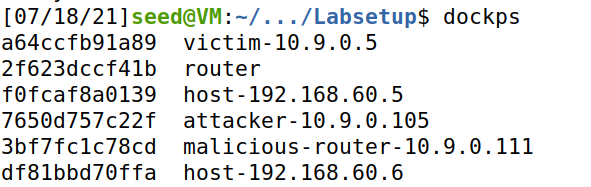
**Lab3 ICMP Redirect Attack**

57118101 卞郡菁

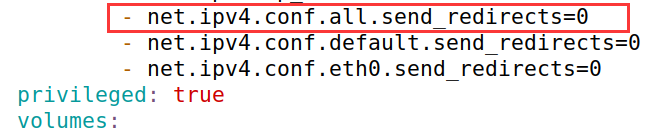
1. 容器构建环境

cd Desktop/Labs\_20.04/Network\ Security/ICMP\ Redirect\ Attack\ Lab/Labsetup/



1. 配置文件

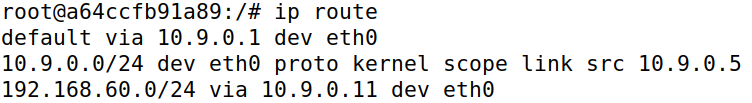
在docker-compose.yml中，将net.ipv4.conf.all. accept\_redirects的值设为0以接收ICMP重定向信息。



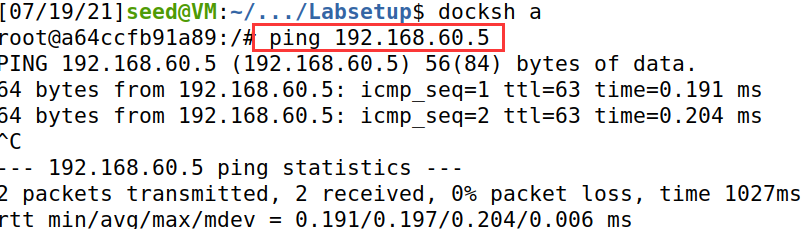
**Task 1: Launching ICMP Redirect Attack**

-重定向至本地局域网-

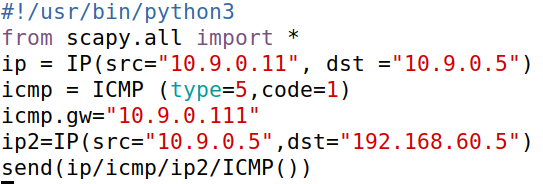
首先查看victim主机的ip route：



在victim主机上ping 192.168.60.5，发现能够正常ping通：



在攻击机上编写脚本Attack.py：

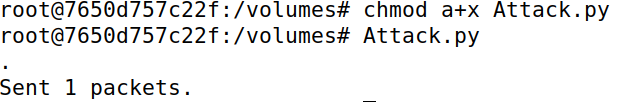


其中：

①ip为重定向的报文，攻击机10.9.0.111伪装成原本正确的路由10.9.0.11发送给victim主机10.9.0.5；

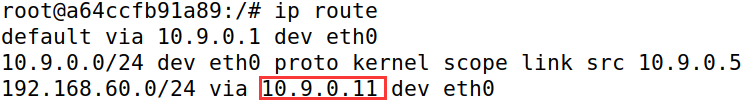
②ip2为捕获的报文，是victim主机10.9.0.5 ping目标子网192.168.60.0/24时发送的报文。

在攻击机上运行攻击脚本，注意需与victim主机发送icmp报文的同时进行（即ping 192.168.60.5 时）。

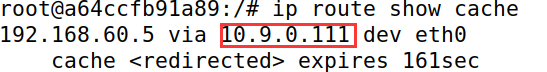


**结果表明：**

1. **此次攻击不会影响路由表**——在路由表中，通过的路由依旧没有变化，依然是10.9.0.11.



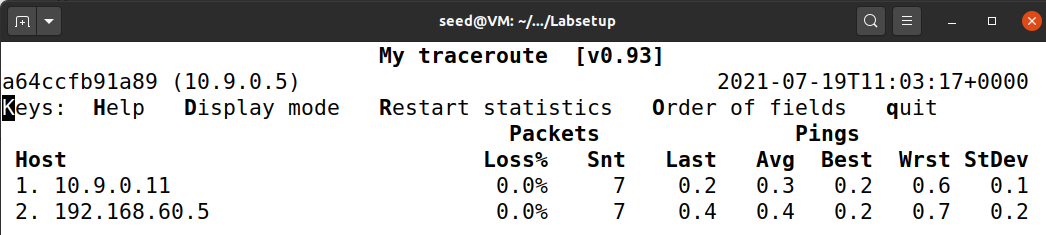
1. **此次攻击影响了路由表缓存** ——这一条信息覆盖了原本通过10.9.0.11的路由表信息；直到这一条缓存到期或被覆盖，都会对victim主机访问产生影响。



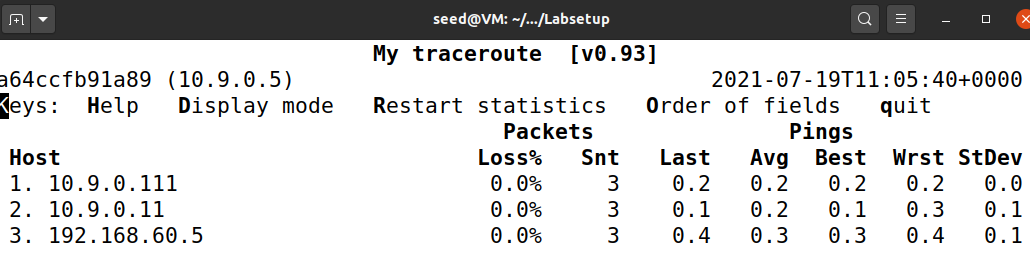
发现发送至 192.168.60.5 的数据包的网关已经被重定向为恶意路由器地址。

1. **此次攻击影响了数据包首先到达的路由（traceroute）：**

攻击前：

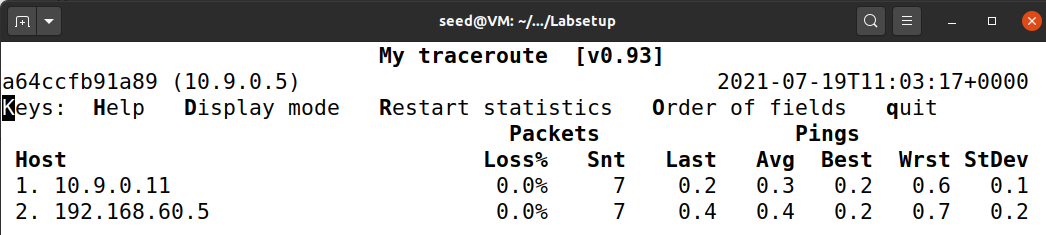


攻击后：mtr -n 192.168.60.5，发现新增了一个10.9.0.111且为第一项。



**• Question 1: 是否可以重定向到非本地局域网计算机？**

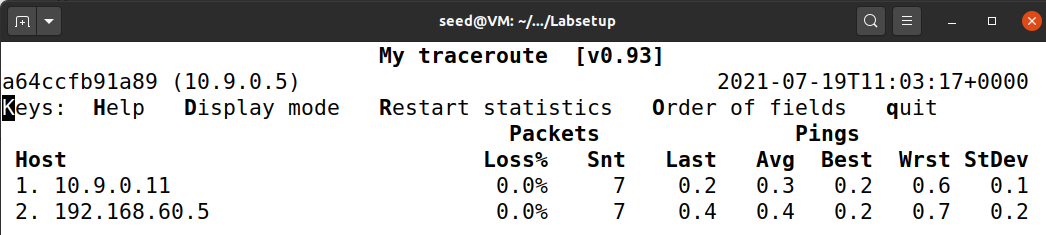
不可以。将icmp.gw修改为百度的ip地址202.108.22.5，mtr -n 192.168.60.5结果如下：



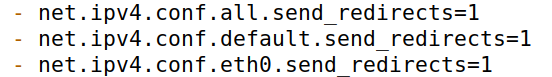
**• Question 2: 是否可以重定向到ip不存在的计算机？**

不可以。将icmp.gw修改为不存在的本地地址1.1.1.1.，mtr -n 192.168.60.5

结果如下：

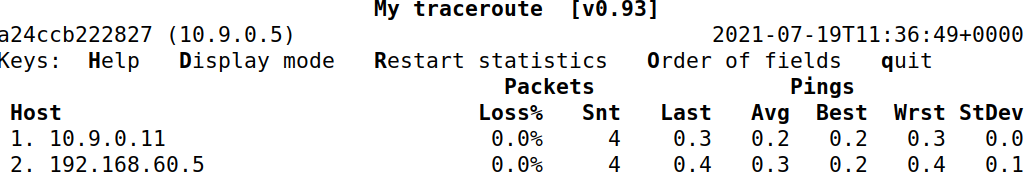


**• Question 3: 配置文件docker-compose.yml三个参数的意义？**

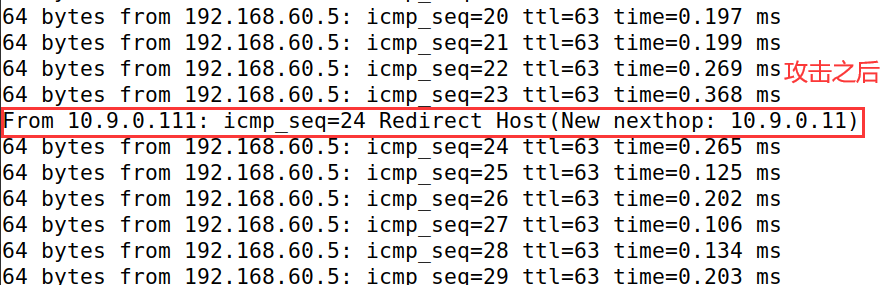


参数为0的目的为关闭 ICMP 重定向。将值修改为 1 则代表允许发送重定向消息。

发现攻击失败：路由器还是10.9.0.11。



究其原因：10.9.0.111发现直接将10.9.0.11作为网关更近，所以发送此重定向报文，改回了原来的路由器。



**Task 2: Launching the MITM Attack**