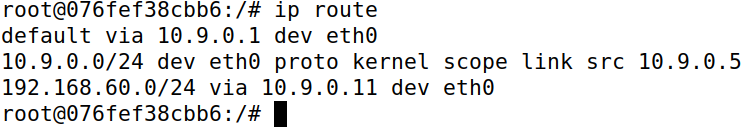
**ICMP Redirect Attack Lab**

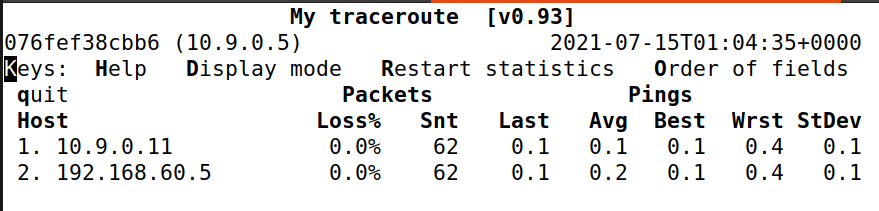
**57118113 蔡义涵**

**Task 1: Launching ICMP Redirect Attack**

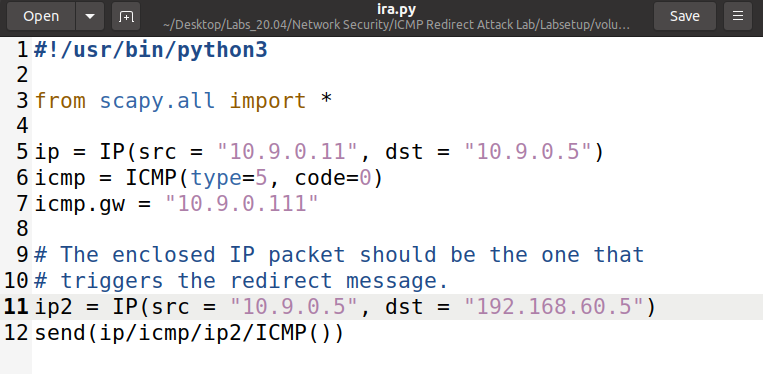
在victim-10.9.0.5上执行ip route：



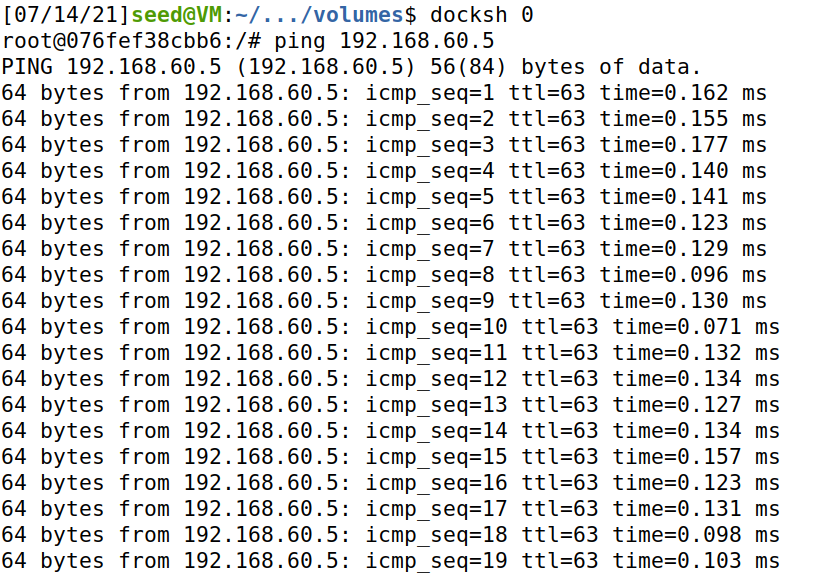
可以看到，victim容器目前使用10.9.0.11（即192.168.60.11）作为192.168.60.0/24的路由。在victim-10.9.0.5上执行mtr -n 192.168.60.5



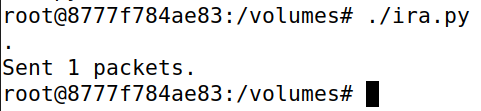
完成ira.py



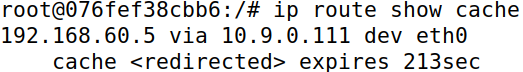
首先在victim-10.9.0.5上ping192.168.60.5,



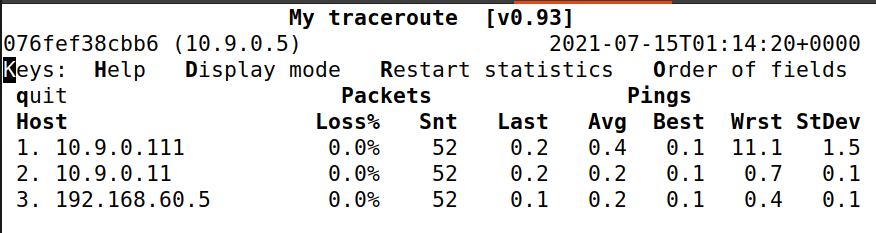
随后在attacker-10.9.0.105上执行ira.py



查看victim-10.9.0.5的路由缓存，



查看victim-10.9.0.5的路由路径，



根据以上截图可以判断，攻击成功。

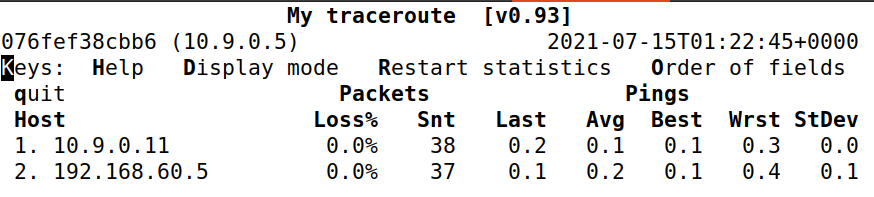
**Question1：**

尝试重定向到其他地址



使victim-10.9.0.5 ping192.168.60.5,并在attacker-10.9.0.105上执行ira.py，查看路由缓存和路由路径





发现攻击失败。

**原因**：猜测原因是无法直连外网主机，因此寻找不到外网主机。

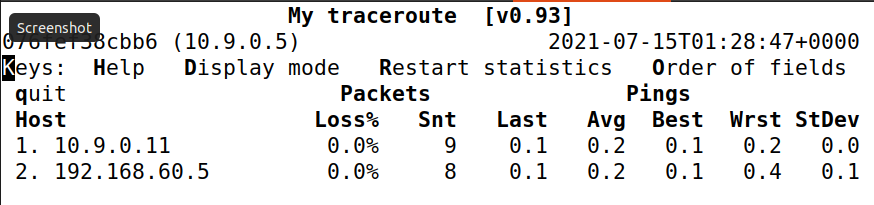
**Question2：**

尝试重定向到本网段内的不存在主机的地址



使victim-10.9.0.5 ping192.168.60.5,并在attacker-10.9.0.105上执行ira.py，查看路由缓存和路由路径



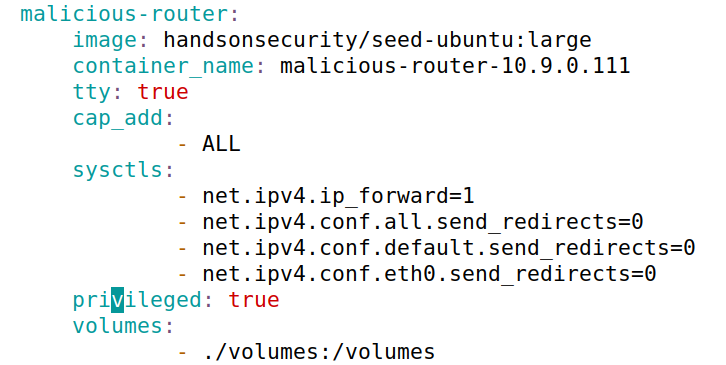


发现攻击失败。

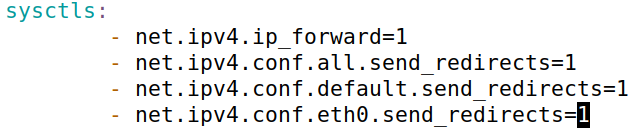
**原因**：原因是不存在这个地址的主机，因此寻找不到目标。

**Question3：**

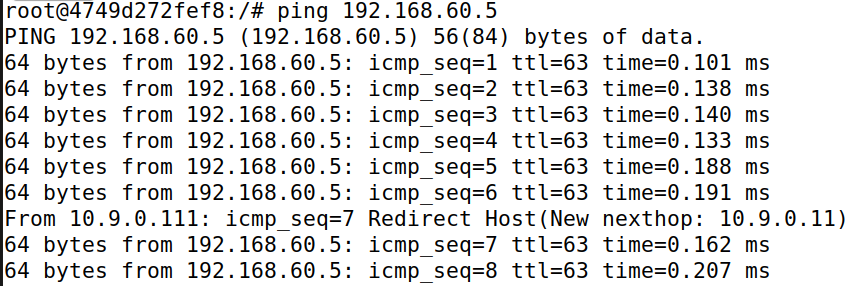
查看docker-compose.yml文件

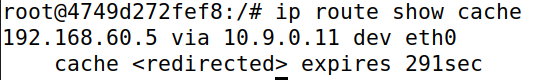


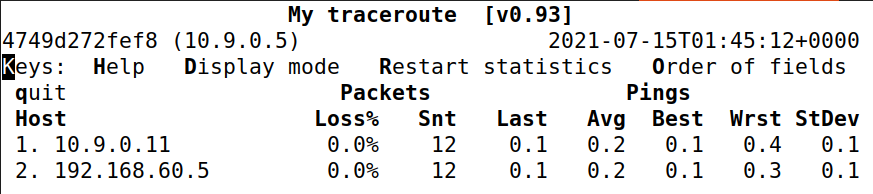
修改其sysctls属性为：



使victim-10.9.0.5 ping192.168.60.5,并在attacker-10.9.0.105上执行ira.py，查看路由缓存和路由路径。





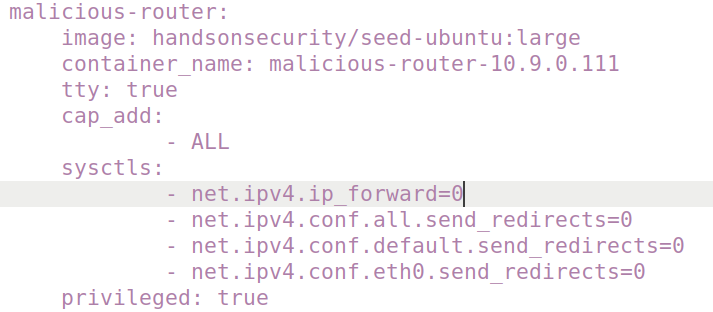


发现victim-10.9.0.5收到了10.9.0.111重定向报文，但攻击失败。

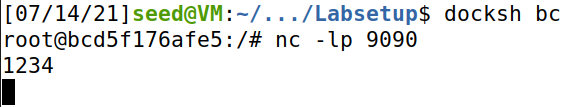
**原因**：原因是开启了Malicious Router-10.9.0.111的ICMP重定向功能。Victim-10.9.0.5遭受攻击向其寻址时，Malicious Router-10.9.0.111返回了重定向报文，将其定向到了默认网关，纠正了错误。

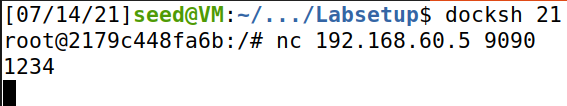
**Task 2: Launching the MITM Attack**

首先修改docker-compose.yml文件，将net.ipv4.ip\_forward设置为0

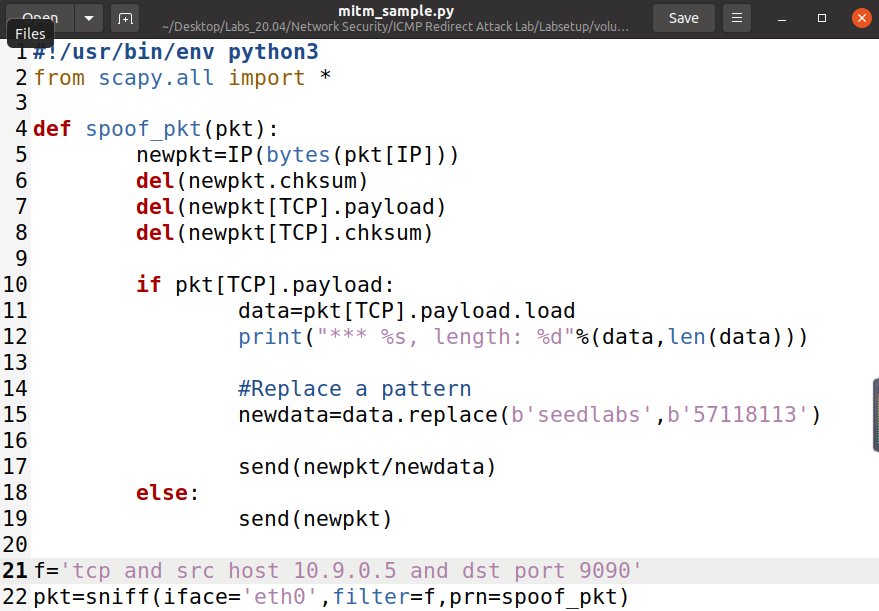


在host-192.168.60.5上执行nc -lp 9090，在victim-10.9.0.5上执行nc 192.168.60.5 9090，建立tcp连接。

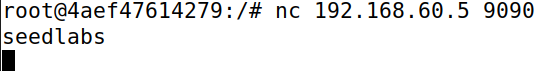


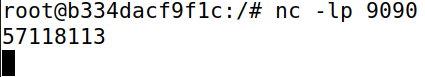


完成程序mitm\_sample.py，将tcp报文data中的’seedlabs’字段改为’57118113’。



先执行icmp重定向攻击到10.9.0.105中，随后建立上述tcp连接，并在10.9.0.105上执行上述程序。



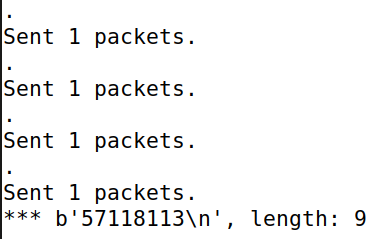


发现攻击成功。

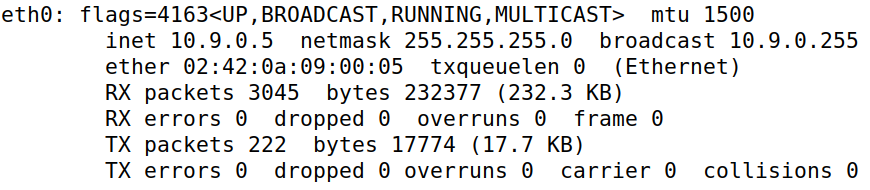
**Questions1：**只需要捕获从victim-10.9.0.5到host-192.168.60.5的报文即可，因为tcp连接中信息源来自victim。

**Questions2：**

Filter=’tcp and src 10.9.0.5’时，发现mitm攻击成功，但mitm\_sample.py程序无限循环发包。

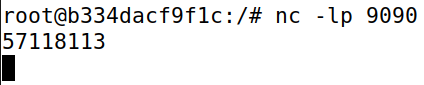


在victim-10.9.0.5上运行ifconfig，查看eth0网卡对应的mac地址为02:42:0a:09:00:05。

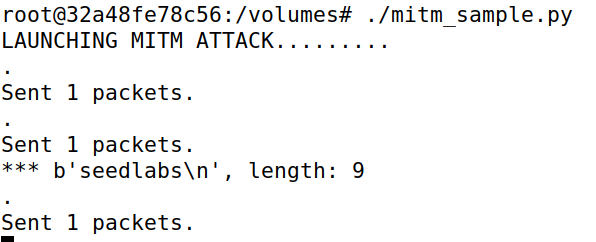


修改filter=’tcp and ether src 02:42:0a:09:00:05’,再次执行攻击。





攻击仍然成功，mitm\_sample.py运行结果为：



发现程序仅发了一个包。

**原因**：原因是对IP进行过滤会导致程序捕捉到自己发送的欺骗包，导致无限循环；而根据MAC地址只会一开始10.9.0.5发出的包会被捕捉到。