击成功

1. B的ip不在A的缓存中



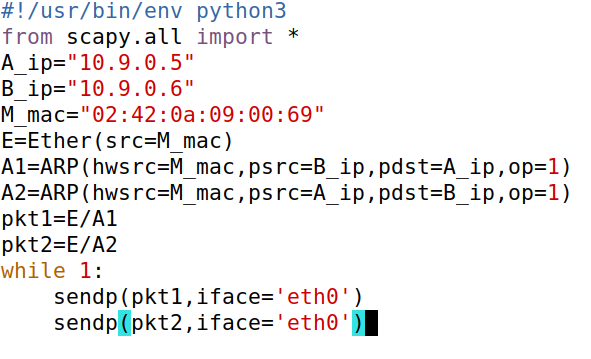
未运行攻击程序前，缓存中不存在B的ip地址



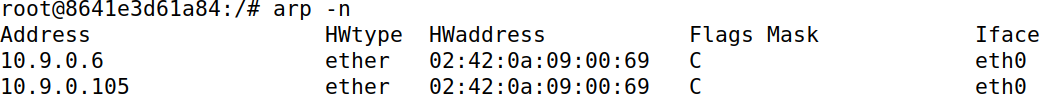
运行攻击程序后，发现只有主机M的地址，攻击失败，说明免费arp报文和reply报文类似，只能更新arp缓存条目而不能增加

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

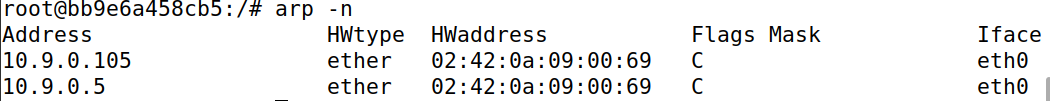
**Step 1 (Launch the ARP cache poisoning attack).**



构造攻击代码如上，对主机A和B都发送请求包进行攻击，并设置循环发送报文，防止假条目被真条目替代



运行攻击代码后主机A的ARP缓存如上图，

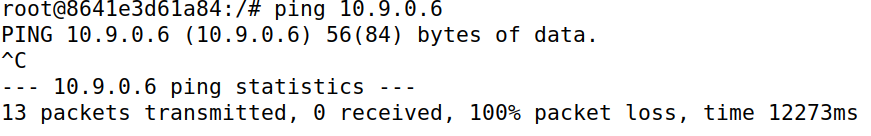


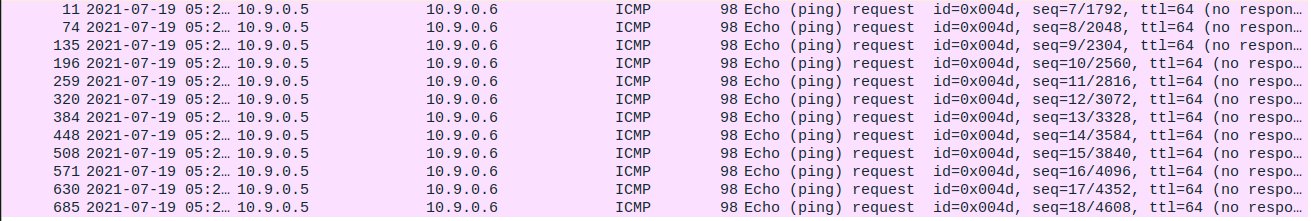
主机B的ARP缓存如上图所示

**Step 2 (Testing).**

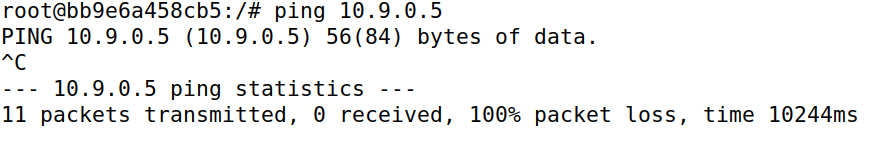


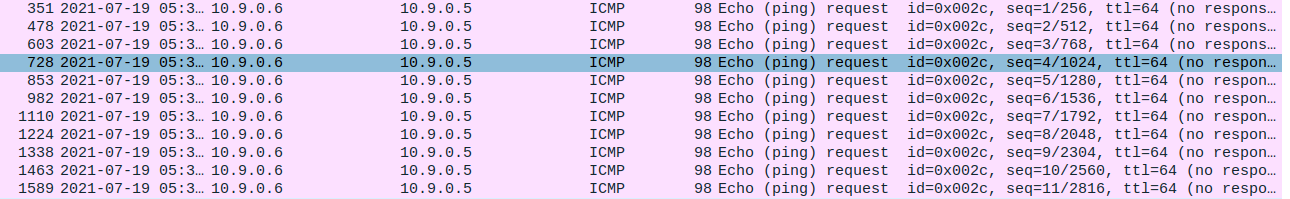
关闭主机M上的转发，再次运行攻击程序后





在主机A中ping主机B的地址结果如上图所示，发现ping不通且使用wireshark抓包的所有icmp包都无响应



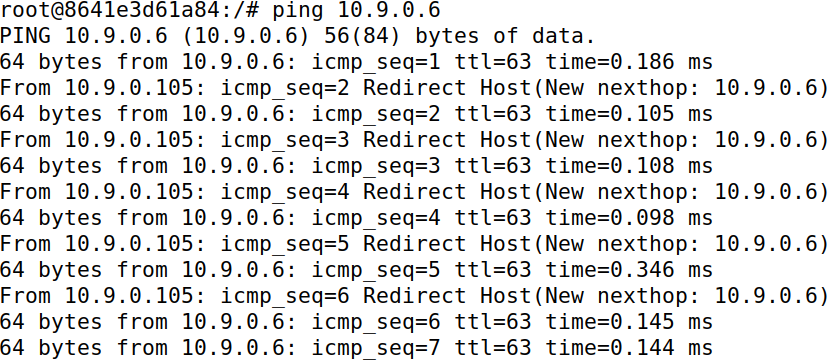


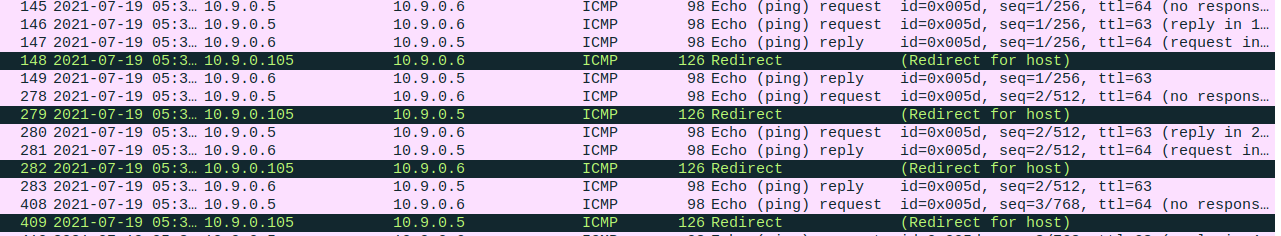
在主机B中ping主机A的地址，发现同样ping不通，且使用wireshark抓包的所有icmp包都无响应

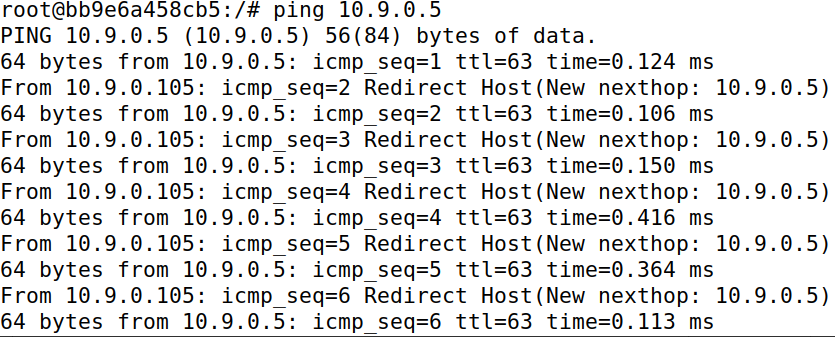
**Step 3 (Turn on IP forwarding).**

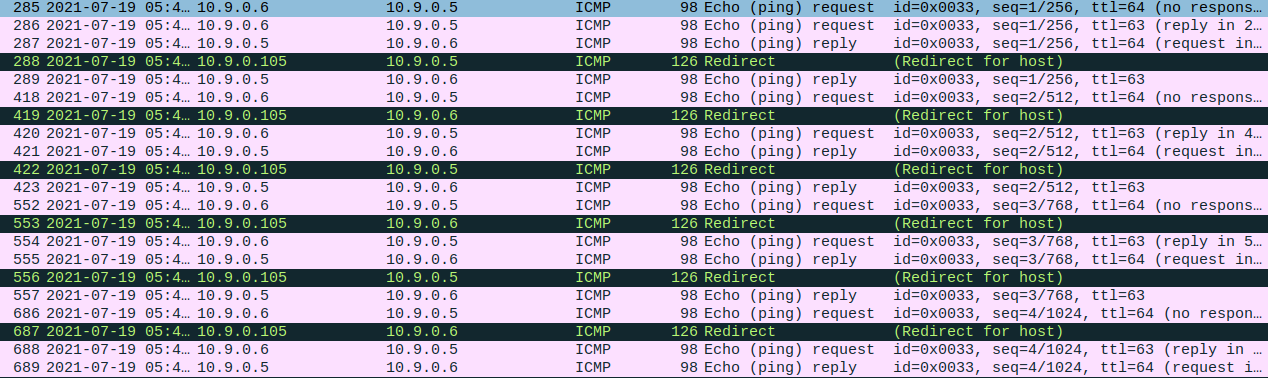


打开主机M的ip转发，并重复step 2中的操作









发现此时主机A与主机B能互相ping通，且使用wireshark抓包所得的icmp报文有响应了，同时也出现了一些重定向报文

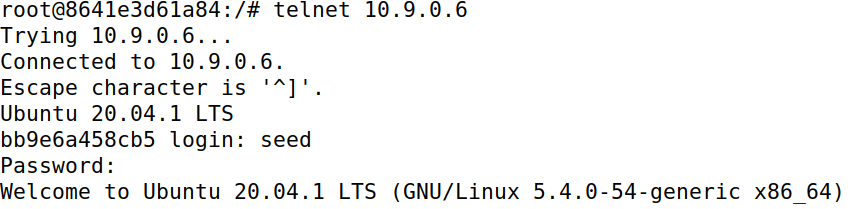
**Step 4 (Launch the MITM attack).**



构造攻击代码如上



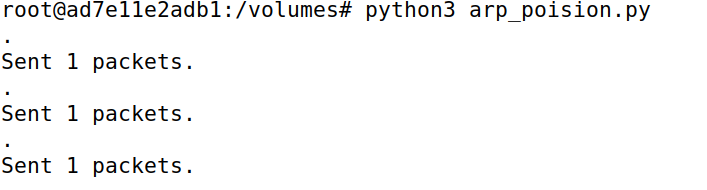
开启主机M的ip转发



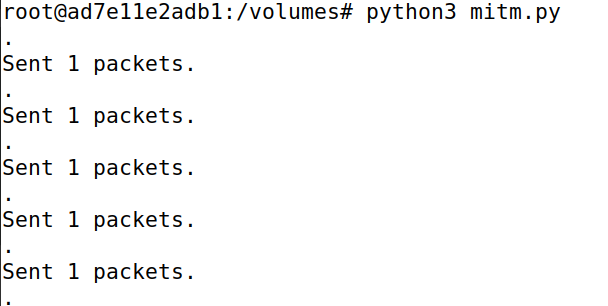
在主机A上telnet主机B



关闭主机M的ip转发



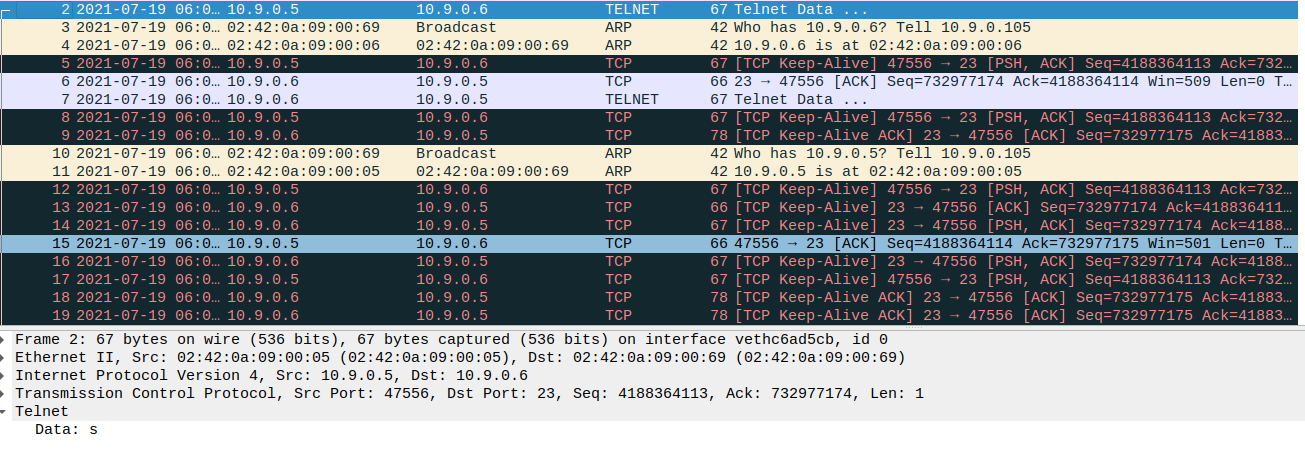
首先运行step 1的代码，修改主机A的cache



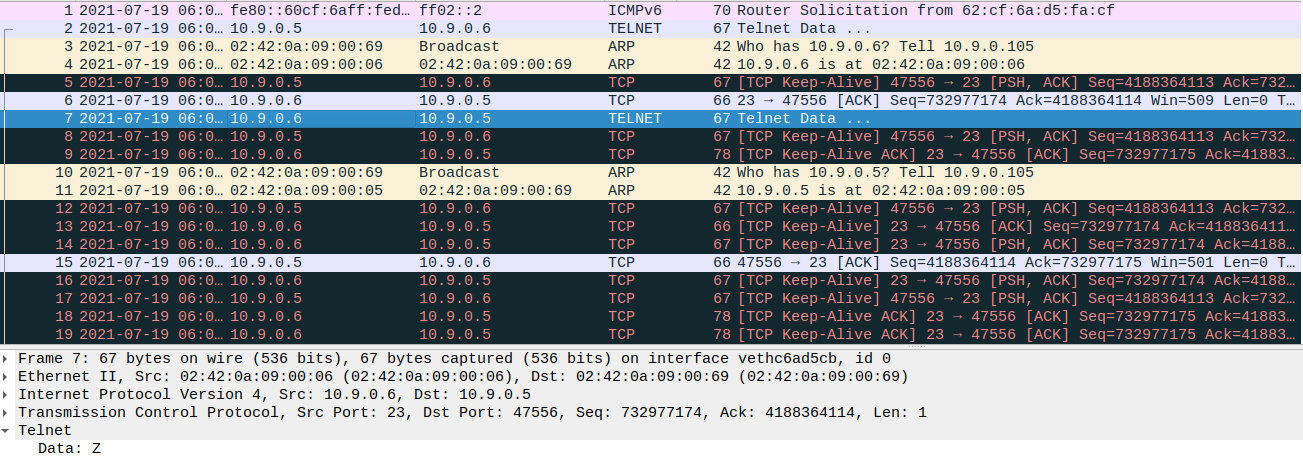
接着运行刚才构造的攻击代码，并在主机A的远程登录窗口输入‘seedlab’



发现在主机A中的输入都变成Z，攻击成功



使用wireshark抓包后，可从报文中看出第二个报文中我们输入的是字母’s’



但是在第七个报文中收到的返回值却是字母’Z’,说明被成功攻击

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



构造攻击代码如上，与Task2 step4 的代码相似，修改了数据部分，将字符串“yang”

替换为“AAAA”

先运行Task2 step1的攻击代码进行arp欺骗，接着使用netcat监听，运行刚构造的攻击代码后



在主机A中输入字符串‘yang123aaa’



发现主机B中接收到的信息中’yang’被替换成了’AAAA’，说明攻击成功