**Lab1-report**

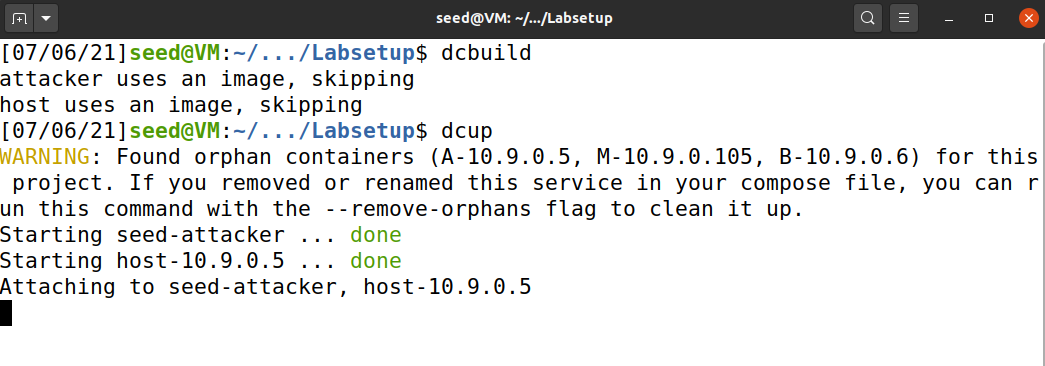
57118239 张鹏

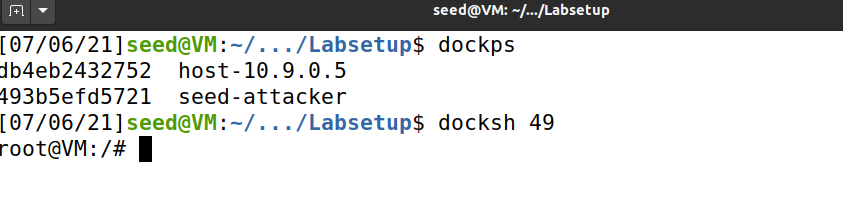
task1：

task1.1A：

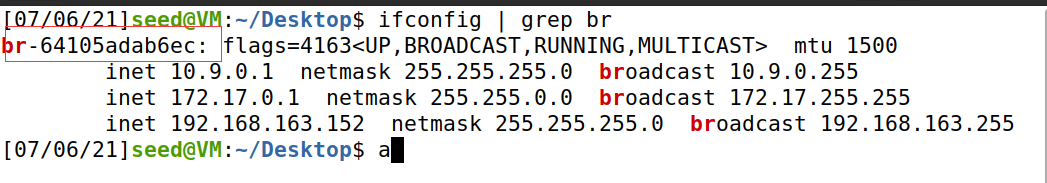
本次实验通过python中的scapy模块来实现报文的监听和伪造。

首先通过docker登录attacker容器

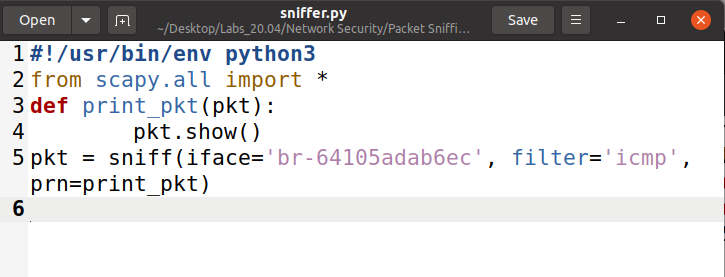




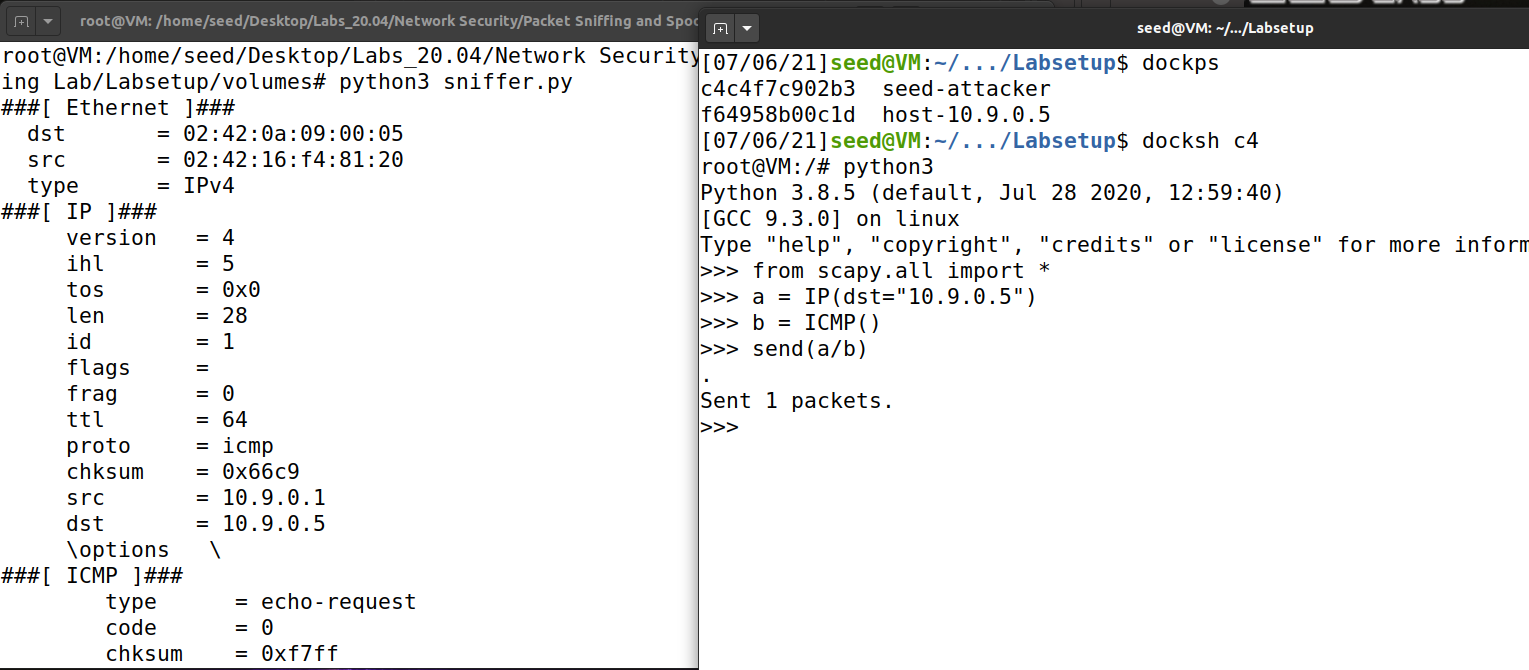
通过ifconfig确定需要监听的接口



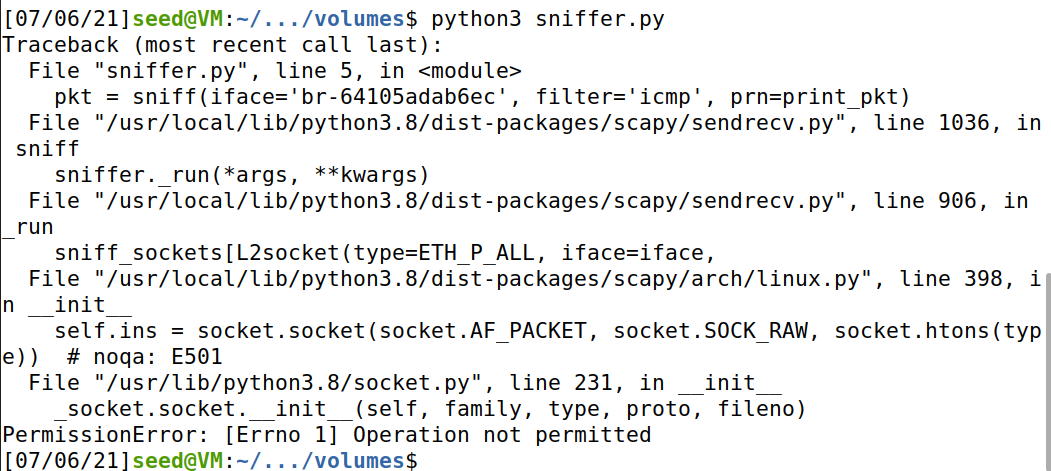
通过sniff来监听数据包，关键字参数prn的值是监听到符合filter规则的报文后所调用的函数，以下实验中定义了print\_pkt函数用于显示报文的内容



构造一个ICMP报文并发送，可以观察到被监听到了



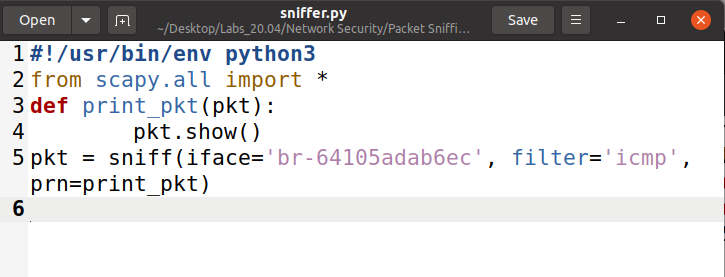
当没有root权限要运行此程序的时候，可以发现程序会报错，因为其权限不够。



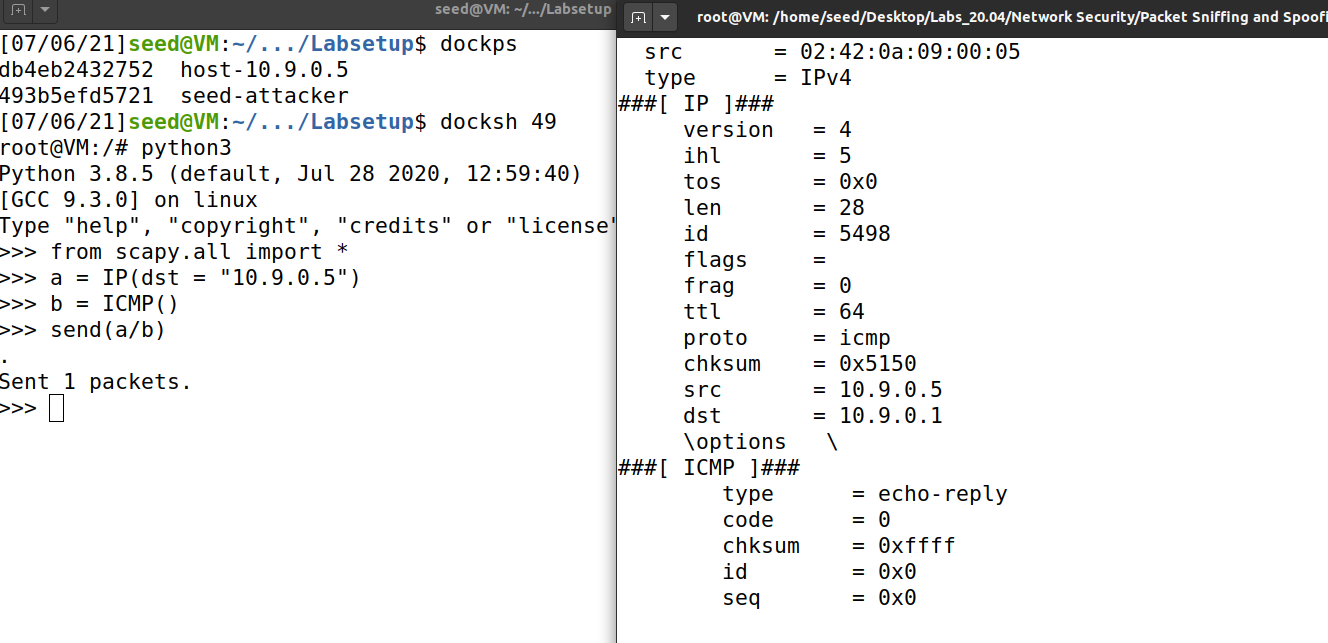
task1.1B：

此实验的要求是通过更改filter规则，来实现对不同报文的监听。

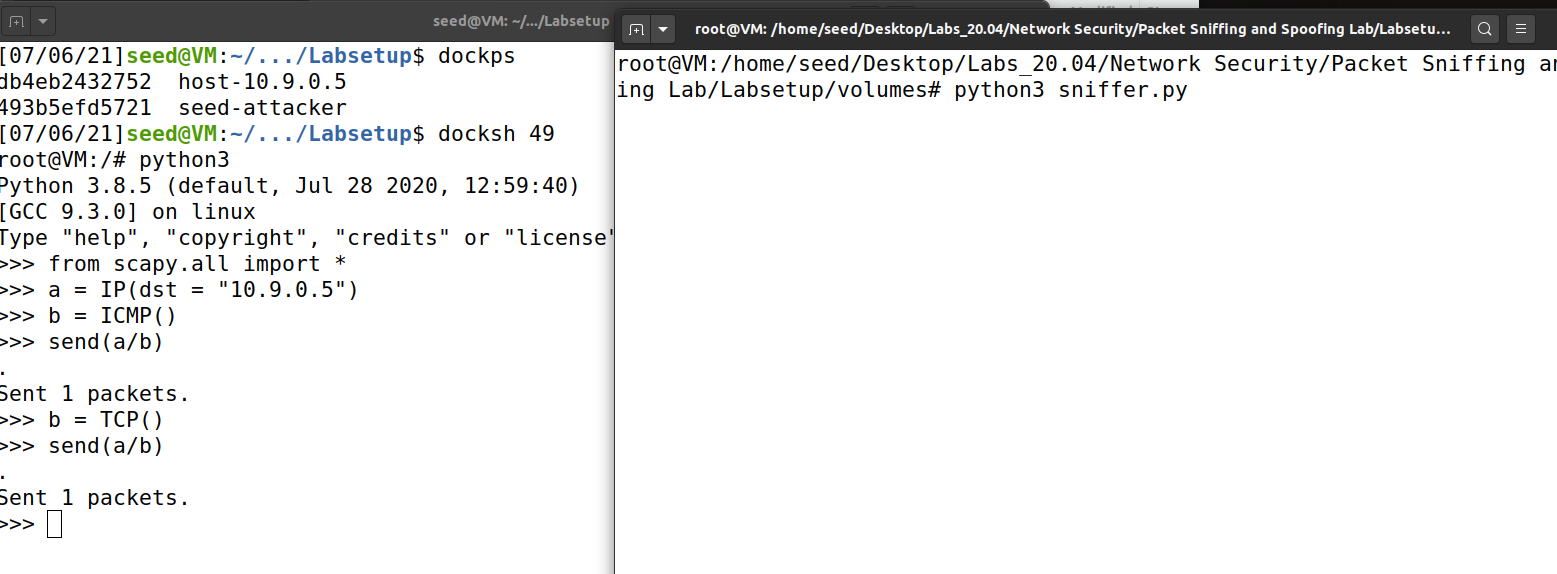
下图为第一个规则，只监听ICMP报文。



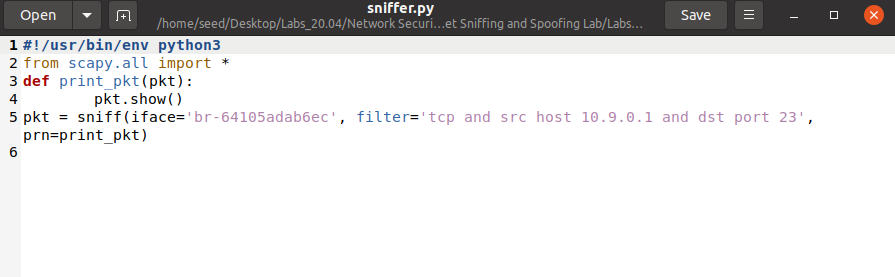
当发送ICMP报文时，可以发现监听到了。



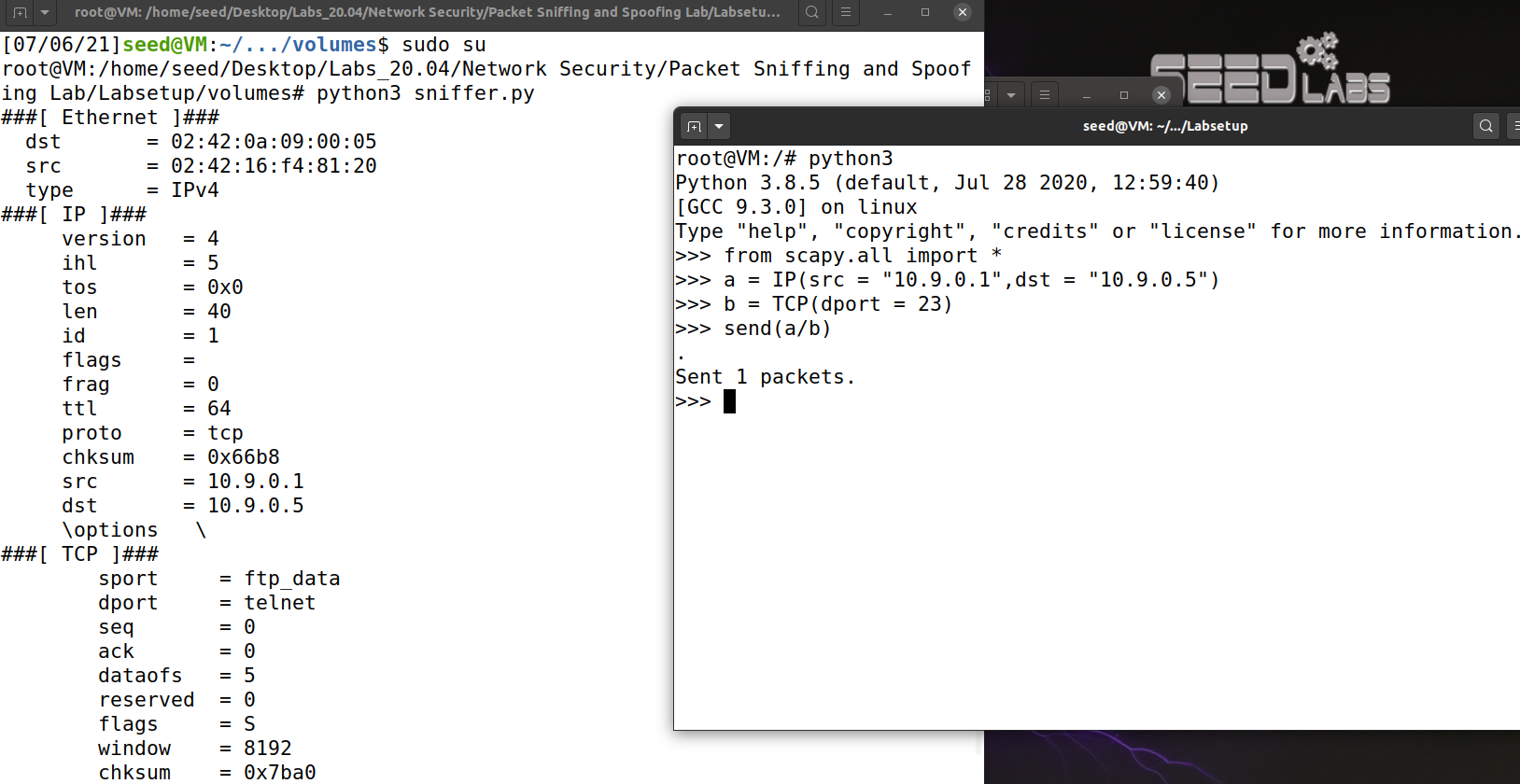
当发送的不是ICMP报文，可以发现监听程序并没有返回结果。



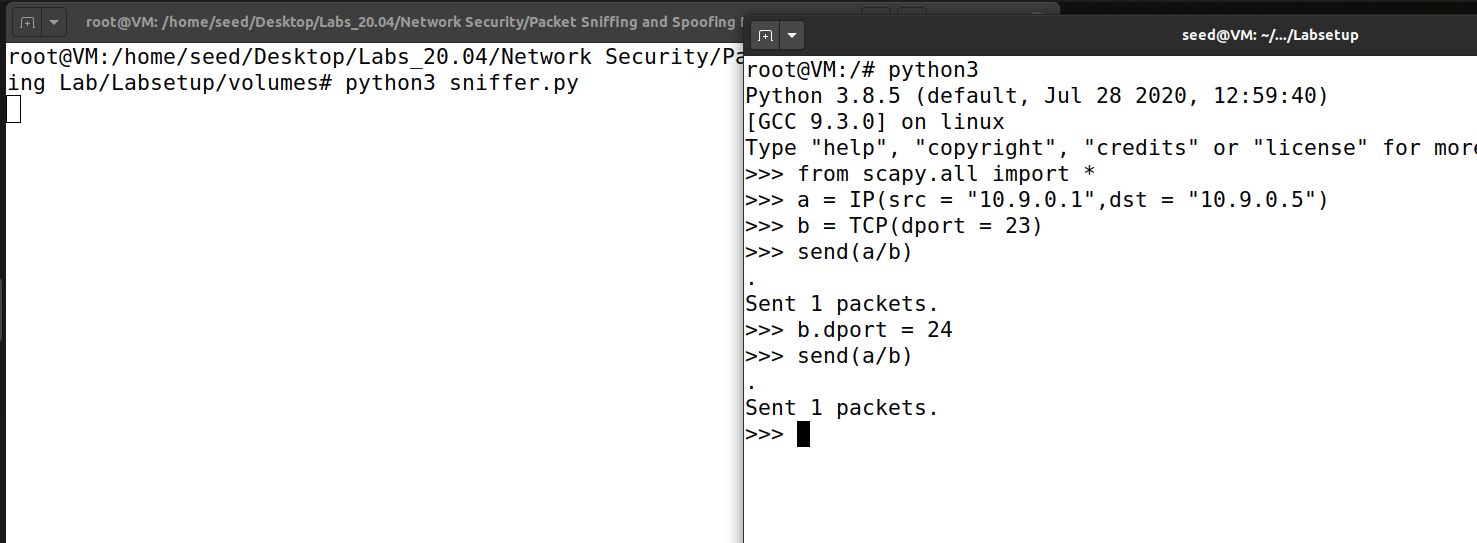
以下第二种是只监听tcp报文，且源地址是10.9.0.1和目的端口是23。



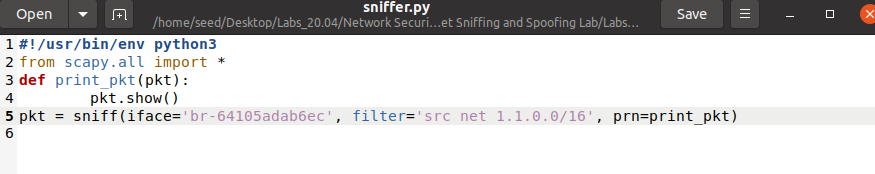
构造一个符合filter规则的报文，可以发现监听程序展示了其报文的详细信息。



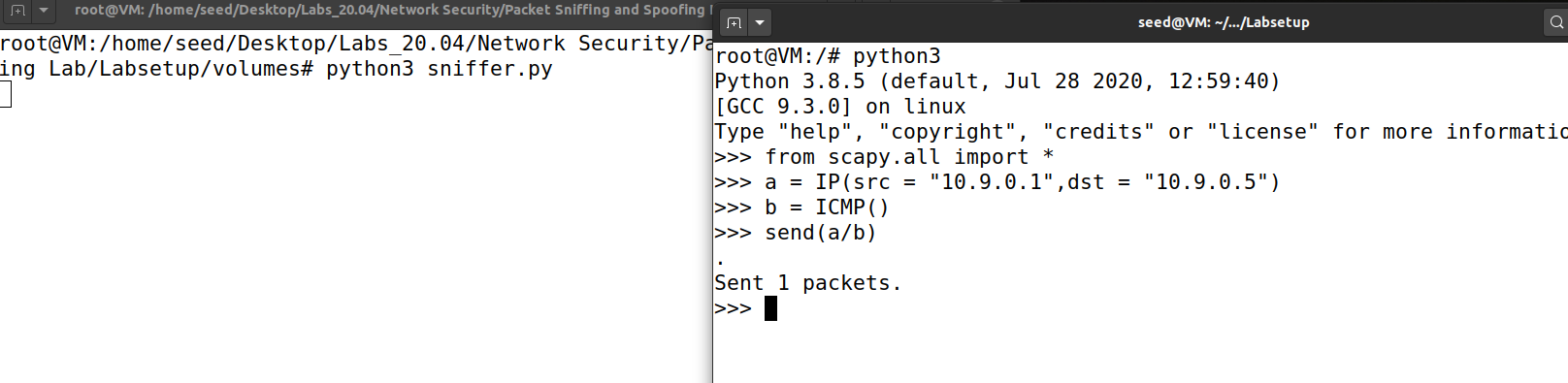
将刚刚构造的报文的目的端口号进行更改，在发送，可以发现监听程序没有输出。



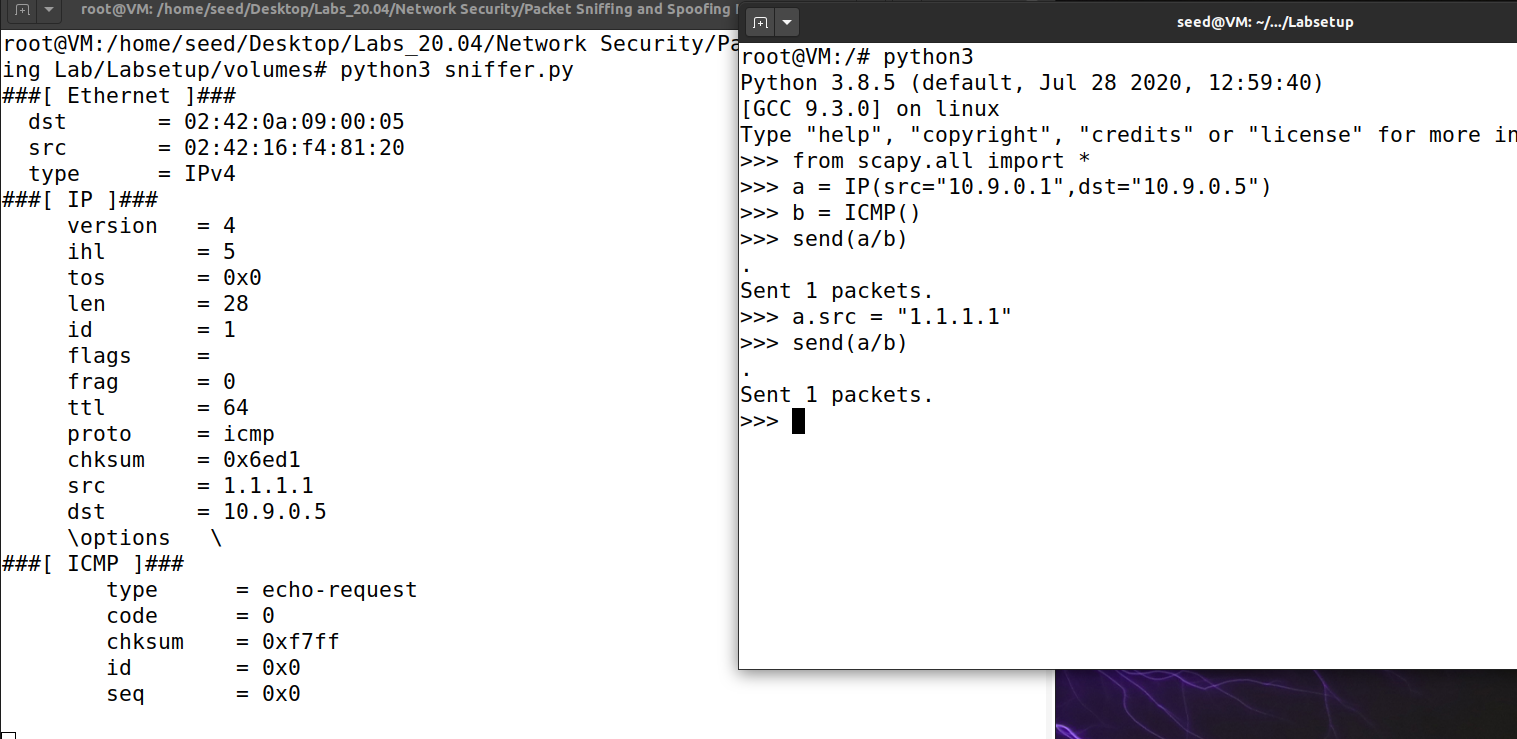
以下第三种是监听源地址网段是1.1.0.0/16的报文。



构造一个源地址不是此网段的报文可以发现监听程序没有输出。



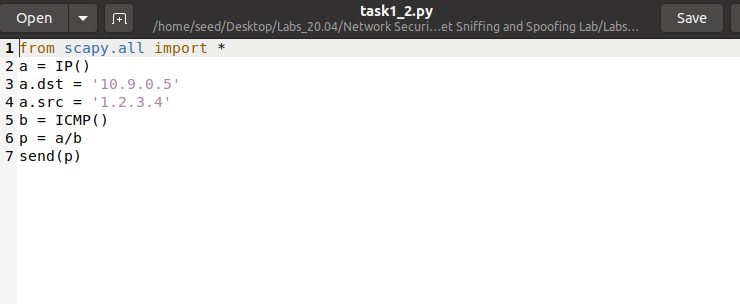
构造一个源地址是此网段的报文可以发现监听程序展示了该报文的相应信息。



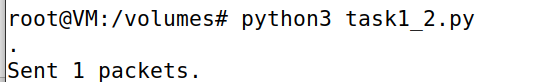
task2：

该实验的目的是根据其提供的代码进行一些必要的修改，可以构造任意源IP地址的ICMP报文。

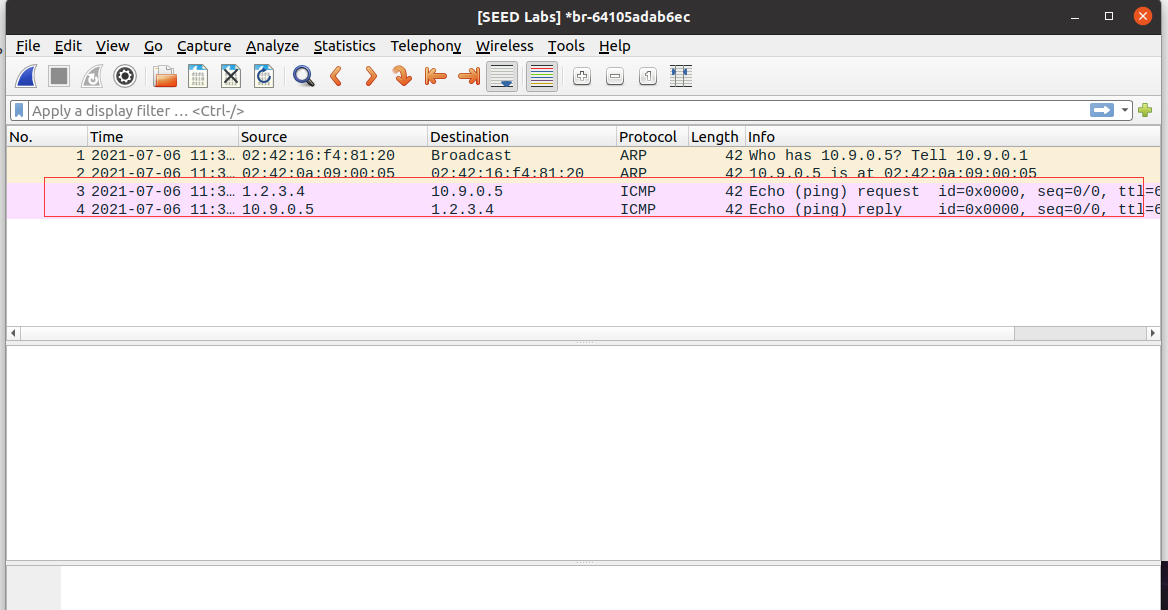
下面的实验中将宿地址设置为10.9.0.5，源地址随意设置成了1.2.3.4。

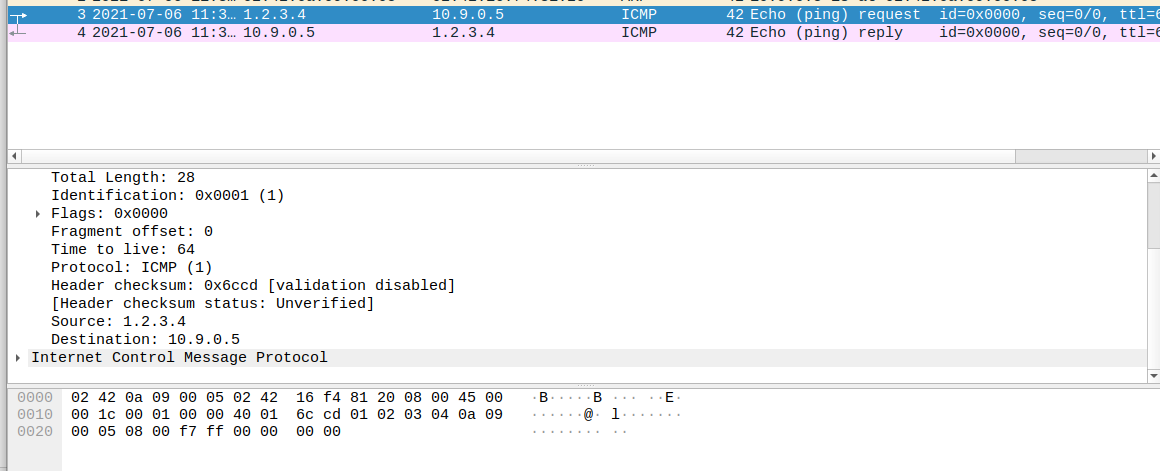


attacker的vm中运行该段代码，则其伪造了一个源地址是1.2.3.4，宿地址是10.9.0.5的ICMP报文。



通过wireshark软件，我们可以捕获到发送的ICMP报文及其内容。

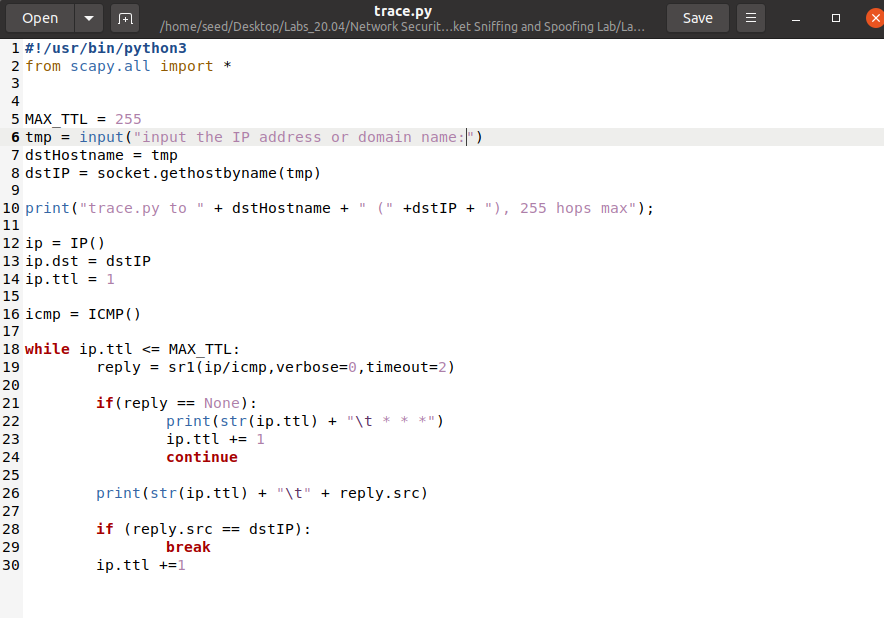




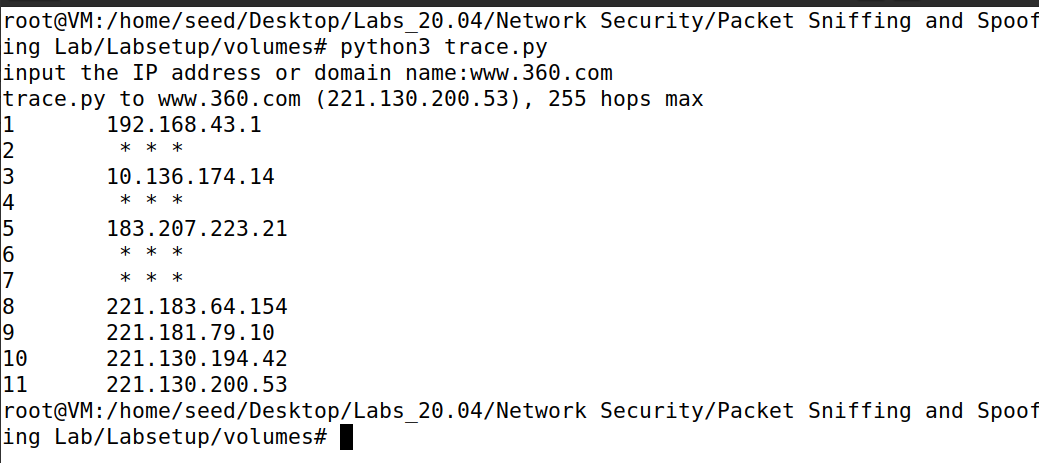
task1.3：

该实验的目的是让我们通过scapy实现traceroute的功能，原理是ttl在为0的时候会被路由器丢弃，同时返回一个ICMP error，通过将ttl从1开始不断递增，可以得知从该地址到目标地址所跳转的地址。

代码的核心思想：运行程序后由用户主动输入需要traceroute的IP或者domain name，一开始设置ttl为1，构造一个ICMP报文，然后通过观察响应报文，如果是源地址是否为目标地址来判断是否到达，未到达则对ttl进行自增，进入下一次判断。

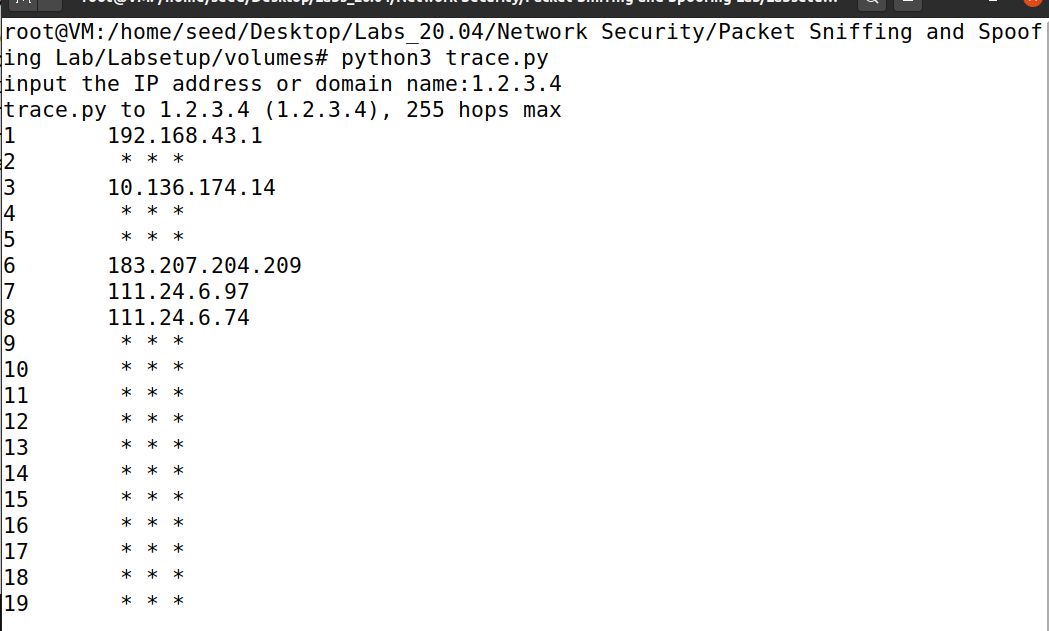


运行代码，对[www.360.com](http://www.360.com)进行traceroute，结果如下



可以得到结果，中间有几跳没有显示应该是对应主机的防火墙封掉了ICMP的信息。

对1.2.3.4进行traceroute，结果如下：



后续仍然没有结果，猜测可能该地址并不存在或者不可达。

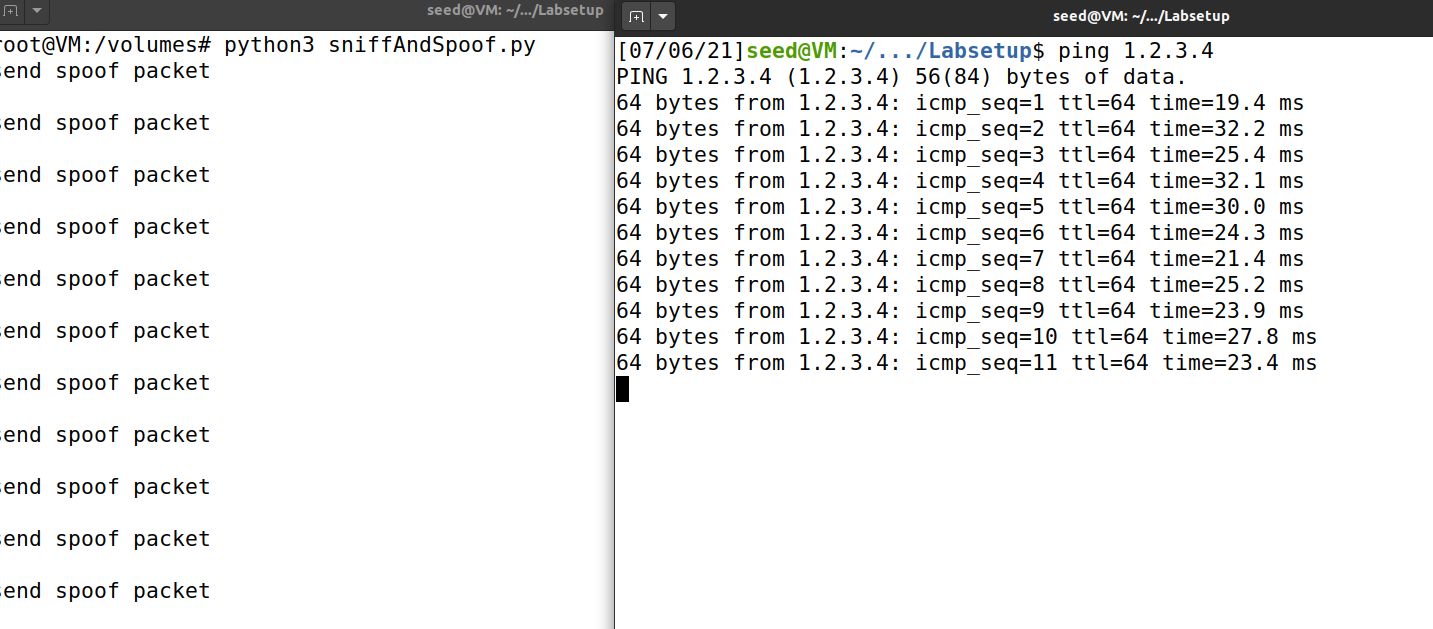
task1.4：

该实验的目的让我们通过监听ICMP请求报文，然后伪造ICMP的响应报文。

通过查阅ICMP报文的类型，可以知道实验中要求的echo request报文的type值是8，所以当监听的icmp报文的type不是8的时候可以直接结束。构造的ICMP报文为ICMP响应报文，type为0，id、seq、负载内容、长度与请求报文相同，源宿地址互换。这样就伪造好请求报文，发送即可。

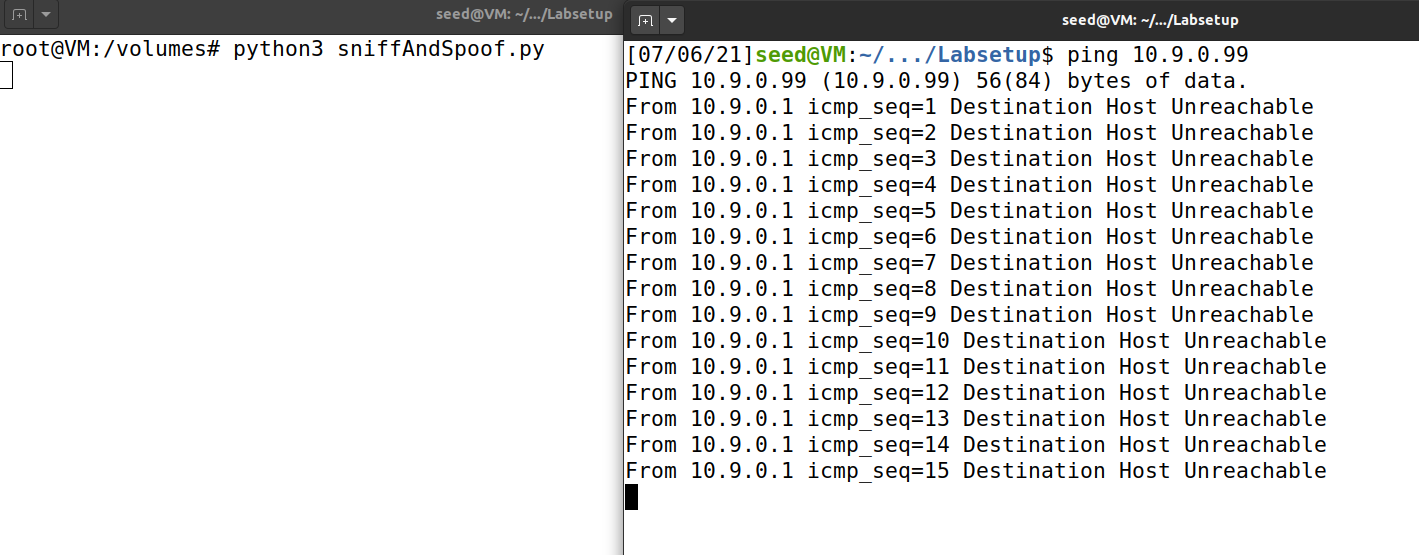


下图是ping 1.2.3.4（一个在互联上不存在的主机）



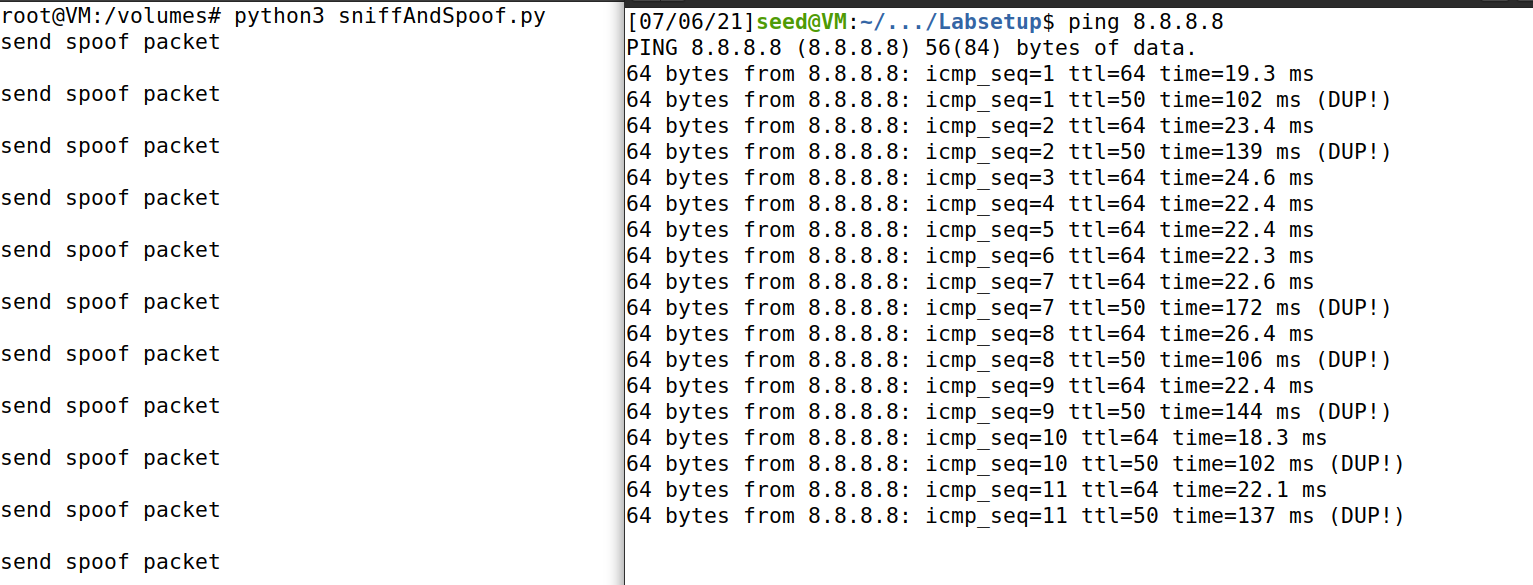
可以观察到伪造程序伪造了ICMP响应报文并发送给了ping该地址的主机，尽管该地址的主机并不存在。

下图是ping 10.9.0.99（一个在局域网内不存在的主机）



可以观察到因为所在的局域网内并不存在该主机，所以ping之后返回了目的主机不可达的信息。

下图是ping 8.8.8.8（一个在互联上存在的主机）



可以观察到ping该地址后伪造程序伪造了响应报文。

ping的报文应该需要经过attacker的代表的网关，所以到达互联网的数据报文会被程序监听，然后伪造响应报文，而发往内网的报文不需要发往网关，所以不会被监听并伪造。

总结：

本次实验介绍了使用python及scapy进行数据报文的监听和伪造，数据报文的监听利用BPF进行过滤是一个非常重要且常用的技术，而伪造数据报文则是攻击者经常做的事情，通过对这次的实验，对数据报文的监听和伪造有了更深的理解，对于从事网络安全方面以及防止被攻击者进行欺骗，这些概念尤其重要。