**第一次实验**

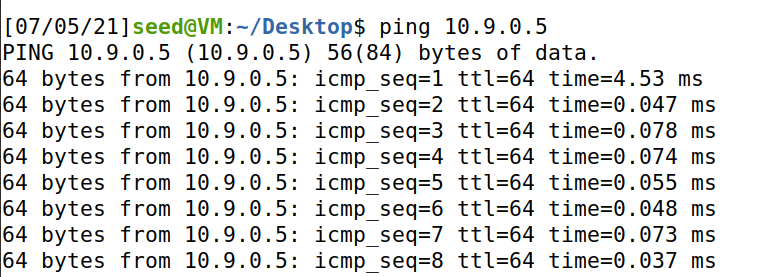
57118122 李泽厚

1.1 (a)

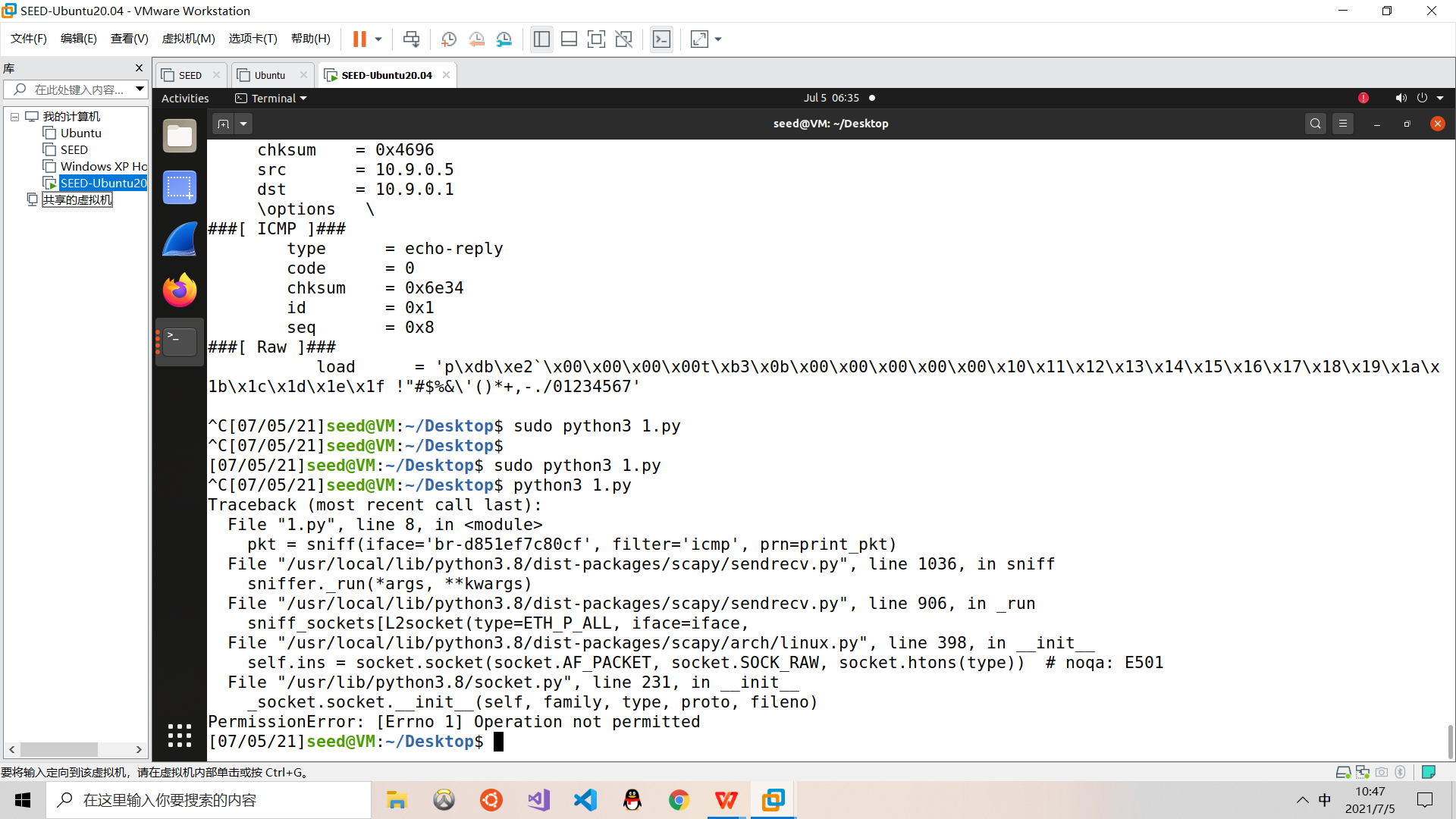
首先，以使用sudo，以root权限运行题中所给出的脚本（将网卡号改成自己的）：

IMG_256

可以得到如下结果：



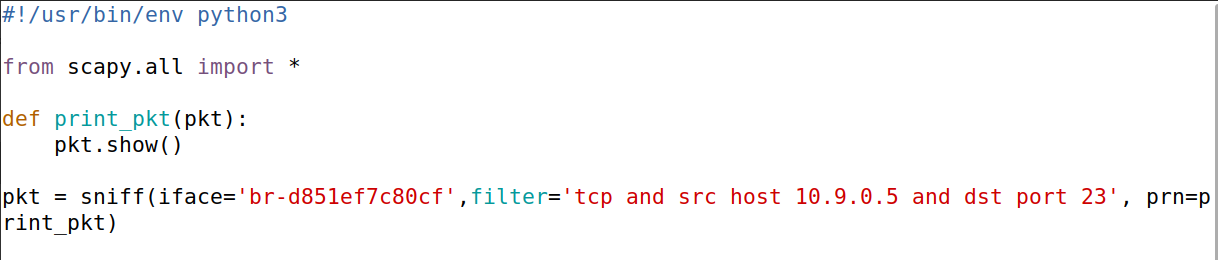
当不使用sudo运行脚本时，显示操作不被允许，根据报错可以看到这是因为ptk函数的执行需要root的权限。



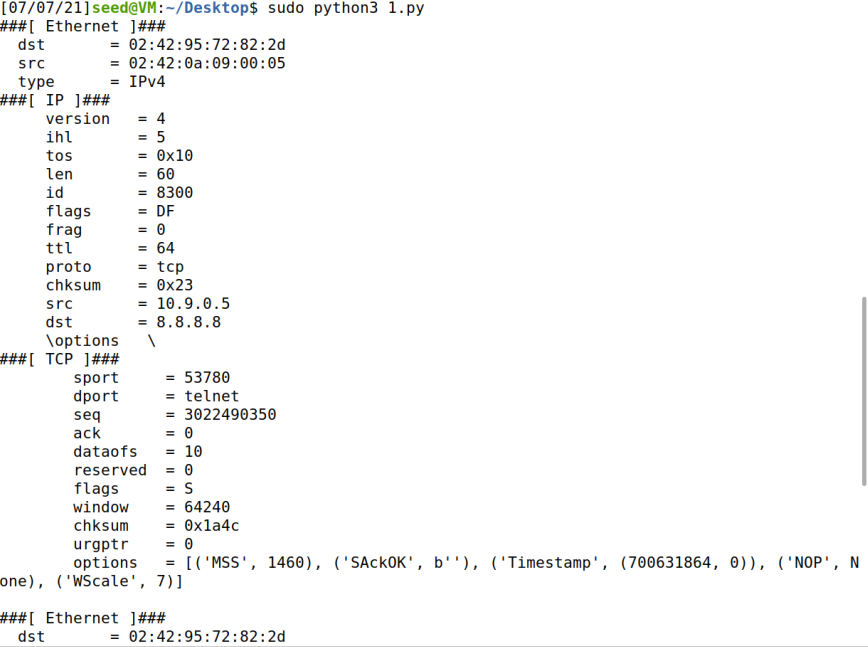
* 1. （b）

1）即在1.1(a)中的操作，这里不再重复演示；

2）执行如下脚本：

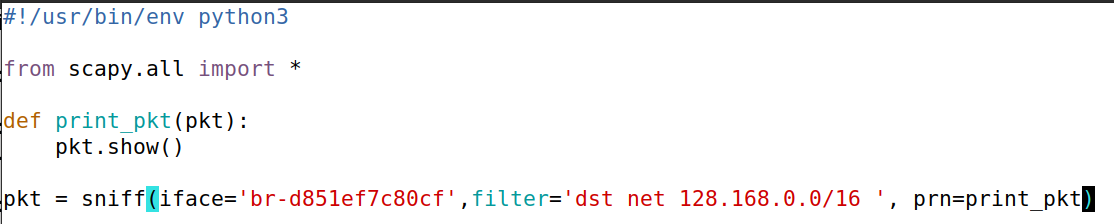


然后进入host container，执行命令 telnet 8.8.8.8，sniff脚本会得到如下结果：

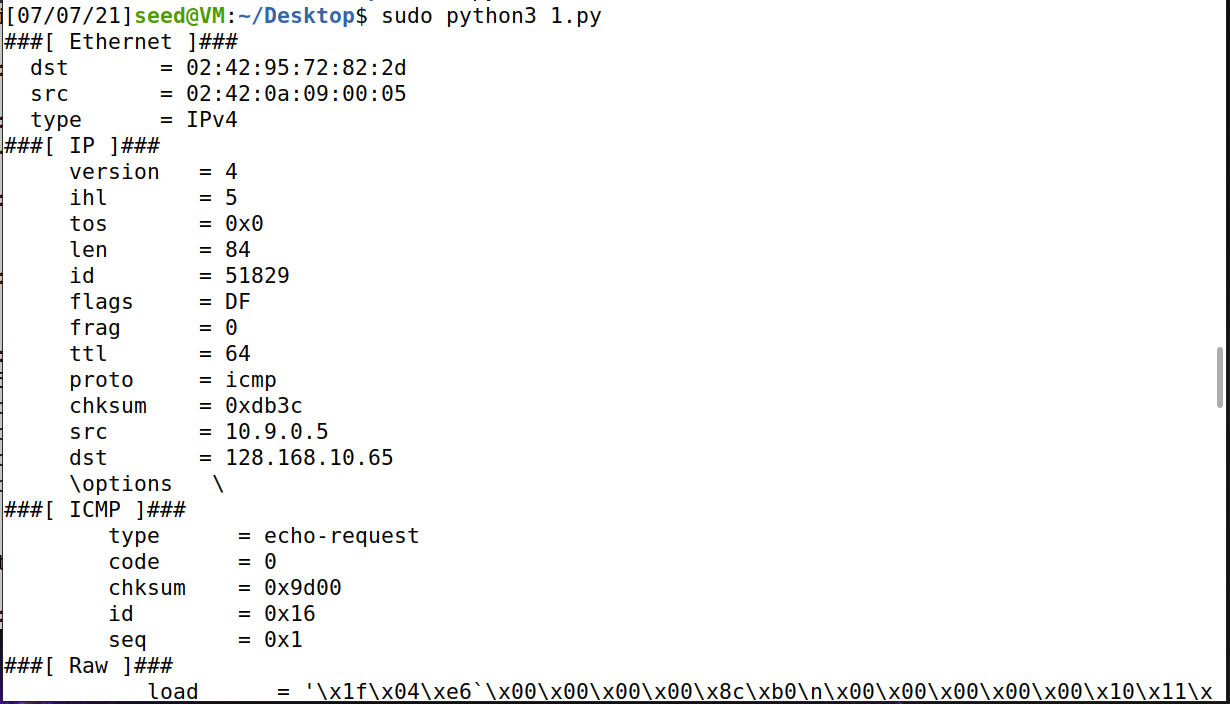


可见，嗅探到了TCP报文。

1. 执行如下脚本（设定目的网络为128.168.0.0/16）：

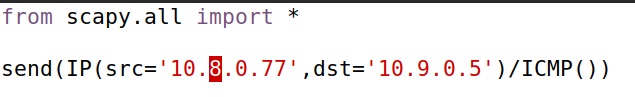


然后进去host container，执行 ping 128.168.10.65 ，得到如下结果：



如图，已经成功嗅探到。

执行如下脚本：

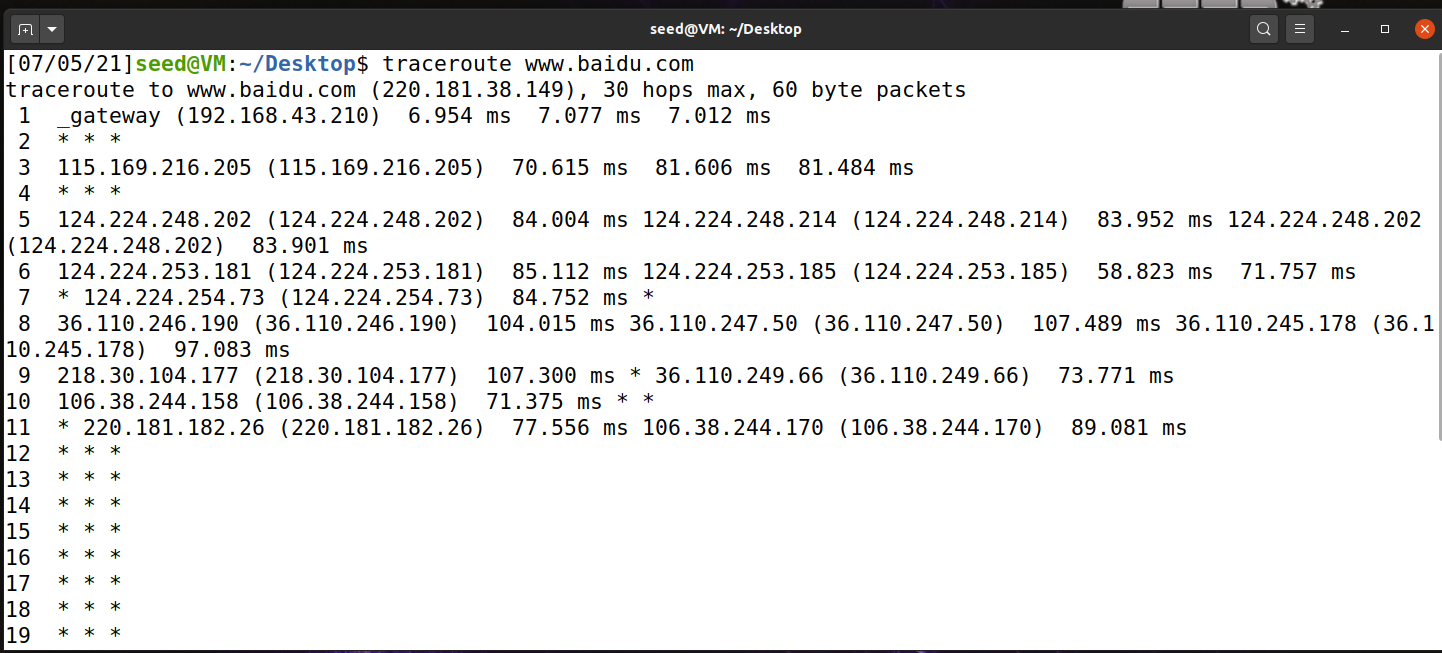


打开wireshark，监听，欺骗成功：

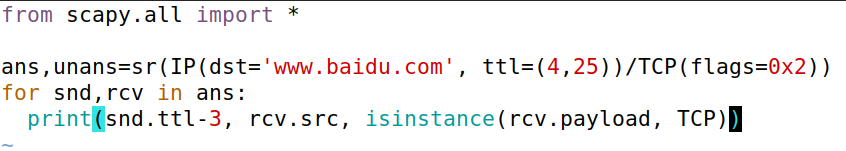
IMG_256

1.3

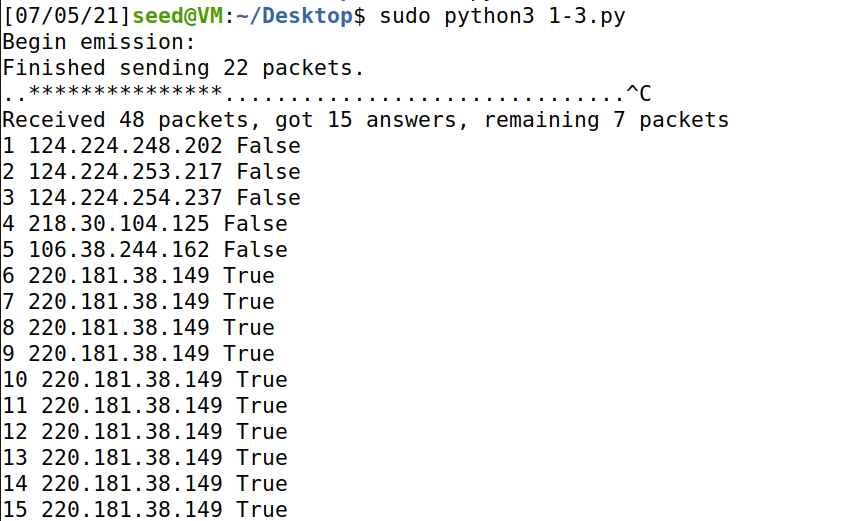
我们先在控制台上 对百度进行traceroute：



然后运行如下脚本：

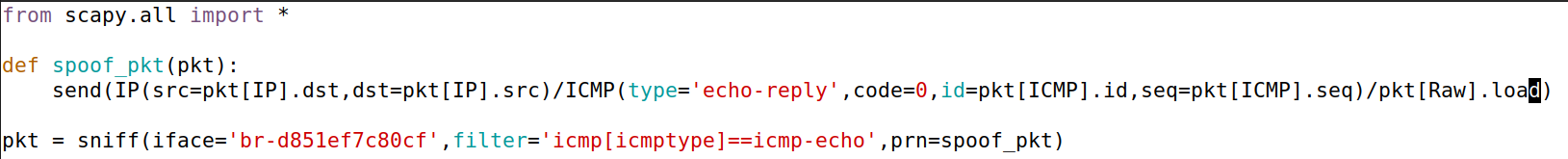


得到如下结果（和刚刚在控制台执行traceroute的结果是一致的）：

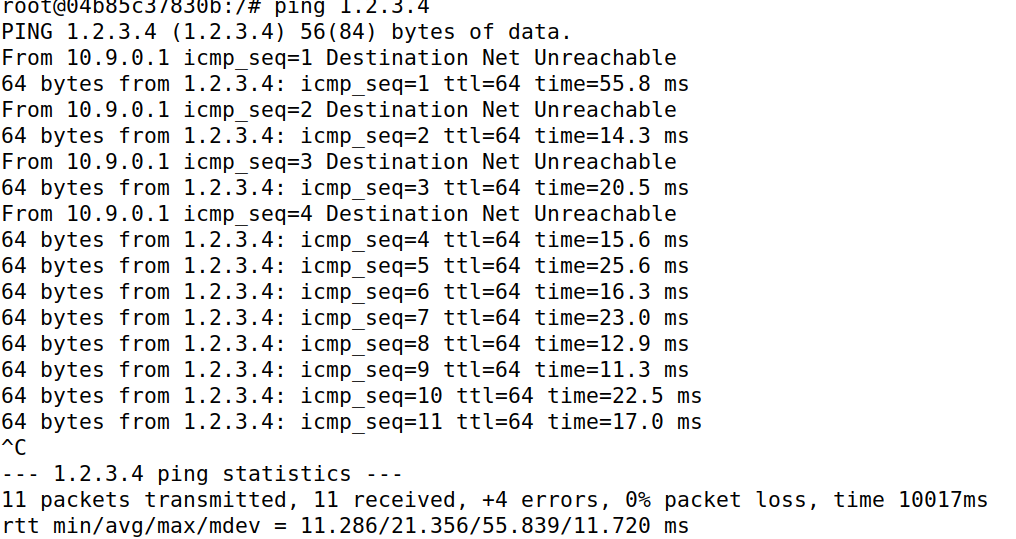


1.4

运行如下脚本：



然后进入host，在host的终端上执行 ping 1.2.3.4 的操作（1.2.3.4是一个不存在的地址），可以发现，一共成功了11次



这时我们看脚本运行的终端，发现正好进行了11次发包。

