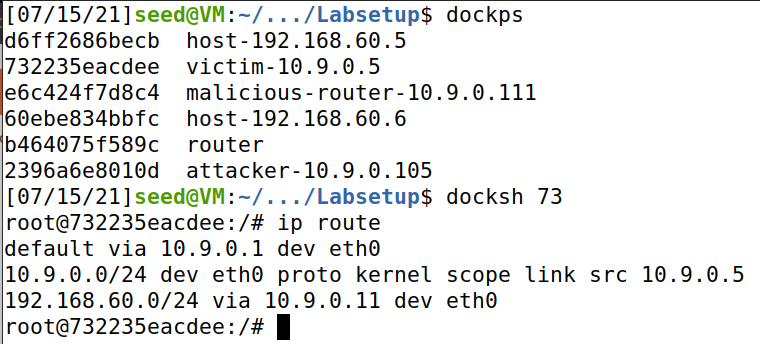
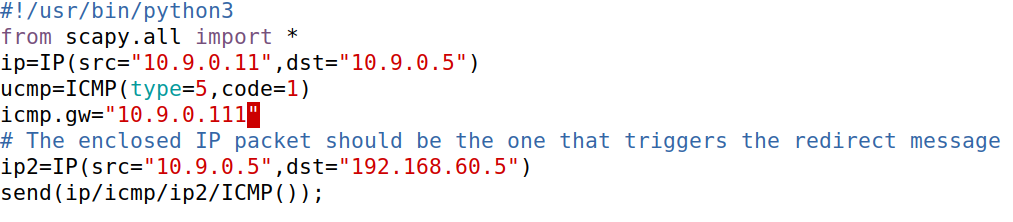
**57118110 杨紫瑄**

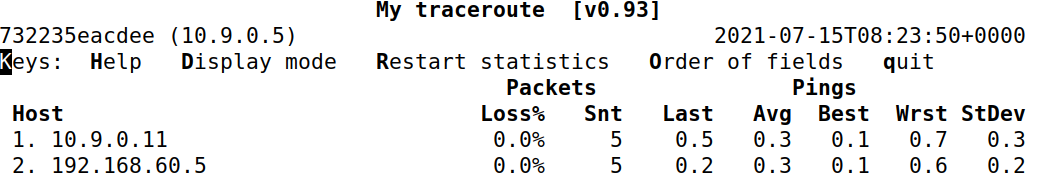
**Task1 Launching ICMP Redirect Attack**



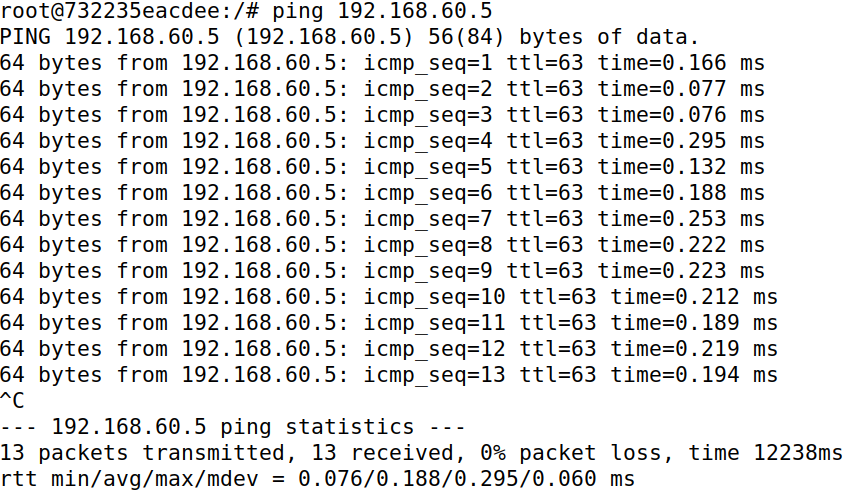
查看被攻击主机的路由表，其中可看出局域网192.168.60.0/24的网关地址为10.9.0.11



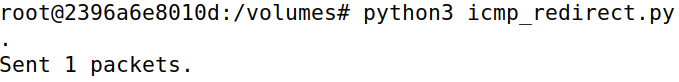
编辑攻击代码如上



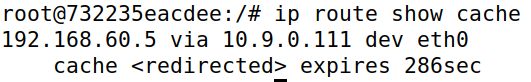
在攻击前，查看被攻击主机的路由如上



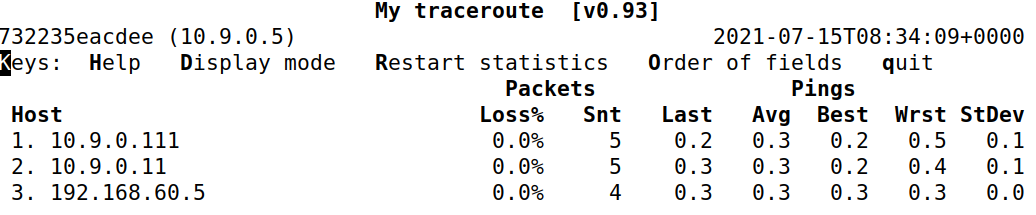
在被攻击主机中ping 地址192.168.60.5



随后在attacker中运行攻击程序



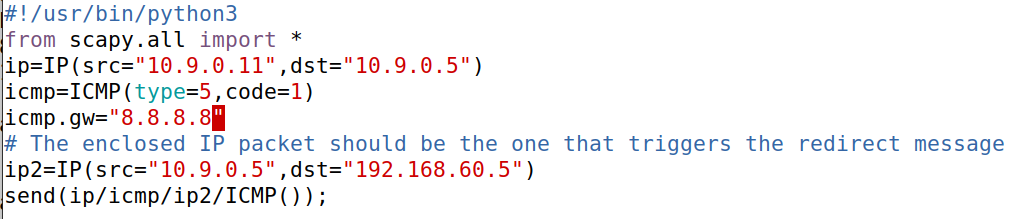
在被攻击主机中查看攻击后的路由缓存，发现发送至192.168.60.5的数据包已被重定向为恶意路由地址



再次查看被攻击主机的路由发现数据包会首先到达恶意路由，说明重定向攻击成功

**问题回答：**

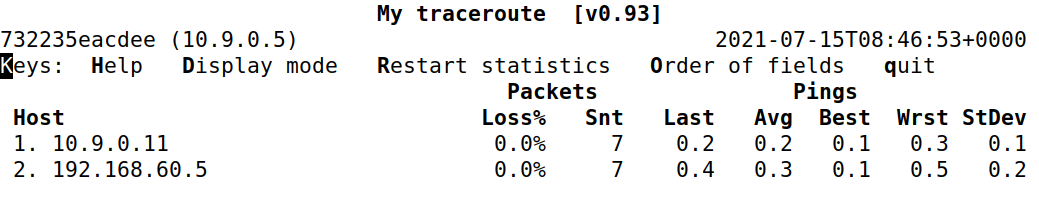
1. **可以使用ICMP重定向攻击重定向到远程机器吗?即分配给icmp.gw的IP地址是一台不在本地局域网内的计算机。请出示您的实验结果，并说明您的观察结果。**



将重定向的网关地址改为8.8.8.8

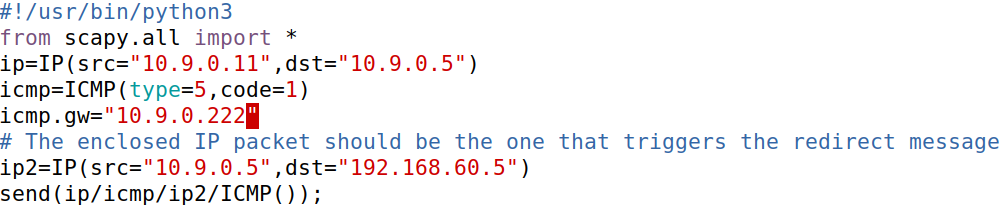


重新进行攻击后发现没有产生路由缓存



查看路由后发现没有变化，说明路径并未被导向8.8.8.8，说明不能重定向到远程计算机

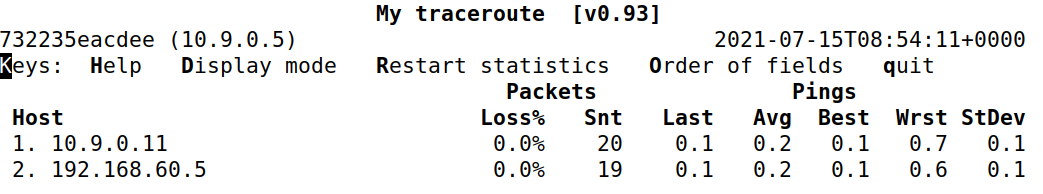
1. **是否可以使用ICMP重定向攻击来重定向到同一网络中不存在的计算机?即分配给icmp.gw的IP地址是一台离线或不存在的本地计算机。请出示您的实验结果，并说明您的观察结果。**



将icmp.gw的地址改为不存在的计算机地址10.9.0.222

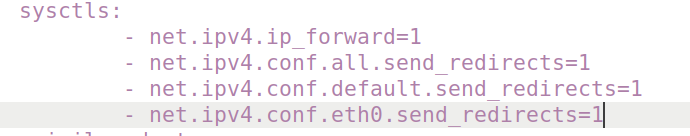


重新攻击后发现没有产生路由缓存

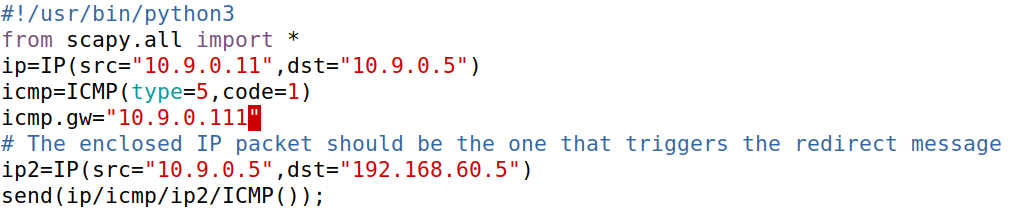


且没有导至10.9.0.222,说明不能重定向到同一网络上不存在的计算机

1. **如果你看一下在docker-compose.Yml文件中，您将发现恶意路由器容器的以下条目。这些条目的目的是什么?请将它们的值改为1，并重新发起攻击。请描述并解释你的观察结果。**



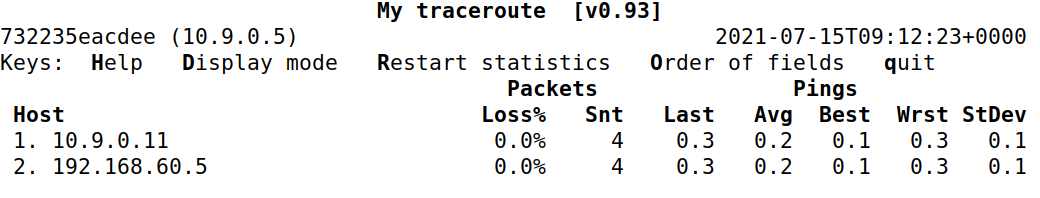
这些条目的目的是关闭或开启ICMP重定向，将值改为1后重启容器



将icmp.gw的地址改回10.9.0.111后重新攻击

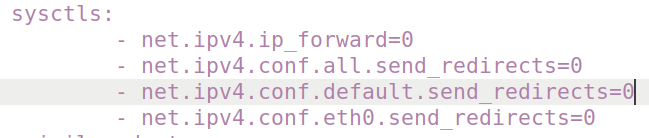


发现没有产生路由缓存

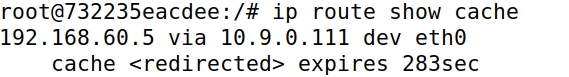


查看路由路径中也没有恶意路由，说明重定向攻击失败

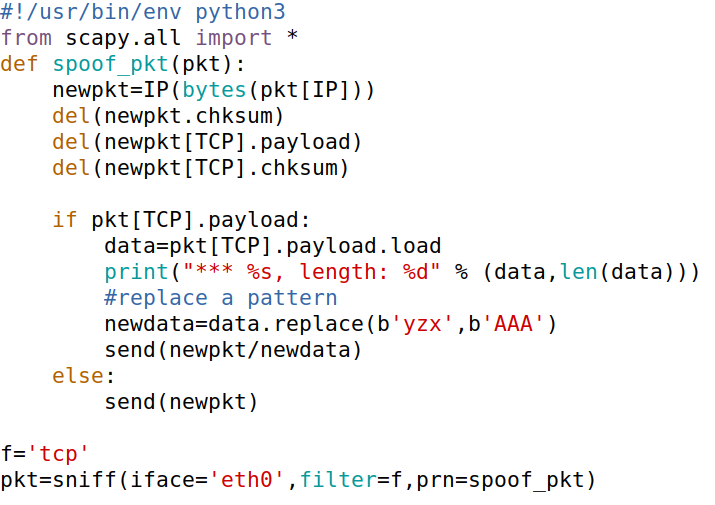
**Task2 Launching the MITM Attack**



修改docker-compose.yml文件中的标记位并关闭恶意路由的转发功能，重启容器



发送重定向攻击将路由重定向导恶意路由器



构造如上攻击程序，在目的容器中输入nc -lp 9090 打开端口监听，并在被攻击主机中输入nc 192.168.60.5 9090 命令连接目标主机端口，在恶意路由上执行攻击程序后，在被攻击主机中输入’yzx’





发现目标主机成功接收到了字符串并将其转换成AAA，说明中间人攻击成功

**问题回答：**

1. **在你的MITM程序中，你只需要捕获一个方向的流量。请指明方向，并说明原因。**

在过滤器中增加mac地址过滤

* 1. 被攻击主机发送至目标主机



过滤改为如上图所示





重新进行攻击并监听后发现目标主机可以成功接收被攻击主机中输入的字符，并将其转换

* 1. 目标主机发送至被攻击主机



将过滤改为上图所示





再次进行攻击并监听后发现目标主机无法监听到被攻击主机的输入

综上所述，在中间人攻击的程序中只需要捕获从被攻击主机发送至目的主机的流量，这是因为我们关闭了恶意路由器的转发功能，所以恶意路由器接收到来自被攻击主机的数据包后，不会发送数据包给目的主机，导致目的主机没有接收到流量，所以应该捕获从被攻击主机发送到目的主机的流量。

1. **在MITM程序中，当你从A(10.9.0.5)捕获nc流量时，你可以在过滤器中使用A的IP地址或MAC地址。其中一个选择是不好的，会产生问题，即使两个选择都可能有效。请两种都试一下，用你的实验结果来说明哪一种选择是正确的，并解释你的结论。**
   1. 使用MAC地址过滤

在问题（4）中已经实现且攻击可以成功进行

* 1. 使用IP地址过滤

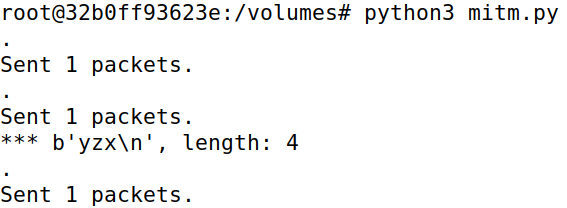


将过滤改为如上图所示  

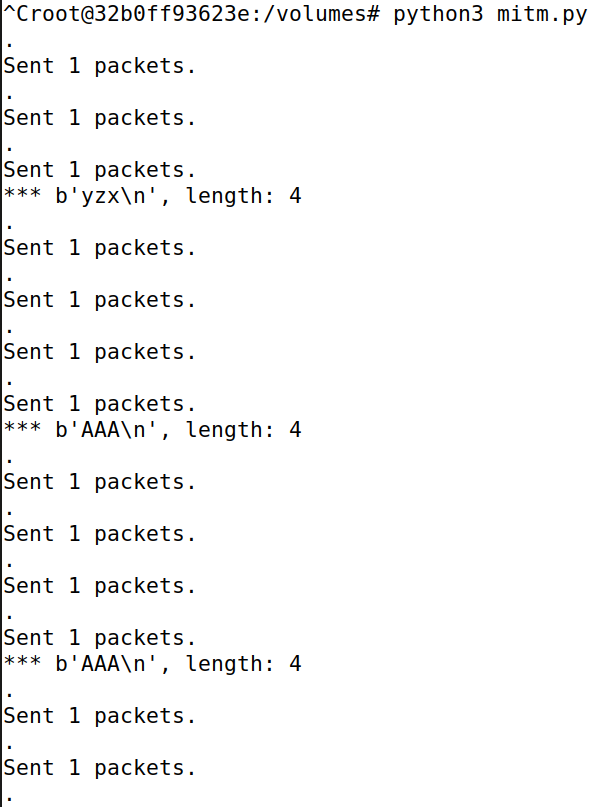



发现中间人攻击也可以成功实现

但是比较IP地址过滤和MAC地址过滤后，发现存在以下问题：



上图所示的是在过滤地址为MAC地址的情况下，每发送一行信息，恶意路由器会发送一个数据包，但使用IP地址过滤时，路由器则会发送大量数据包，如下所示



上图所示是过滤地址为IP地址时，每发送一行信息，恶意路由器会不断地发送数据包，这是因为来自被攻击主机的数据包和伪造的数据包的IP地址相同，所以程序会对攻击者修改后重发的报文再次进行捕获和重发，造成一个循环，这会导致资源的浪费和性能的低下。但是二者的MAC地址是不同的，所以当使用MAC地址过滤时，恶意路由器只会发送一个数据包。

综上所述，使用IP地址和MAC地址都能够成功进行中间人攻击，但是使用MAC地址过滤是更好的选择，它可以防止多次捕获自己修改后发送的报文，提高程序的效率，避免浪费系统的资源。