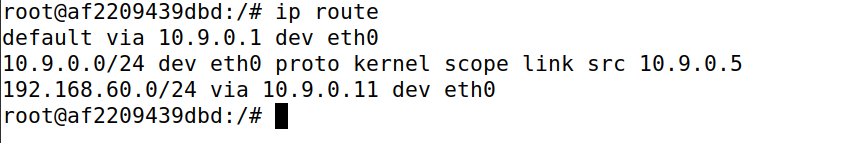
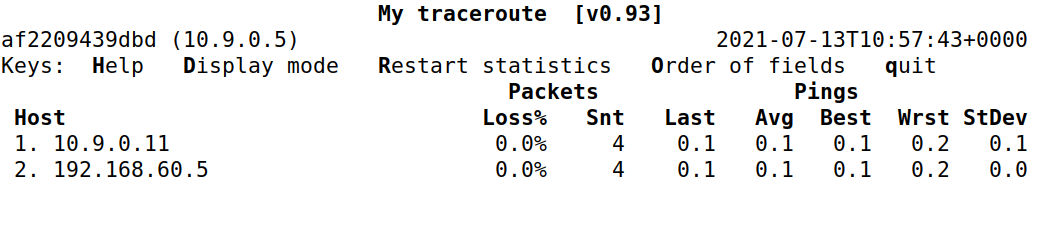
**第三次实验报告**

­­­­­­57118121 刘洪飞

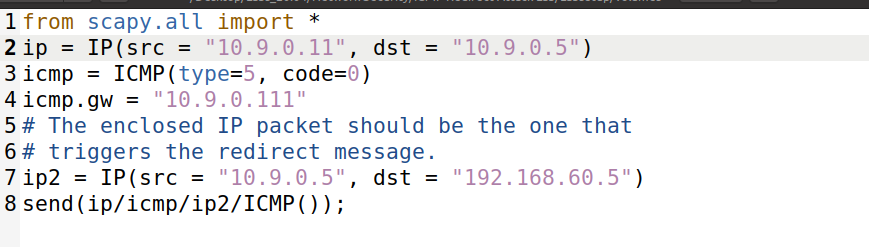
Task1

查看受害者路由

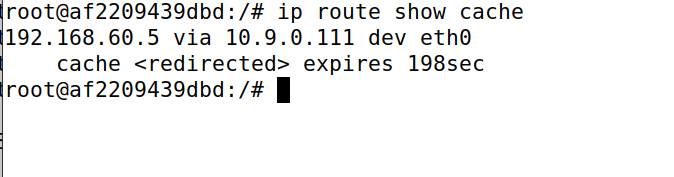


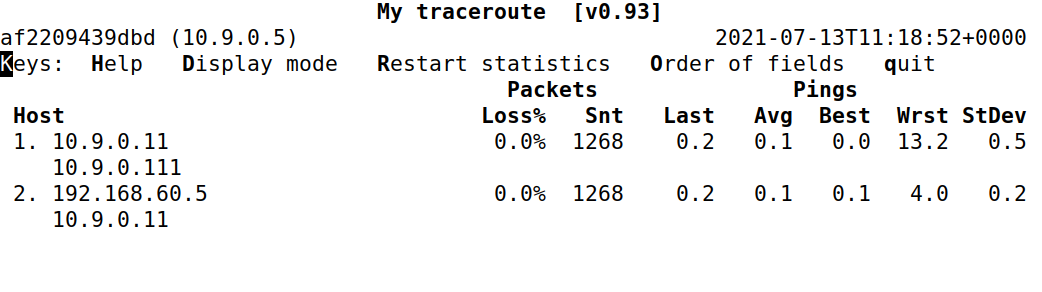


代码



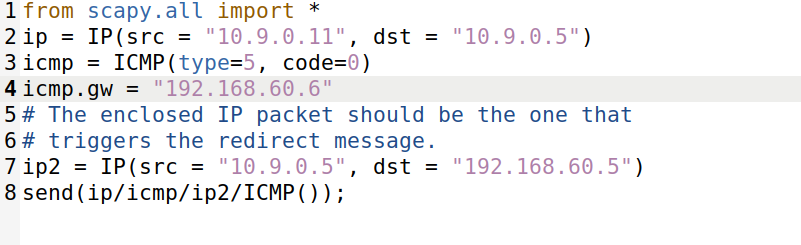
Ping过程中运行代码，发现攻击成功





问题1

修改网关

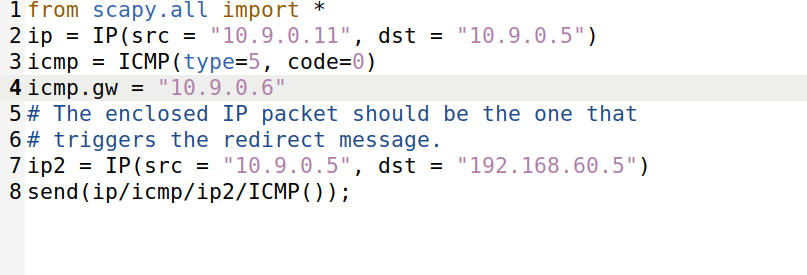


攻击失败

是因为网关不在local LAN里面，默认路由定位成功

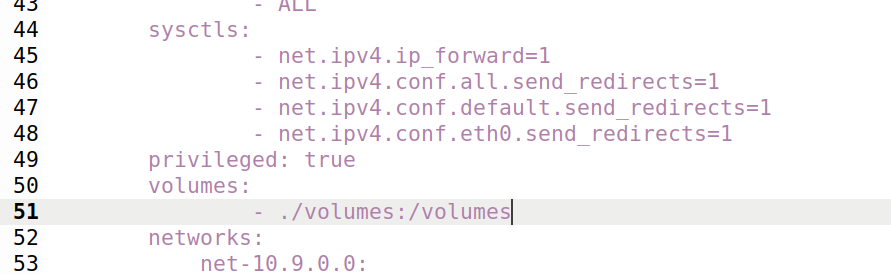
问题2

网关改为不存在的地址10.9.0.6



因为网关不存在，无法定位路由，使用了默认路由，攻击失败

问题3

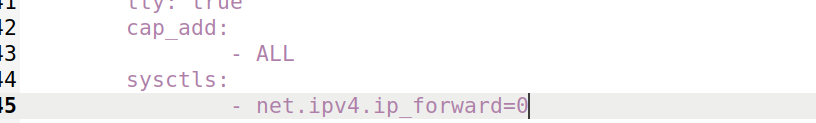


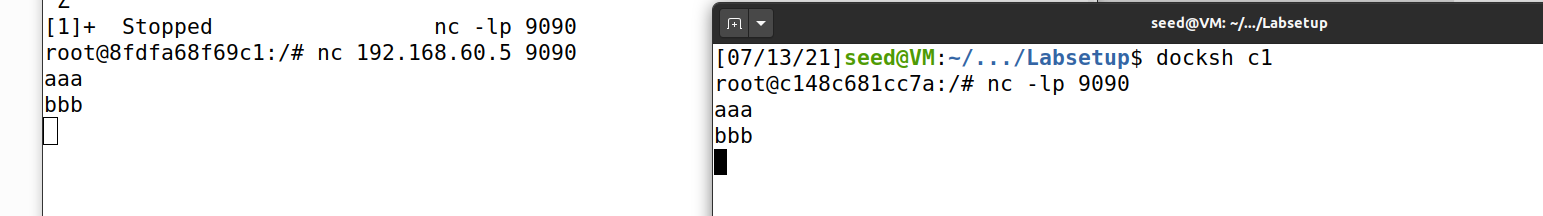
攻击失败

原因是恶意路由器发现自己收到的报文不正确，传送至原来的默认路由

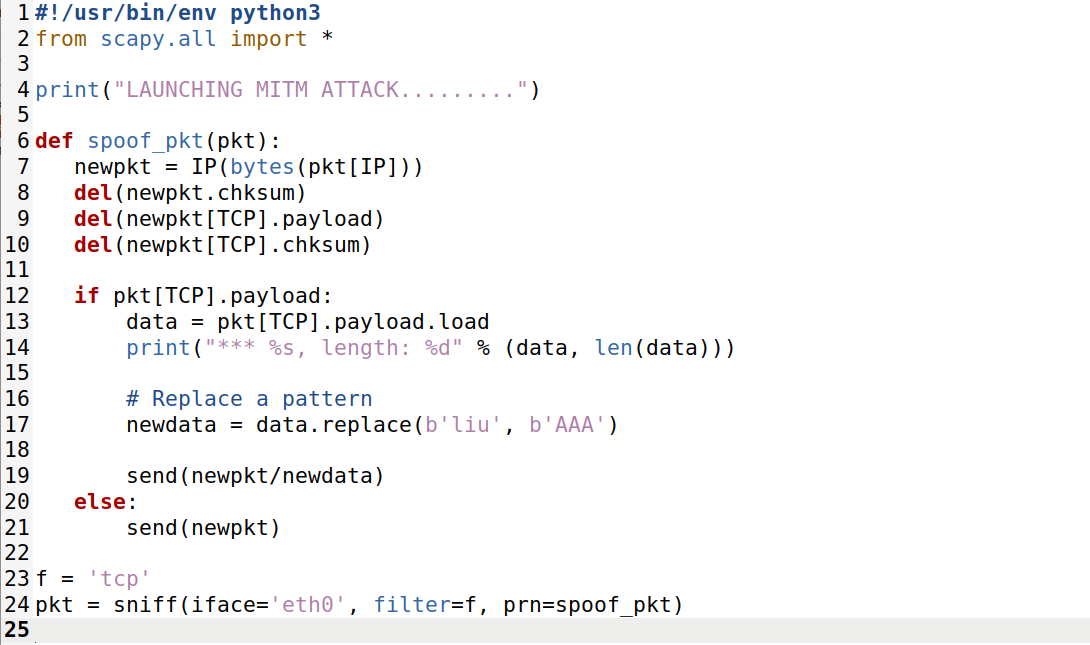
Task2

搭建好环境





代码，攻击需要重复第一个实验之后进行



攻击成功 liu修改为AAA

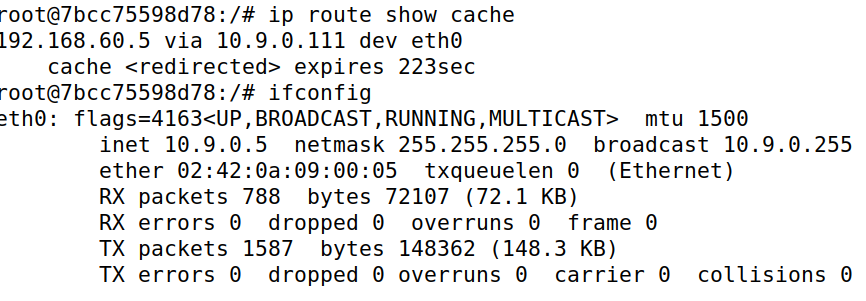


问题4

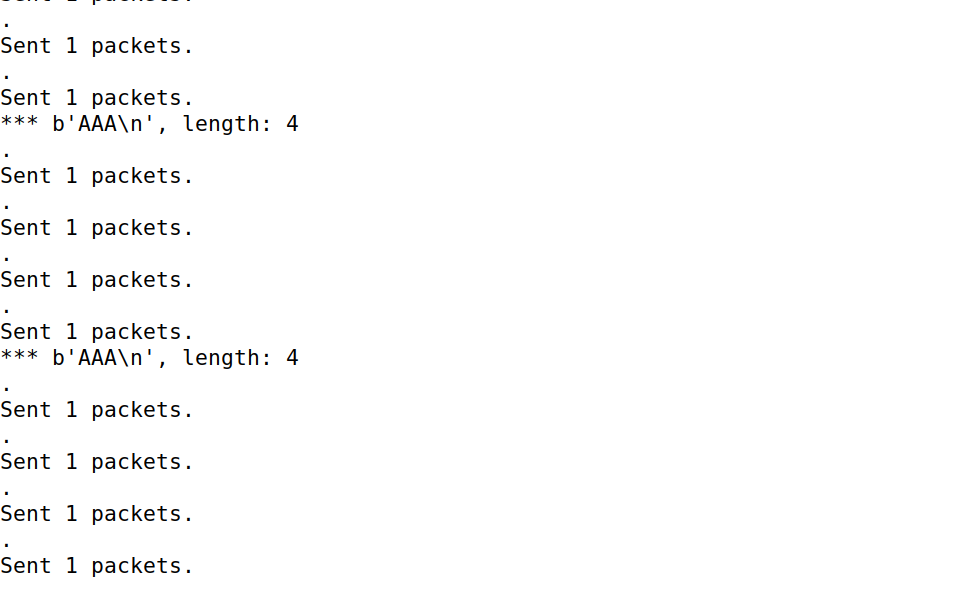
仅仅需要捕获一个方向的包，即从 10.9.0.5 向 192.168.60.5 的包。因为 ICMP 重定向是单向的重定向，从 10.9.0.5 通过 tcp 包发送至 192.168.60.5，所以另一方向的包没有价值。

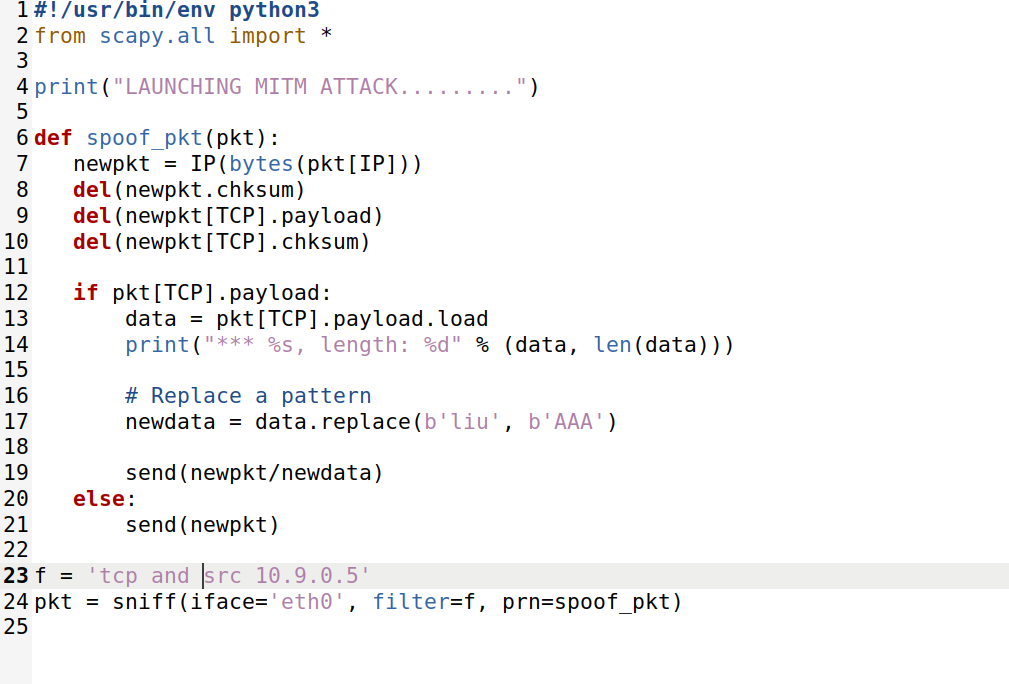
问题5

查看ip和mac地址



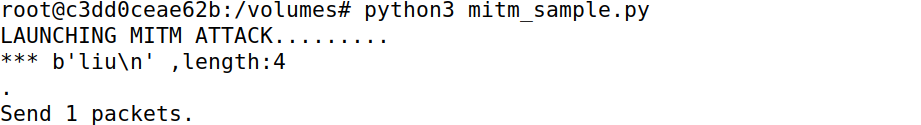
IP过滤，攻击成功，但是wireshark捕获大量报文，由于恶意软件发送过程中使用IP源地址没有变化，也会再次循环发送报文，影响性能







MAC地址过滤，攻击成功并没有大量报文，原因应该是MAC地址会修改不同的MAC地址，并不会重复发送，不影响性能。





综上，由于MAC地址过滤不会影响性能，而IP过滤会影响性能，所以选用MAC地址过滤