**Lab3 Report**

57117107 赵笛言

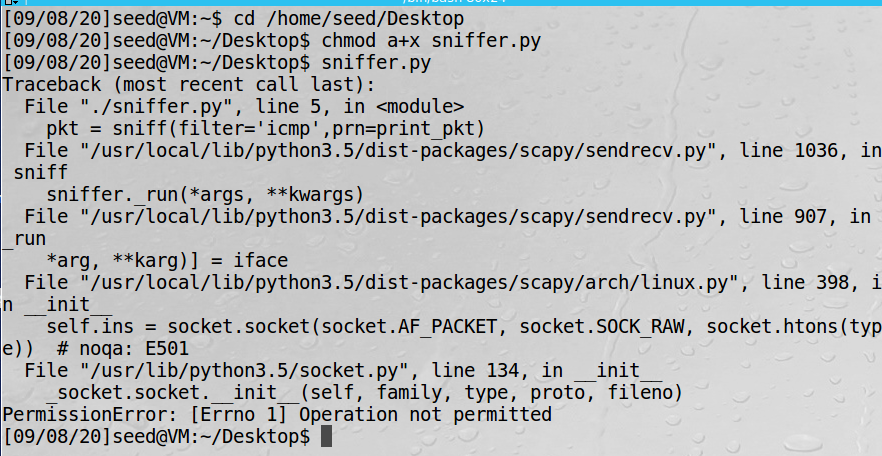
提前说明：由于virtual box在同时运行多个虚拟机时网络设置困难，在纠结了一天无法解决同时保证虚拟机互相ping通且能连接外网的问题，于是Lab1后期更改了实验环境，导致报告中会穿插出现ip地址、子网地址等的转变。（此问题仅存在于lab1）

**Packet Sniffing and Spoofing Lab**

**Task1:** Using Tools to Sniff and Spoof Packets

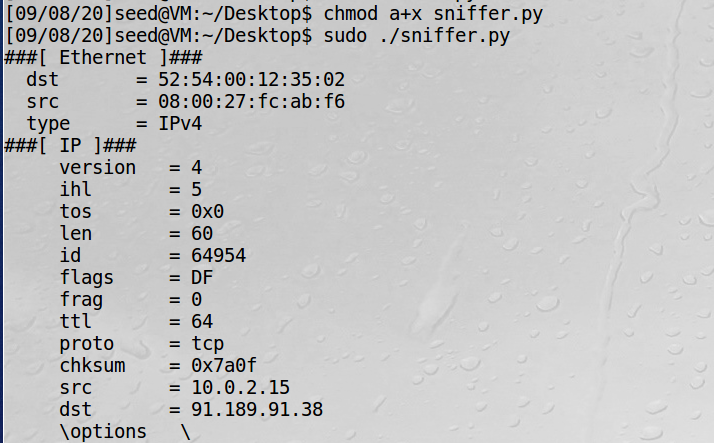
Set:使用sudo pip3 install scapy 命令安装scapy。

Task1.1A：在没有root权限的情况下，运行运用了scapy的sniffer程序。



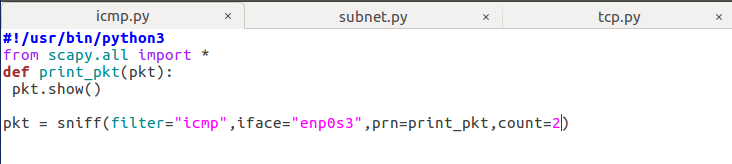
如图所示，没有权限。

有root权限时，能够实现报文监听。

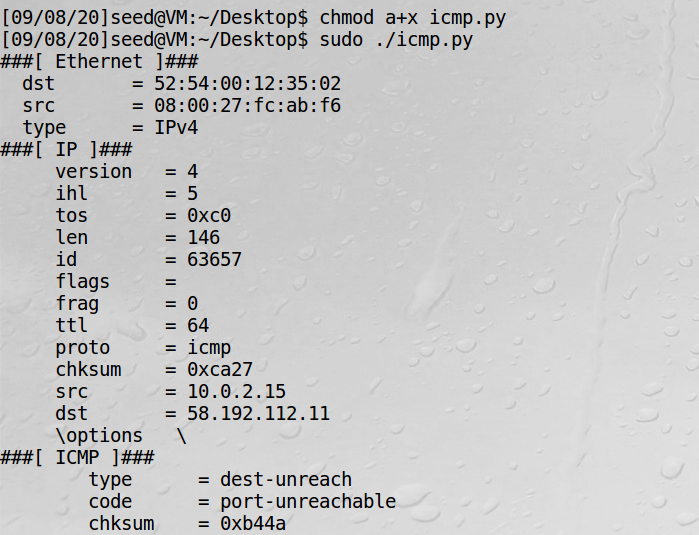


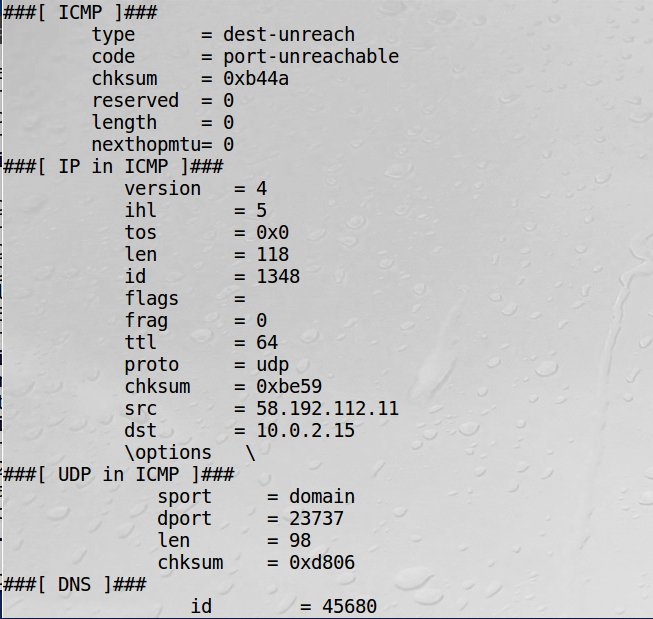
Task1.1B

1. Capture only the ICMP packet



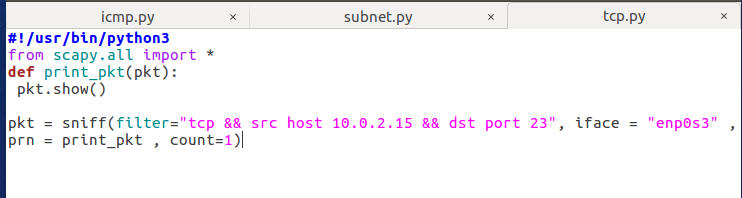
可以快速监听到报文：





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

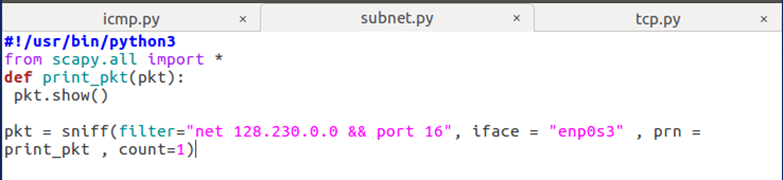
程序如图：



放置监听了很久都没有报文，后来发现可以通过监听本机电脑并人为制造报文从而被检测到。

1. 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.

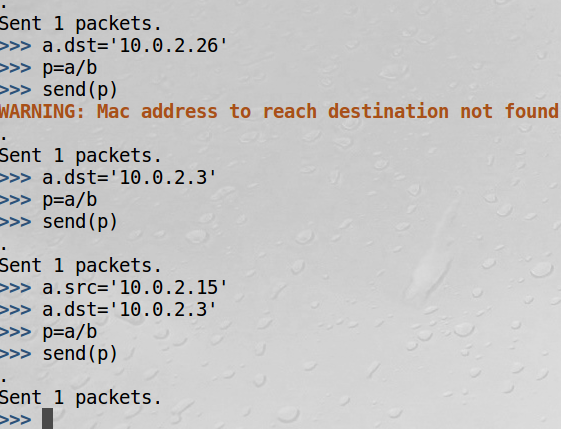
程序如图：



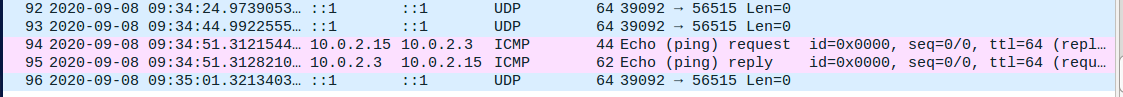
情况如上。

Task1.2：Spoofing ICMP Packets

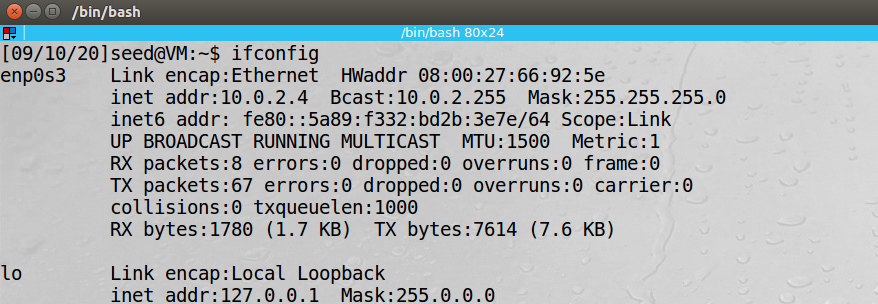
通过模拟手册所给方式伪造报文。（图中为部分）



观察wireshark，发现以发送方为10.0.2.15 ping通了10.0.2.3。



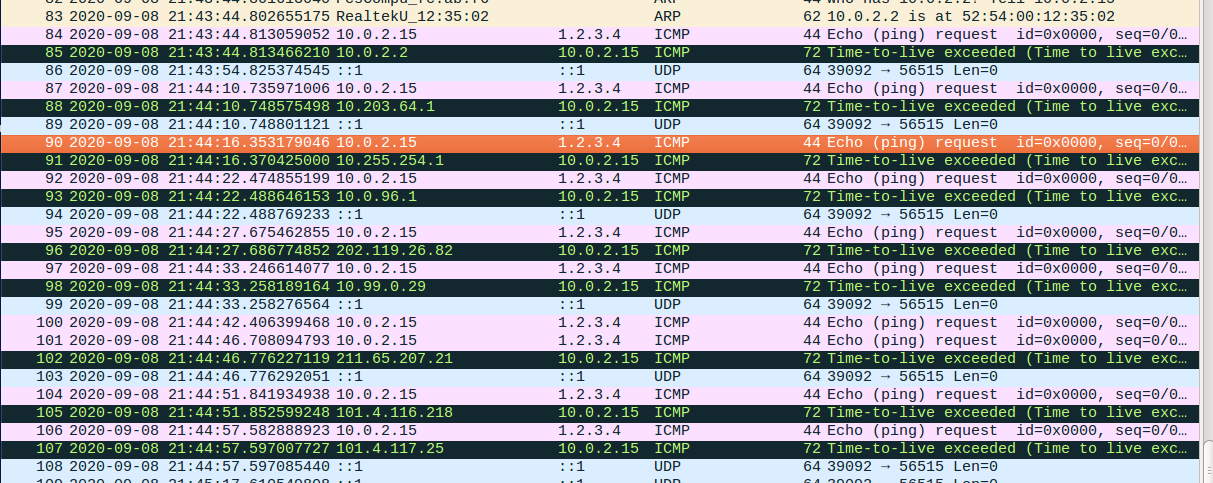
而虚拟机实际的ip为10.0.2.4，成功伪造。



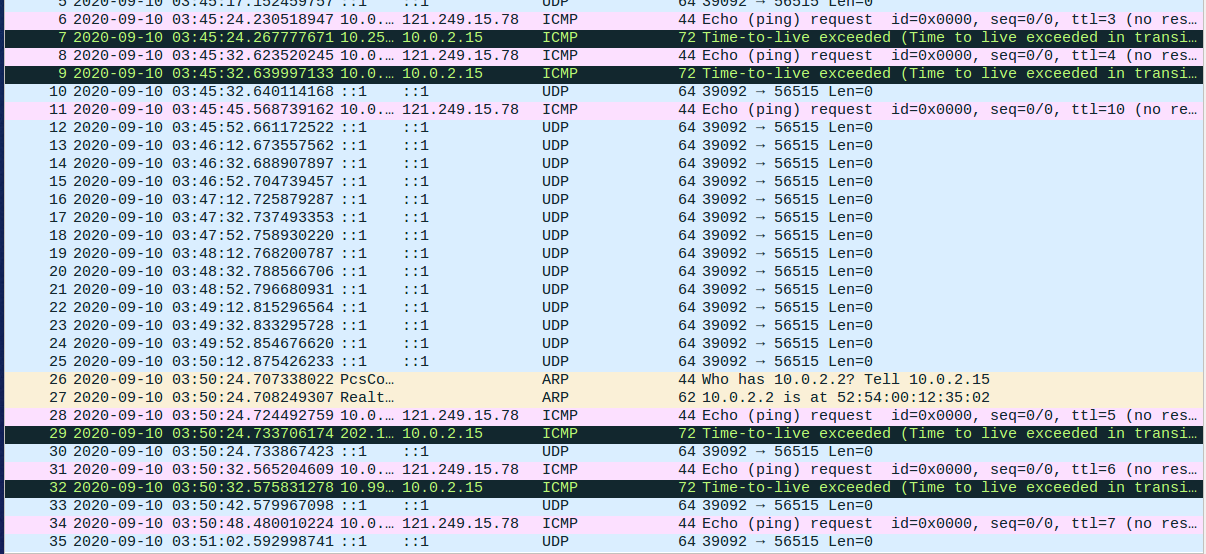
Task1.3：Traceroute

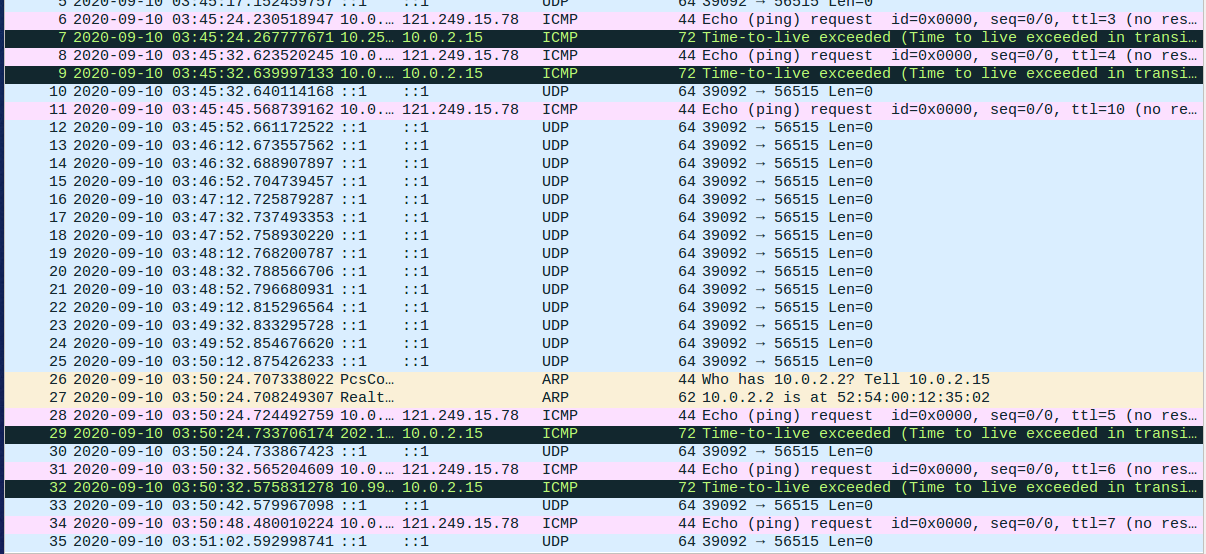
通过设置ttl来查看路径路由以及估计源ip与目的ip距离。

1. 当目的ip地址（1.2.3.4）不存在，可以查看路由：



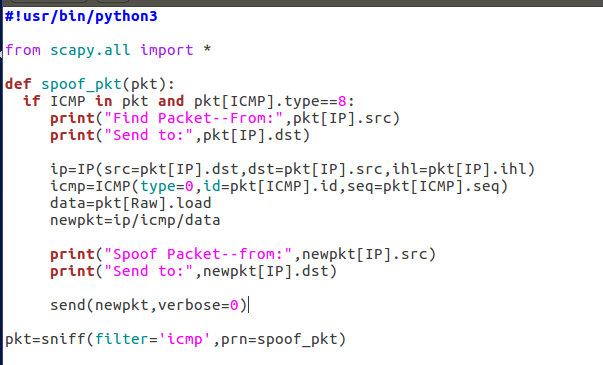
1. 当设置为存在的地址，除了查看路由还可以估计距离：（三跳）





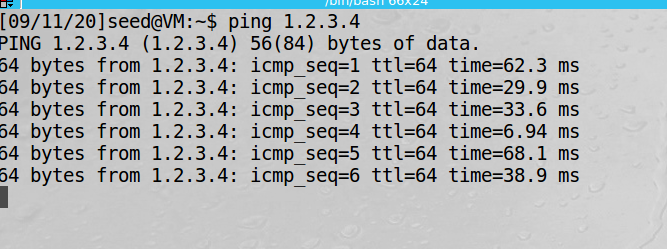
Task1.4 Sniffing and-then Spoofing

监听伪造的程序如下：



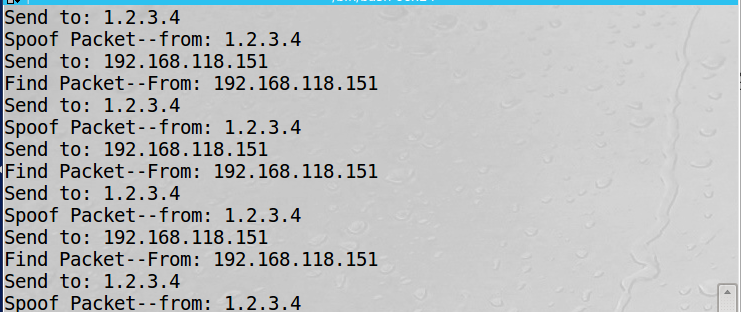
此时存在虚拟机A（192.168.118.150），虚拟机B（192.168.118.151），该程序为于虚拟机A。

当用虚拟机B尝试去ping某个不存在网址，很快ping通，界面为：



认为自身ping通了网络。

而此时A如图：



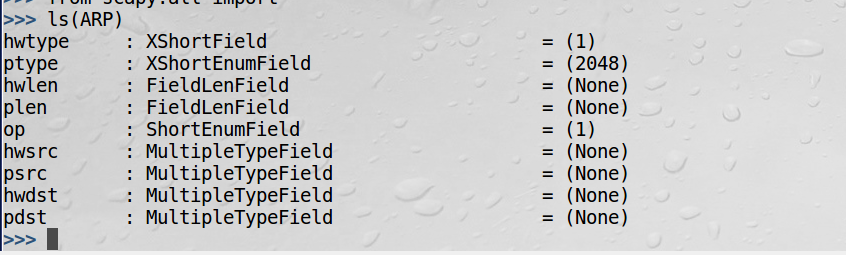
监听并伪造成功。

**ARP Cache Poisoning Attack Lab**

Task1：ARP Cache Poisoning

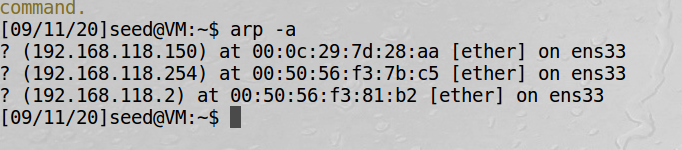
设有主机A（被攻击），B（被冒名伪造），M（攻击）。

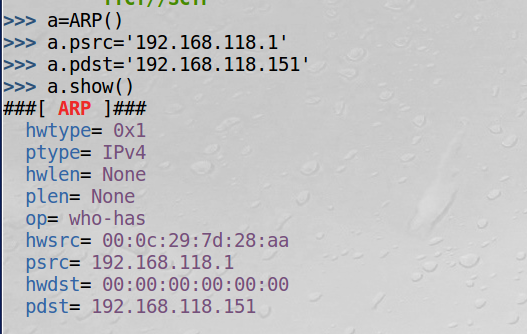
IP地址分别为：192.168.118.151；192.168.118.1；192.168.118.150

Set：

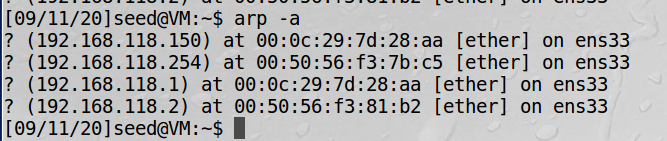
Task1A:

先查看A的arp表：



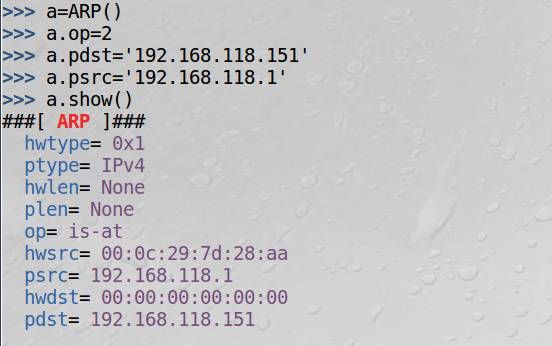
主机M将src地址改成B的地址，将数据包发送，

A将错把请求来源当成B，并且更改B的MAC地址。

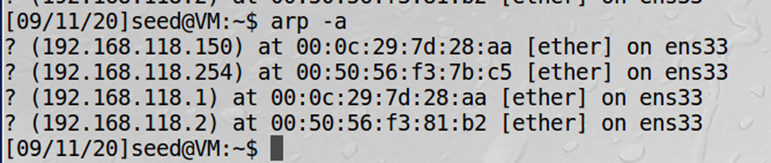


Task1B：

刷新去掉上面的攻击，再发送如下arp报文：

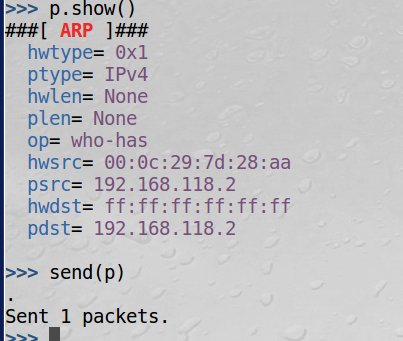


这时A的arp表同样被攻击成功。

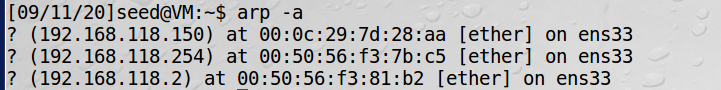


Task1C:

发送如下arp包



攻击没有实现。



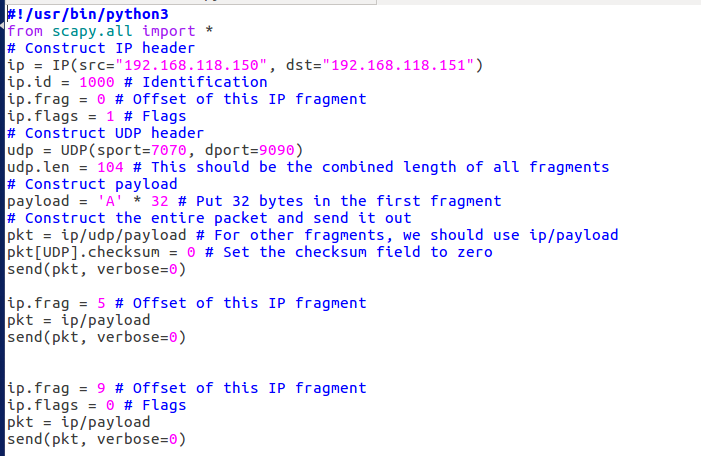
**IP/ICMP Attacks Lab**

Task1：IP Fragmentation

Task1.a: Conducting IP Fragmentation

如图所示构造数据包。

需要注意ip.frag分别为0、5、9（相隔四字节），且前俩段数据ip.flags应当设置为1表示数据未传输完毕。总长度为32\*3+头部8=104字节。

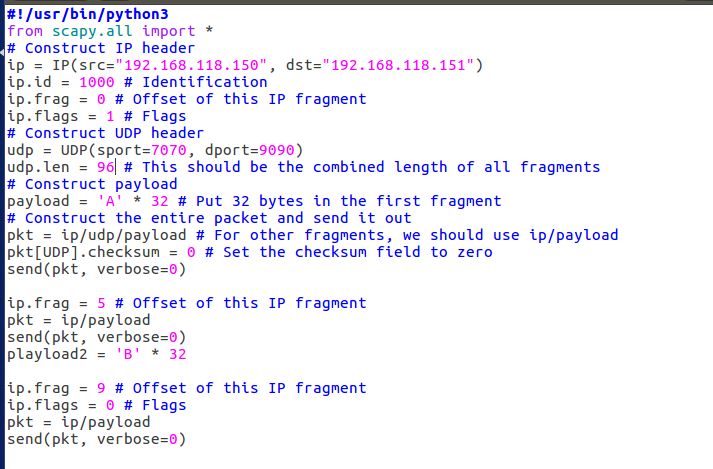


观察wireshark：成功发送长为96字节的数据。





Task1.b: IP Fragments with Overlapping Contents

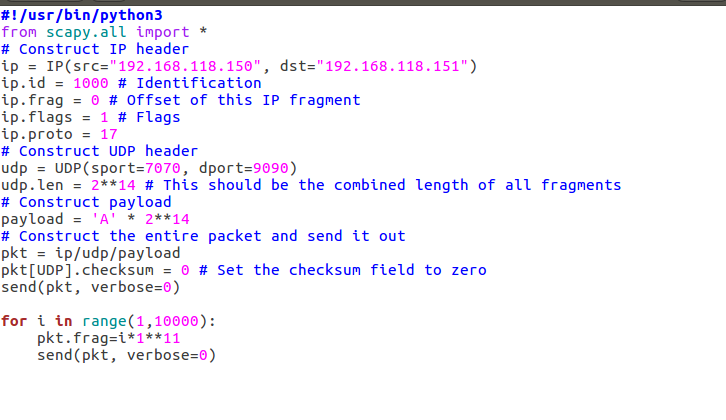


实际是让分片重合，将第二段数据改成B，观察wireshark，可以发现第二个包的数据被覆盖而不是第一个包。

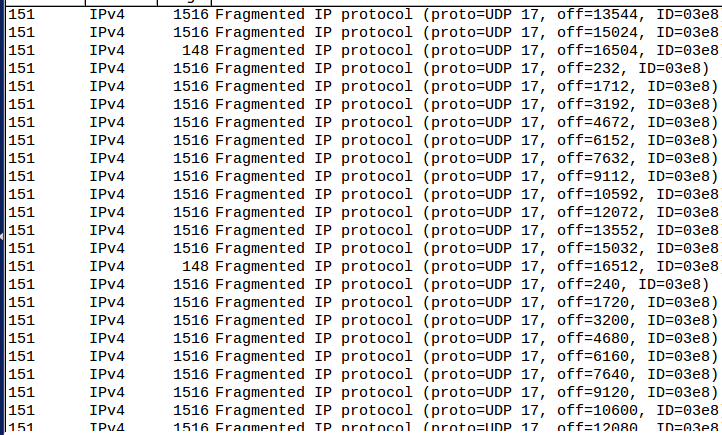
而交换发送顺序与上述情况一致，发送的顺序不会影响覆盖结果。IP报文会在接受全部数据后重组。

Task1.c: Sending a Super-Large Packet

实现该攻击程序如图所示：

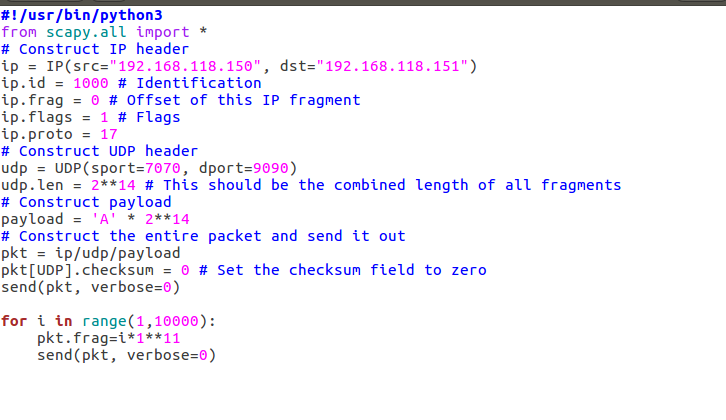


而在被攻击的主机上观察wireshark，在不断接受报文，无法正常与其他设备通信：

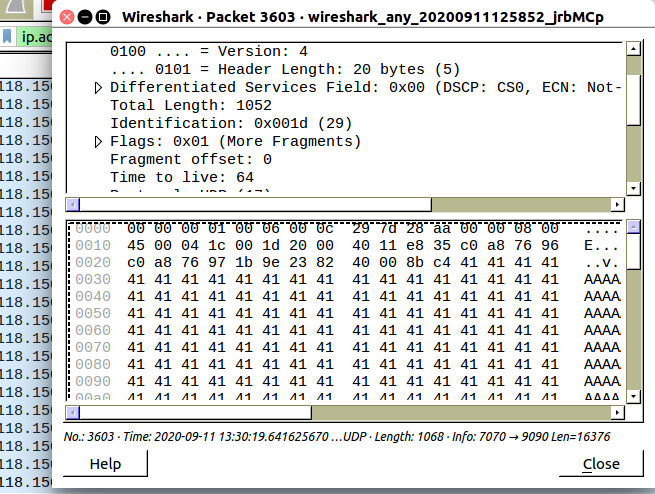


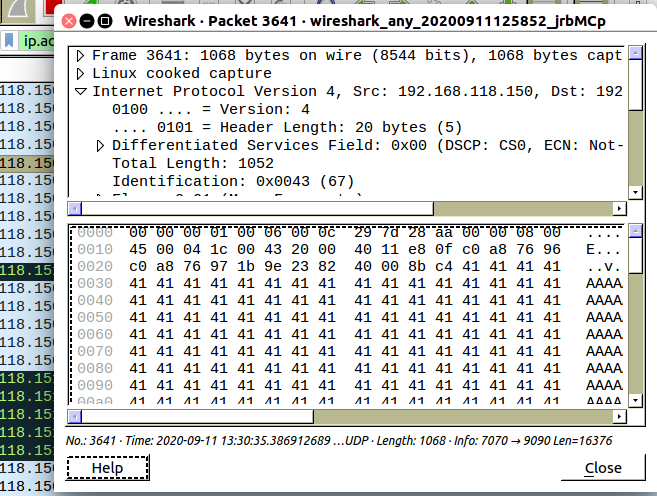
Task1.d: Sending Incomplete IP Packet

攻击程序如下：



此时观察被攻击主机wireshark：不断接受报文且id不同





再观察一下负载：（无明显异常）

