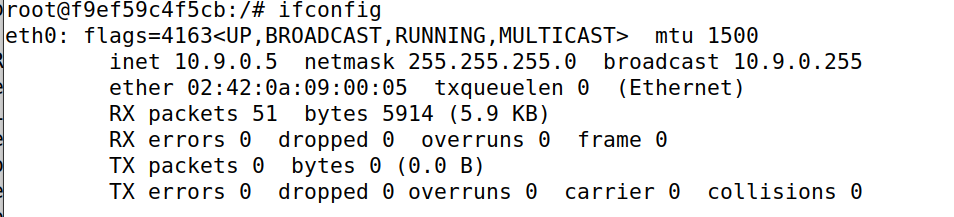
**第四次实验报告**

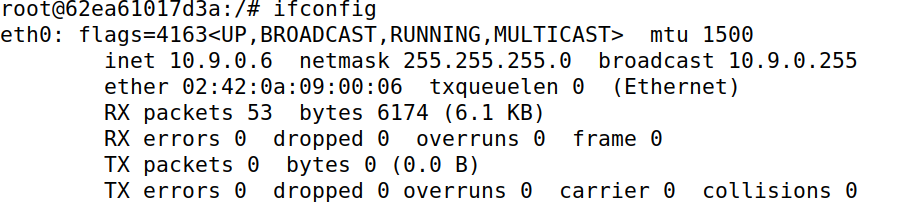
­­­­­­57118121 刘洪飞

Task1.a

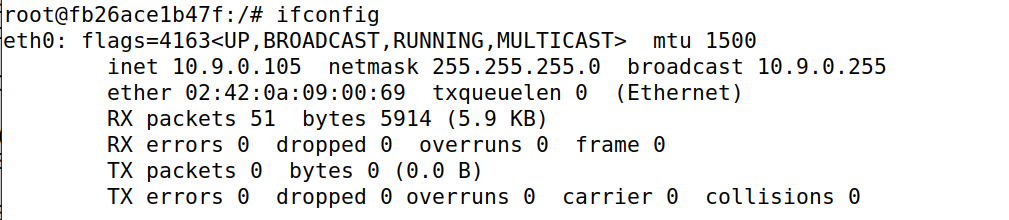
A 的信息



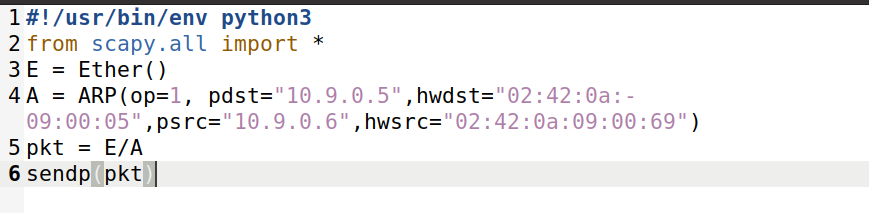
B的信息



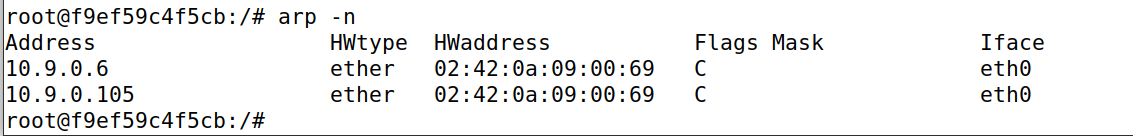
Attackers的信息



使用如下代码攻击

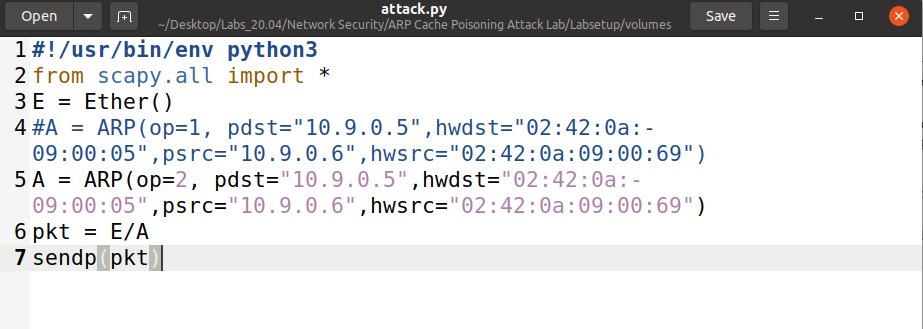


结果：攻击成功

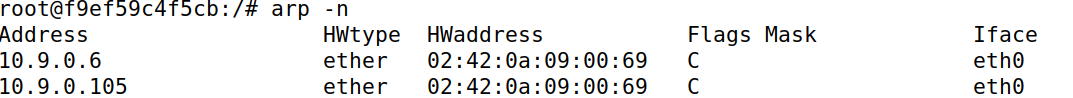


Task1B

代码

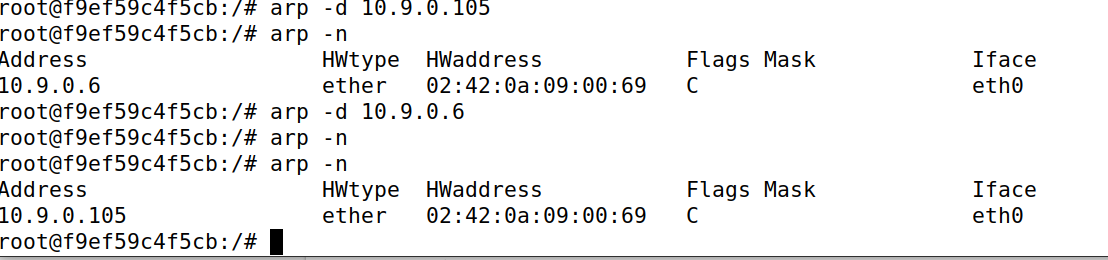


1）B已经在cache里面，攻击成功



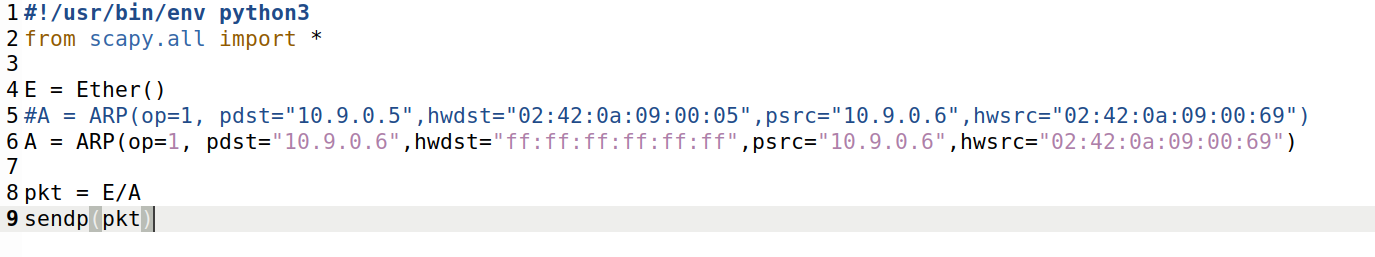
2）B不在cache里面

清除缓存，之后攻击，发现攻击失败

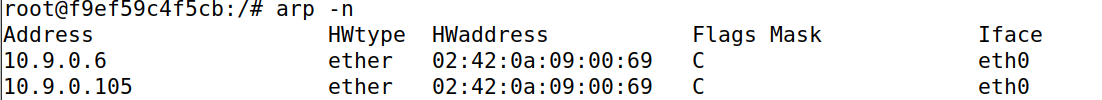


Task1c

代码如下



1）B已经在cache里面，执行后，攻击成功



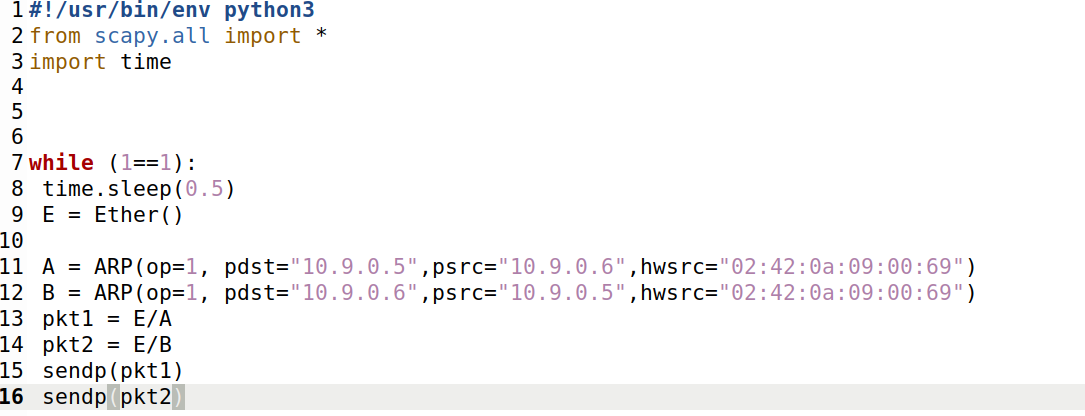
2）B不在cache里面，攻击失败



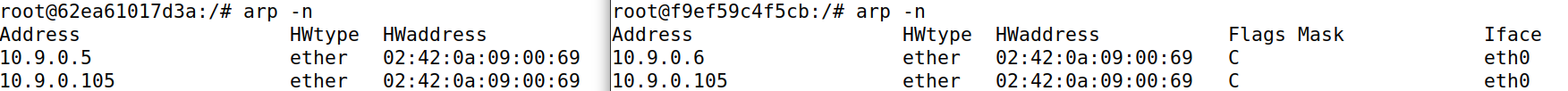
Task2

Step1

使用如下代码攻击

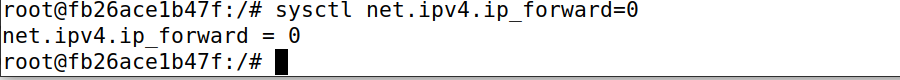


攻击成功



Step2

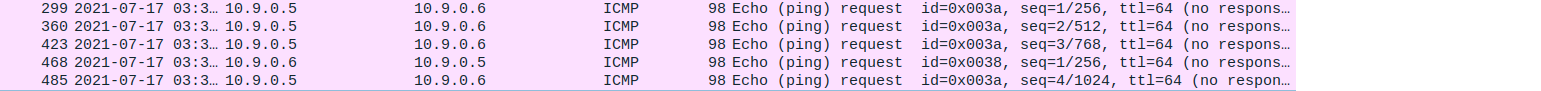
调完设置，相互ping发现无法ping通







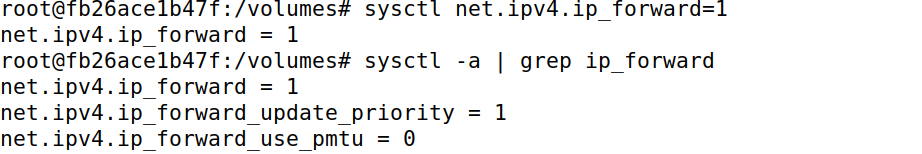
Wireshark抓包如下



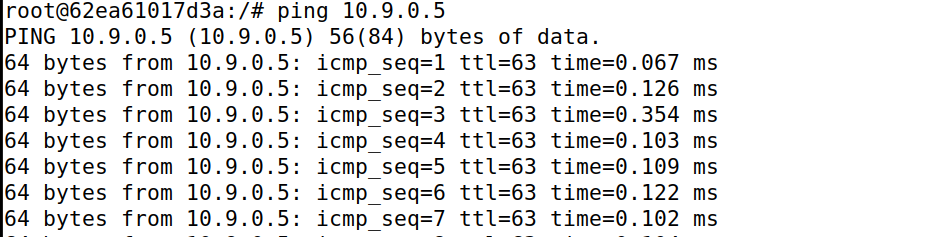
发现 icmp 报文都没有 response，因为所有报文都没有到达目标主机

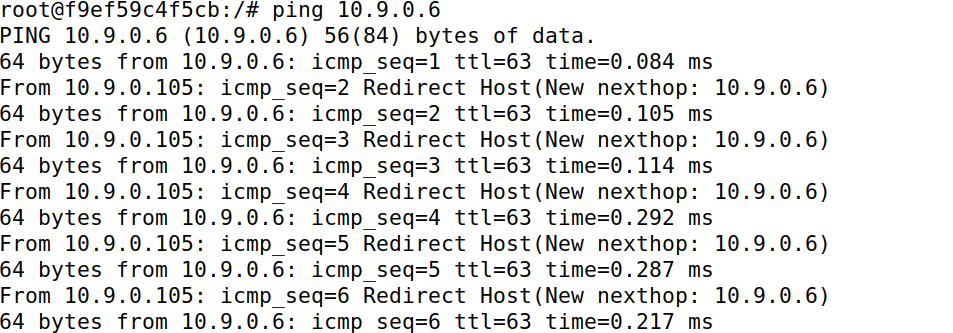
Step3

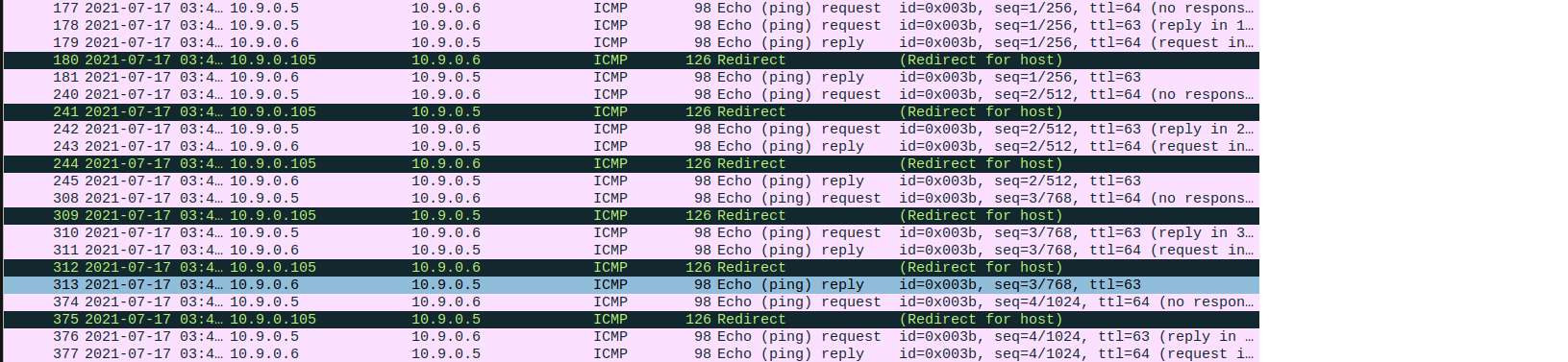
打开attacker的IP转发功能



发现重复step2，可以ping通



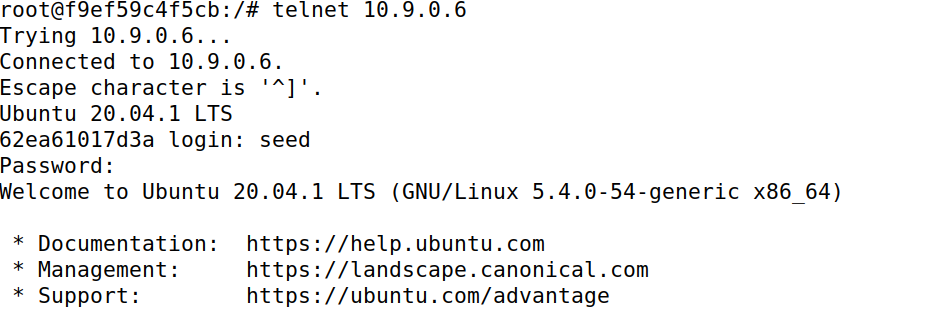




发出的 icmp 重定向报文，为attacker收到报文后发送的重定向报文，以达到修正路由的目的。

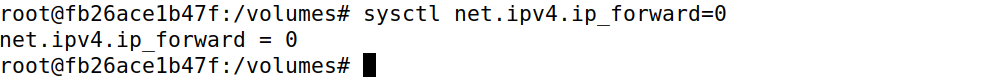
Step4

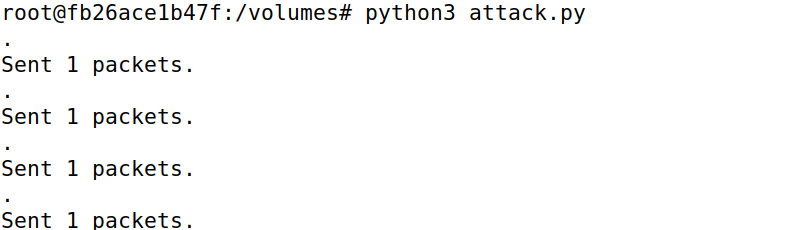
Telnet连接



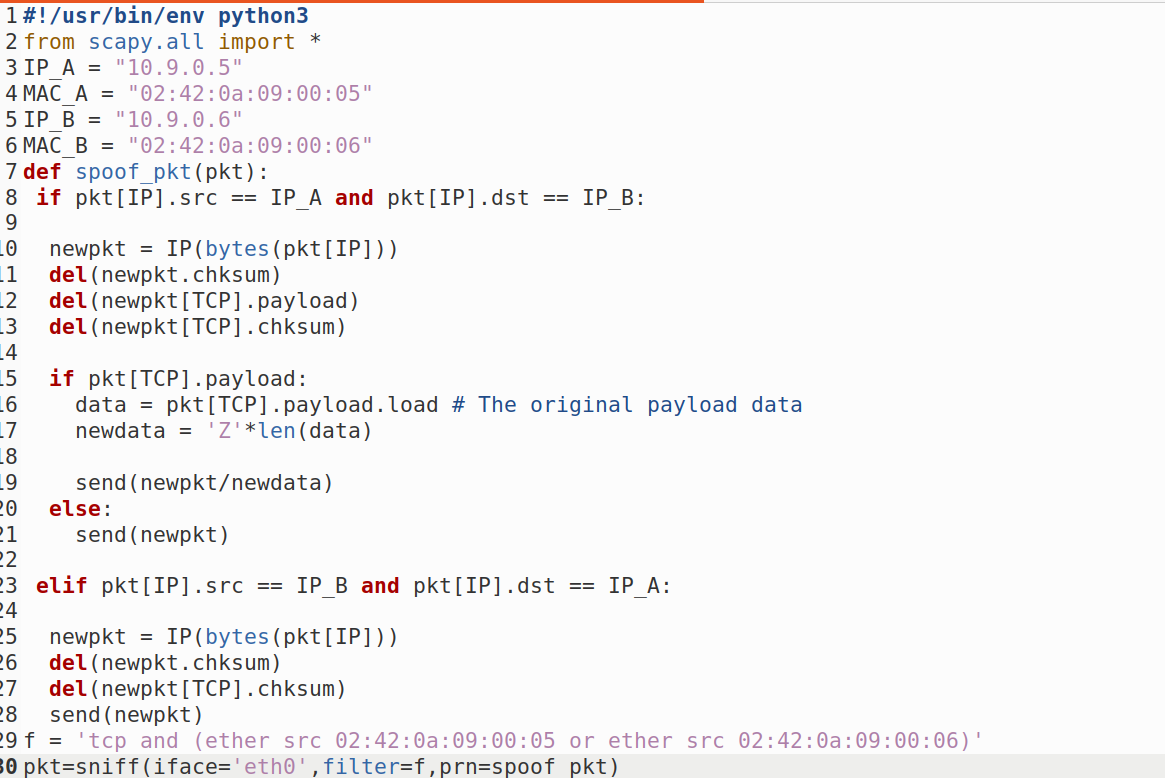


进行攻击，Telnet无法操作

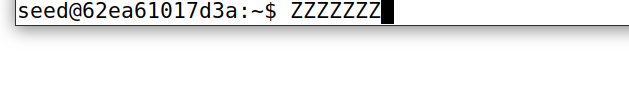




代码如下，，其将所有截取的 A 发往 B 的有负载的 tcp 报文中的负载更改为等数量的字符Z，再发往 B

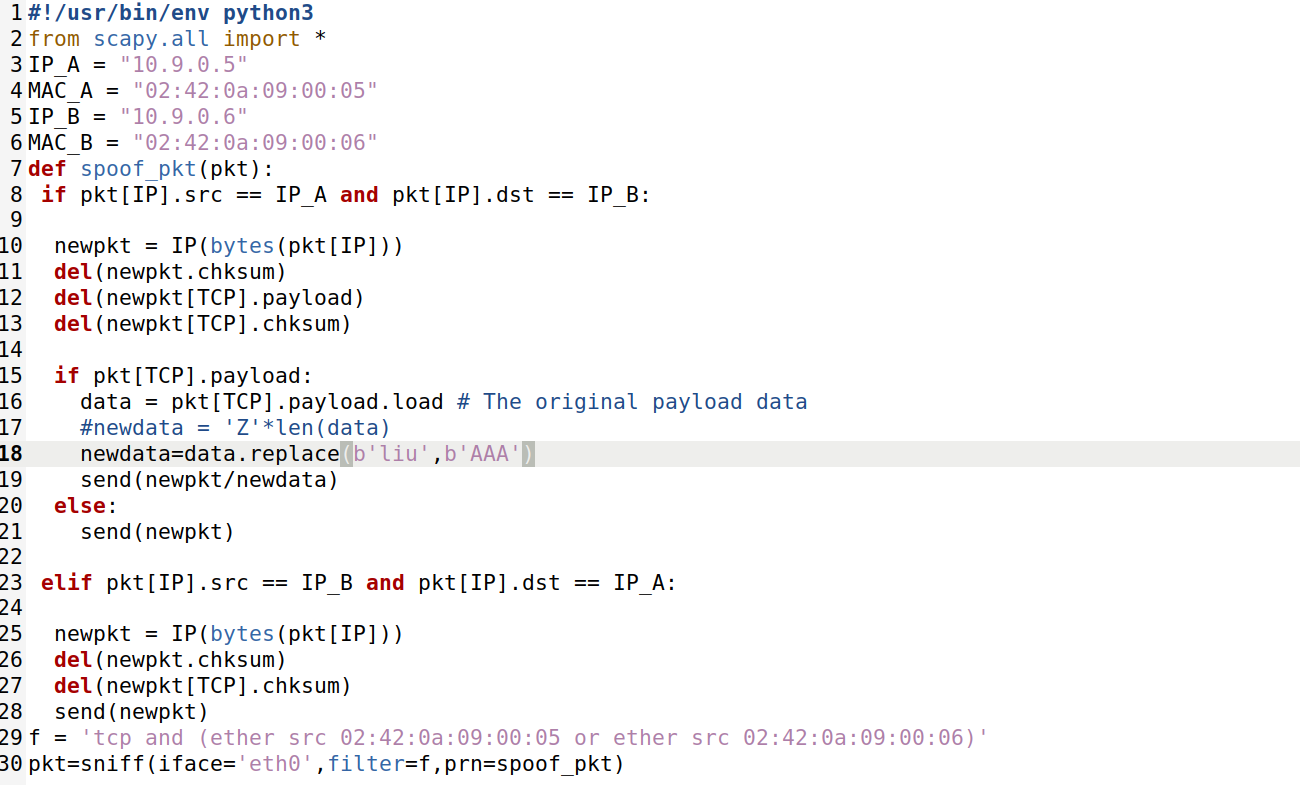


执行攻击，发现所有的输入都替换成了Z

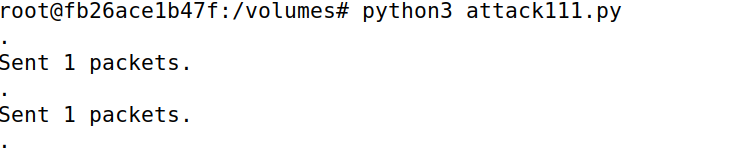


Task3

代码如下



实施攻击



攻击成功，liu被替换成为AAA

