**lab3实验报告**

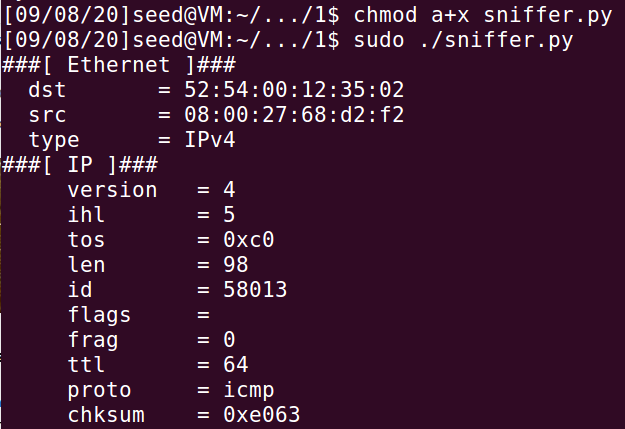
57117133 臧宇豪

**一、Lab1** **：Lab Task Set 1: Using Tools to Sniff and Spoof Packets**

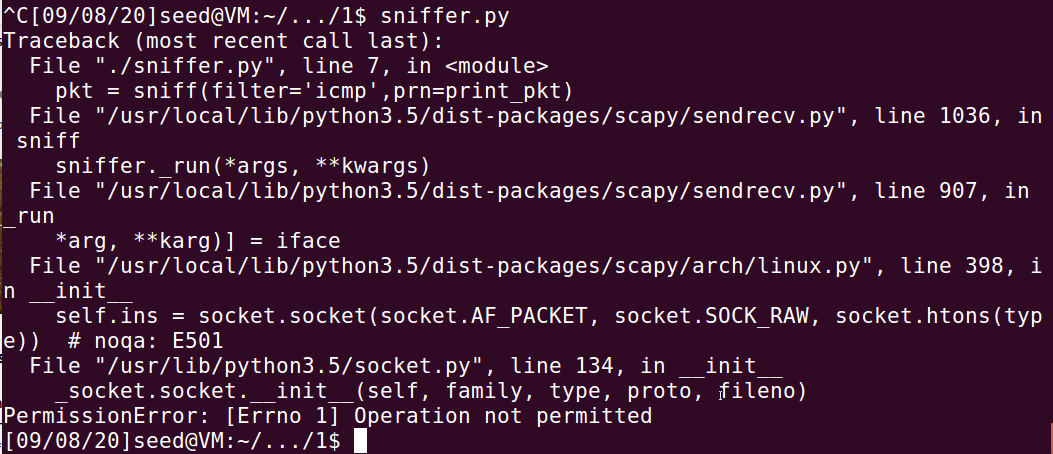
**Task 1.1: Sniffing Packets**

Task 1.1A：

当用sudo ./sniffer.py 命令时，执行成功，结果为：



当使用sniffer.py命令时，执行失败：



Task 1.1B：

命令语法设置如下：

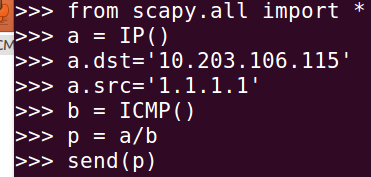
• Capture only the ICMP packet：**filter = ‘icmp’**

• Capture any TCP packet that comes from a particular IP and with a destination port number 23. ：**filter = ‘ip src xxx.xxx.xxx.xxx and tcp and dst port 23’**

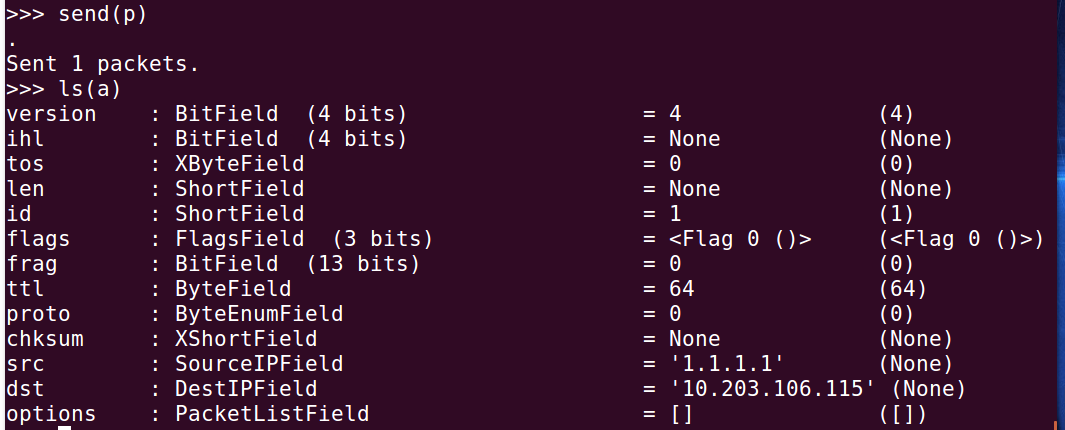
• Capture packets comes from or to go to a particular subnet. You can pick any subnet, such as 128.230.0.0/16; you should not pick the subnet that your VM is attached to ：**filter = ‘net 128.230’**

**Task 1.2: Spoofing ICMP Packets**

代码修改如图所示：

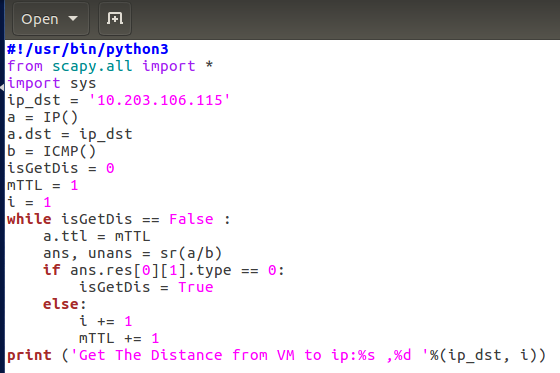


添加后成功发送并收到数据包。

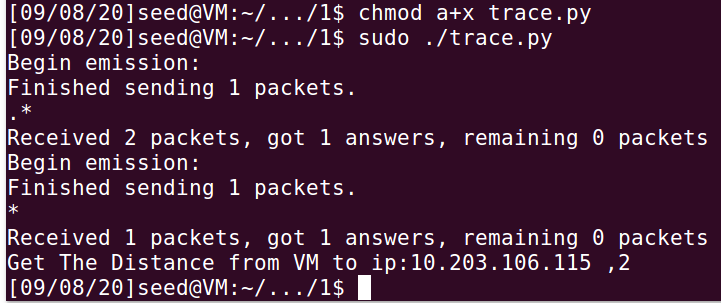


**Task 1.3: Traceroute**

自行设计测试代码如下（举例测试虚拟机到宿主机的距离）：

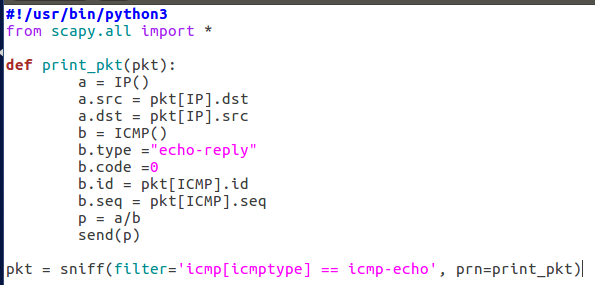


运行后成功获取距离：



**Task 1.4: Sniffing and-then Spoofing**

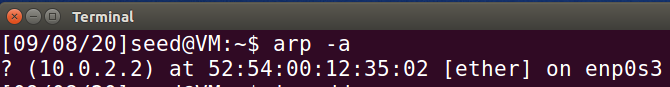
代码设计如下：

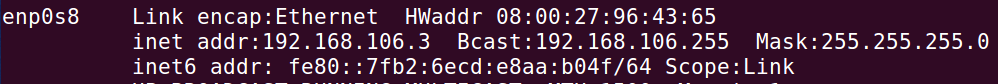


**二、Lab2** **：Task 1: ARP Cache Poisoning**

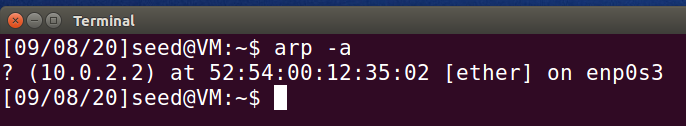
**Task 1A (using ARP request)：**

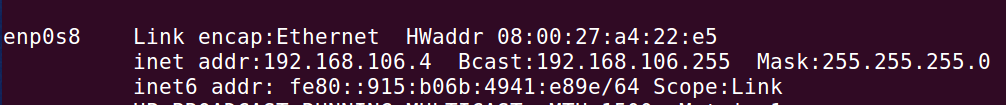
A的arp信息和地址信息（IP：192.168.106.3）：



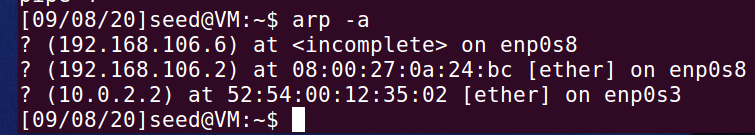


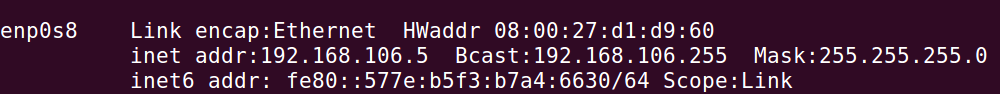
B的arp信息和地址信息（IP：192.168.106.4）：



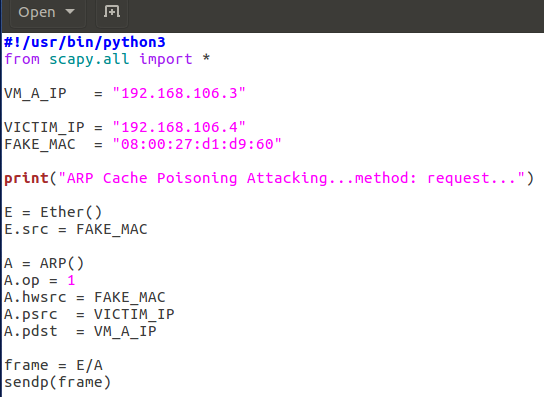


M的arp信息和地址信息（IP：192.168.106.5）：

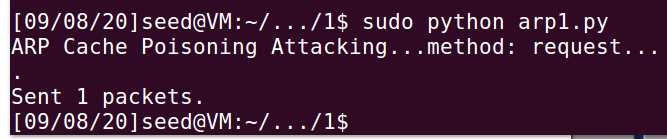




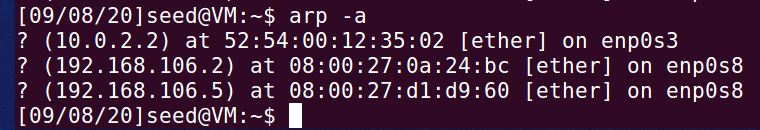
攻击代码如图所示：



执行攻击：

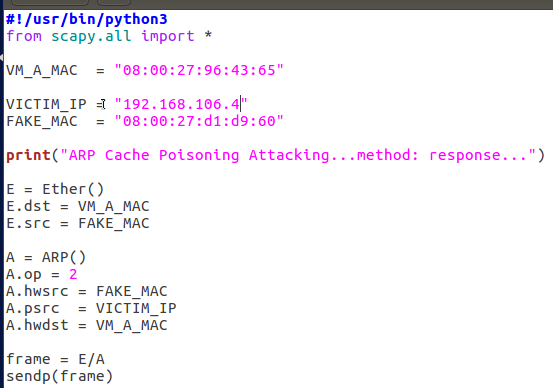


攻击结果：

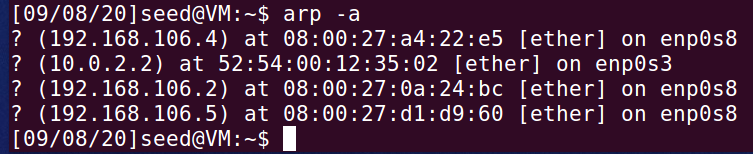
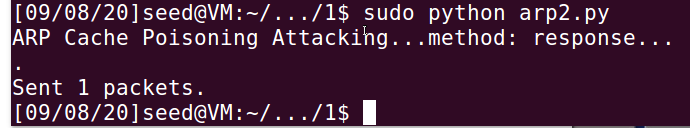


**Task 1B (using ARP reply)：**

代码如图：

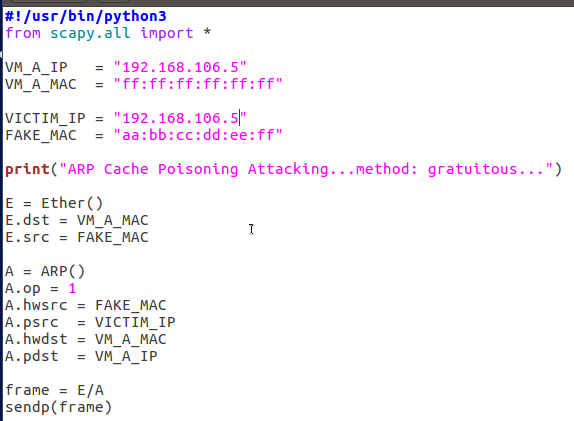


执行攻击代码后：



**Task 1C (using ARP gratuitous message)**

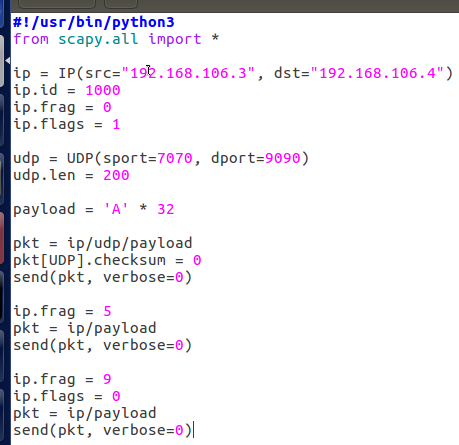
攻击代码如图所示：



**三、Lab3** **：Tasks 1: IP Fragmentation**

**Task 1.a: Conducting IP Fragmentation**

代码如图所示：

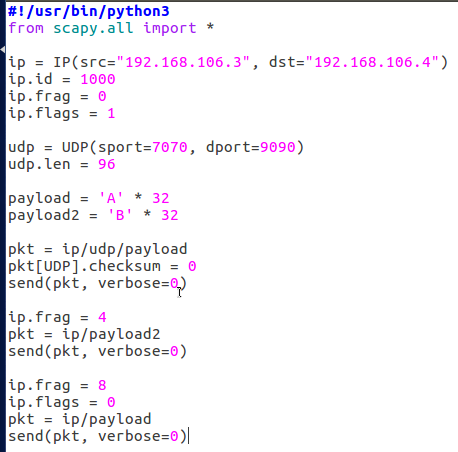


成功输出结果。

**Task 1.b: IP Fragments with Overlapping Contents**

K为8：

（1）先发第一个片段：



运行结果是第二个片段的前8个字节覆盖了第一个片段的最后8个字节。

（2）先发第二个片段

由于报文是全部拼装后输出，因此同样会覆盖。

**Task 1.c: Sending a Super-Large Packet**

令udp=65535，持续发送报文碎片，等到总长度大于65535时，UDP服务器崩溃。

**Task 1.d: Sending Incomplete IP Packet**

代码如下：



可以发现，充当UDP服务器的虚拟机内存占用不断升高。