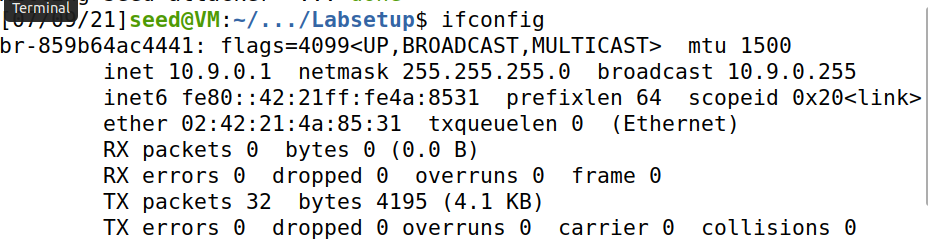
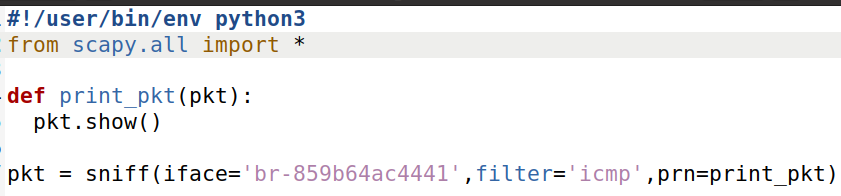
**Lab 1. Report**

**1.1A**

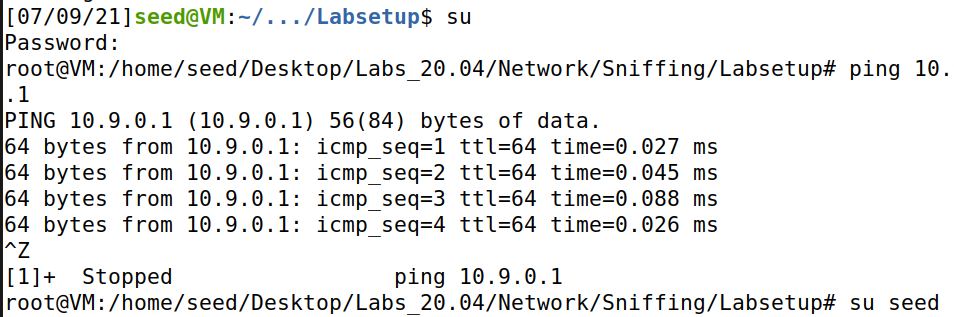
①获取HASH值和对应IP：



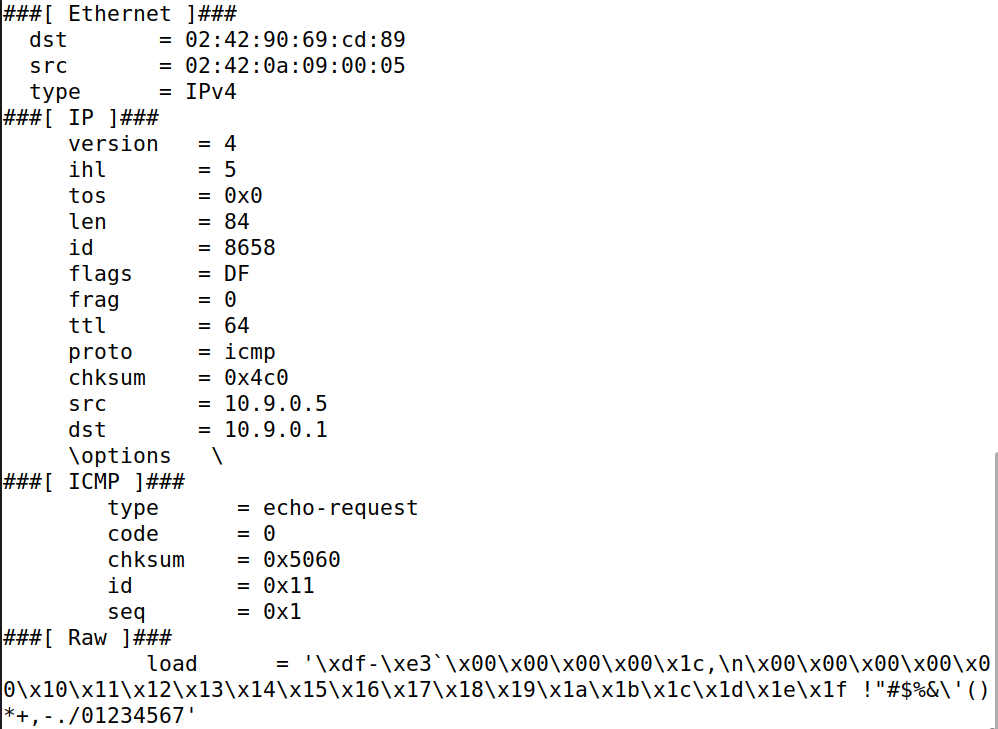
②编写sniff.py



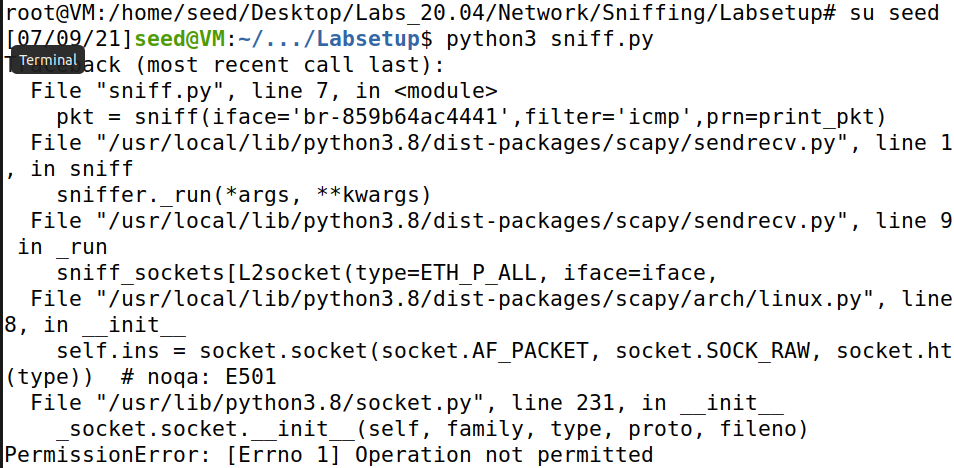
③ping主机地址



④在权限情况下嗅探icmp报文：

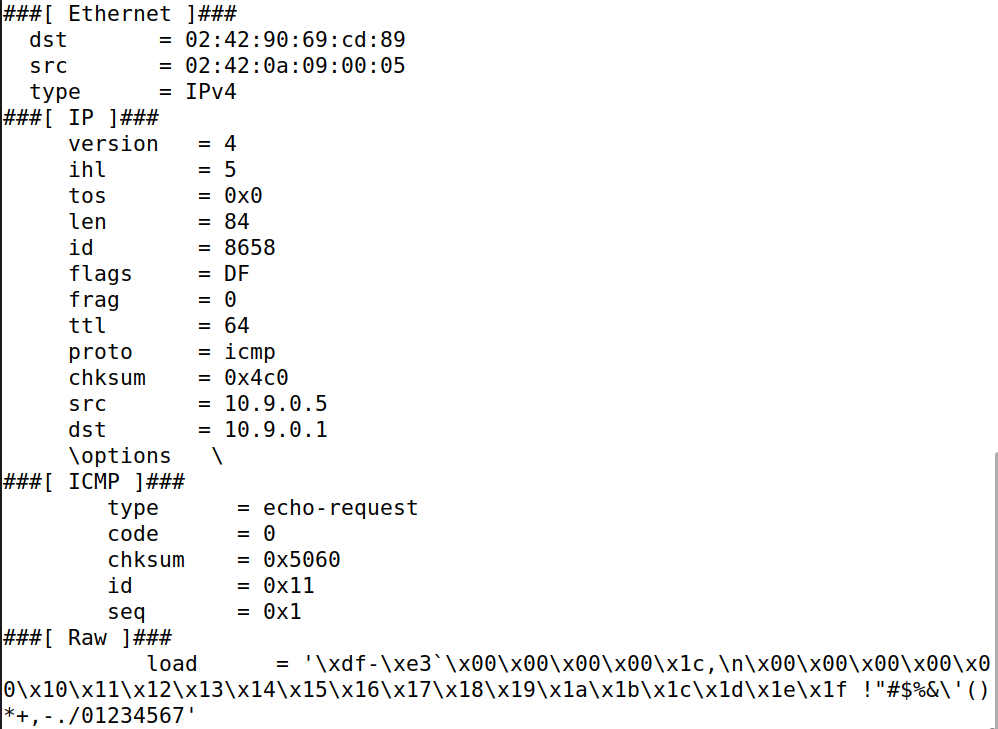


⑤若无权限嗅探：

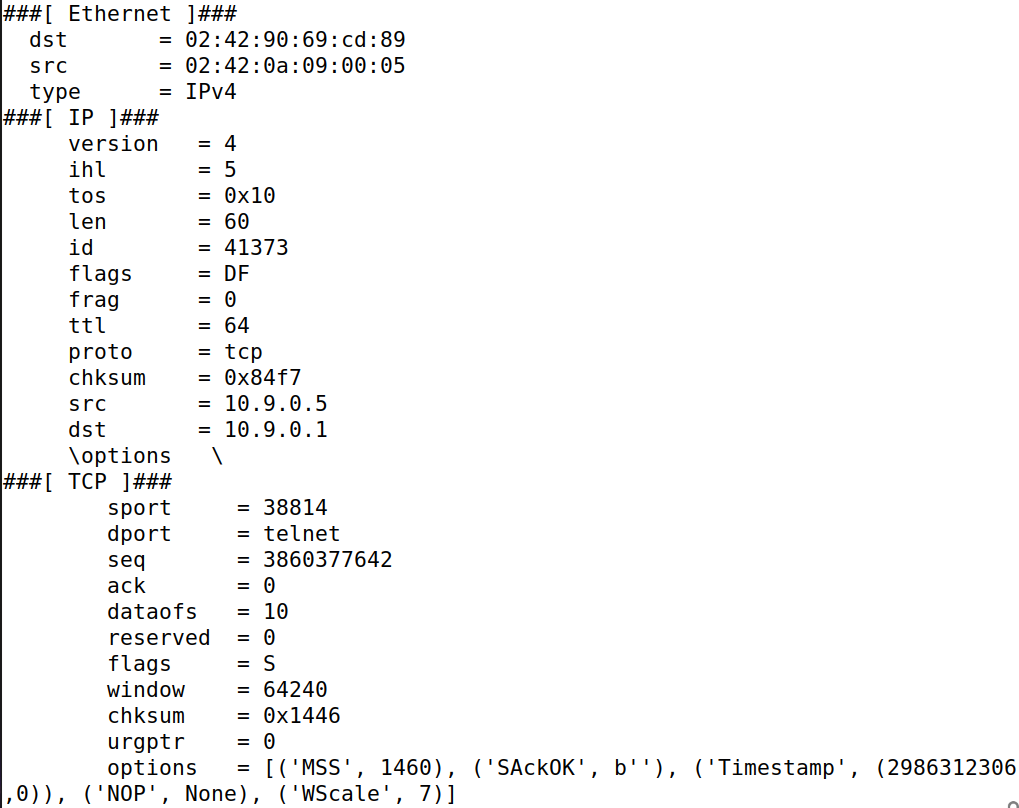
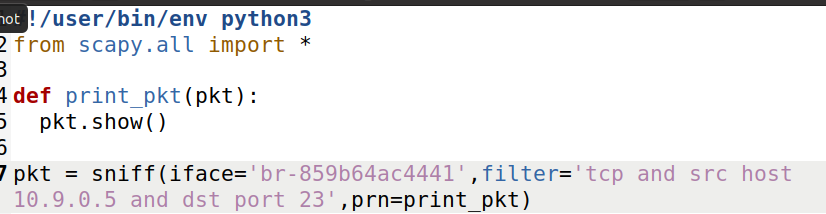


**1.1B**

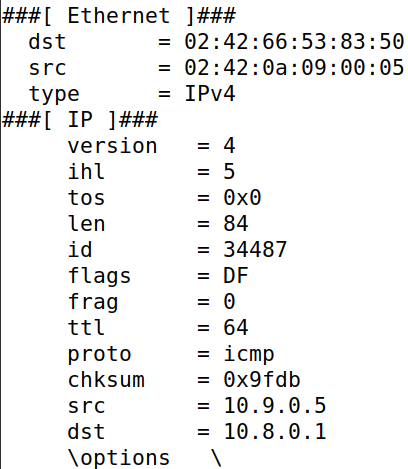
①fliter=’icmp’即为1.1A的icmp报文嗅探



②将A中的filter改为filter=’src host 10.9.0.5 and tcp dst port 23’，进行嗅探

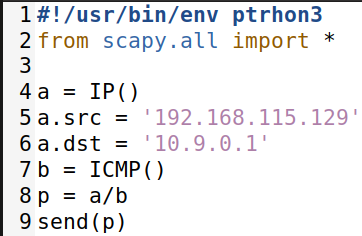


②将fliter改成虚拟机dst net 10.8.0.0/16



**1.2**

①编写test.py，以自己的ip为源ip



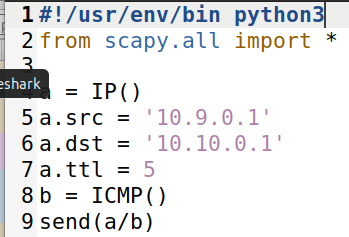
②通过wireshark观察结果：



成功伪造icmp报文

**1.3**

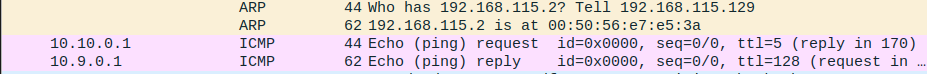
①编写traceroute.py：



②当ttl为4时，通过wireshark观察，no request



③将ttl改为5

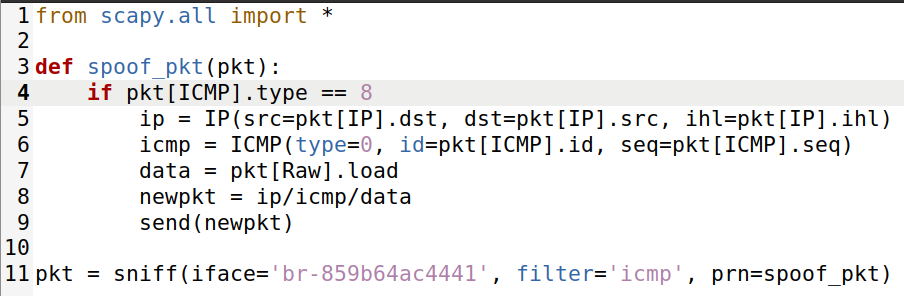


出现request

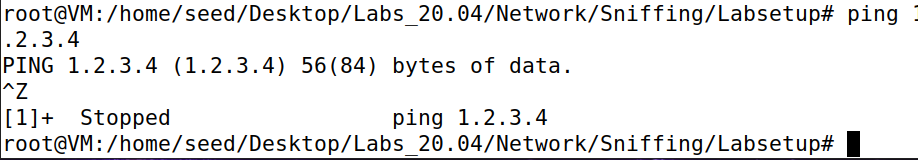
则从10.9.0.1到10.8.0.1总共有5个路由

**1.4**

①编写test.py：

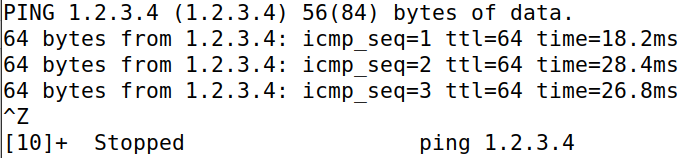


②若未进行ip欺骗，ping1.2.3.4时



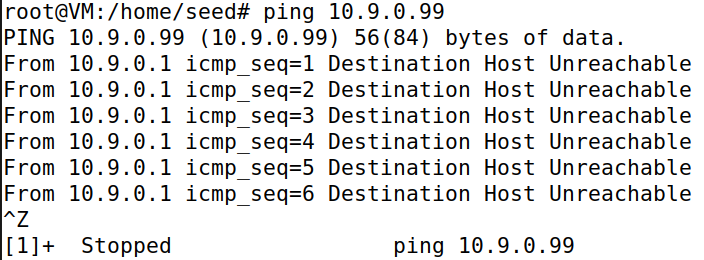
无法ping通，因为无法ping通不存在的主机

③进行ip欺骗时



可以ping通

④ping 10.9.0.99，由于该ip在LAN上不可达，所以无法ping通且会出现提示。



⑤ping 8.8.8.8：

