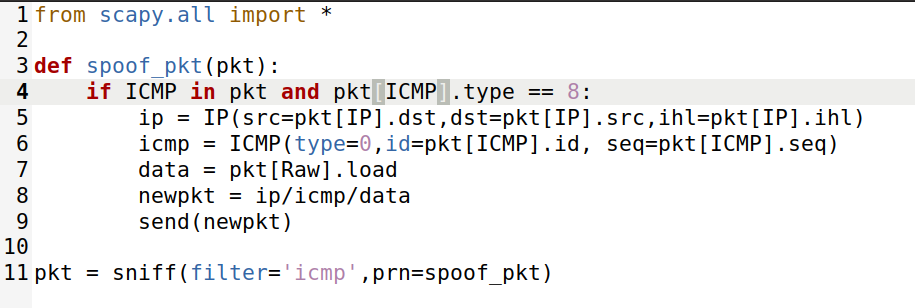
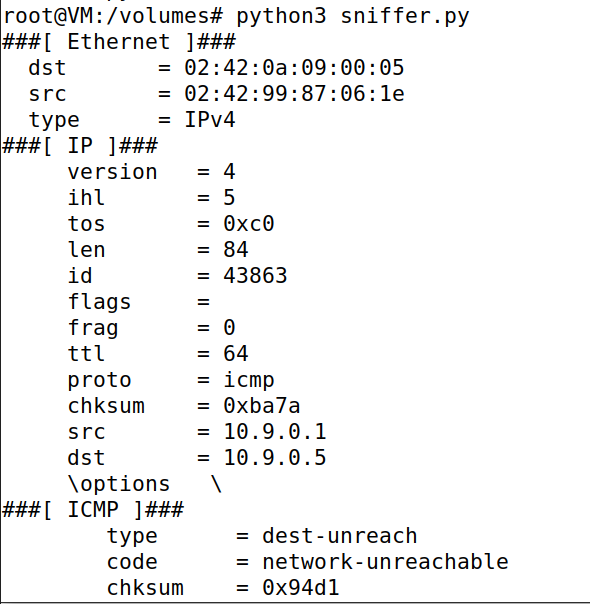
57118127孙博

**1.1A**

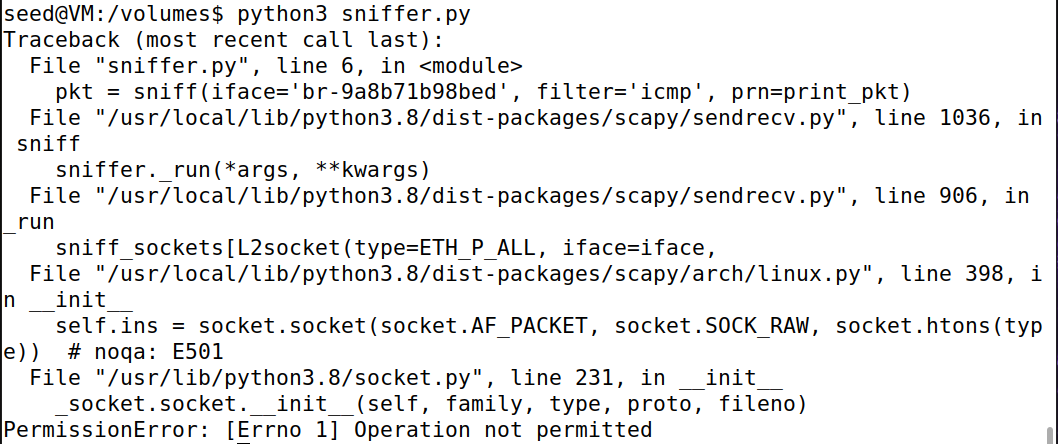
代码



Root权限运行程序后的输出



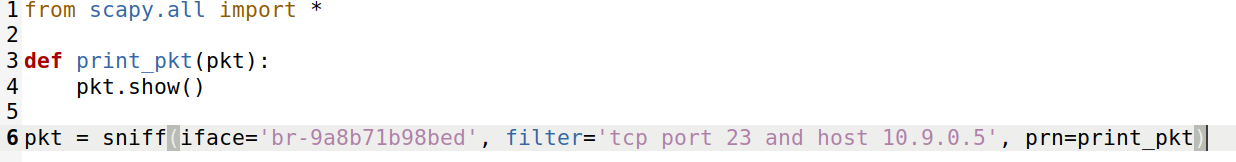
普通用户权限操作



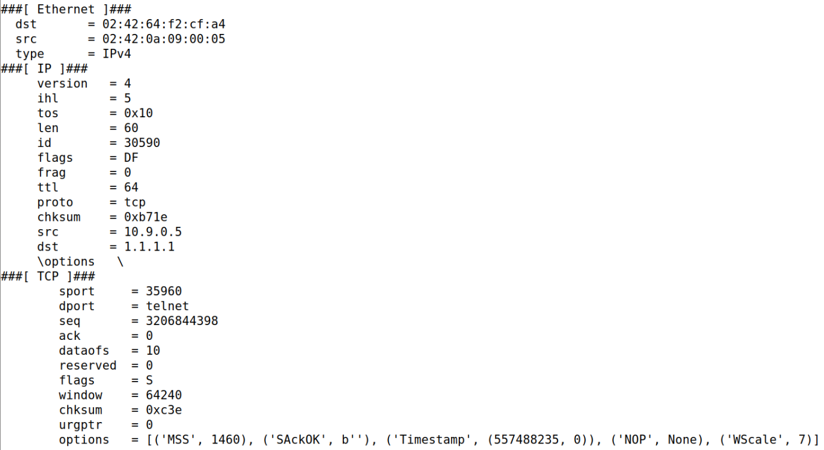
**1.1B**

ICMP情况下输出同1.1A

捕获从特定IP发出的，目的端口为23的TCP包

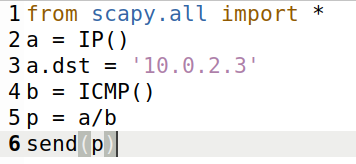


对任意一个特定的IP进行telnet监听，输出如下

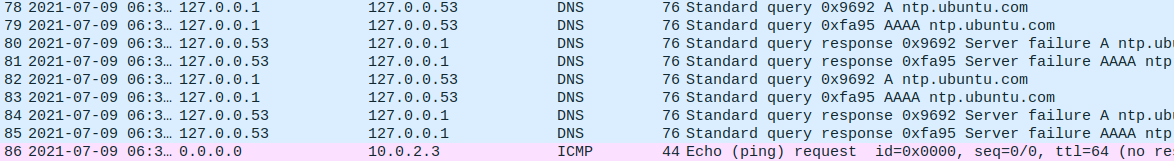


**1.2**

Spoofing.py代码

****

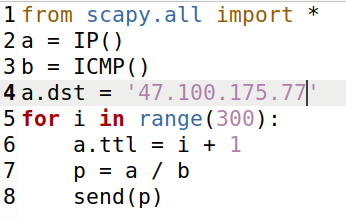
在攻击者的docker中运行 用wireshark监听



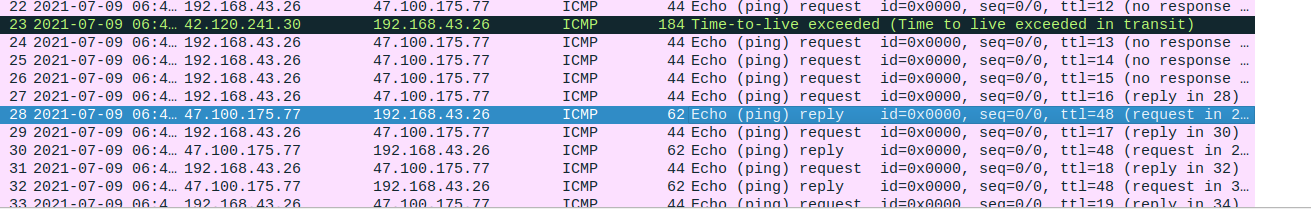
达成目的地址的伪装

**1.3**

ֵ用Scapy来估计虚拟机与目标地址间的跳数

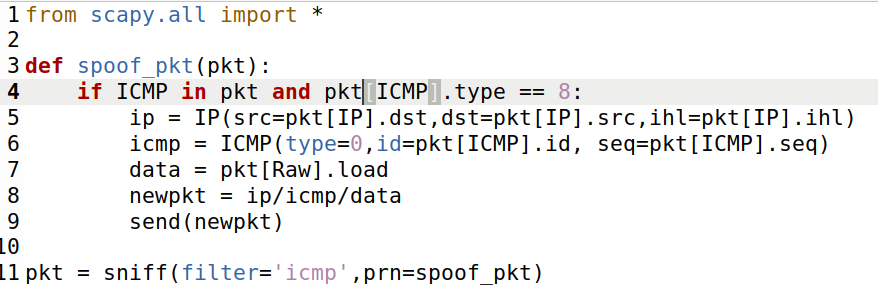


每次将ttl递增，用wireshark查看



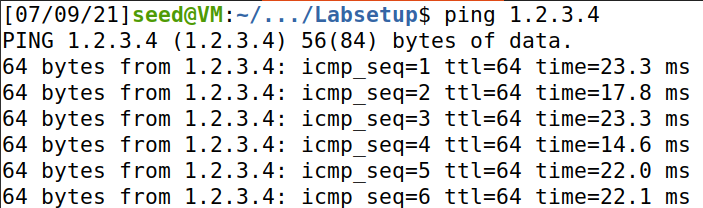
第一个Echo的Reply出现在ttl为16的时候，为此跳数约为16

**1.4**

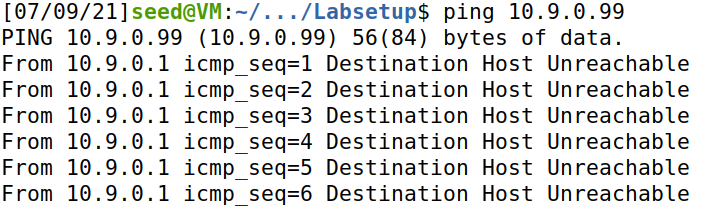


通过捕获ICMP报文，将其原宿地址对调，并设置ICMP类型为Reply，再发出

宿主机中ping1.2.3.4（不存在的IP）



Ping10.9.0.99



Ping8.8.8.8

