ARP Cache Poisoning Attack Lab

**姓名：齐天一 学号：57118223**

主机A：10.9.0.5

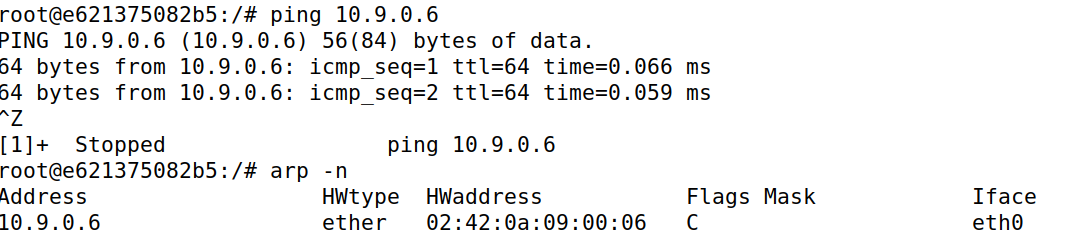
主机M：10.9.0.105

主机B：10.9.0.6

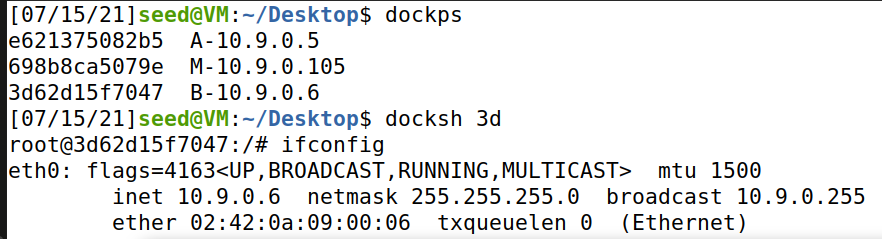
**Task1：**

**Task1A：**

①在A主机上ping B主机，并输入arp -n指令查看缓存

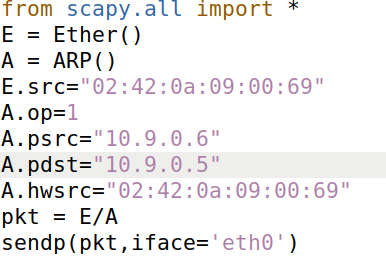


在B主机中输入ifconfig，查看mac地址

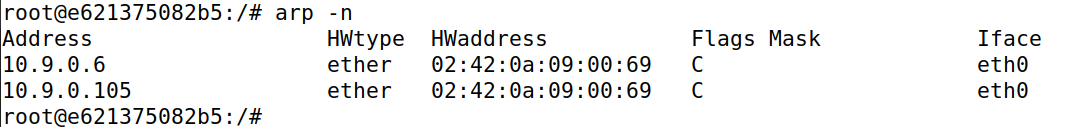


可以看到此时缓存中主机B对应的mac地址与实际一致。

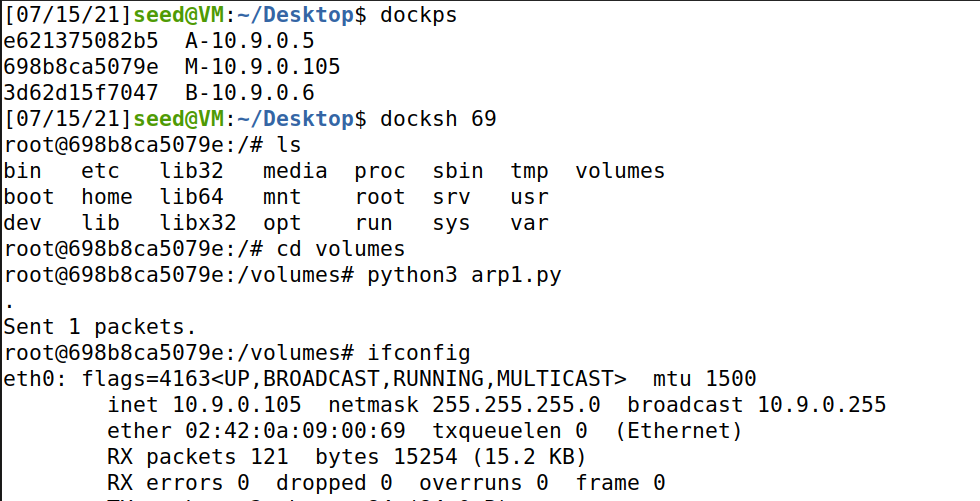
②在攻击者容器中运行如下程序，发起arp缓存攻击



③在A主机上查看arp缓存



在M容器中输入ifconfig指令，查看mac地址



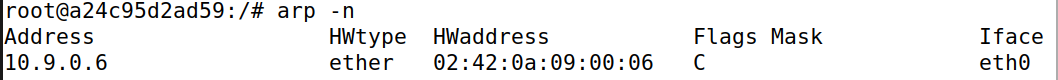
可以看到arp缓存发生了变化，主机M的mac地址被映射为主机B的ip，说明攻击成功。

**Task1.B**

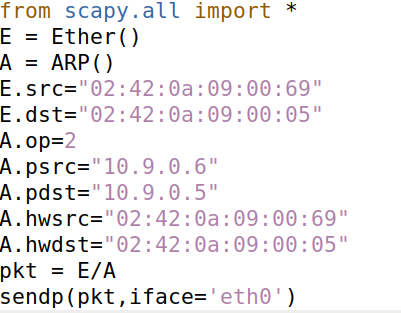
（这里由于关机，所以重启了一下容器）

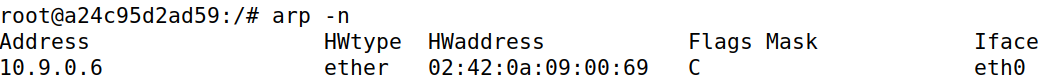
（1）当B的ip已经在A的缓存中

①输入arp -n 查看缓存



②将op值改为2，表示reply报文，并运行程序

  
③重新输入arp -n 查看缓存



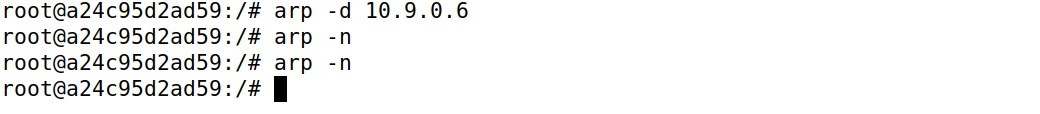
我们可以看到，M的mac地址被映射为主机B，攻击成功。

1. 当B的ip不再A的cache中

①首先清除A中关于B的缓存内容



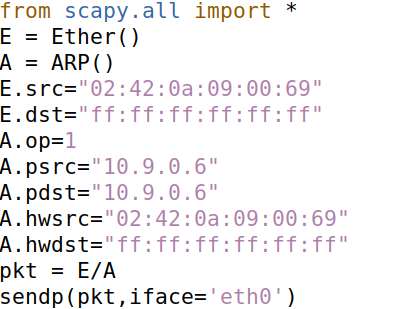
②重新运行程序

  
可以看到，缓存中仍然没有内容！攻击失败了。

造成这种现象的原因是arp的reply包只能更新arp条目但不能新增arp条目，因此当B主机ip不再缓存中时，无法进行攻击。

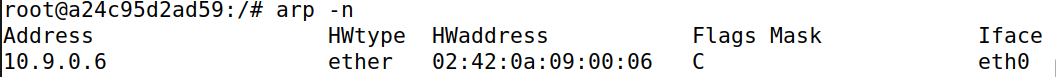
**Task1.C**

按照要求修改程序：

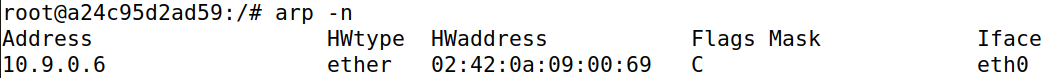


1. 当B的ip已经在A的缓存中

攻击前：



攻击后：

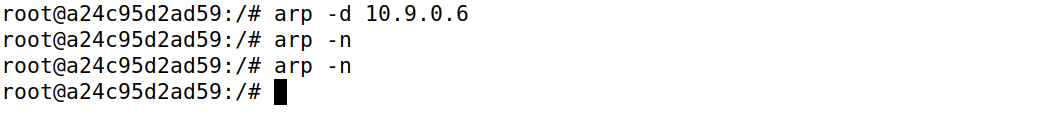


说明攻击成功

1. 当B的ip不再A的cache中

攻击前：

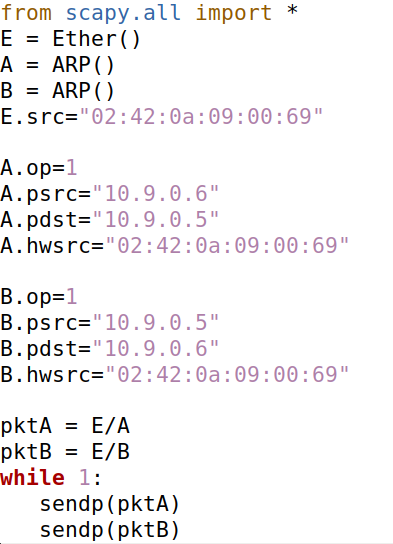


攻击后：  


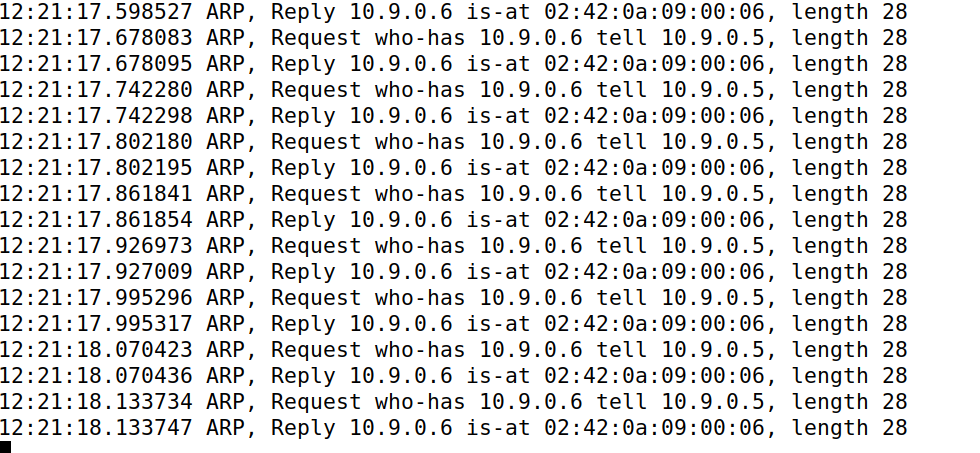
可以看到仍然没有增加，说明攻击失败。

**Task2：**

①修改主机A和主机B的arp缓存，为了能够使得缓存污染保持，修改攻击程序如下，令攻击程序持续发送报文。

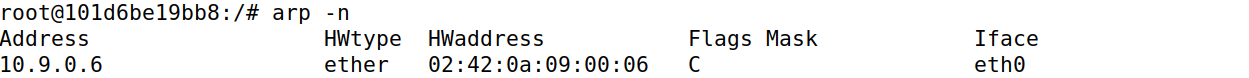


在主机B上使用tcpdump查看：

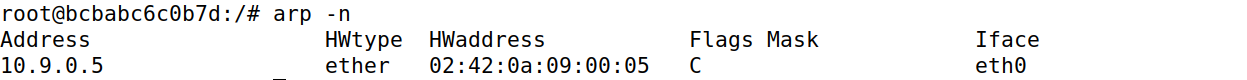
  
可以看到B在不断接收到arp请求报文。

攻击前：

主机A：

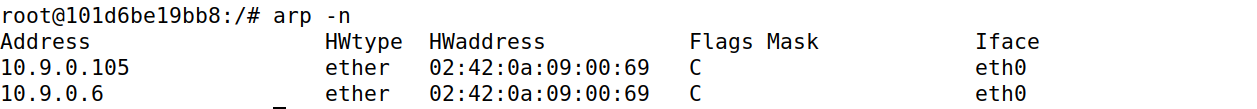


主机B：

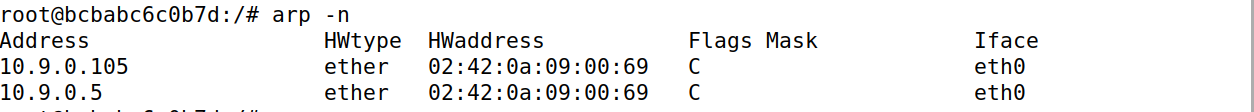


攻击后：

主机A：

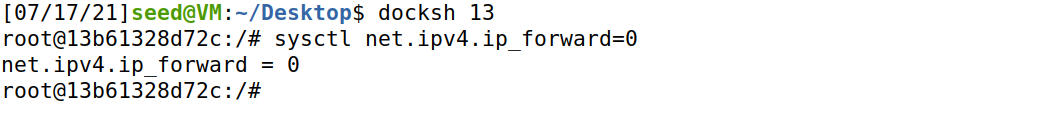


主机B：

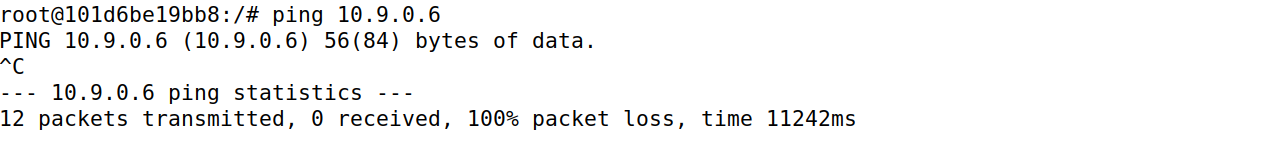


可以看到缓存修改成功。

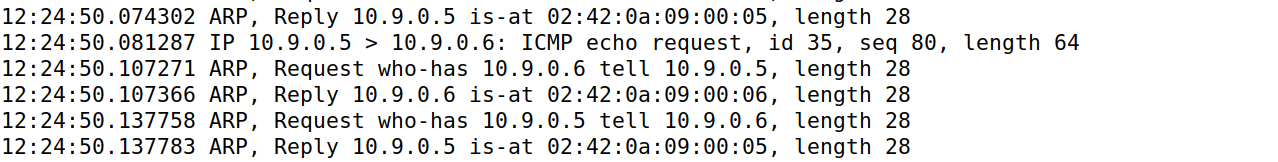
②关闭上M主机的ip转发功能



重新由主机A ping 主机B，发现ping失败了

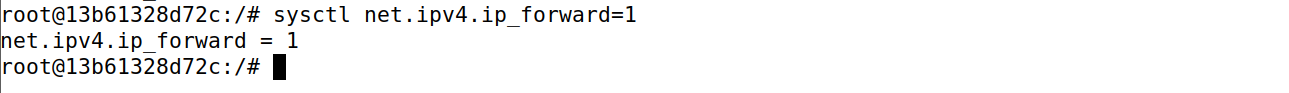


在ping 的同时，使用tcpdump在M主机查看报文情况：

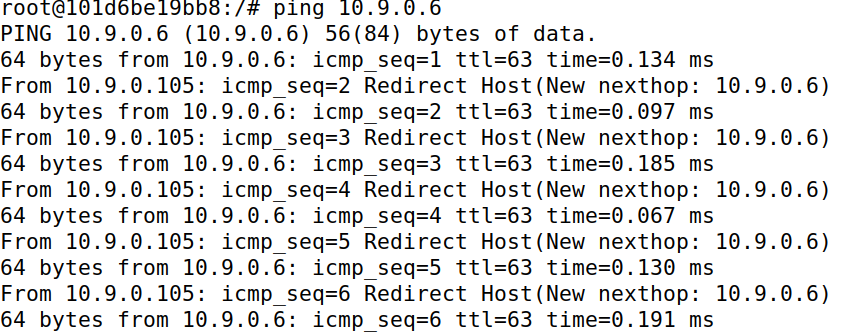


可以看到只有ICMP请求报文，没有应答报文。

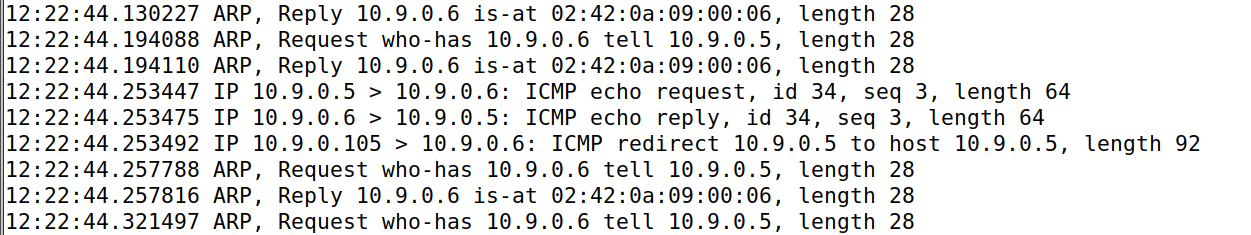
③开启ip转发功能，重新进行实验



重新由主机A ping 主机B，成功：



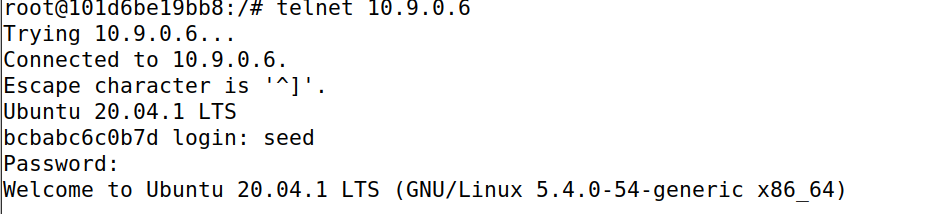
在ping 的同时，使用tcpdump在M主机查看报文情况：



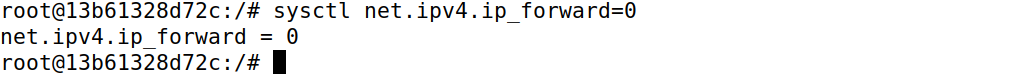
可以看到，发出了ICMP的应答报文，因此能够ping成功。

④进行MITM攻击

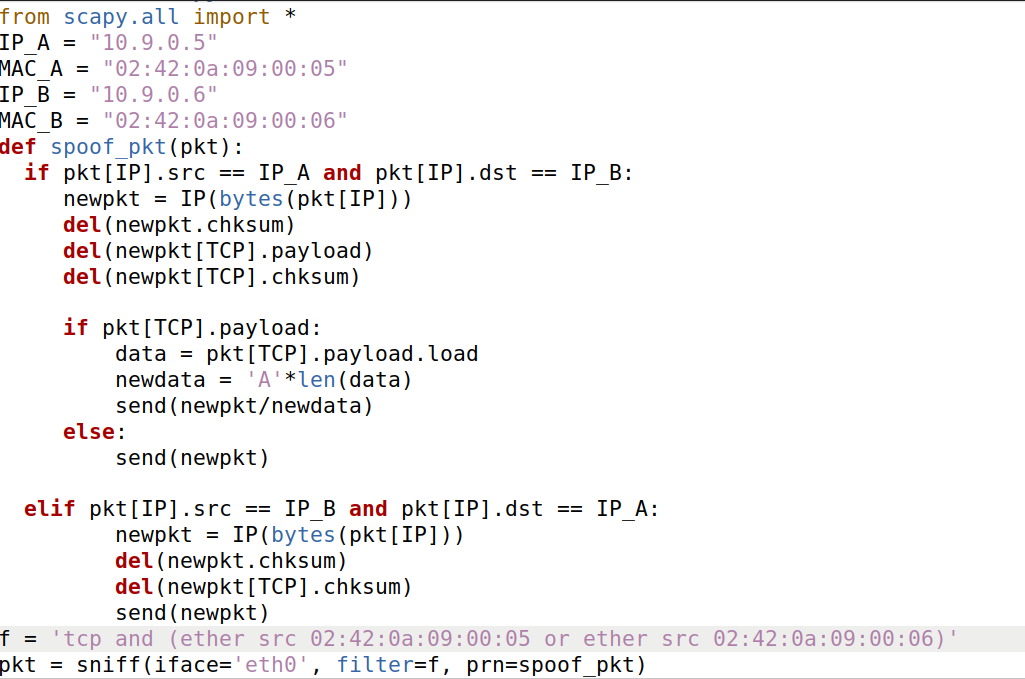
首先让A主机telnet到B主机

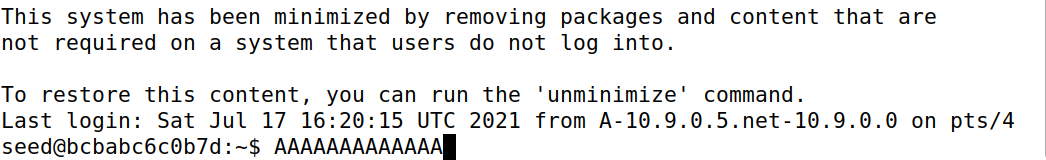


关闭ip转发功能



在M主机运行如下程序：

在A主机上输入任意字符，可以看到所有字符都被转换为A字符

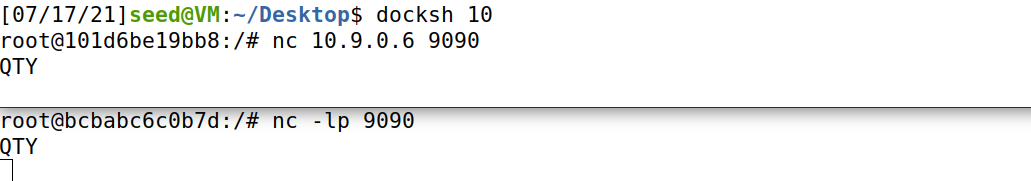


**Task3：**

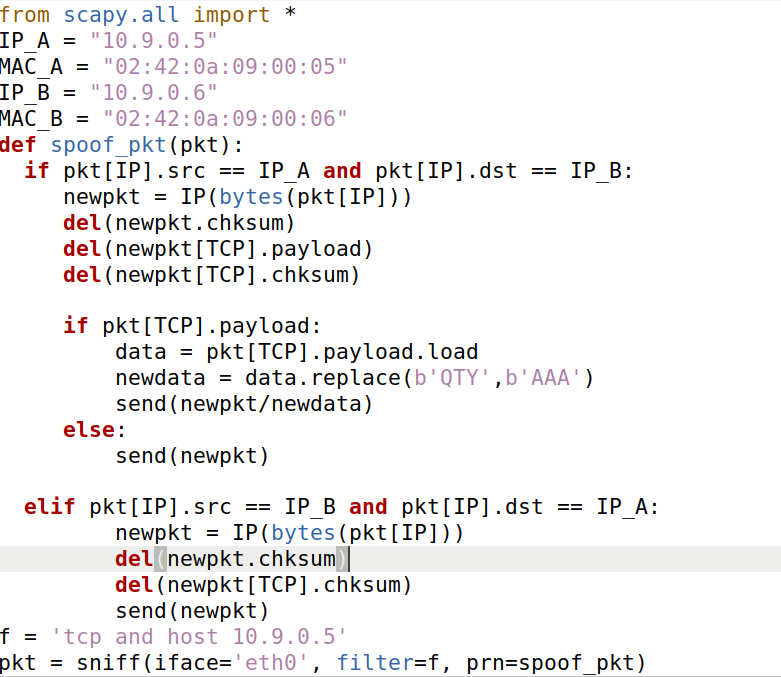
对于Netcat的攻击，其步骤与task2基本相同

①建立Netcat连接

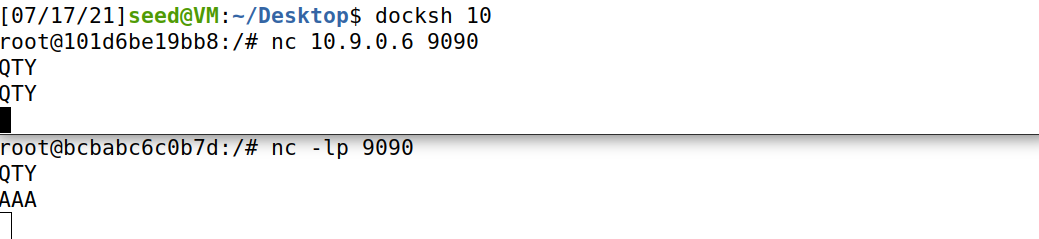
首先开启ip转发功能，B主机打开监听，A主机nc到B主机的9090端口，此时A输入姓名，在B主机处可以看到成功收到了姓名，说明连接成功。



②修改task2的攻击程序，在其中加入替换的语句

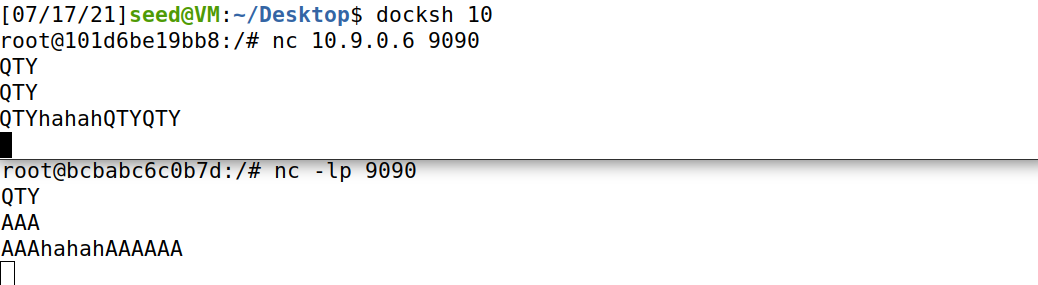


③关闭ip转发功能，并运行程序，在A主机输入“QTY”：



此时在B主机中显示的是“AAA”，说明替换成功！

输入更复杂的语句：



可以看到，语句中三个“QTY”都被替换为“AAA”，说明攻击成功。