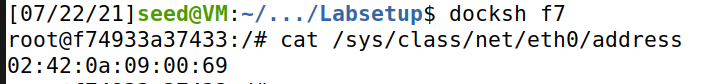
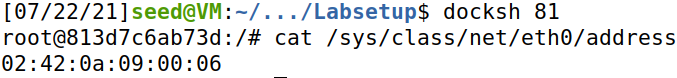
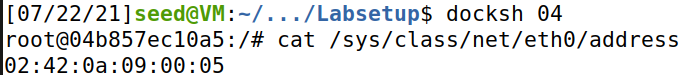
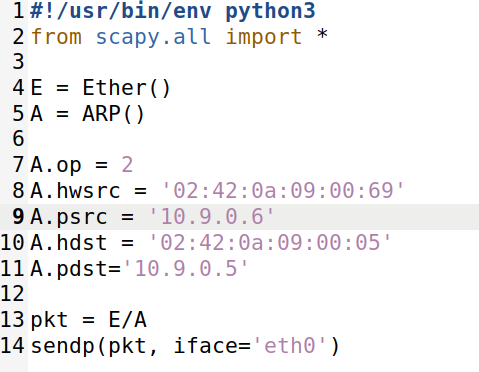
Task1

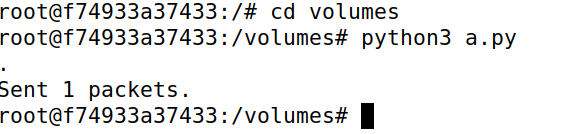
首先查看三台主机上的mac地址



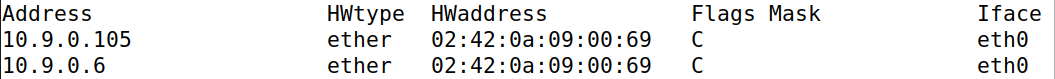
代码如下



执行攻击代码：



可见攻击成功



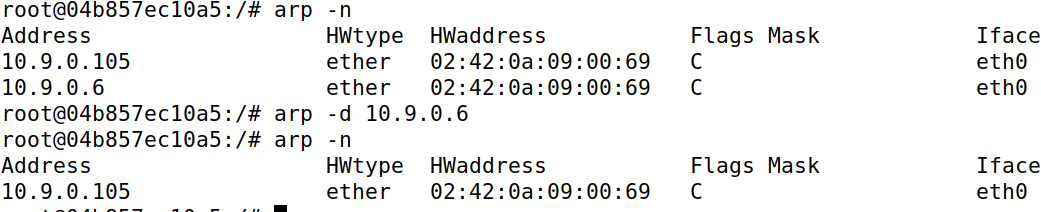
Task 1.B

Scenario1:

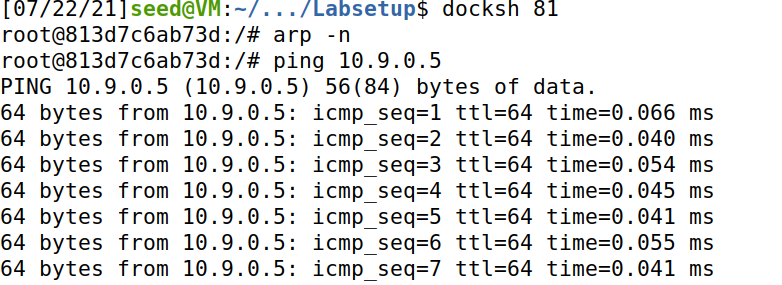
代码如下



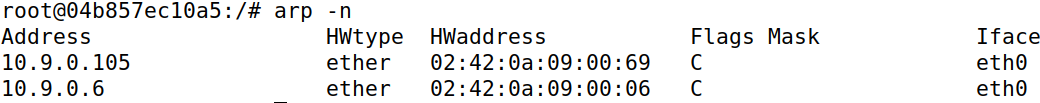
首先清除a中关于b的缓存

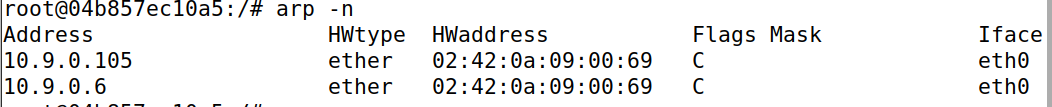


登录B pingA



运行代码后（运行代码前后）

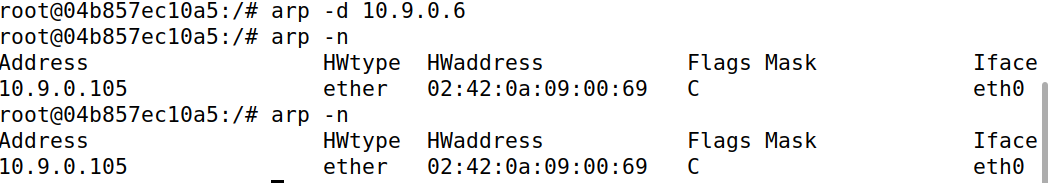




可见攻击成功

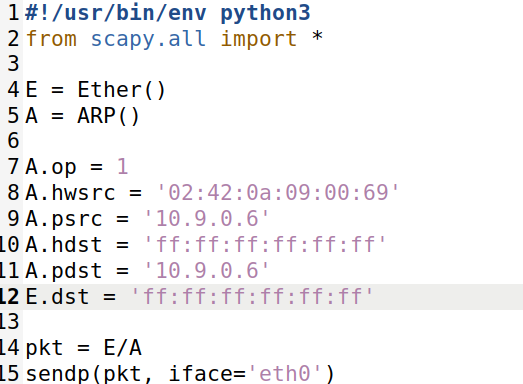
Scenario2：

清除a中关于b的arp缓存 重新执行代码（俩次分别为运行攻击代码前后）



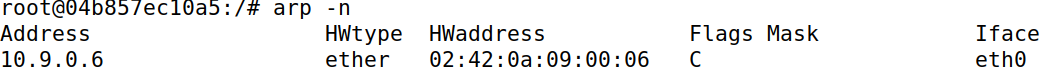
Task1.c

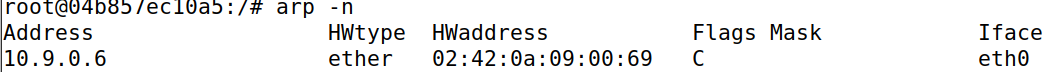
修改代码为



Scenario1：

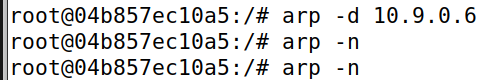
执行代码，攻击成功（俩次arp为运行攻击代码前后）





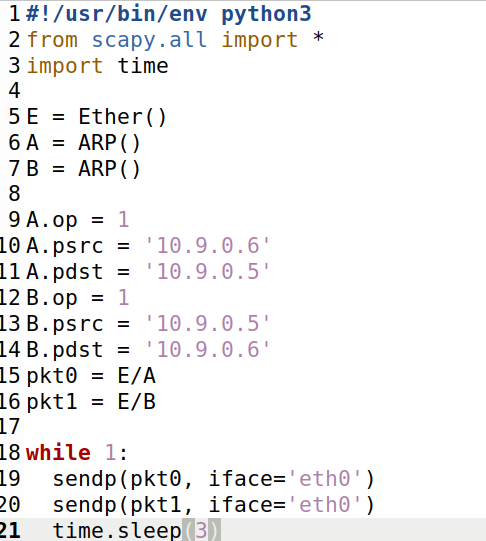
Scenario2：

重新执行代码 攻击失败

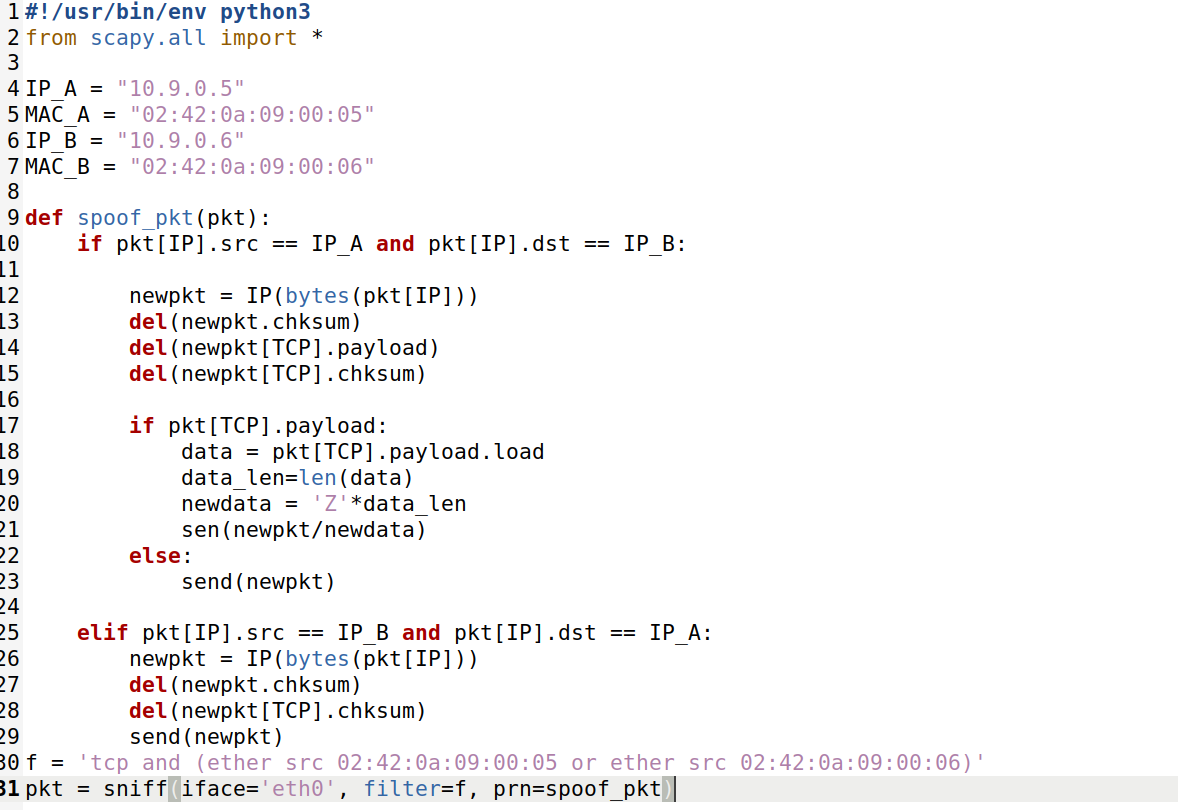


Task2

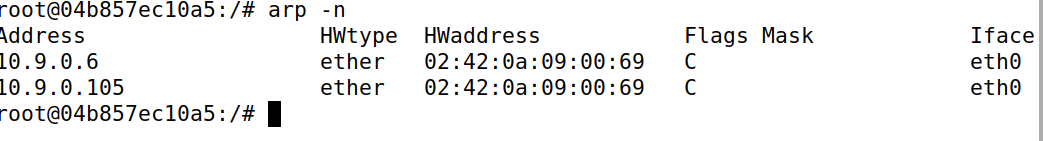
将task1代码修改如下：

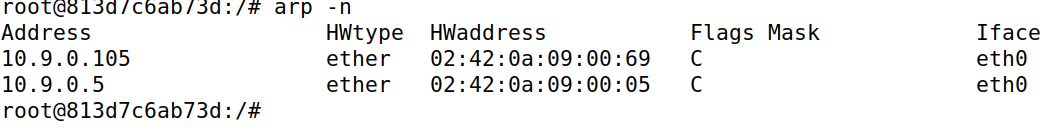


代码如下：



执行代码，发现A和B中关于对方的ip地址都被与M的MAC地址绑定





在将 IP forward置0后：

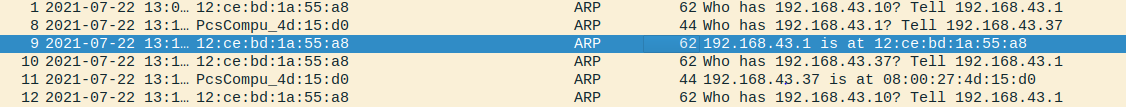


在wireshark中进行抓包。可以看出ARP报错：

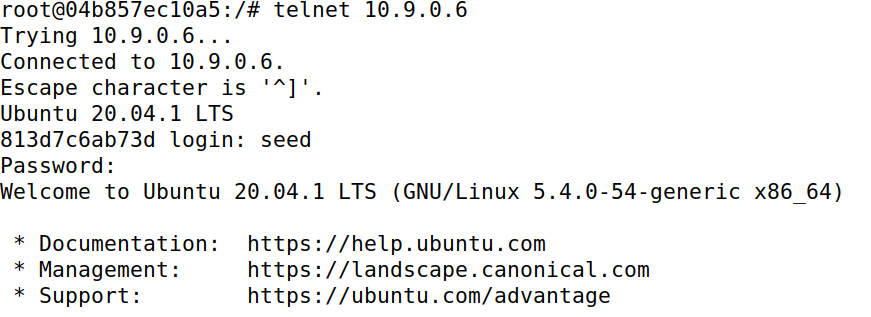


再将IP forward置为1：

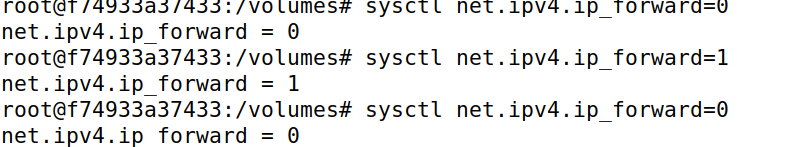




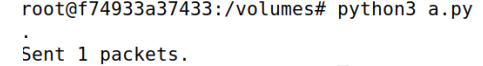
之后将 IP forward置1 建立Telnet连接



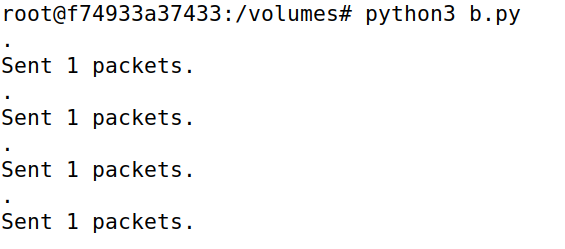
然后IP forward置为0



再将AB中对方IP地址定向为M的Mac地址：



之后开始攻击：

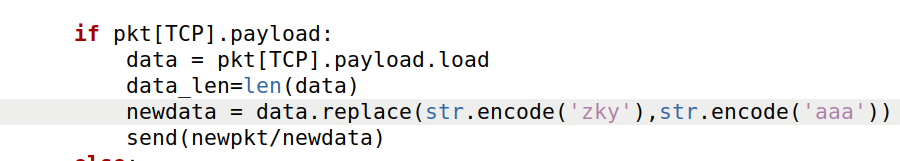


可见在A中所有的输入都变成了Z：



Task3

代码如下更改



连接后结果如图

