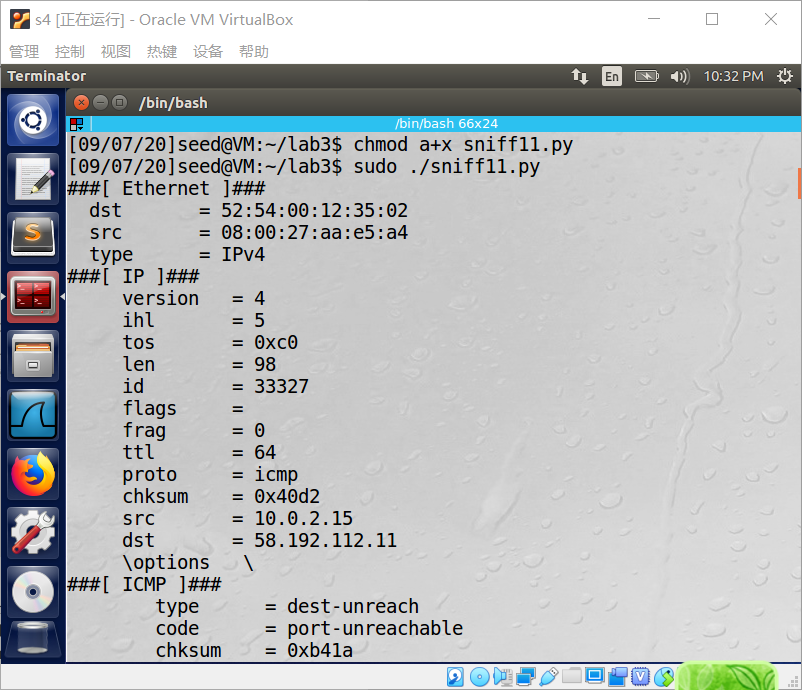
Lab3

57117140 庞乃瑜

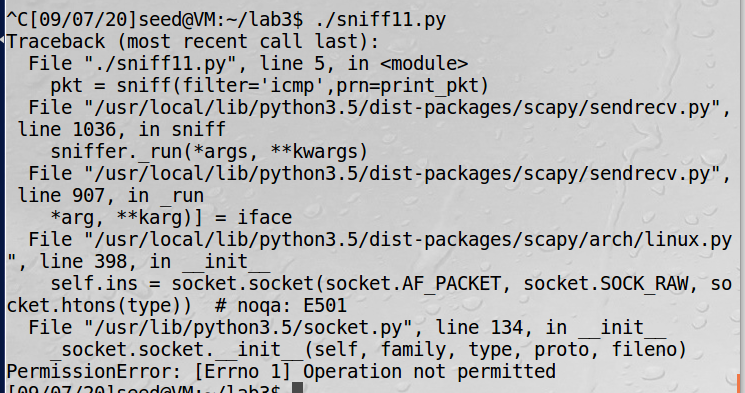
Task1:

Task1.1:

A



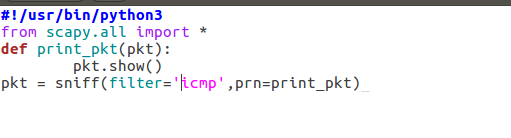
使用root权限的时候可以监听到报文



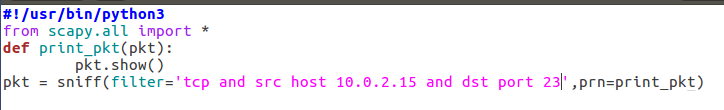
没有使用root权限的时候不能监听报文，因为scapy使用的是pcap实现，而使用pcap需要root权限，故不使用root权限执行sniff程序时，会报权限error

B：

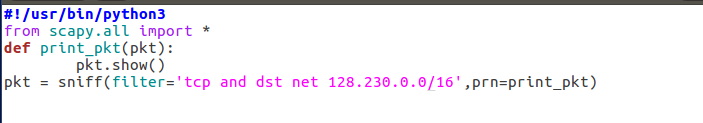
• Capture only the ICMP packet



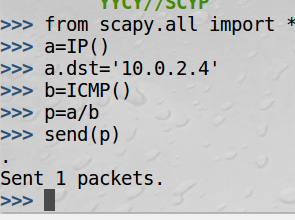
• Capture any TCP packet that comes from a particular IP and with a destination port number 23.

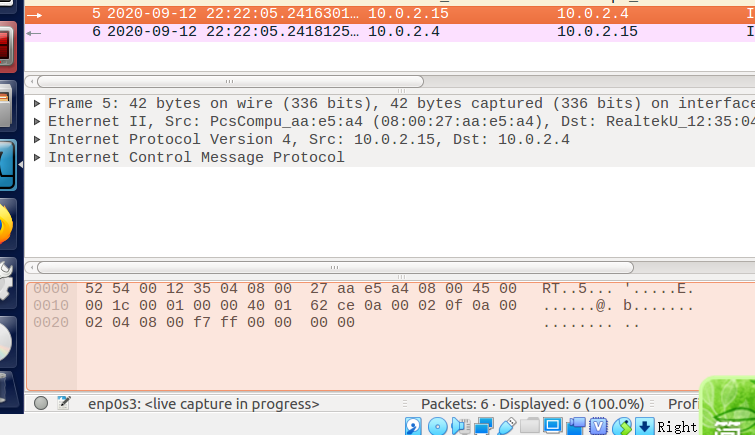


• Capture packets comes from or to go to a particular subnet. You can pick any subnet, such as 128.230.0.0/16; you should not pick the subnet that your VM is attached to.



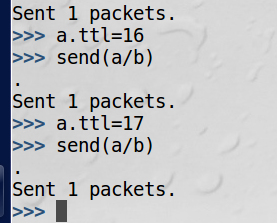
Task1.2:

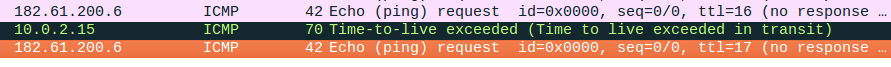




Wireshark成功捕获

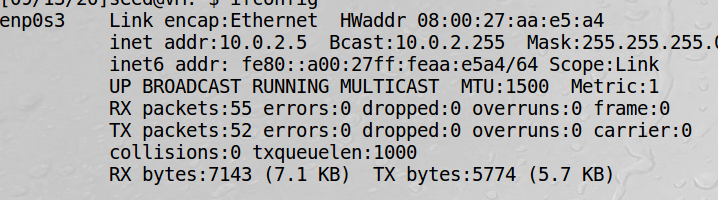
Task1.3:

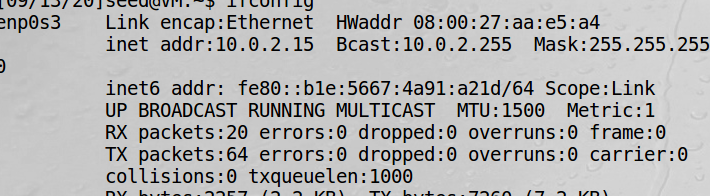


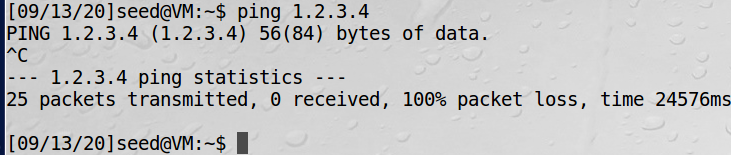


Ttl为17时可到达

Task1.4:





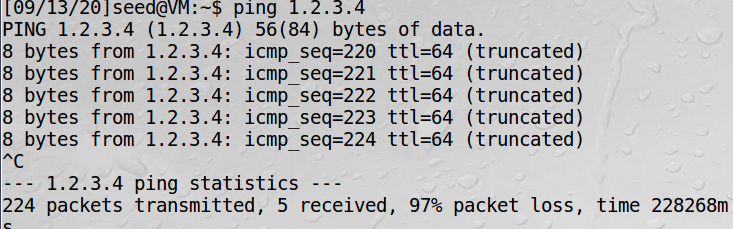


Ping 1.2.3.4无响应

在另一虚拟机上构造响应报文



成功收到响应报文



ARP Cache Poisoning Attack Lab

Task1:

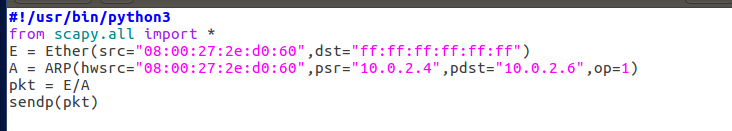
主机与对应的IP、MAC关系

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

Task1A

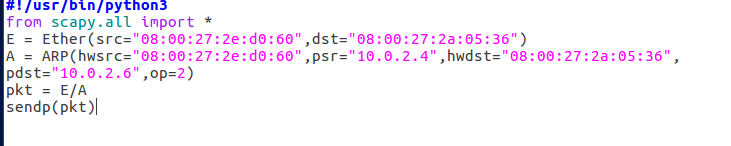


M向A发送报文



发现B的P与M的MAC地址相匹配

Task1B:

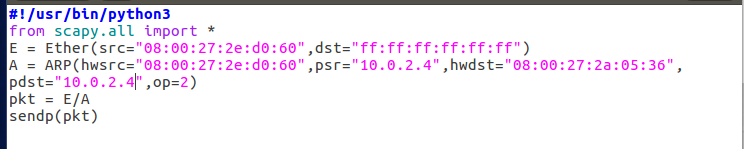


M向A发送的回应报文



可以看到B的地址与M的MAC匹配

Task1C:

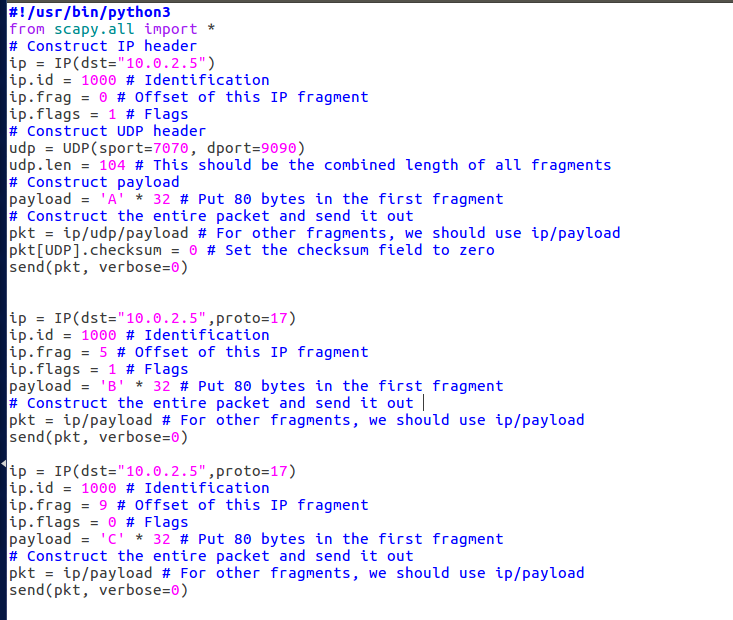


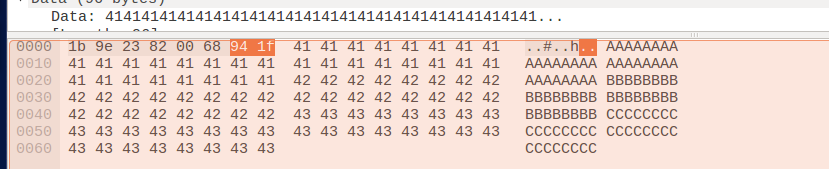
M发送的报文如上



IP/ICMP Attacks Lab

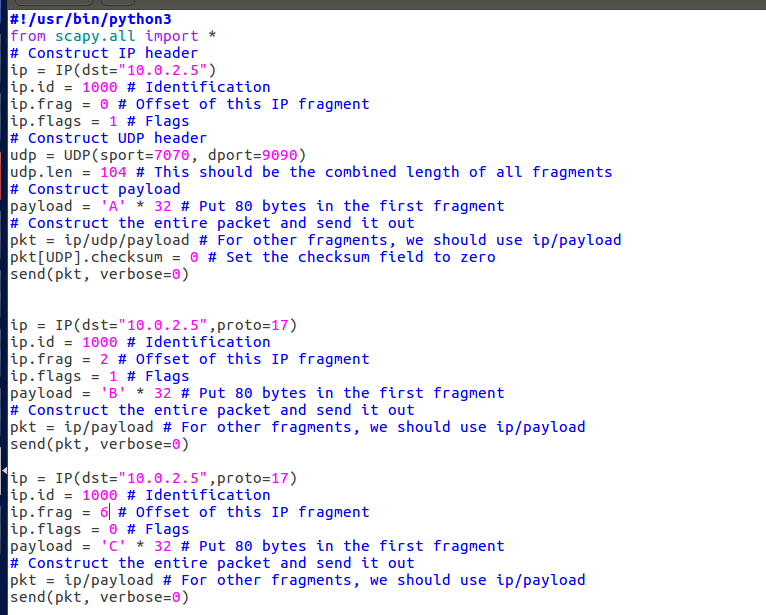
Task1a：

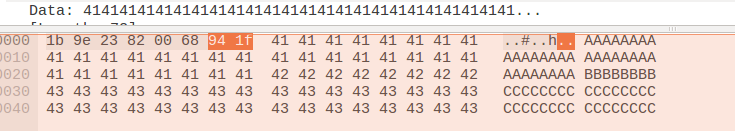


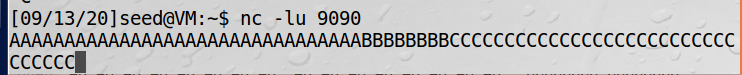




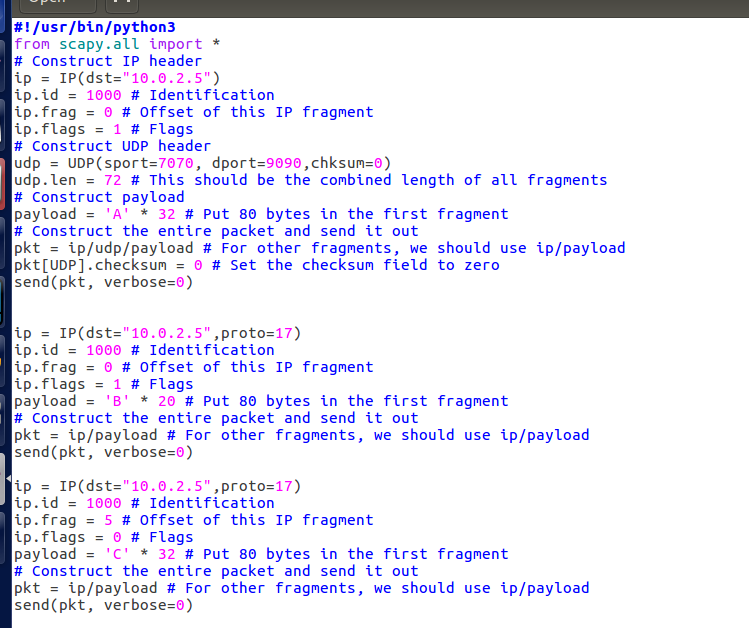
Task1.b:

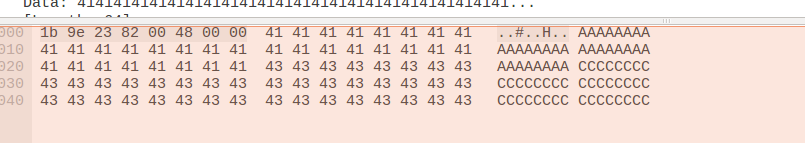


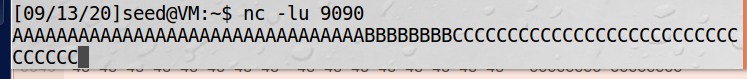
将第二分段的偏移设置为2 第三分段的偏移为6 K为16



第一段完全覆盖第二段时

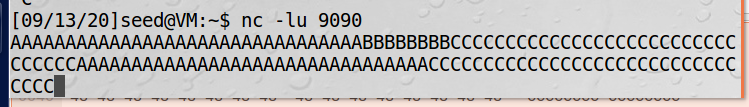




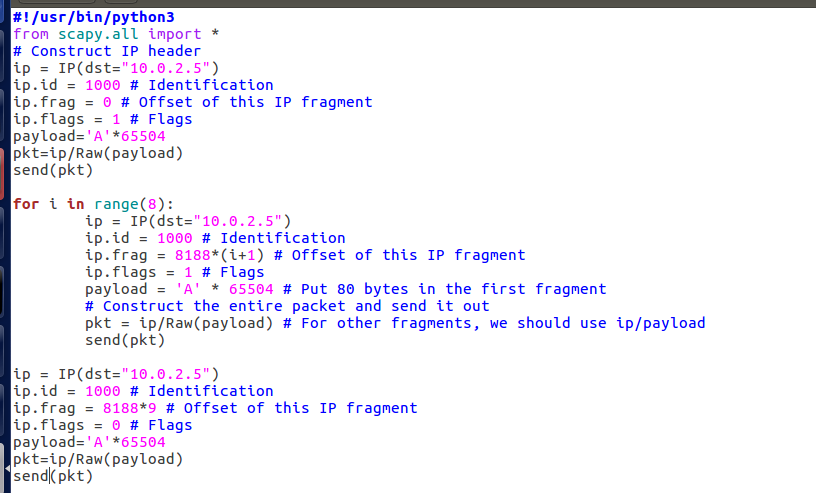


终端没有打印

先发送第二段再发送第一段，只是重叠时结果不变，完全覆盖时终端打印

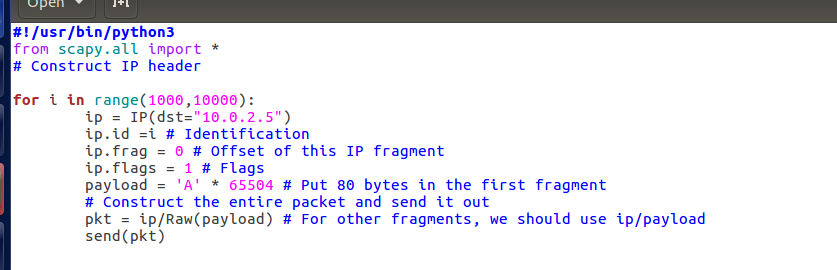


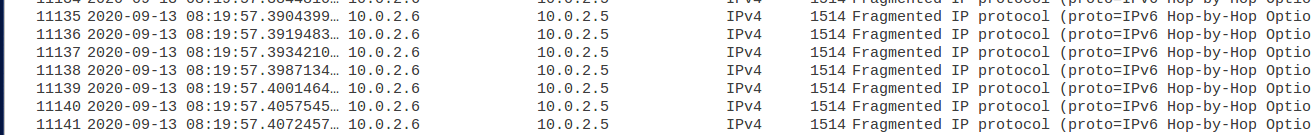
Task1.c:



用wireshark抓包发现 会显示非法碎片

Task1.d：





虚拟机变卡