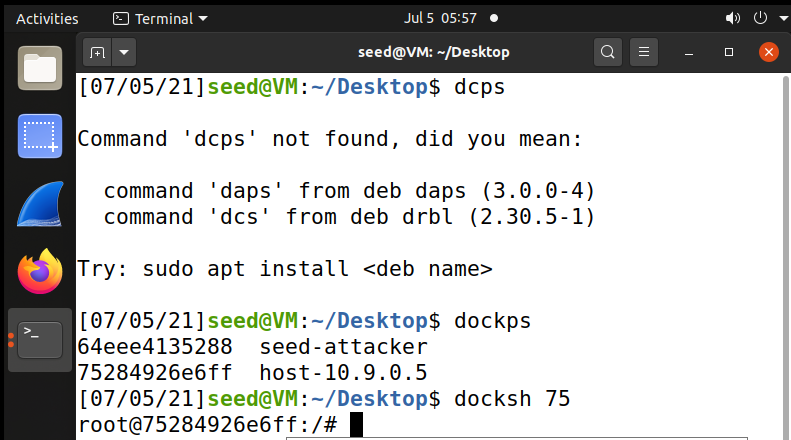
**第一次实验报告**

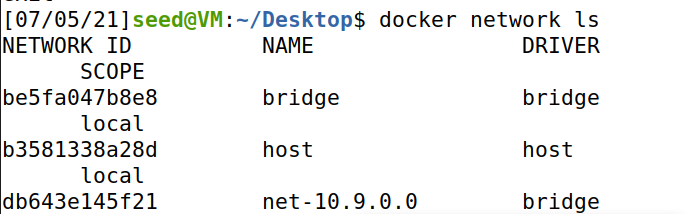
57118216 丰思飏

1.1

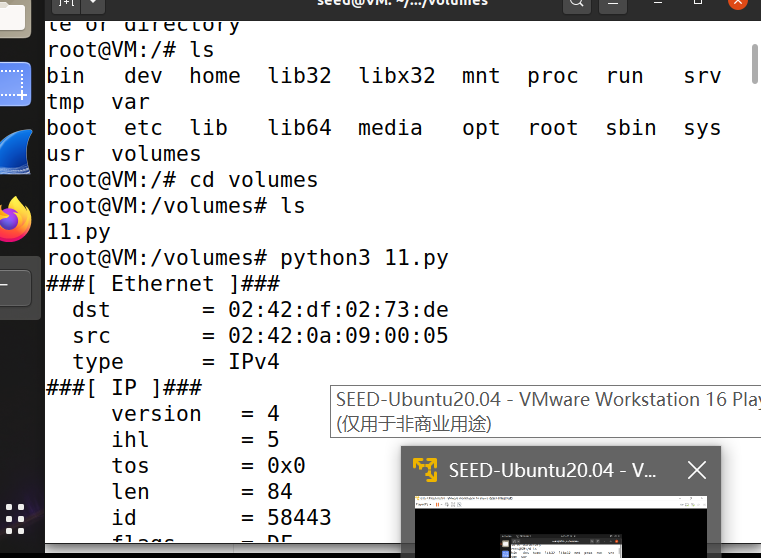
获取对应哈希值



获取10.9.0.0的网络ID

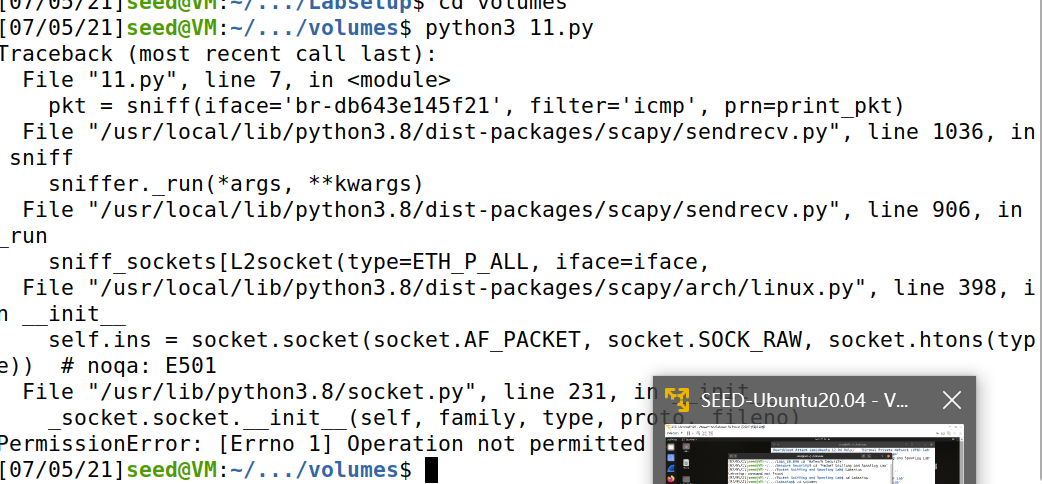


运行嗅探程序并抓包



1.1A

非root权限下，运行程序无效



1.1B

ICMP结果与1.1中相同

TCP使用Telnet获取报文

#!/usr/bin/env python3

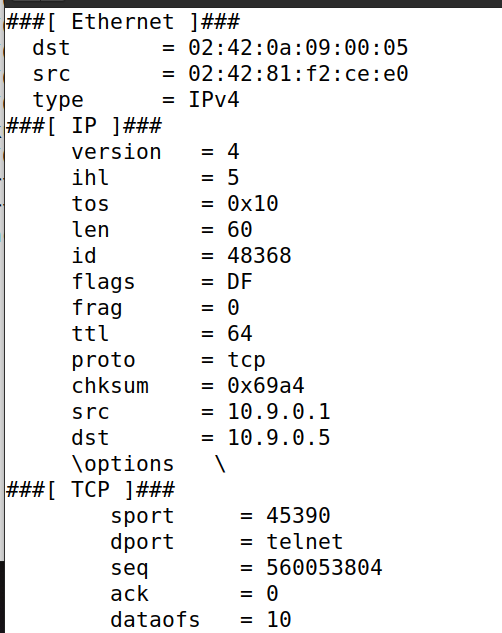
from scapy.all import \*

def print\_pkt(pkt):

pkt.show()

pkt = sniff(iface='br-db643e145f21', filter='tcp and src host 10.9.0.1 and dst port 23', prn=print\_pkt)





子网

嗅探程序

from scapy.all import \*

def print\_pkt(pkt):

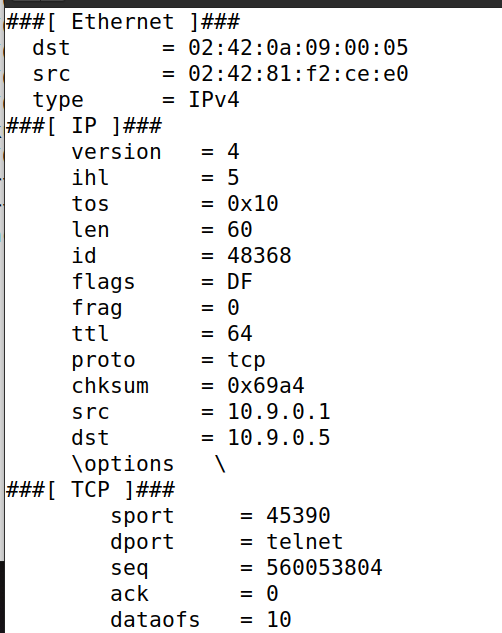
pkt.show()

pkt=sniff(iface='br-db643e145f21',filter='dst net 128.230.0.0/16',prn=print\_pkt)

发包程序

from scapy.all import \*

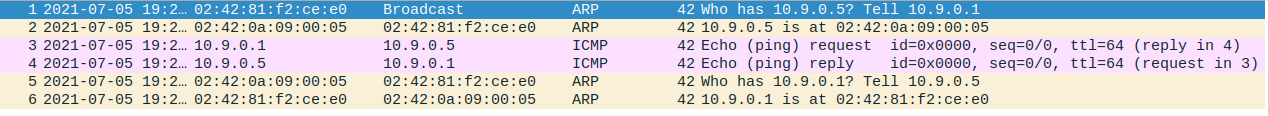
send(IP(dst='128.230.0.0/16'))



1.2

from scapy.all import \*

send(IP(dst='10.9.0.5')/ICMP())



1.3

首先设置桥接网络，主机IP信息如下



网络适配器信息



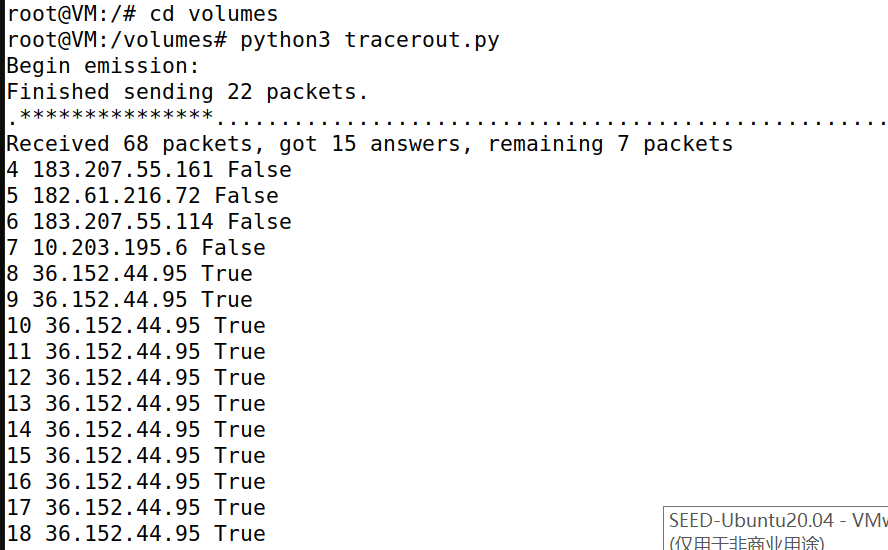
运行以下程序

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))



发送22个包后到达

1.4

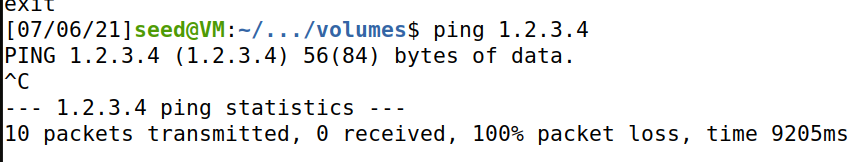
from scapy.all import \*

def print\_pkt(pkt):

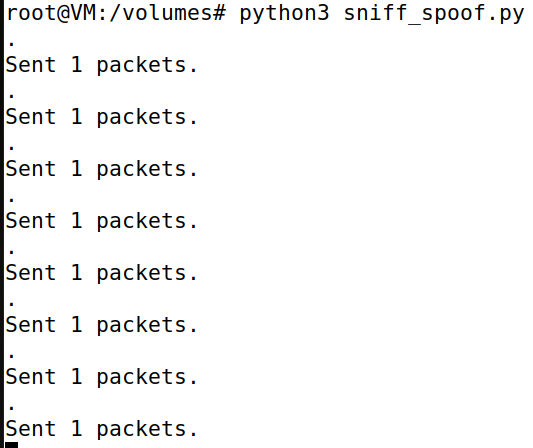
send(IP(src=pkt[IP].dst,dst=pkt[IP].src)/ICMP(type='echo-reply',code=0,id=pkt[ICMP].id,seq=pkt[ICMP].seq))

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

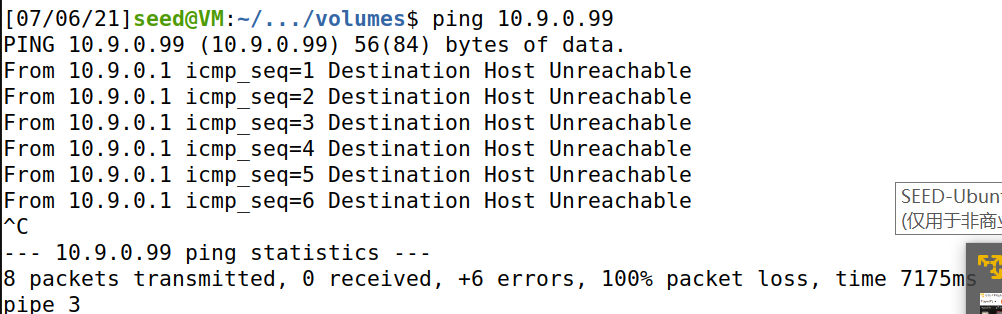
直接ping1.2.3.4



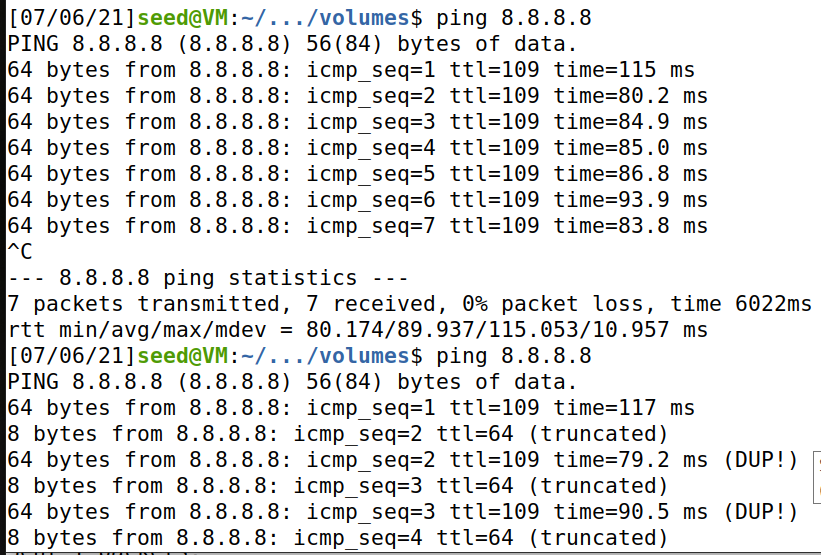
运行sniff\_spoof.py后ping



直接ping10.9.0.99



8.8.8.8



执行程序后应答速度降低