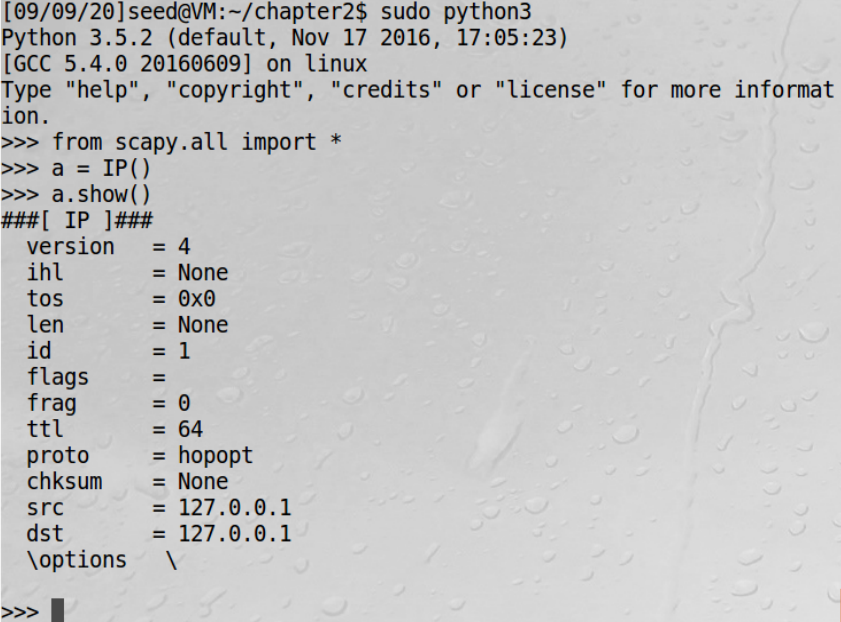
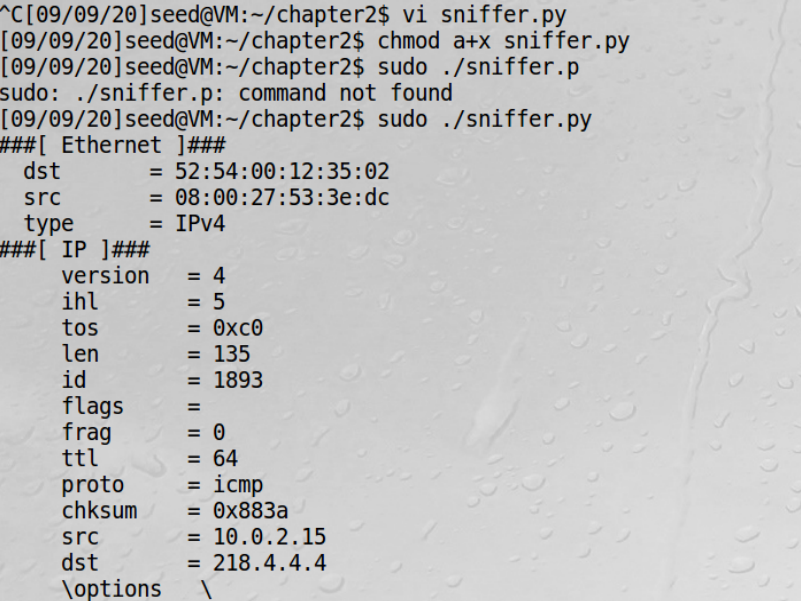
**Lab1 Packet Sniffing and Spoofing Lab**

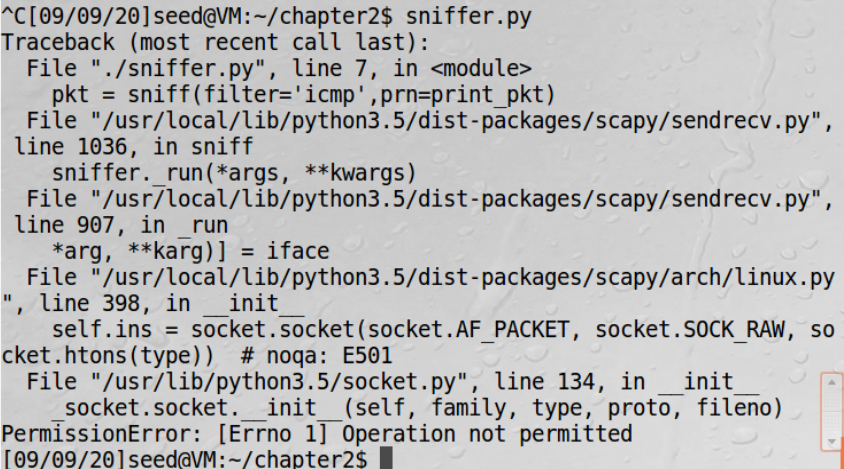
**Lab Task Set1: Using Tools to Sniff and Spoof Packets**





**Task1.1: Sniffing Packets**



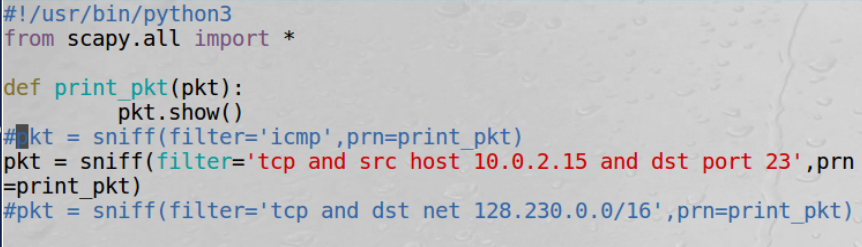


**Task 1.1B**

a).Capture only the ICMP packet



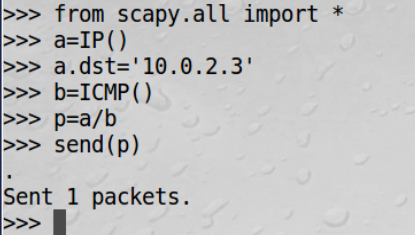
b).Capture any TCP packet that comes from a particular IP and with a destination port number 23.

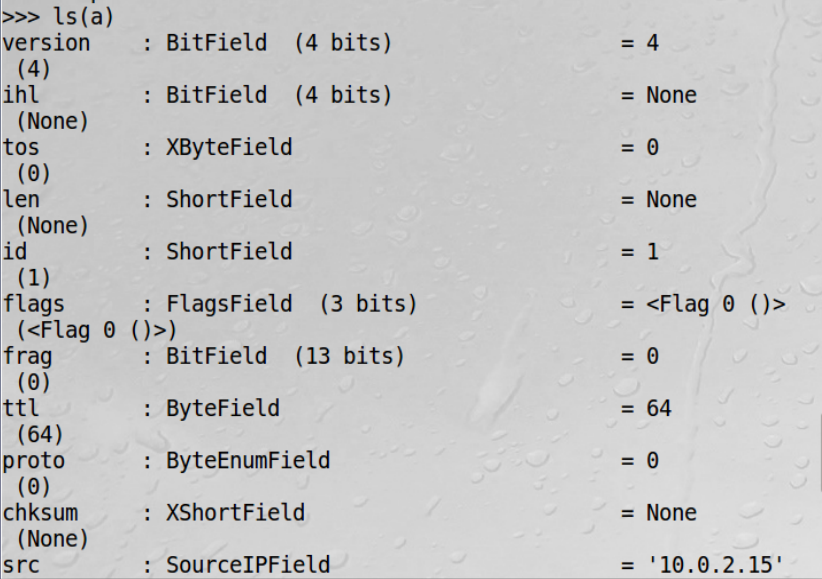


Capture packets comes from or to go to a particular subnet. You can pick any subnet, such as 128.230.0.0/16; you should not pick the subnet that your VM is attached to



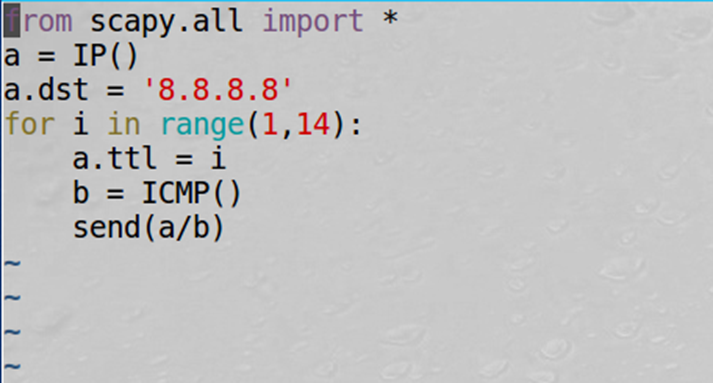
**2.2 Task1.2: Spoofing ICMP Packets**



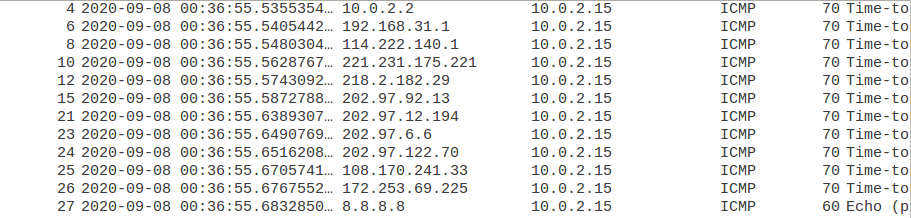


**2.3 Task1.3: Traceroute**

发送程序



抓包结果



**Lab2 ARP Cache Poisoning Attack Lab**

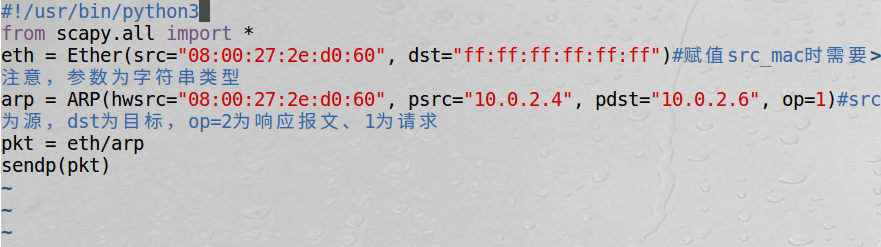
**A**

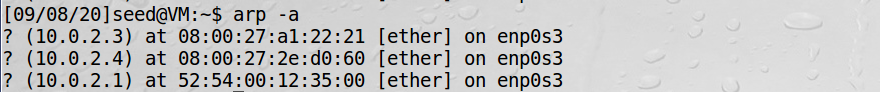
IP地址与MAC地址对应关系

M 10.0.2.5 08:00:27:2e:d0:60

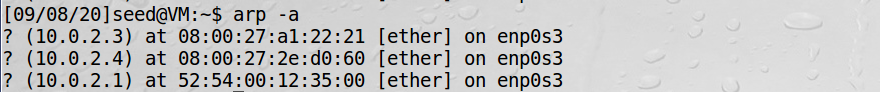
A 10.0.2.6 08:00:27:2a:05:36

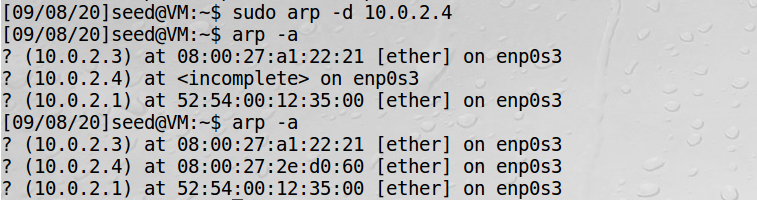
B 10.0.2.4 08:00:27:a2:51:7c



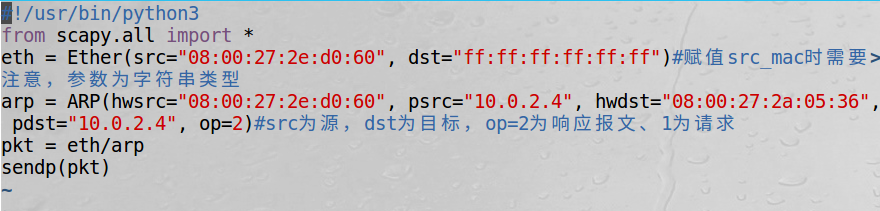


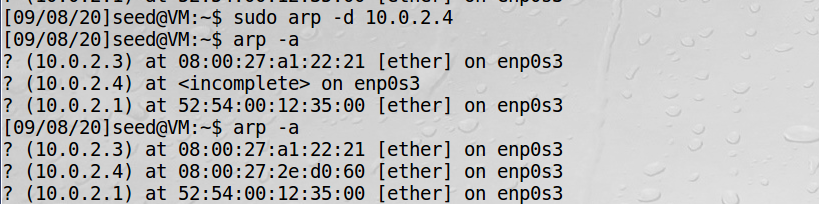
**B**





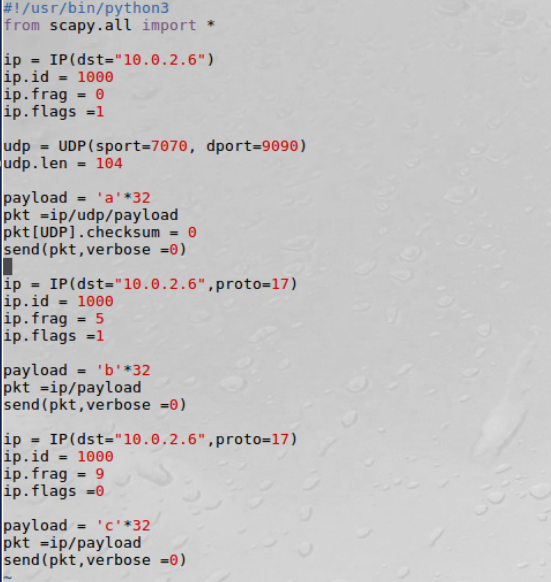
**C**

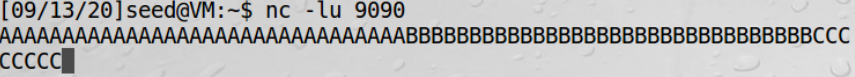




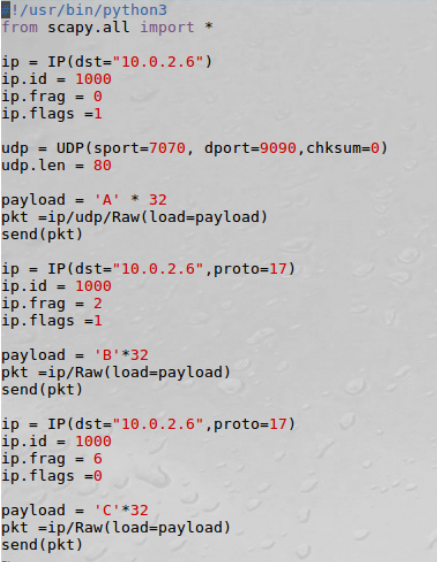
**Lab3 IP/ICMP Attacks Lab**

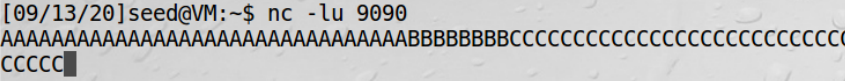
**Task1.a**

****

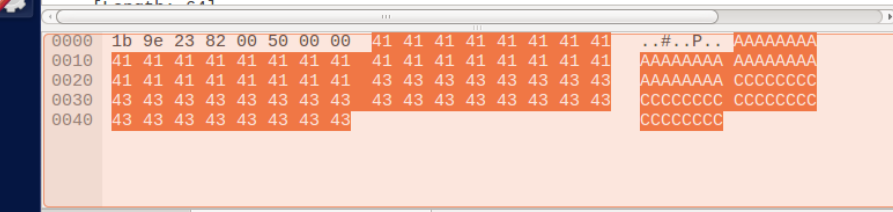
****

**Task1.b**

****

****

如果第一段报文包含第二段报文

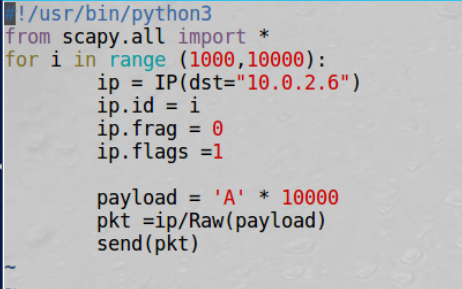


Wireshark结果如图，终端没有输出

**Task1.c**

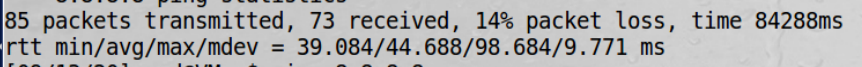
发送超大数据包，接收端显示非法数据帧

**Task1.d**

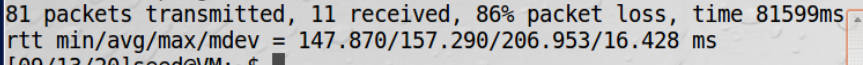
****

向目标主机发送大量报文

发送报文前被攻击主机ping的接受率：



向其发送报文后：



Packet loss 丢失率从14%上升到86%，攻击成功。