# TASK 1.1

* 1. A

代码如下，ifcondig命令下显示的网卡描述为br-a325b4afc03f

#!/usr/bin/python

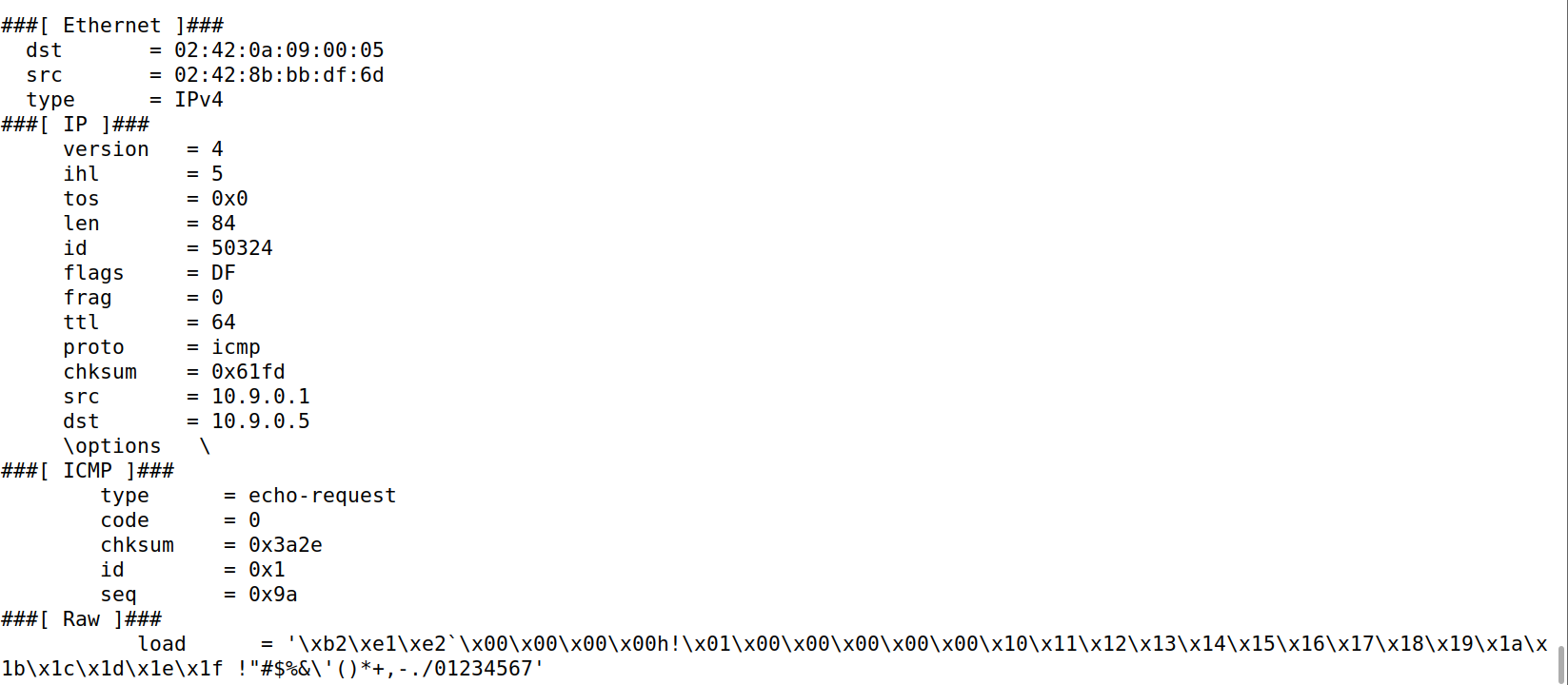
from scapy.all import \*

def print\_pkt(pkt):

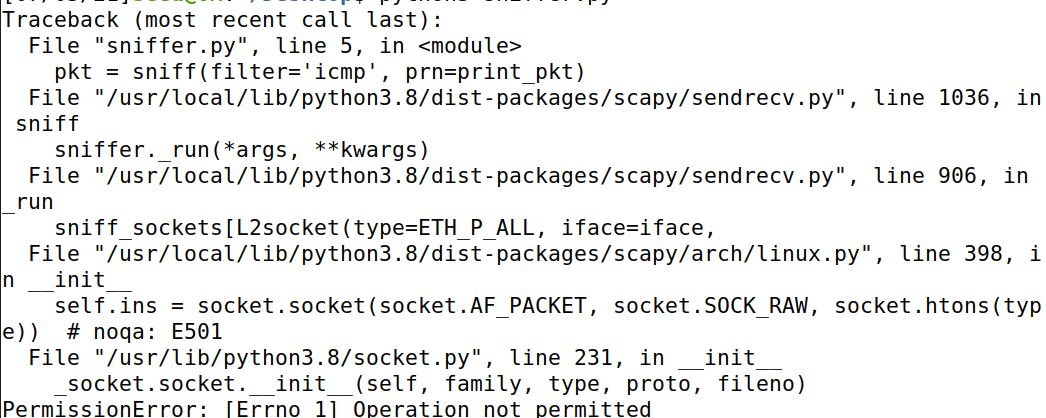
pkt.show()

pkt = sniff(iface='br-a325b4afc03f', filter='icmp', prn=print\_pkt)

使用root权限下，显示如下



未使用root权限时，显示如下：



**B**

代码在A的基础上分别将pkt的值修改成如下所示：

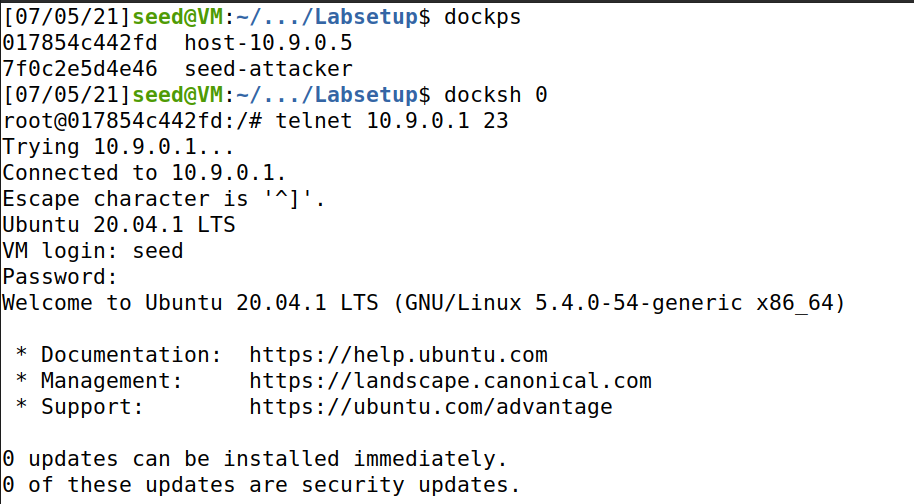
pkt = sniff(iface='br-a325b4afc03f', filter='tcp and dst port 23 and host 10.9.0.5', prn=print\_pkt)

pkt = sniff(iface='br-a325b4afc03f', filter='dst net 172.17.0.0/16', prn=print\_pkt)

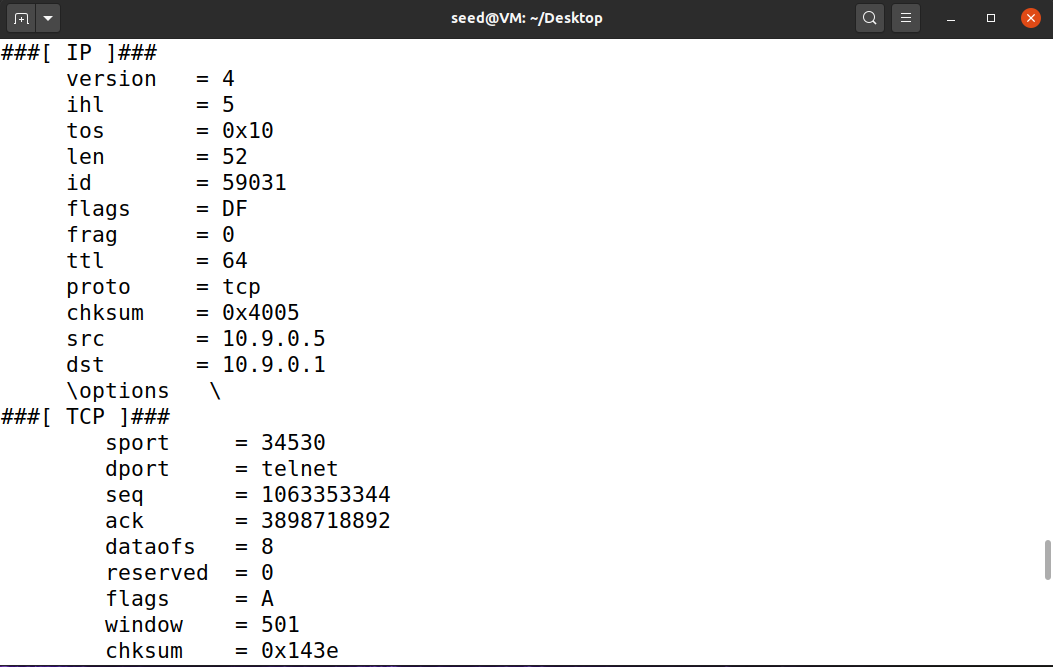
第一项过程与A相同

第二项：

登录10.9.0.5 telnet 10.9.0.1 23

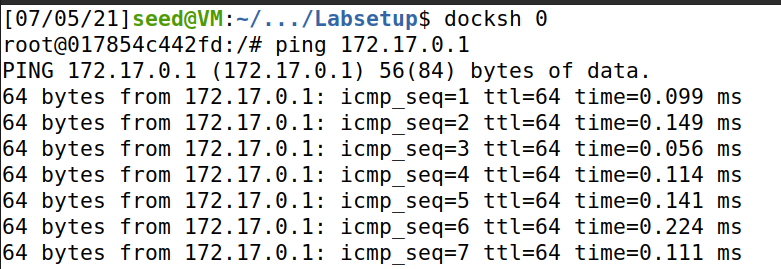


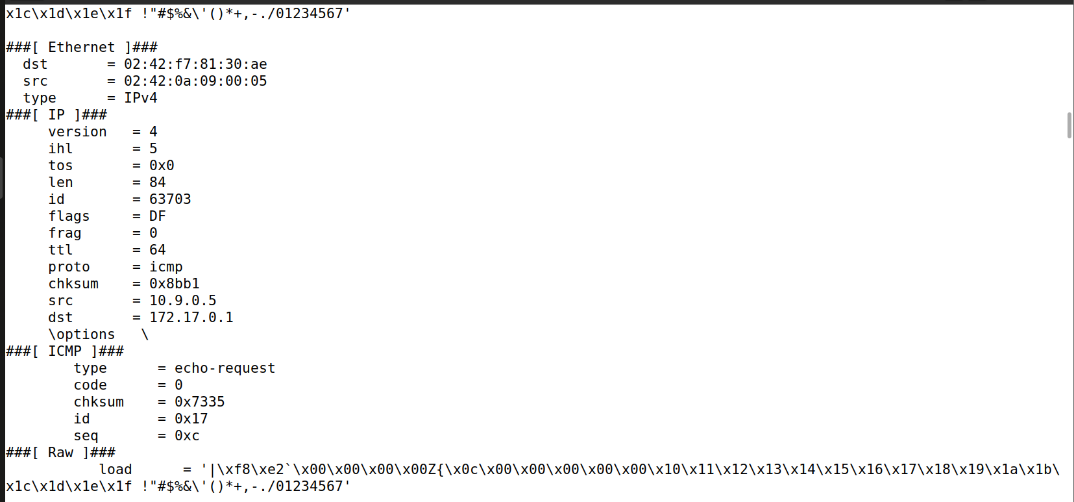
监听到的报文如下



第三项：

登录10.9.0.5 ping 172.17.0.1



程序监听到的报文如下：

1.2

编写如下程序

#!/usr/bin/python

from scapy.all import \*

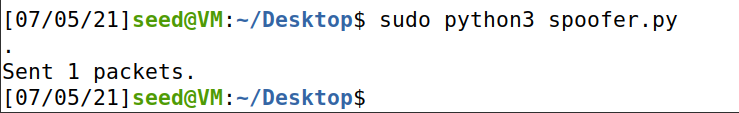
a = IP()

a.dst = '10.9.0.5'

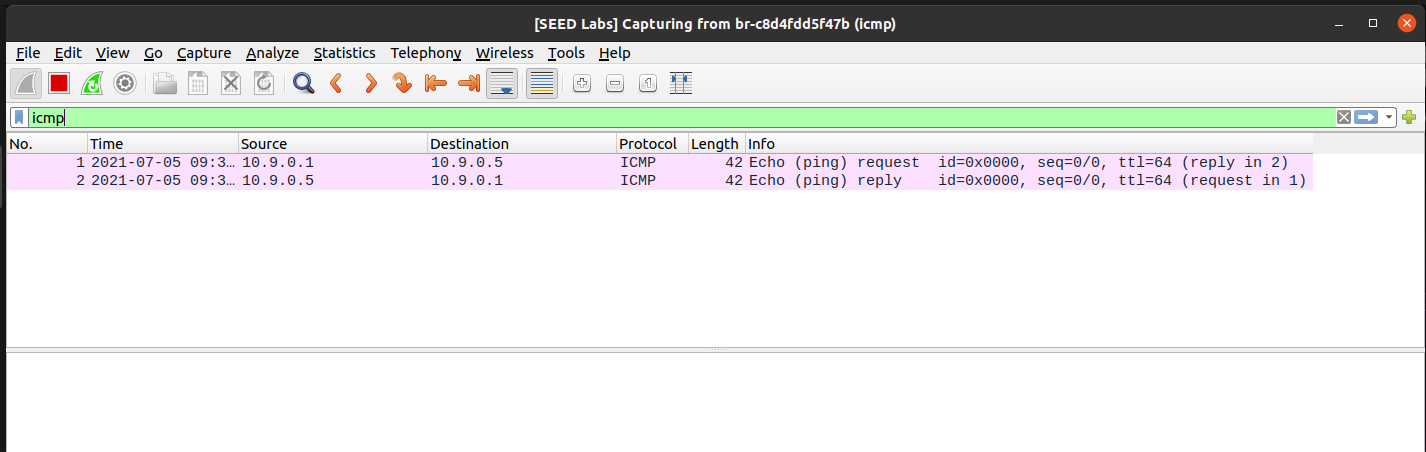
b = ICMP()

p = a / b

send(p)

执行程序发送一个数据包

Wireshark 捕获到的来回的数据包显示如下：



1.3

编写如下程序

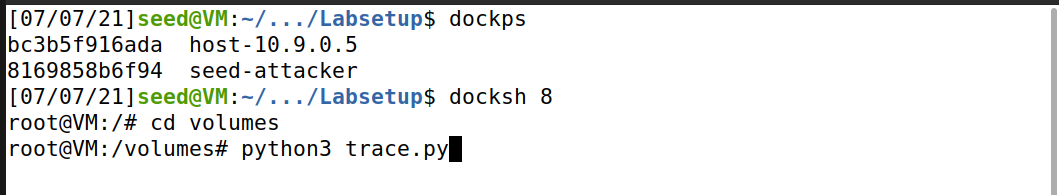
from scapy.all import \*

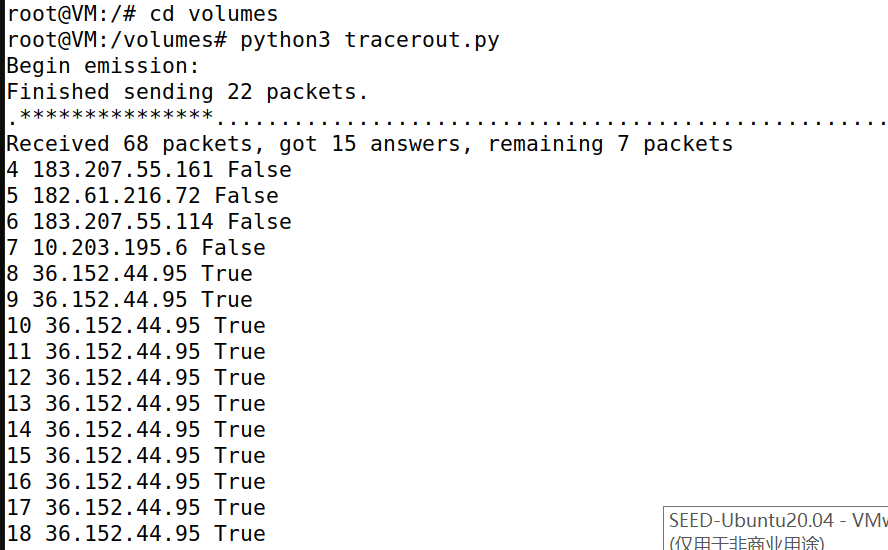
ans,unans=sr(IP(dst='www.baidu.com', ttl=(4,25))/TCP(flags=0x2))

for snd,rcv in ans:

print(snd.ttl, rcv.src, isinstance(rcv.payload, TCP))

在以下主机上运行



其结果如下

1.4

编写的程序如下

from scapy.all import \*

def print\_pkt(pkt):

a=IP()

a.src=pkt[IP].dst

a.dst=pkt[IP].src

a.ihl=pkt[IP].ihl

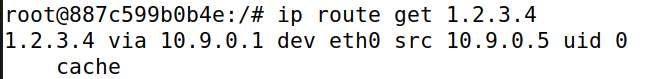
data = pkt[Raw].load

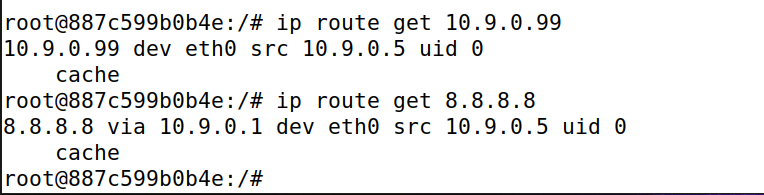
b=ICMP(type='echo-reply',code=0,id=pkt[ICMP].id,seq=pkt[ICMP].seq)

send(a/b/data)

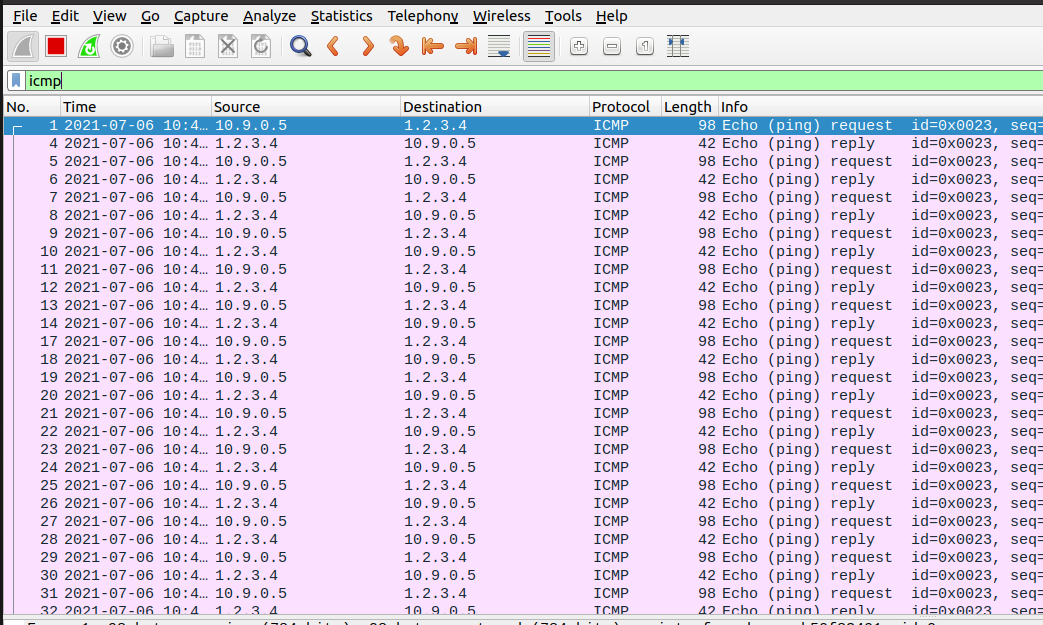
pkt=sniff(iface='br-89d502c52223', filter='icmp[icmptype]==icmp-echo',prn=print\_pkt)

各地址的路由寻址关系



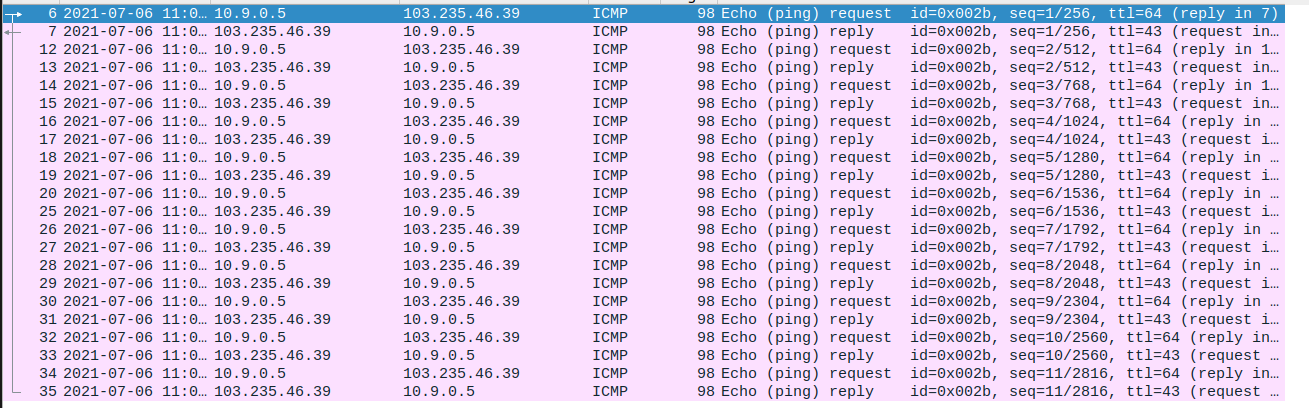


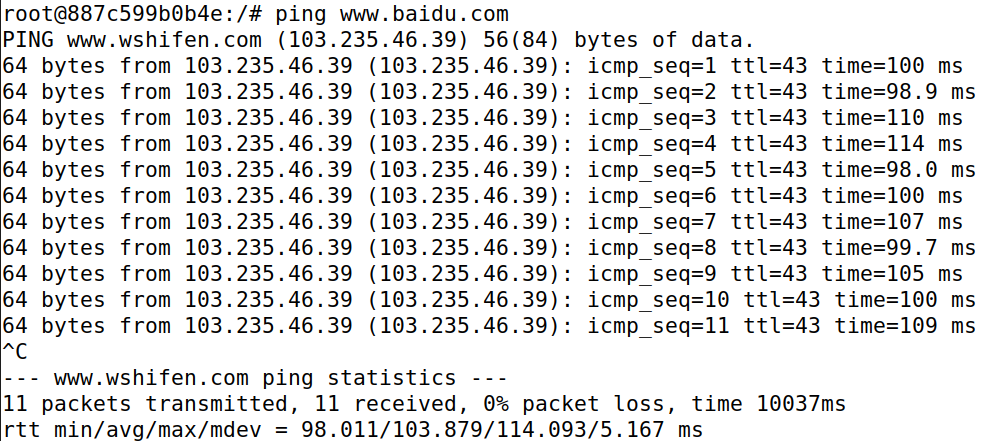
10.9.0.5 ping 1.2.3.4后，wireshark监测到的流量如图



Ping 10.9.0.99时，程序没有响应

Ping 8.8.8.8时，





结论：ping的源地址为10.9.0.5。当ping子网外的不存在地址和真实地址时，其和10.9.0.5不在一个子网下，需要通过网关向外转发，就被运行程序返回了icmp reply。ping子网内不存在地址时，由于默认路由不经过监听的路由器，程序没有响应。