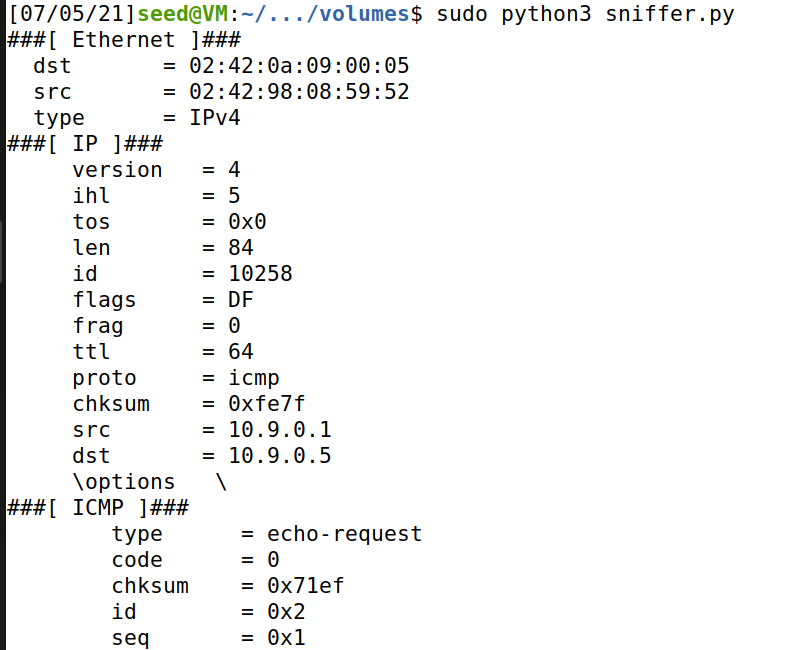
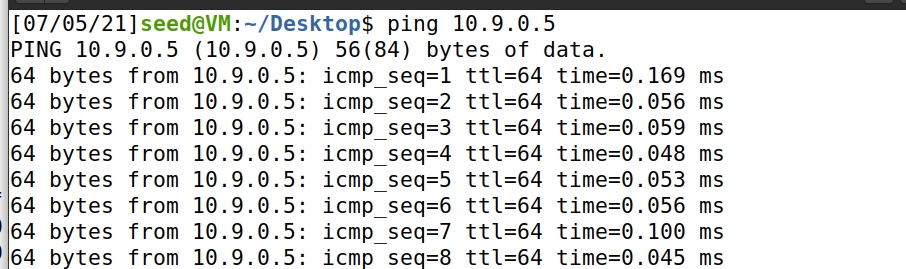
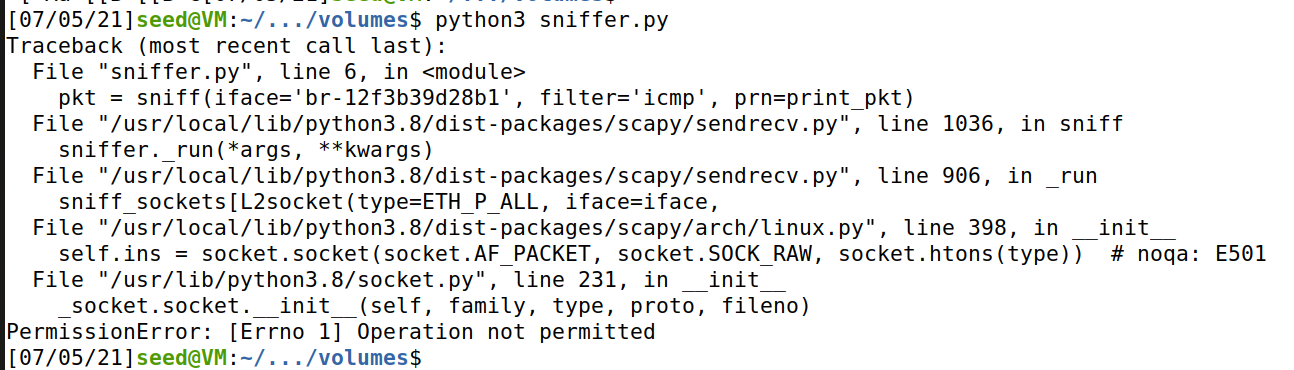
**57118126 苏恒**

**Task1.1 A**





非root权限下无法运行



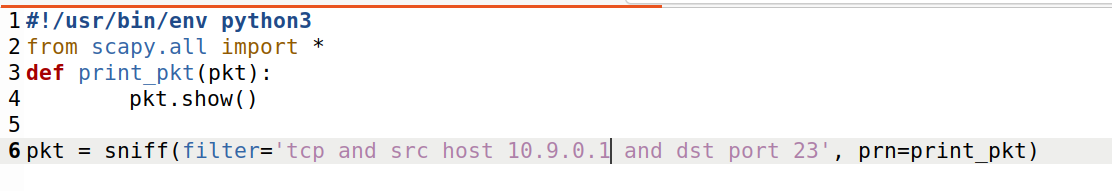
**Task1.1B**

1.ICMP

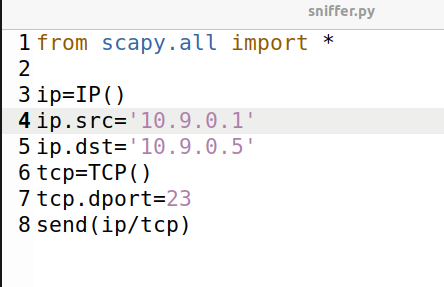
同1.1A

2.TCP

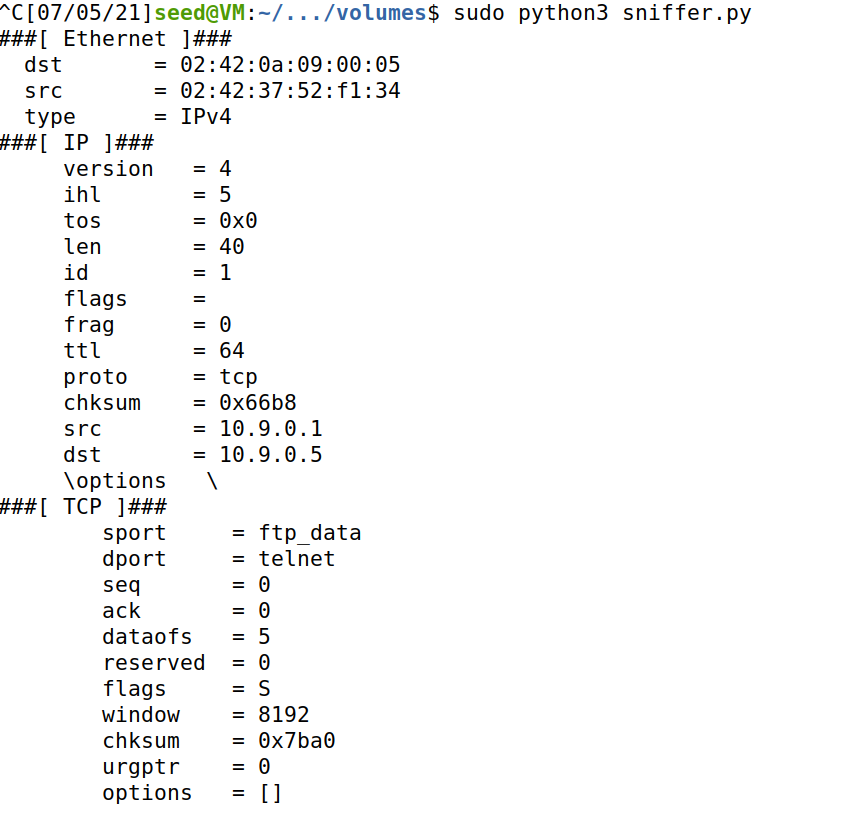
sniffer



发包程序

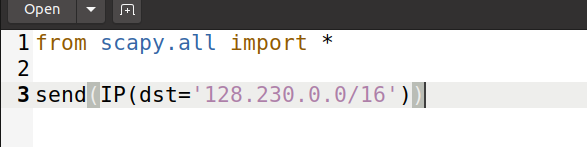


结果

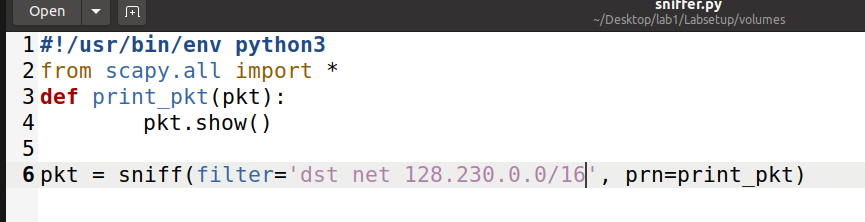


3.网段

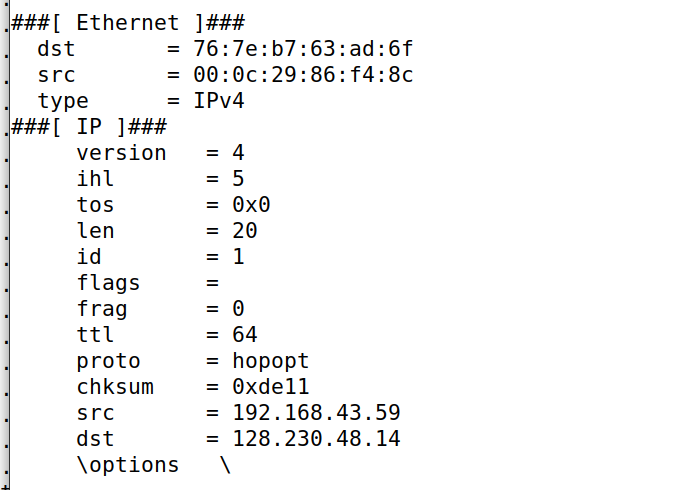
发包程序



Sniffer

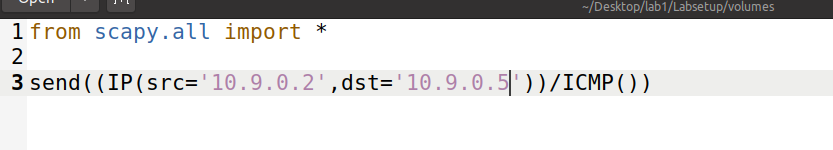


结果

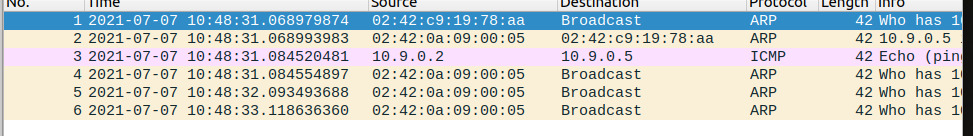


**Task1.2**

发包程序

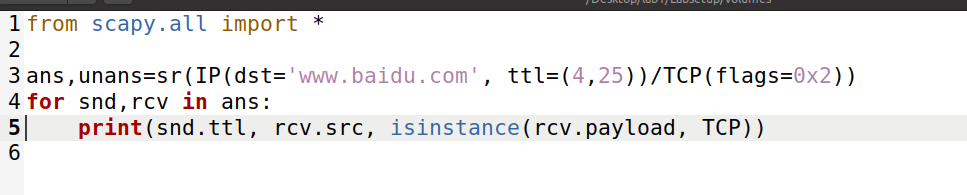


Wireshark查看

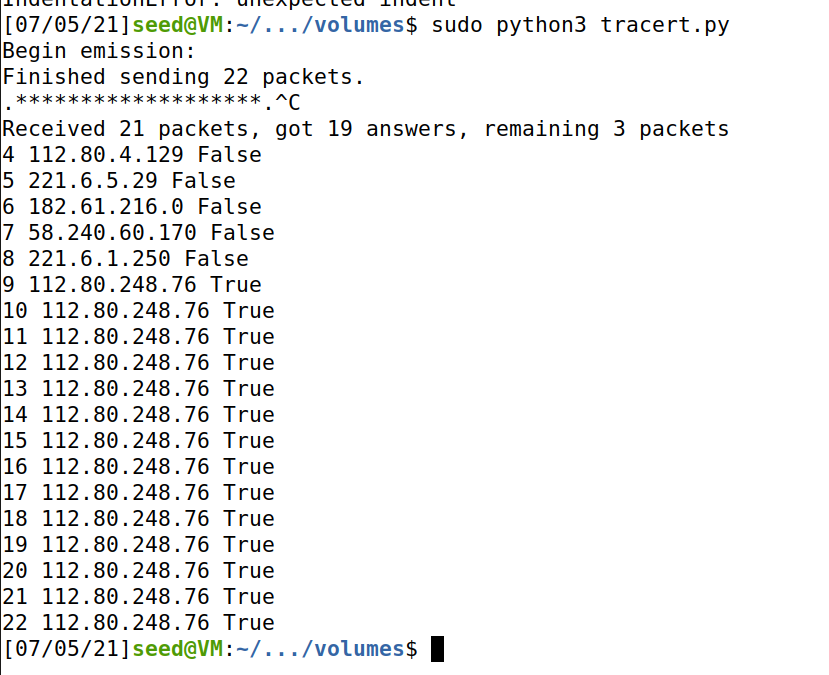


**Task1.3**

发包程序

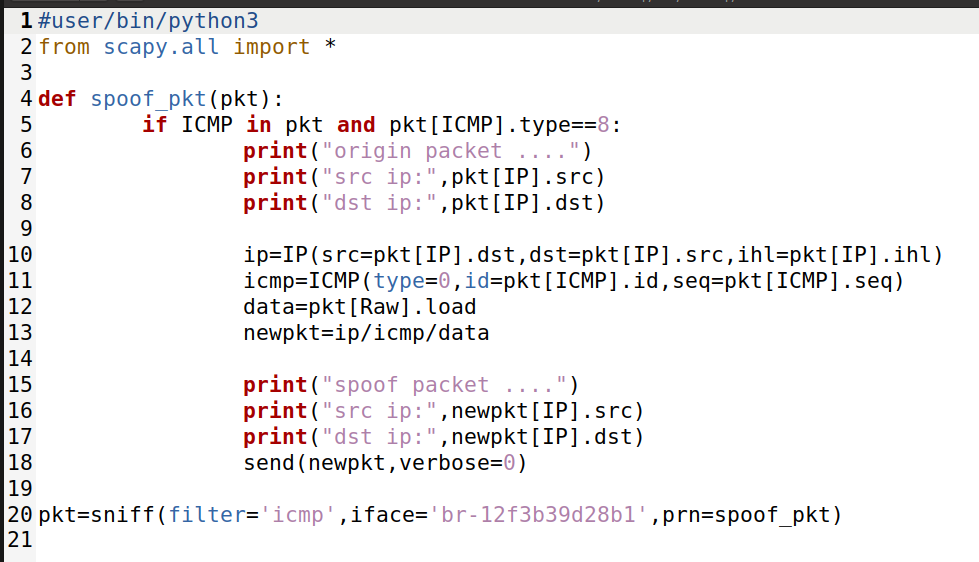


结果

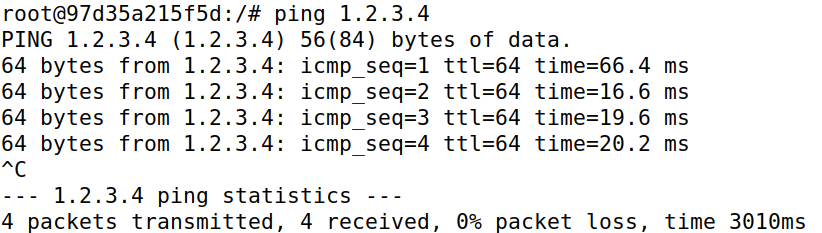


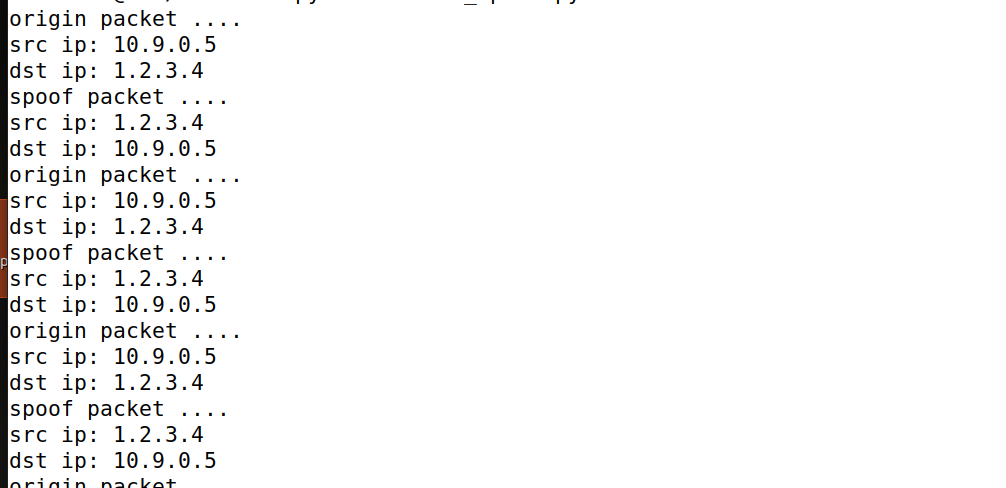
**Task1.4**

Sniff then spoof程序

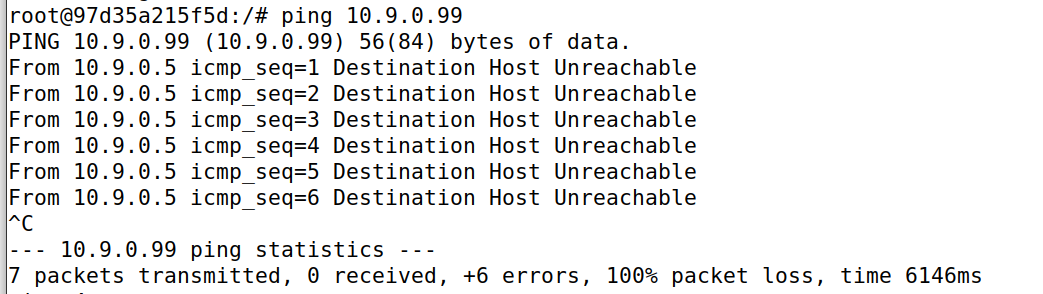


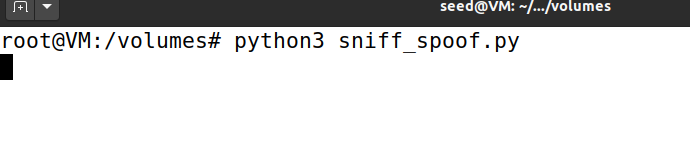
Ping 1.2.3.4

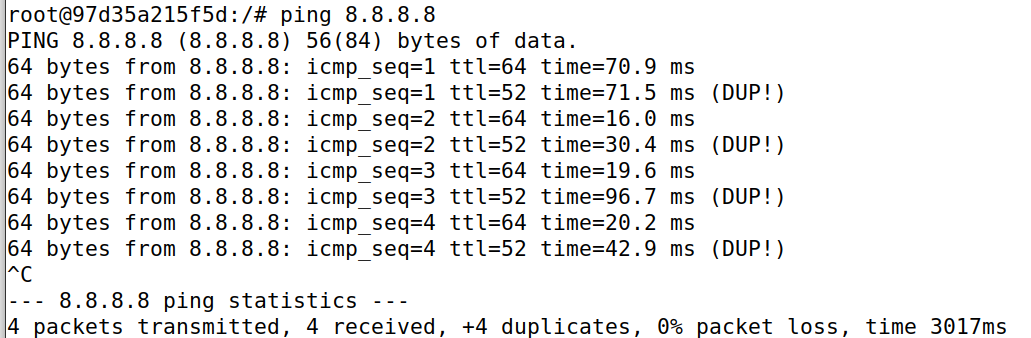


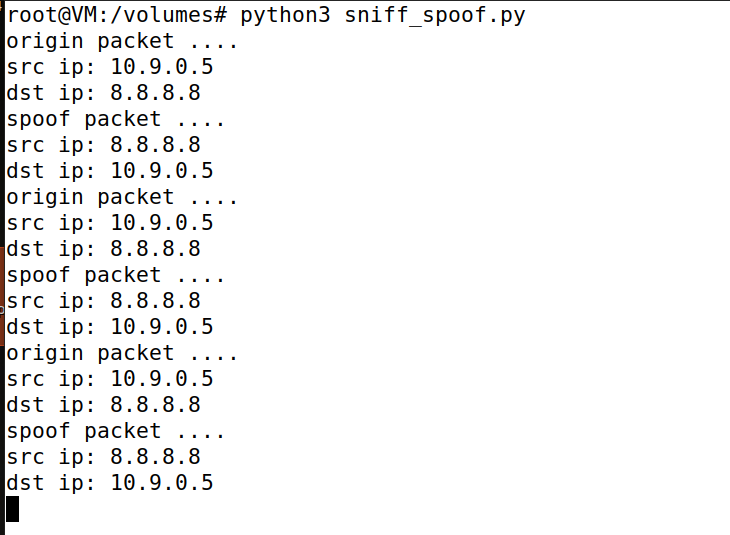


ping 10.9.0.99



Ping 8.8.8.8





结论：由于1.2.3.4和8.8.8.8和host 10.9.0.5不在一个子网下，报文需要通过网关10.9.0.1，就被劫持并伪造了假的icmp reply。而10.9.0.99在同一个子网下，通过ARP广播获得MAC地址来发送，而没有收到ARP响应就ping不通。