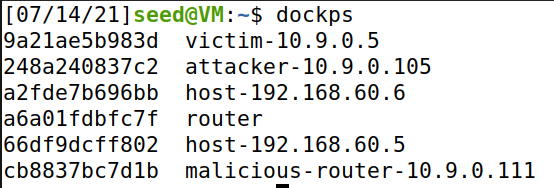
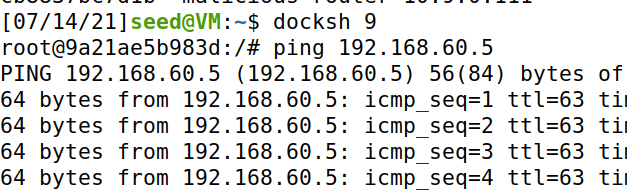
57118108 时真好

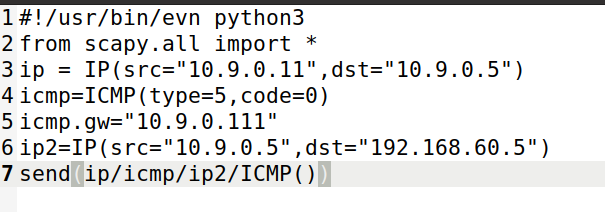
实验环境信息：  


Task1、

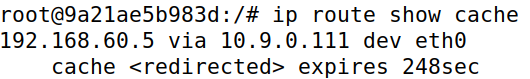
在受害者主机上运行ping命令：

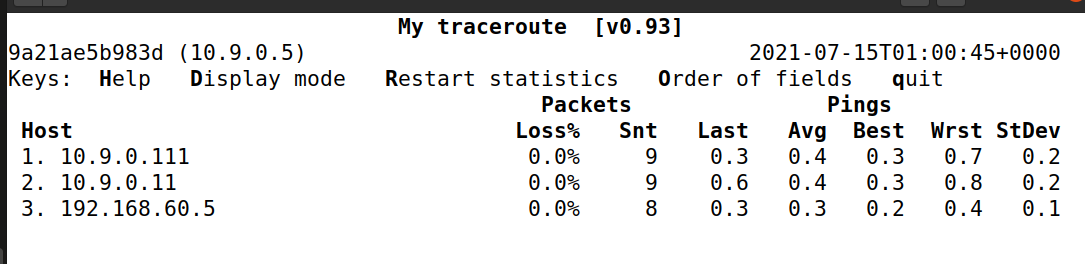


在攻击主机上运行代码：



路由表和traceroute中均增加了重定向信息，攻击成功：

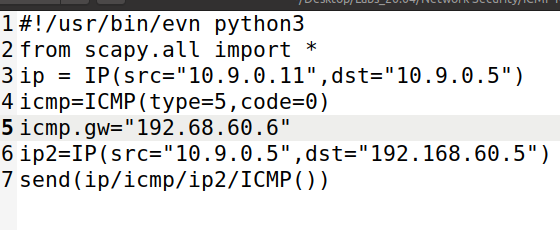




Question1：

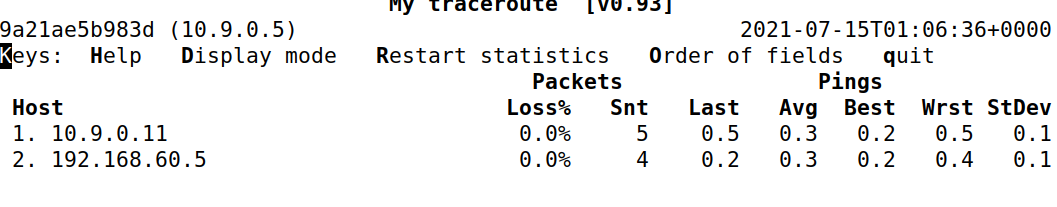
重定向子网到远程主机：

修改攻击程序：



重复上述过程发现攻击不成功：

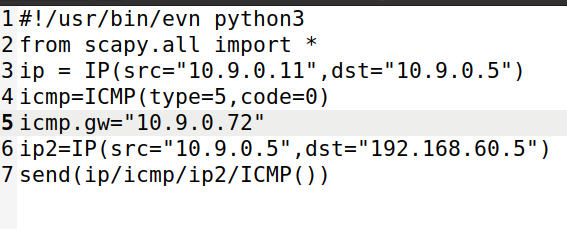
路由表中没有重定向路由且traceroute未经过添加的地址：



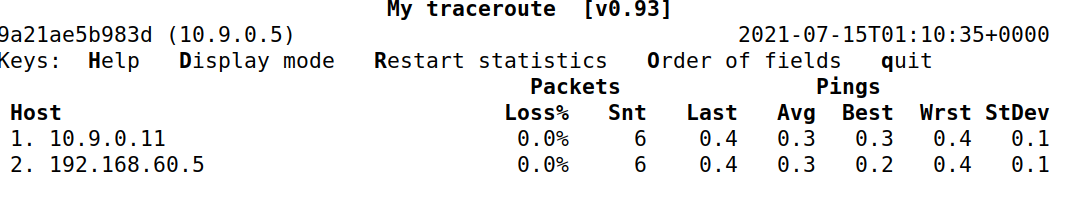
Q2：

重定向到子网中不存在的地址：

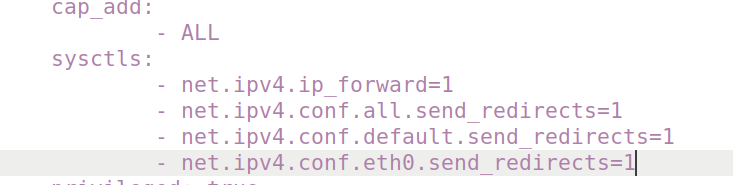
修改程序：



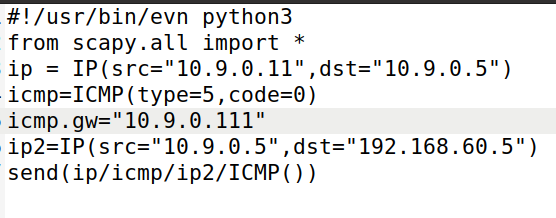
重复上述运行，结果同样攻击失败:

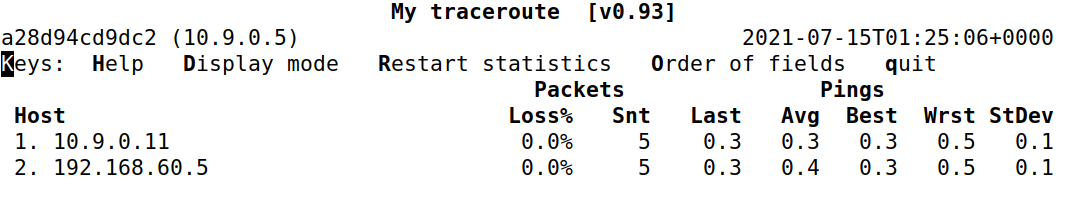


Question3：

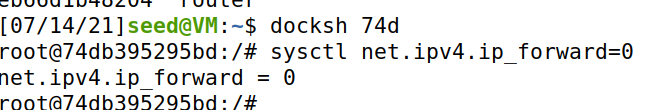
修改配置文件为不允许重定向报文：  


重启dock后采用第一次攻击成功的代码攻击失败：

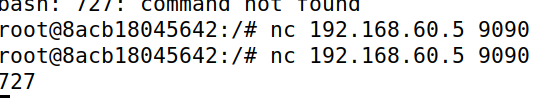


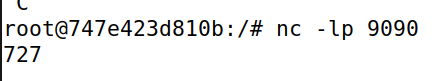


Task2、

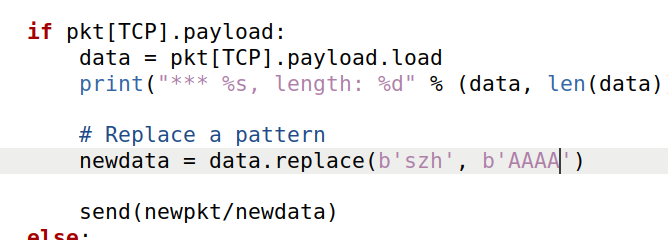


监听端口，通信正常：

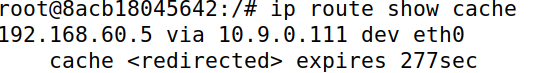




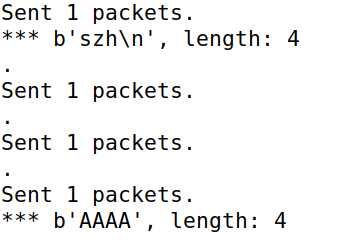
修改攻击程序：

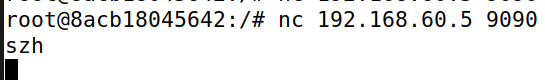


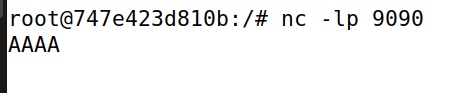
先按照task1中进行重定向攻击，成功：



再在重定向经过的10.9.0.111运行上述修改内容的攻击程序：



攻击结果：报文被篡改：  


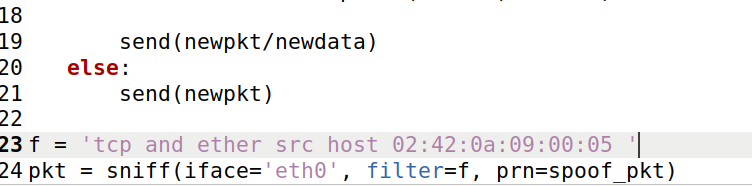


Question4：

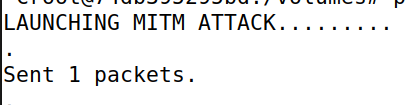
捕获了10.9.0.5到192.168.60.5的流量，因为攻击的目标是修改单向的流量。

Question5：

采用mac地址过滤，修改程序：



攻击程序只发送一个包：



攻击成功：

