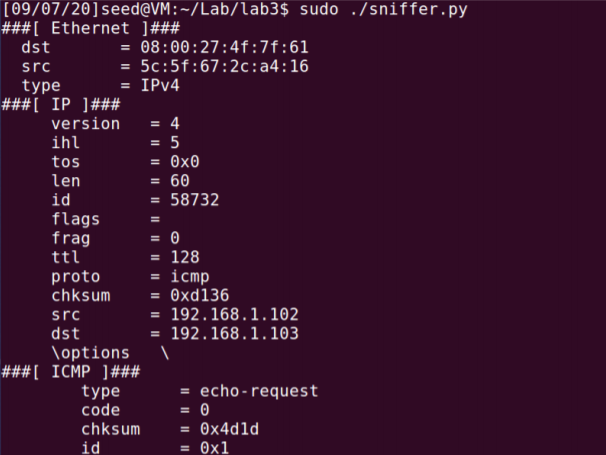
Packet Sniffing and Spoofing Lab

Task set 1

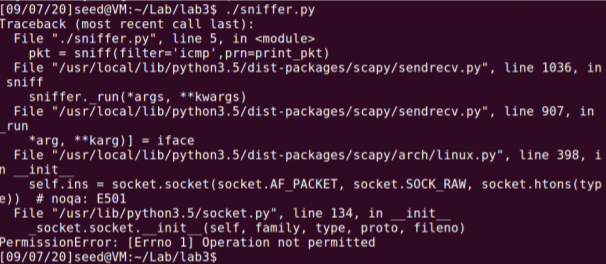
**1.1A**

sudo 下执行：

（此处虚拟机网络设置为桥接网卡，桥接至宿主机无线网卡）



无 sudo：



最后一行显示操作不被允许，权限不足。

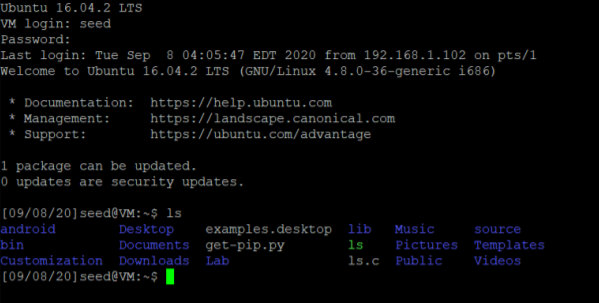
**1.1B**

只抓取 ICMP 包的程序就是上述 1.1A 的示例程序

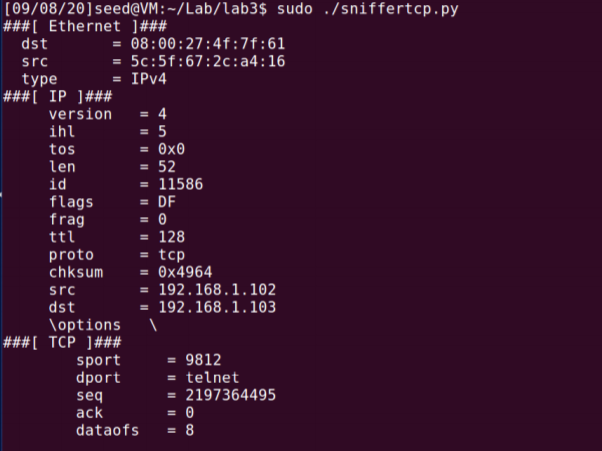
抓取特定 ip 源地址发出的，目的端口是 23 的包：



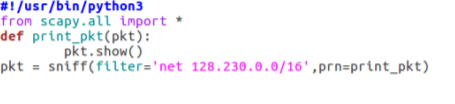
其中 192.168.1.102 是宿主机 ip 23 端口是 Talnet 服务，在虚拟机内运行 sniffer 程序，我们在宿主机上使用 putty 尝试使用 虚拟机的 talnet 服务：



虚拟机：

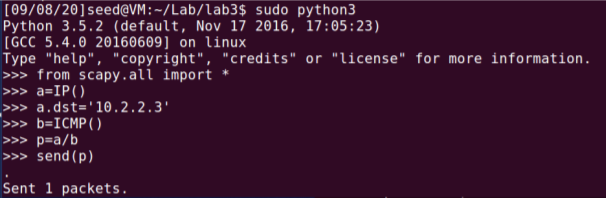


如果使用 22 端口的 ssh 服务，则虚拟机内无输出，说明只抓取目的端口为 23 的包。 抓取属于某子网的数据包程序如下：



**Task1.2**

我们新开一个终端，运行 task1.1 中的 icmp 包的捕获程序，以观察我们的伪造结果 伪造和发送过程：

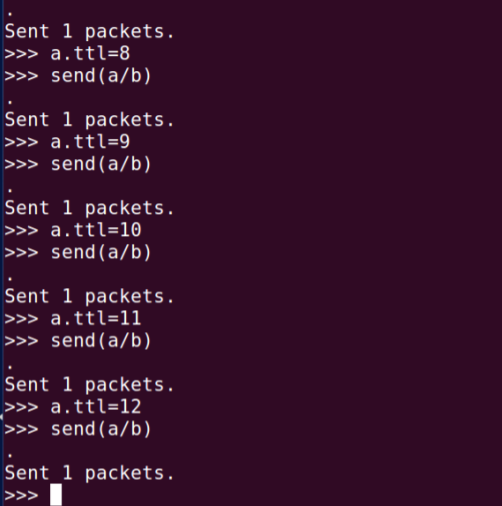


捕获情况：

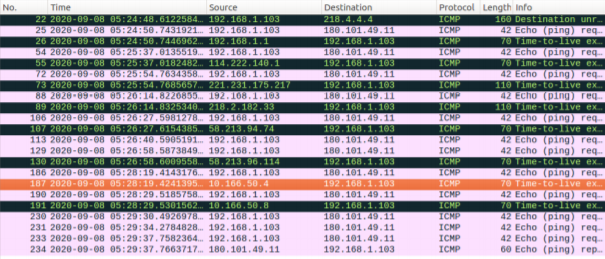


**Task1.3**

我们 ping 向 [www.baidu.com](http://www.baidu.com)

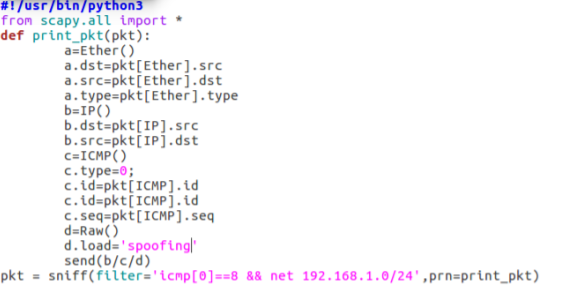


共 12 次 Wireshark 抓取结果：



**1.4**

程序如下：



**1.4. Sniffing and-then Spoofing**

**程序如下：**

from scapy.all import \*

def print\_pkt(pkt):

a = IP()

a.src = pkt[IP].dst

a.dst = pkt[IP].src

b = ICMP()

b.type ="echo-reply"

b.code =0

b.id = pkt[ICMP].id

b.seq = pkt[ICMP].seq

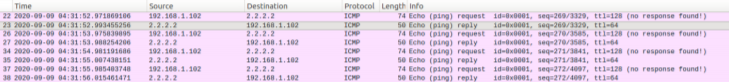
p = a/b

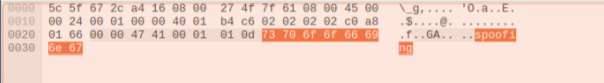
send(p)

pkt = sniff(filter='icmp[icmptype] == icmp-echo', prn=print\_pkt)

网络地址如下，宿主机 IP 为 192.168.1.102/24（无线网卡），虚拟机网卡为桥接网卡，桥接 宿主机无线网卡，IP 为 192.168.1.104/24 宿主机上尝试 ping 2.2.2.2：

虚拟机内：





可以看到我们伪造的包起了效果 关于抓包列表里的（no response found!），如果我们将回复包的负载设置为和请求包一样， 那么这个提示信息就没有了。