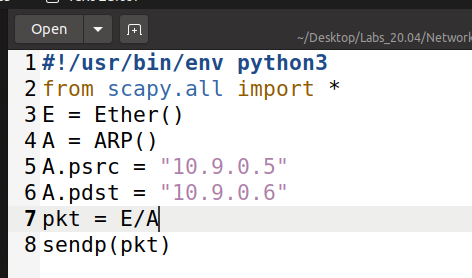
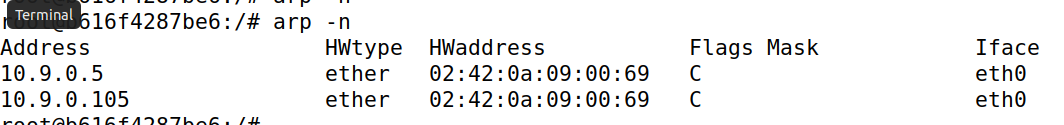
Task1：

1、

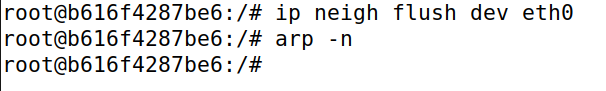
攻击程序：



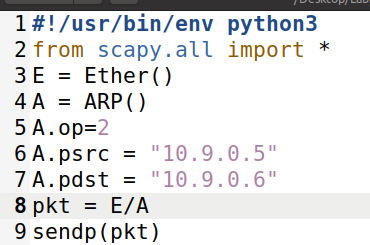
实施攻击后查看被攻击主机的arp缓存，攻击成功：



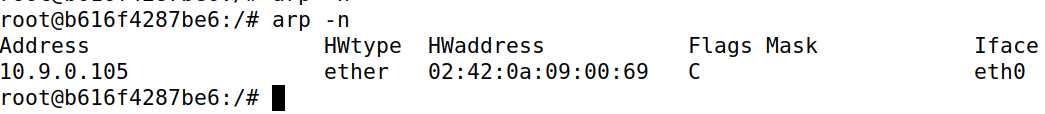
2、

清空缓存：  


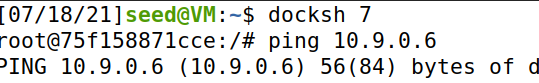
修改程序：

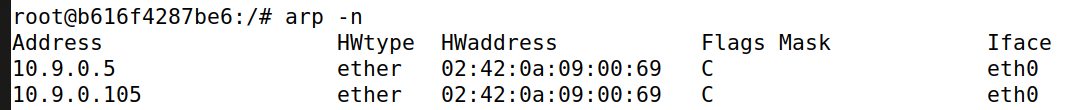


B的ip缓存不在A中：

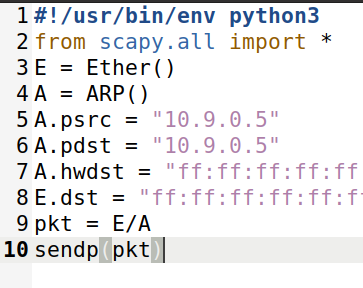


攻击失败

B的缓存在A中：  


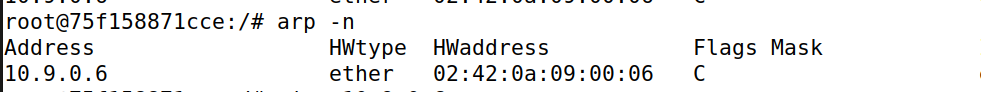
攻击成功：  


3、

修改程序：  


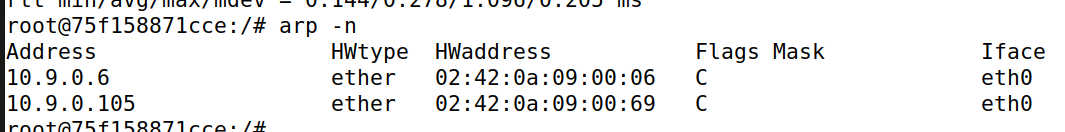
B的ip不在A的缓存中：

攻击失败

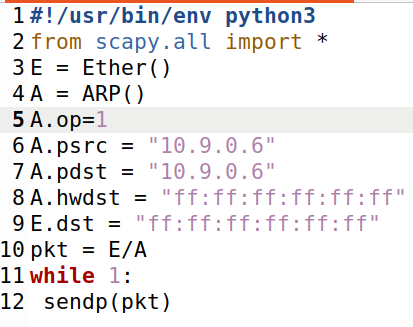


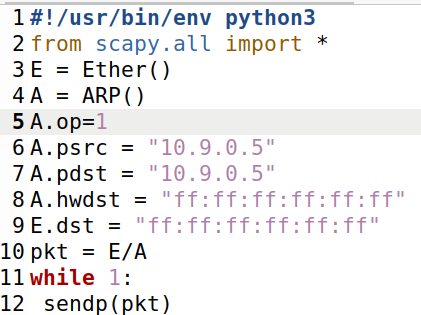
B的ip在A的缓存中：

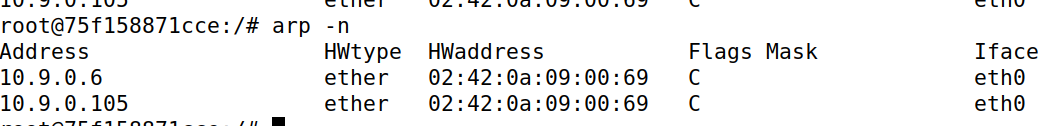
攻击成功：

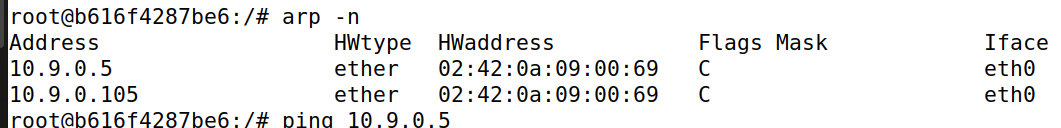


Task2：

1、针对主机A和主机B的持续发包的攻击程序：  


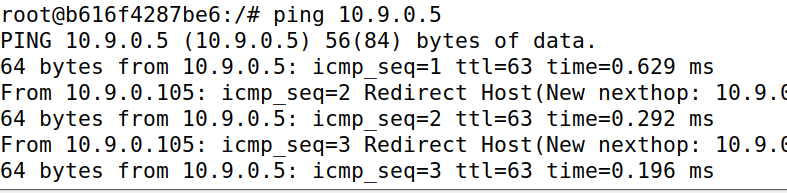


攻击成功：  




运行攻击程序并打开ip转发：



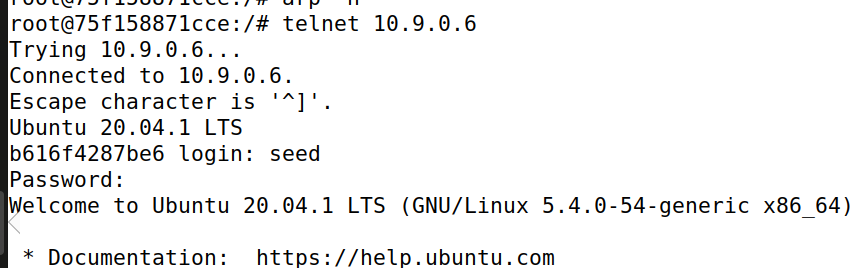
主机B可以ping到主机A：  


2、

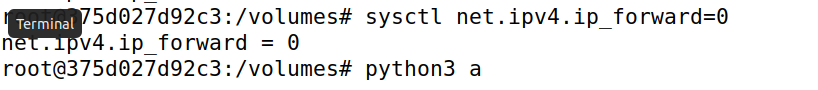
在攻击主机上运行针对A和B的ARP缓存攻击程序，并将允许转发设置为1：



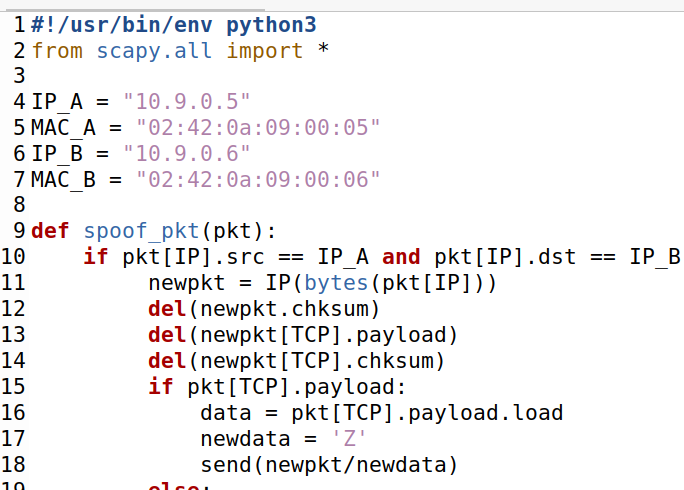
在主机A通过Telnet登录主机B：

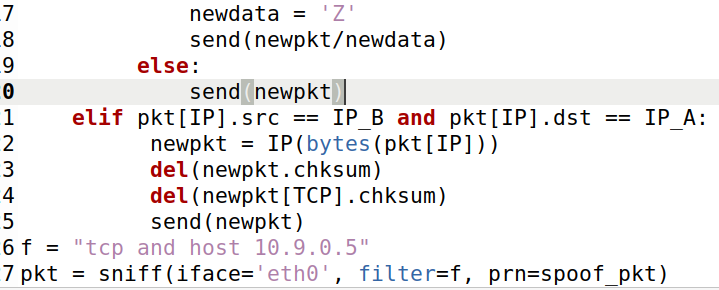


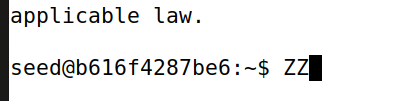
关闭攻击主机的允许转发：



运行攻击程序：



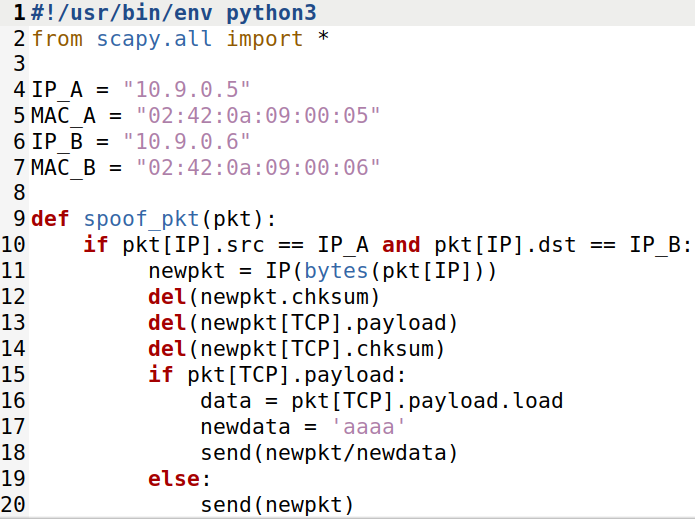


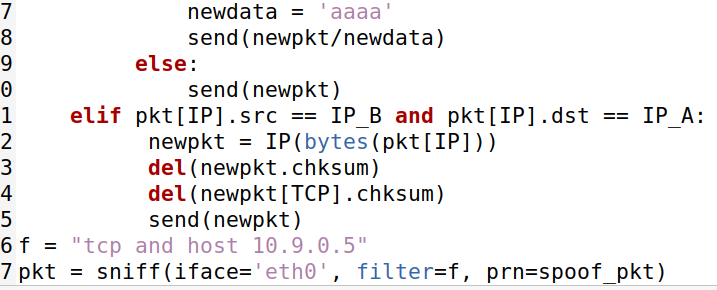
在A终端输入数据，变成了Z:  


Task3：

运行针对A、B主机的ARP缓存攻击程序后

攻击篡改程序：





输入数据后被篡改为指定字符：

