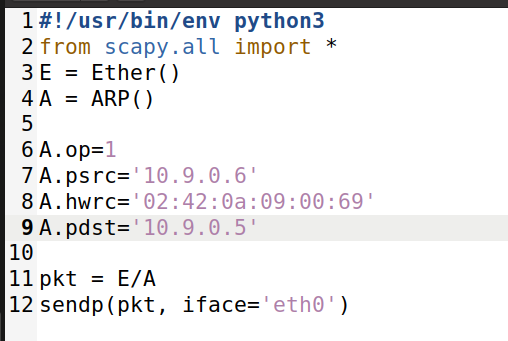
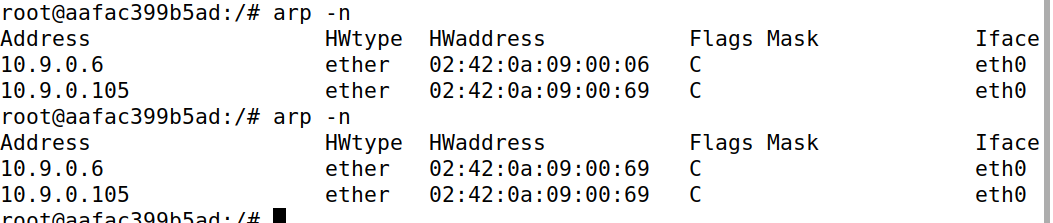
**Task1**

**1.A**

攻击代码



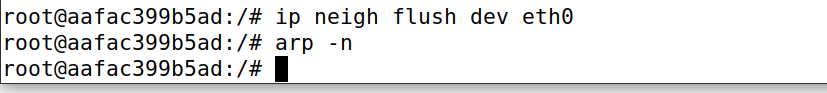
攻击效果



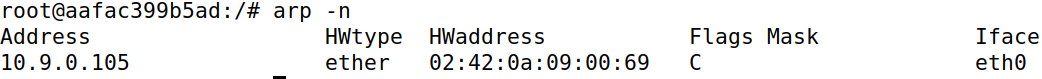
**1.B**

攻击代码将op改为2

不在缓存中的情况：



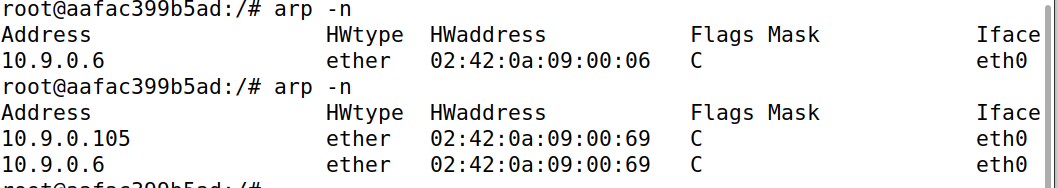
攻击效果



攻击不成功

在缓存中的情况：

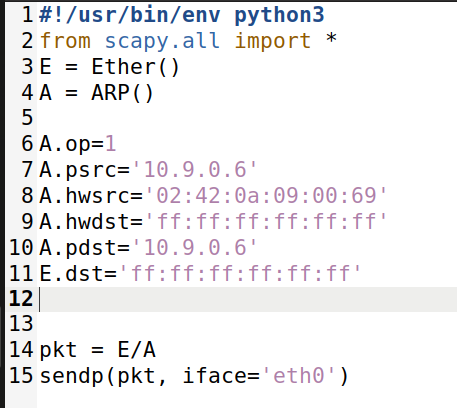
攻击效果



攻击成功

**1.C**

攻击代码

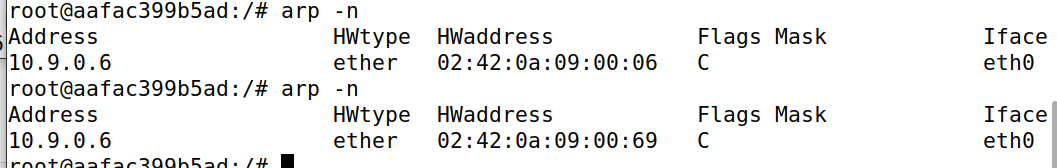


不在缓存中的情况



攻击不成功，因为本来就没有对应arp项所以arp更新报文没有用

在缓存中的情况

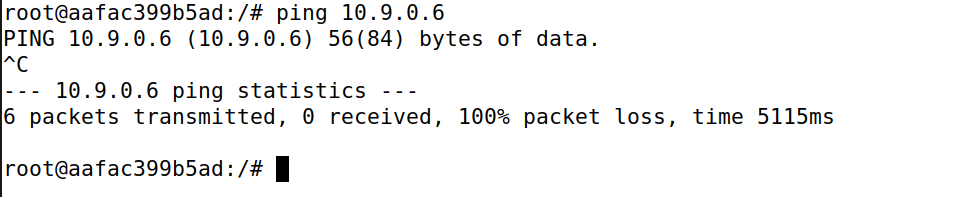
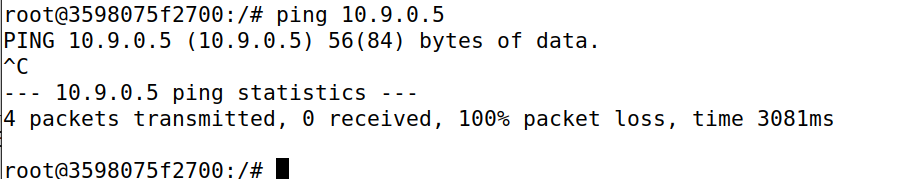


攻击成功

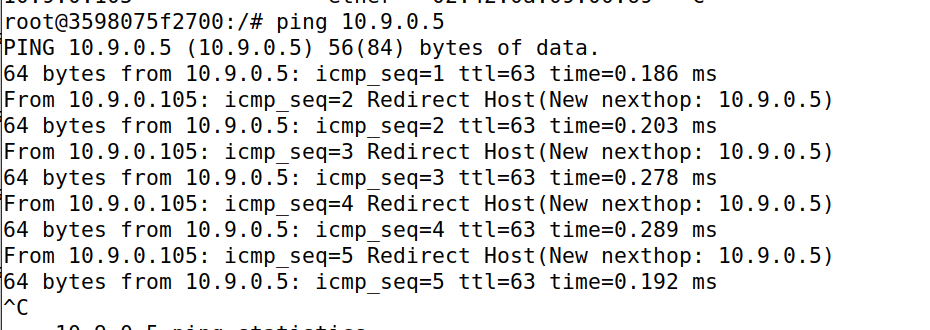
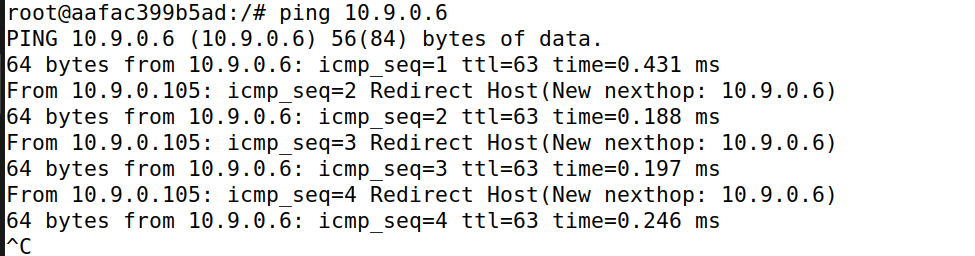
**Task2**

对B的攻击代码就是将psrc和pdst交换。

关闭M的ip转发后AB之间无法ping通，如图

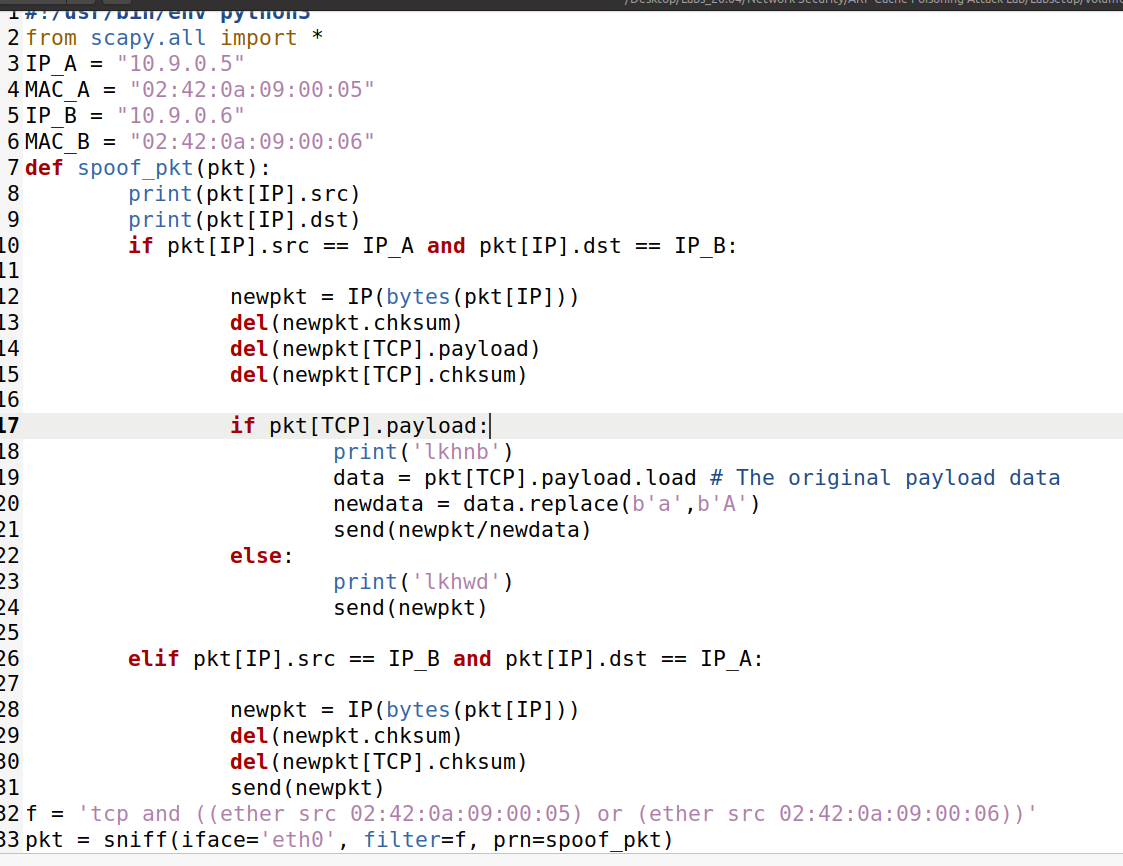


开启M的ip转发后如图



攻击成功，Icmp报文发到了M上

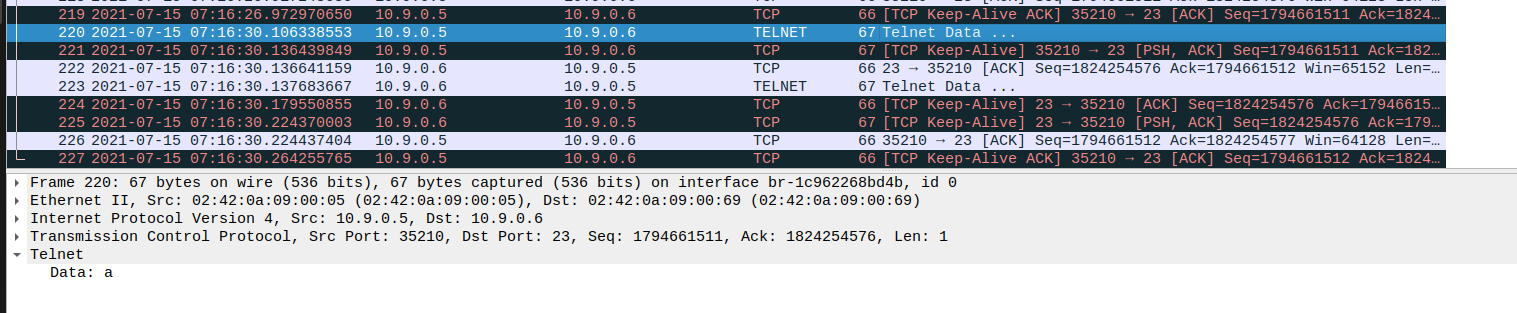
开启M的ip转发功能，A通过Telnet连接B，然后关闭M的ip转发功能，执行sniff&spoof，代码如下

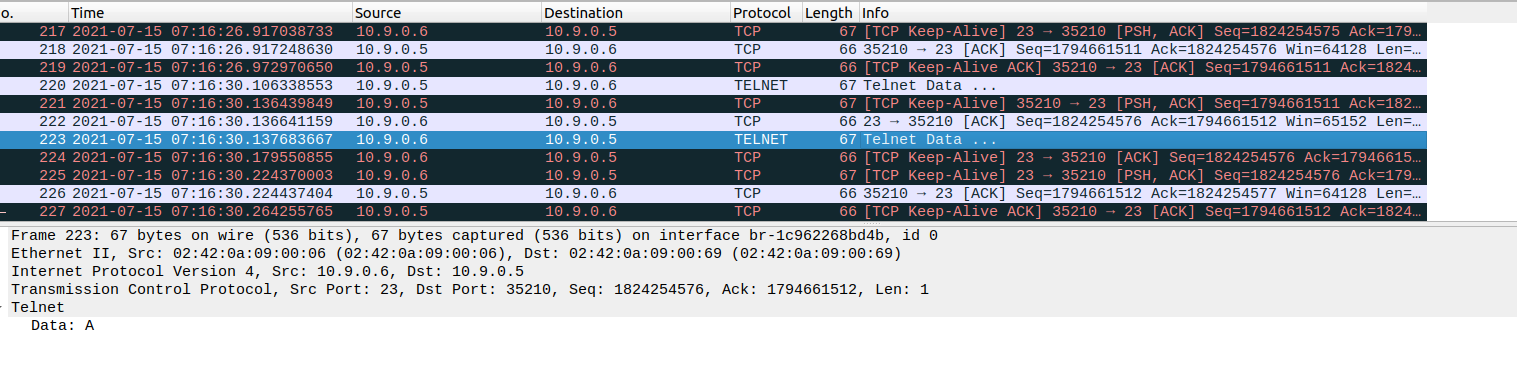


攻击效果如下，在A主机中输入的a都变成了A



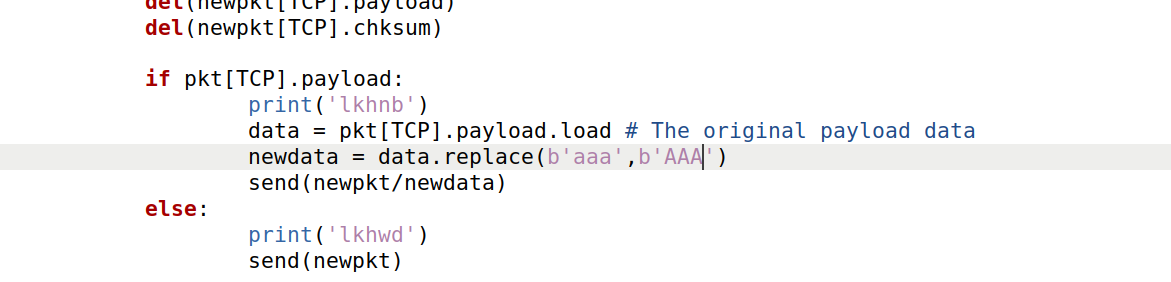
在wireshark中更清楚的看到从A主机发出的报文中数据字段为a，而收到的报文中变成A



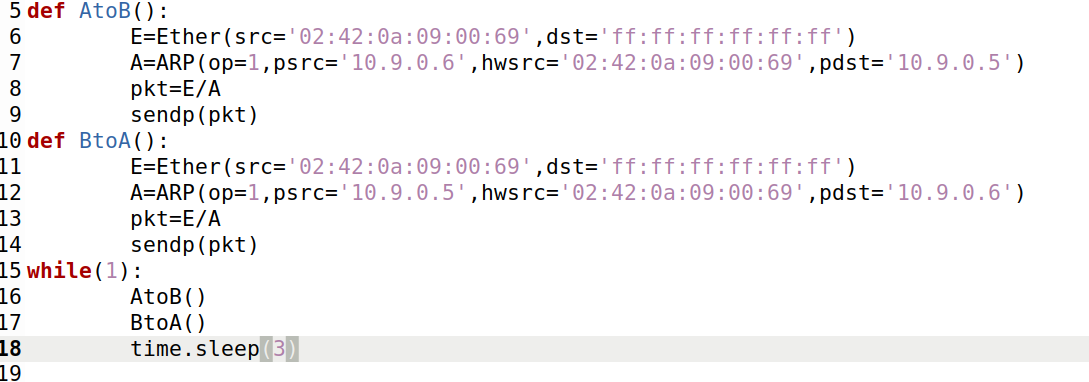


**Task3**

准备工作同task2，建立nc连接后关闭主机M的转发功能，执行攻击代码，替换部分如下



但在实验过程中发现一旦nc连接上之后主机AB会不定期且较为频繁地广播arp请求询问对方ip对应的MAC，然后arp缓存就会被纠正，因此要将先前的arp重定向攻击代码循环执行，如图



攻击效果如下，可以看到在A主机输入aaa在B主机显示的是AAA，攻击成功

