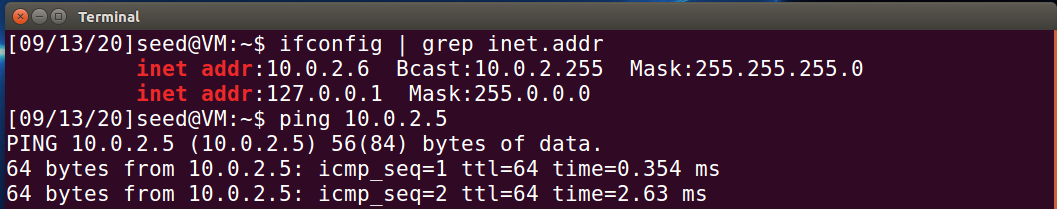
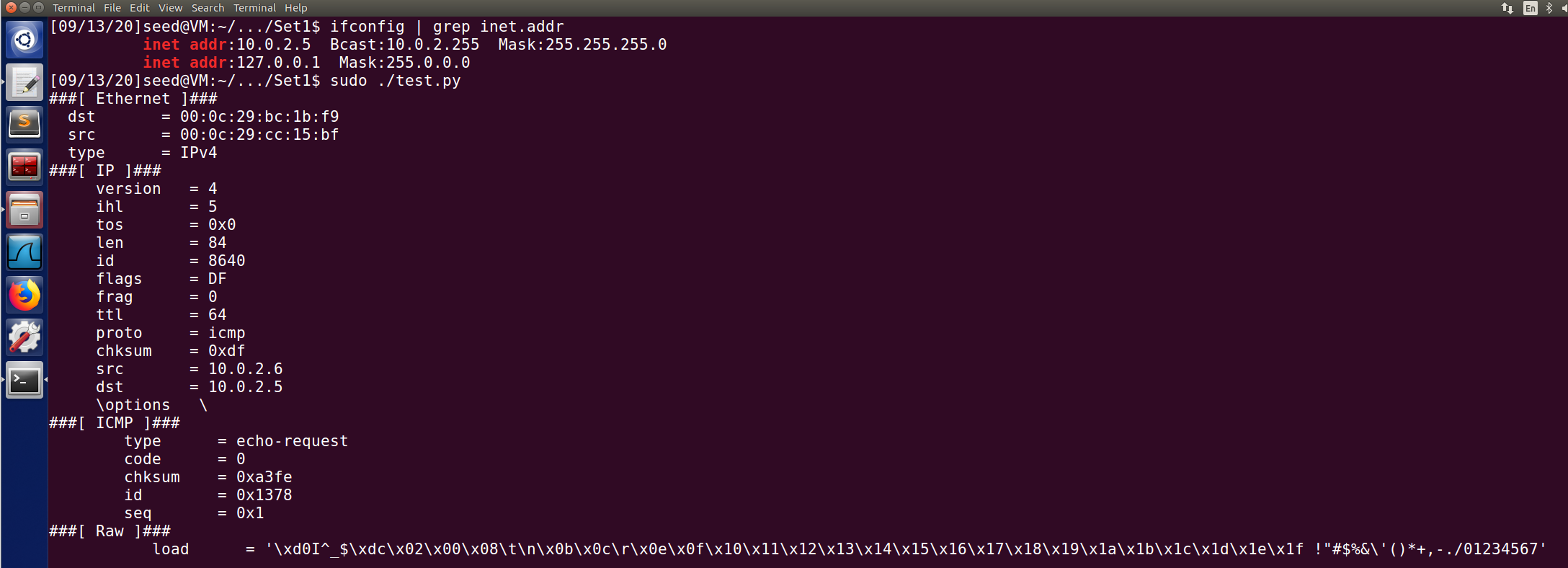
Packet Sniffing and Spoofing Lab

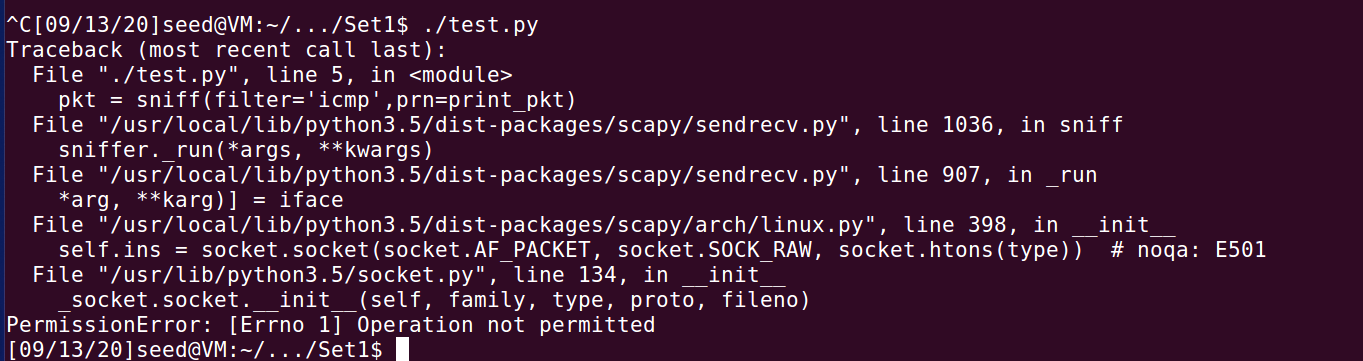
# Task1.1A

在10.0.2.5主机上root权限运行代码，然后在10.0.2.6主机上ping 10.0.2.5:





可以看到抓到了ICMP报文。再用普通用户身份运行代码：

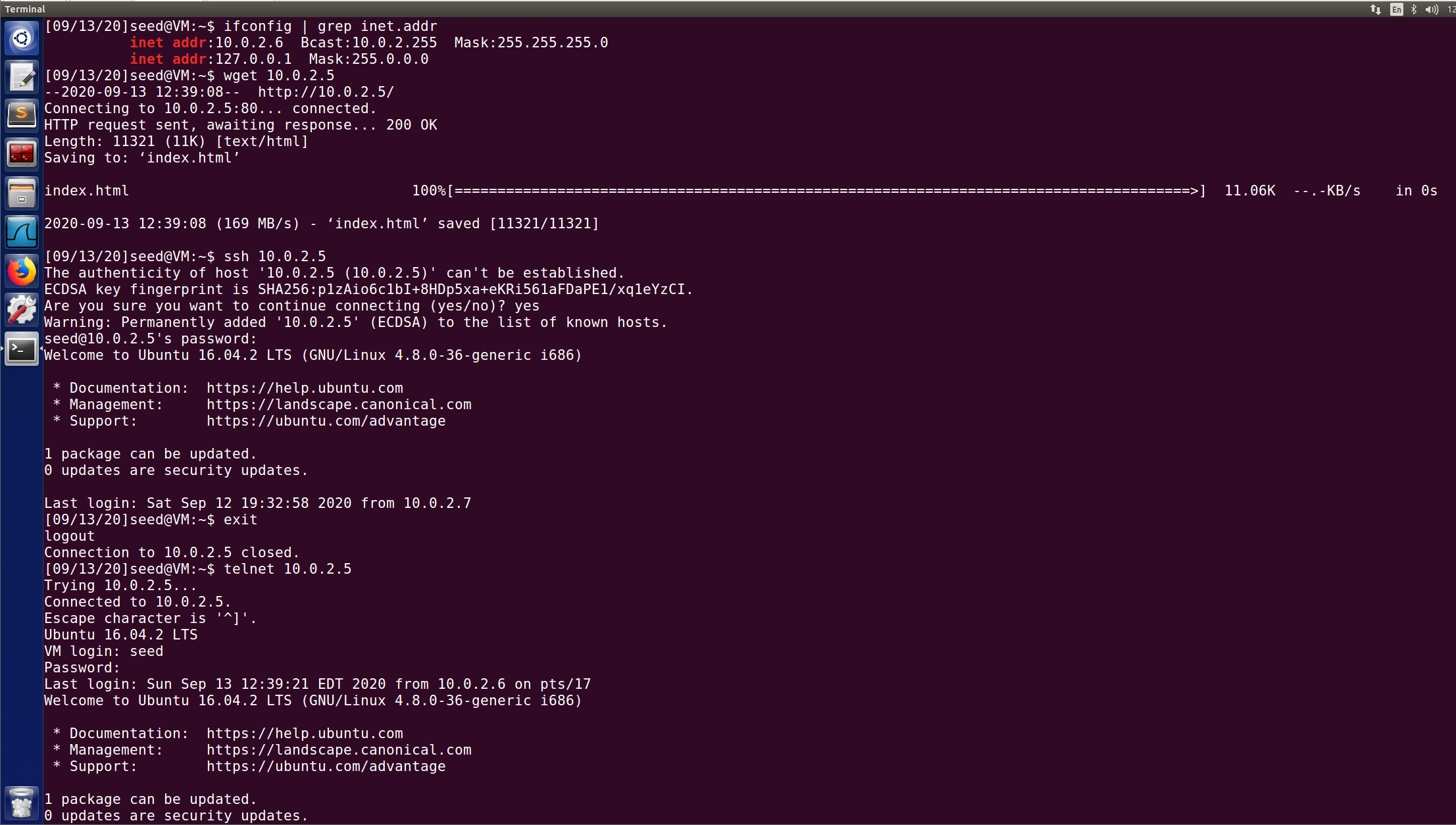


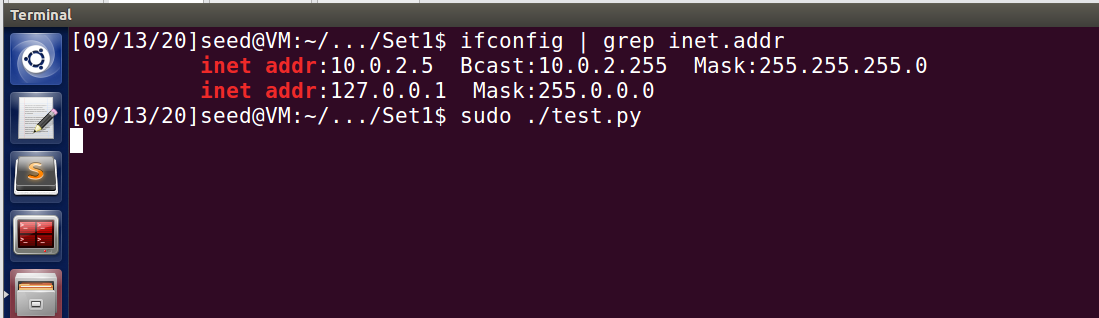
权限不足，无法运行

# Task1.1B

**捕获ICMP报文：**

1.1A的代码无需修改即可，下面我们在10.0.2.6上分别向10.0.2.5发起HTTP请求、telnet连接和ssh连接，查看是否只捕获ICMP报文：





并没有捕获，说明代码没问题。

**捕获来自特定IP地址（选为10.0.2.6）的，目标端口是23的TCP报文：**

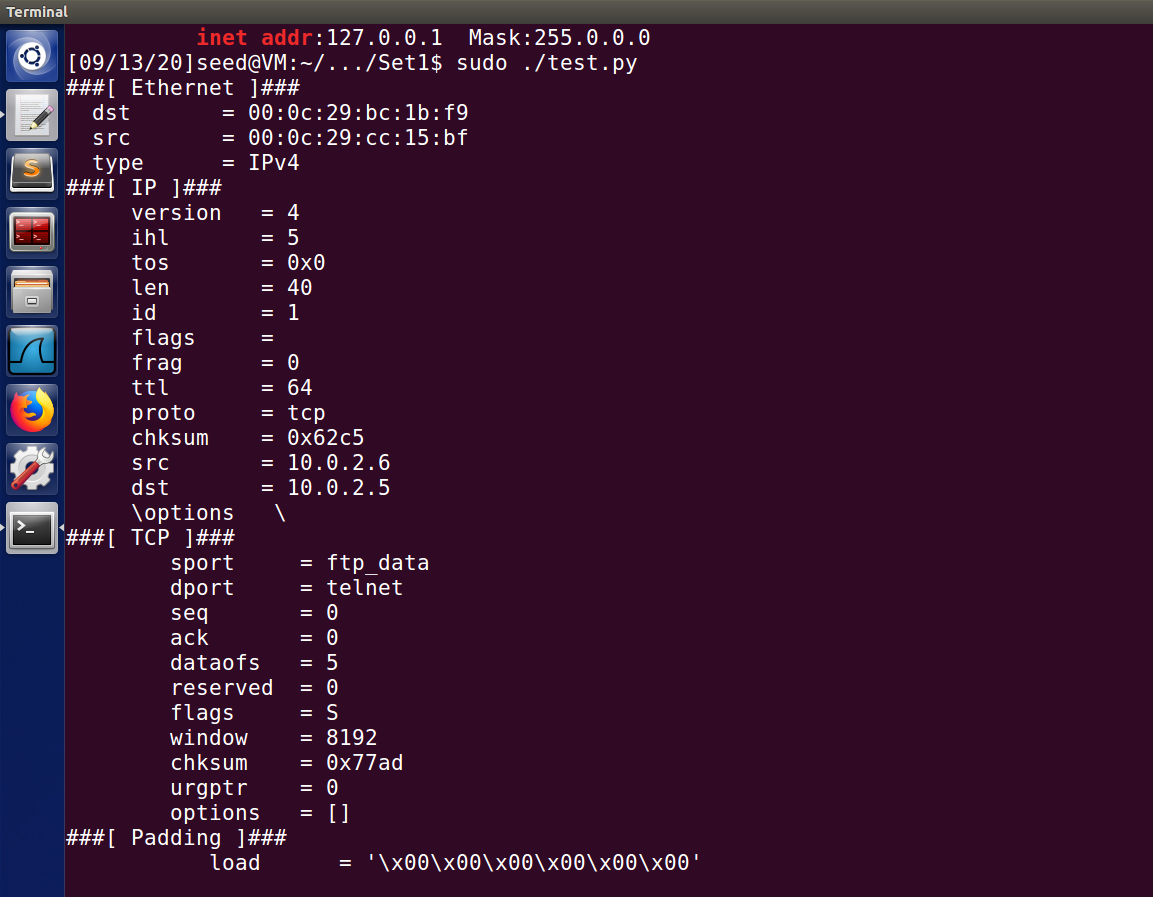
代码修改如下：



然后在10.0.2.6上向10.0.2.5的23端口发起连接:



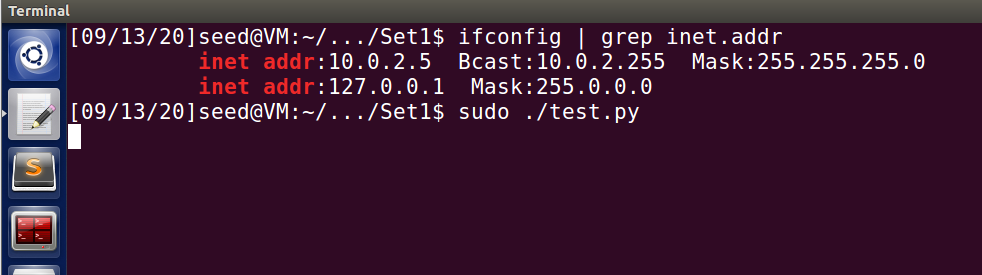
在10.0.2.5上：



发现捕获了报文，然后我们尝试改变IP源地址(src)、目标端口(dport)，再发送：



在10.0.2.5上：



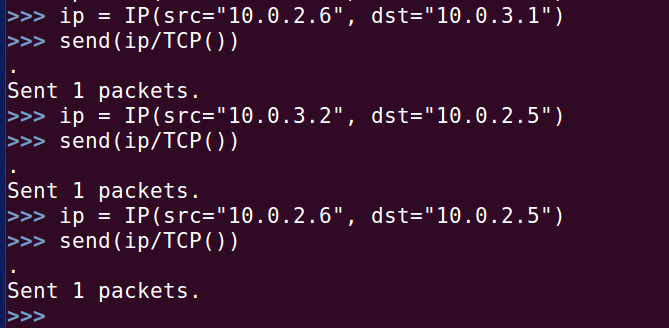
没有捕获任何报文，成功。

**捕获来自/去往特定子网（选为10.0.3.0/24）的报文：**

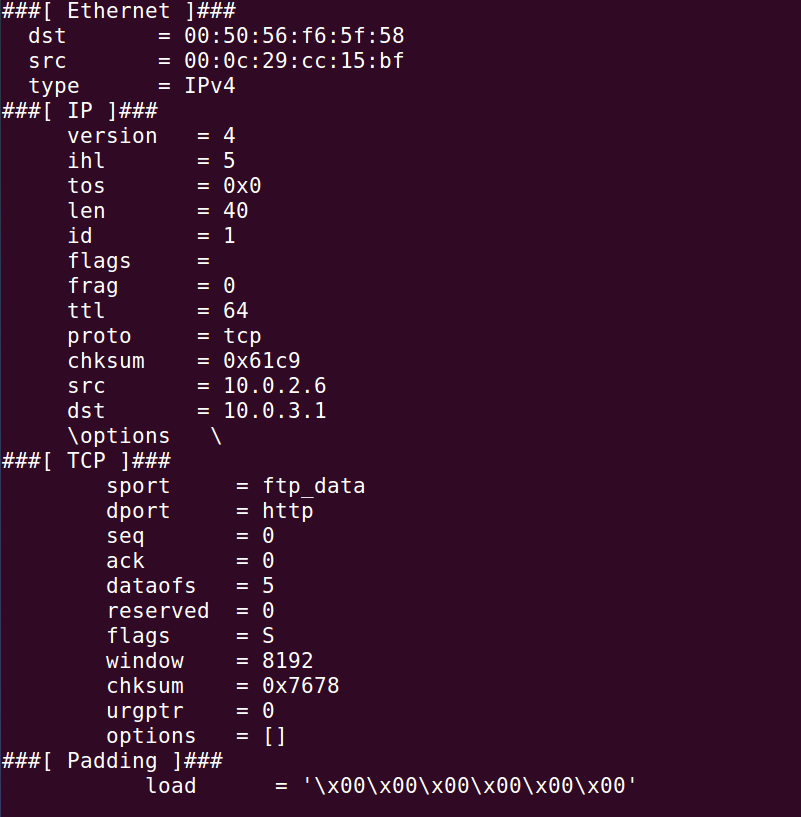
代码修改为：

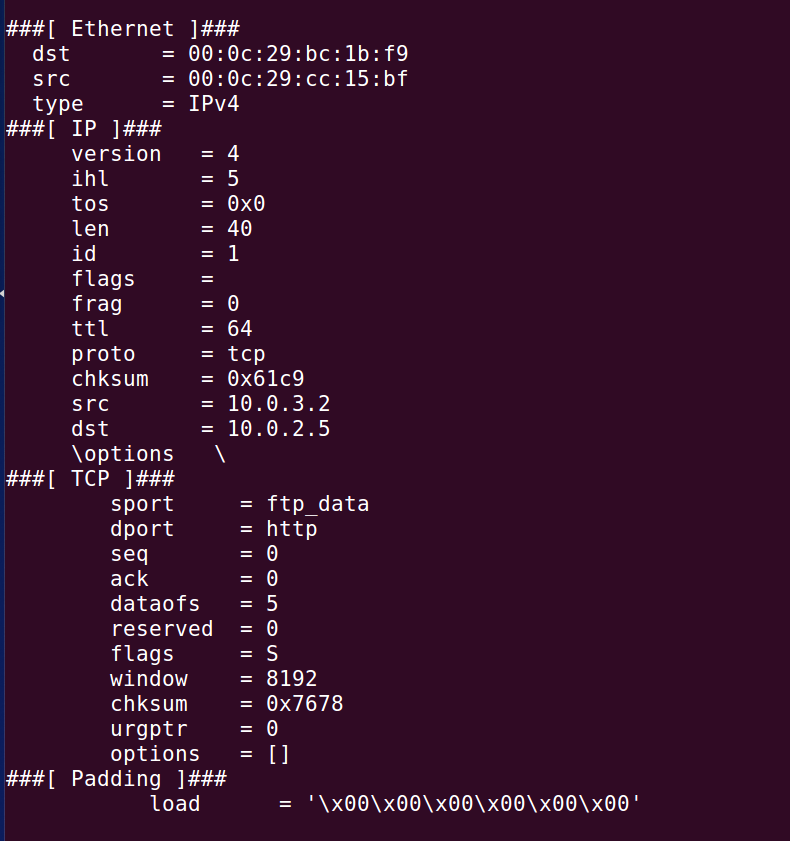


然后运行，在10.0.2.6上构造相关的报文：



在10.0.2.5上查看：

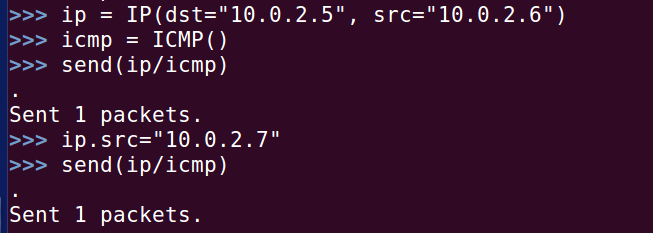


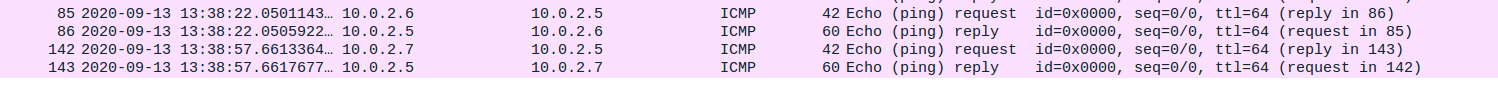


捕获了发送/接收方是10.0.3.0/24子网的报文，没有捕获到其他报文，成功。

# Task1.2

在10.0.2.6上模拟10.0.2.5向10.0.2.6发送ICMP回复请求报文，并通过wireshark抓包：

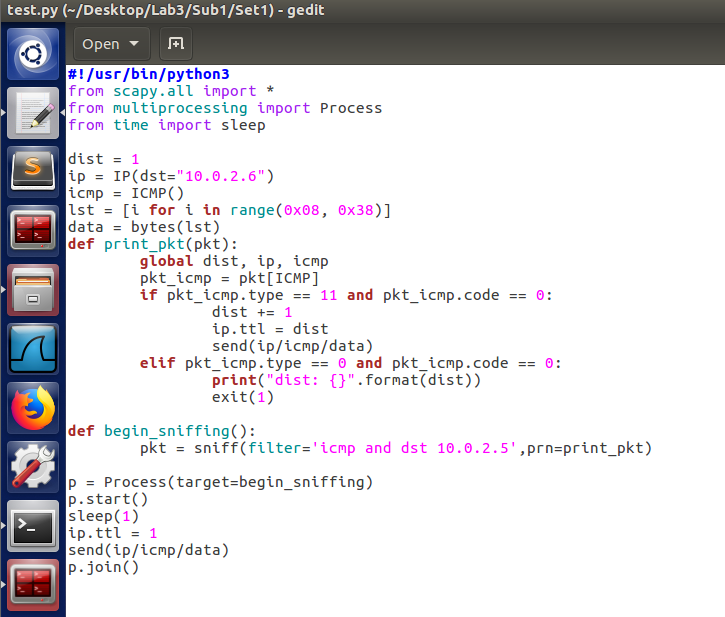




成功伪装发送了ICMP报文

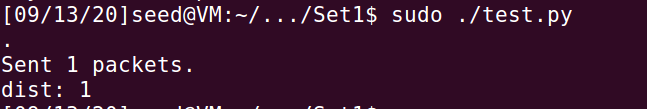
# Task1.3

代码：



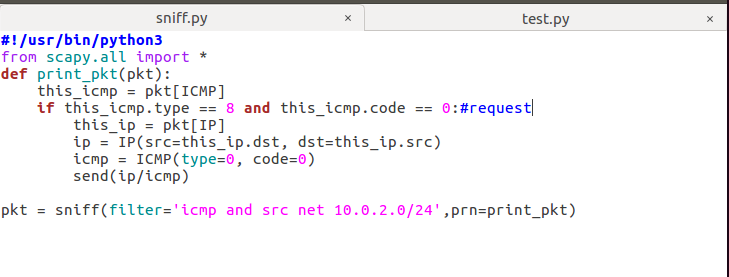
先开一个进程进行ICMP报文监听，然后在另一个进程里，设置TTL为1去发送ICMP报文，开始这个流程，监听到错误，则距离+1，ttl+1，重发报文，监听到回复，就中止，返回距离

效果：



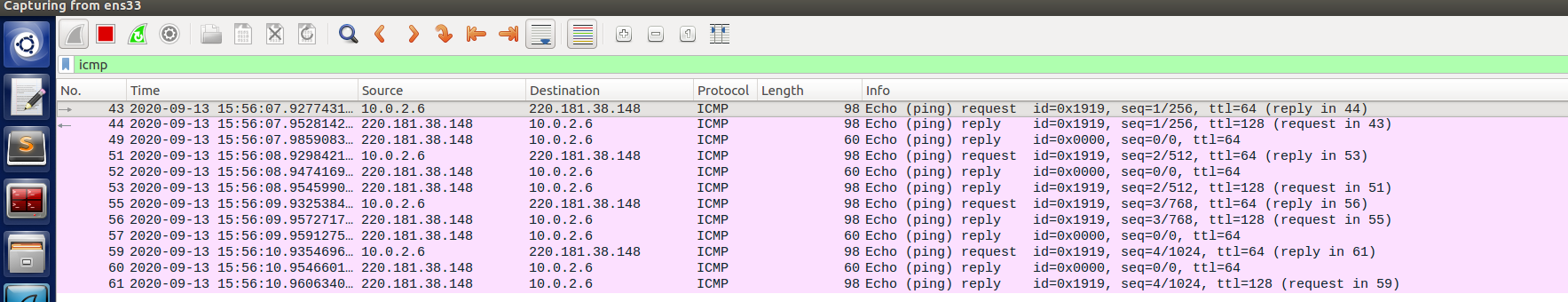
# Task1.4

代码：



监听局域网内主机发出的ICMP报文，如果是echo request，就根据报文构造回复，效果：

在10.0.2.6上ping baidu.com，发4个报文，然后看wireshark：

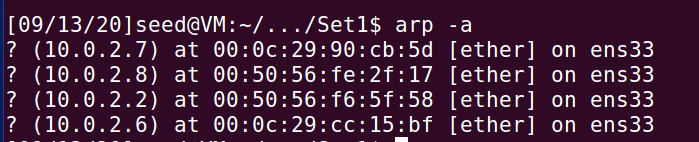


可以看到每次request都有2个reply，成功！

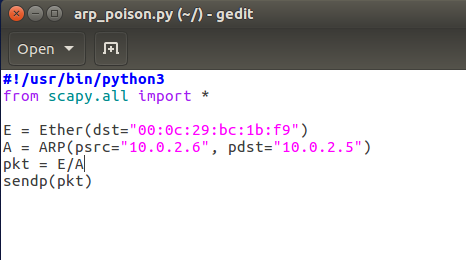
ARP Cache Poisoning Attack Lab

# Task1A

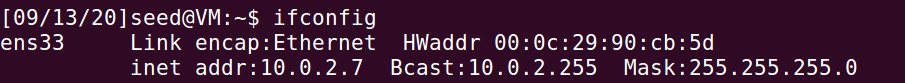
之前：

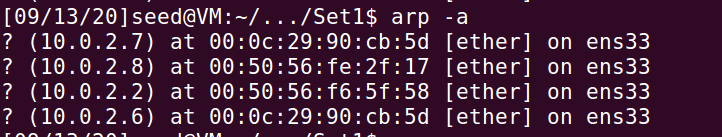


构造报文：



之后：

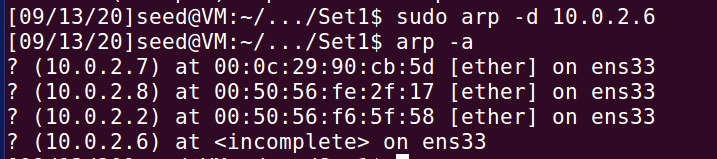




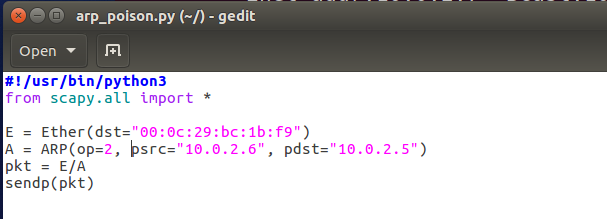
可以看到10.0.2.6的IP重新对应到了10.0.2.7主机的MAC地址，攻击成功

# Task1B

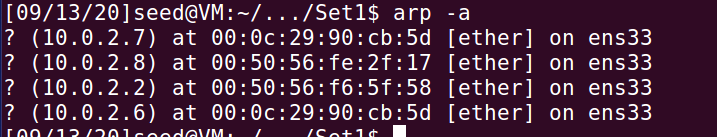
删除10.0.2.5主机上10.0.2.6对应的ARP缓存：



然后构造报文：



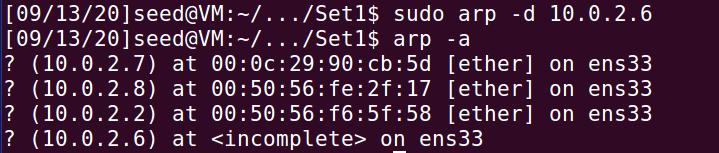
再看ARP缓存：



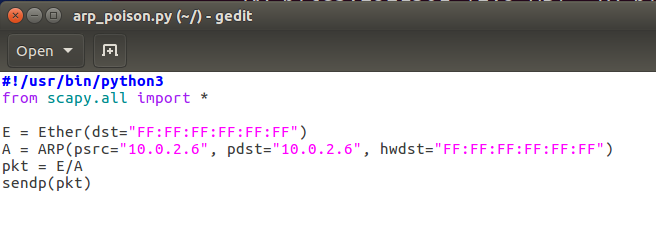
可以看到10.0.2.6对应的MAC地址变成了10.0.2.7的MAC地址，成功

# Task1C

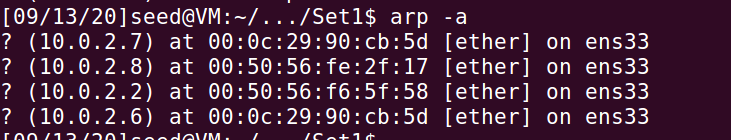
清除ARP缓存：



然后构造报文：



然后再看ARP缓存：

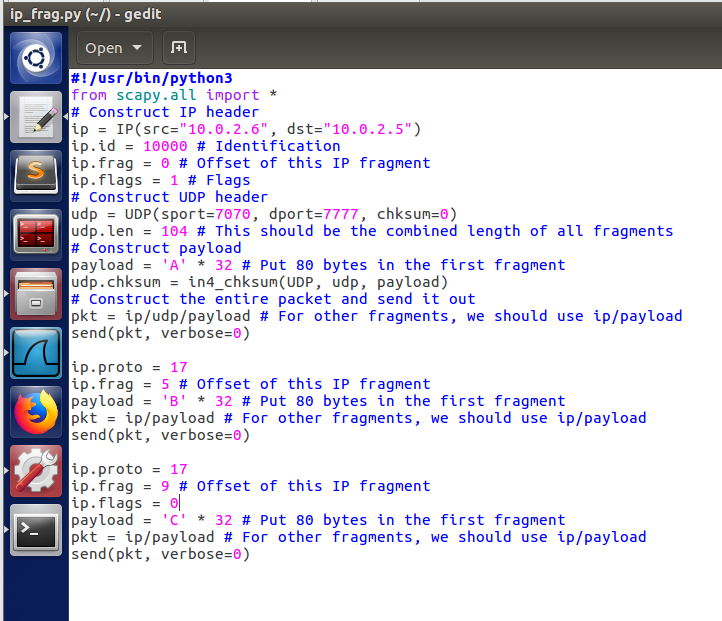


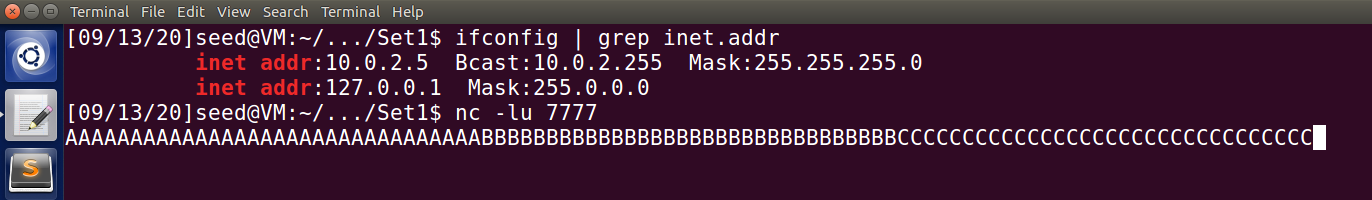
攻击成功！

IP/ICMP Attacks Lab

# Task1a

发送分段报文的程序如下：



然后看UDP服务器：  


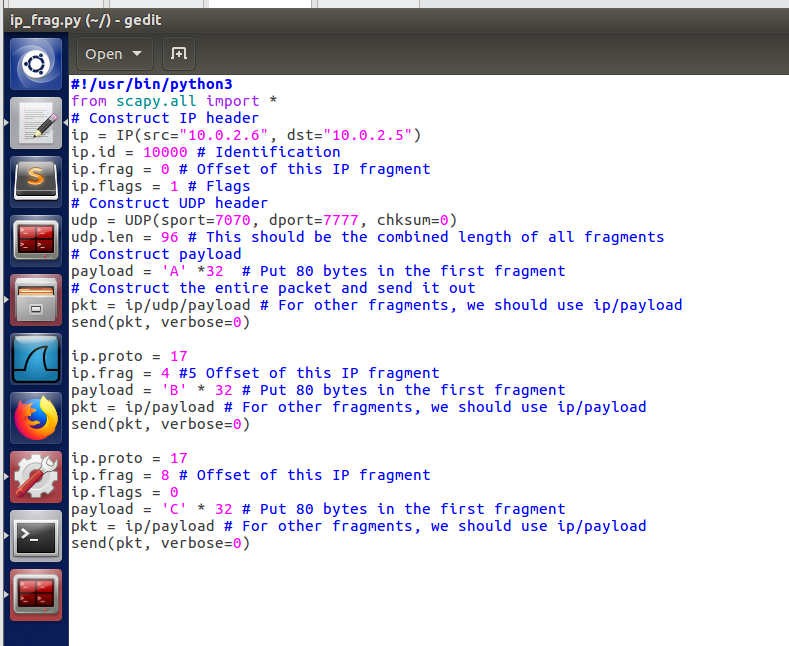
收到了消息，成功！

# Task1b

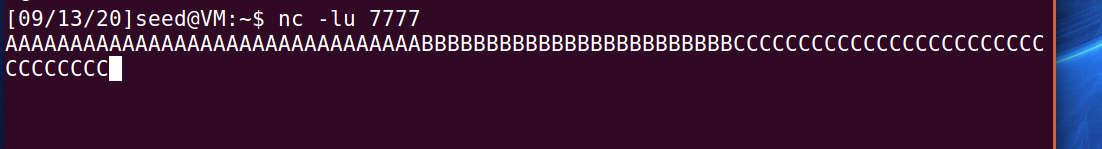
## 1

设置K=8

先发第一个:

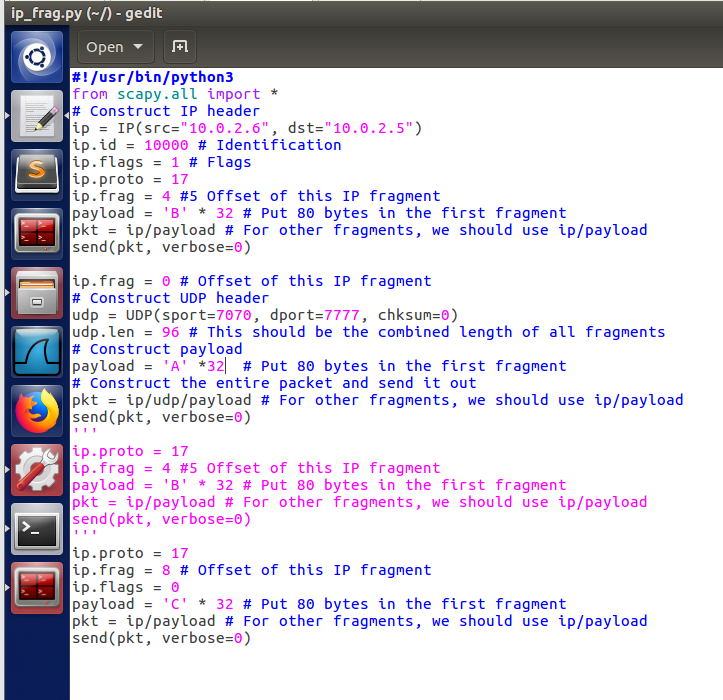


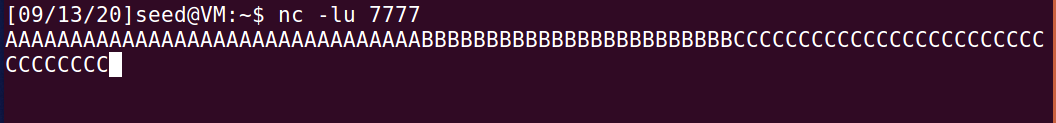
UDP服务器端：



可以看到第二片中，重合的部分被抛弃了

如果先发第二个：

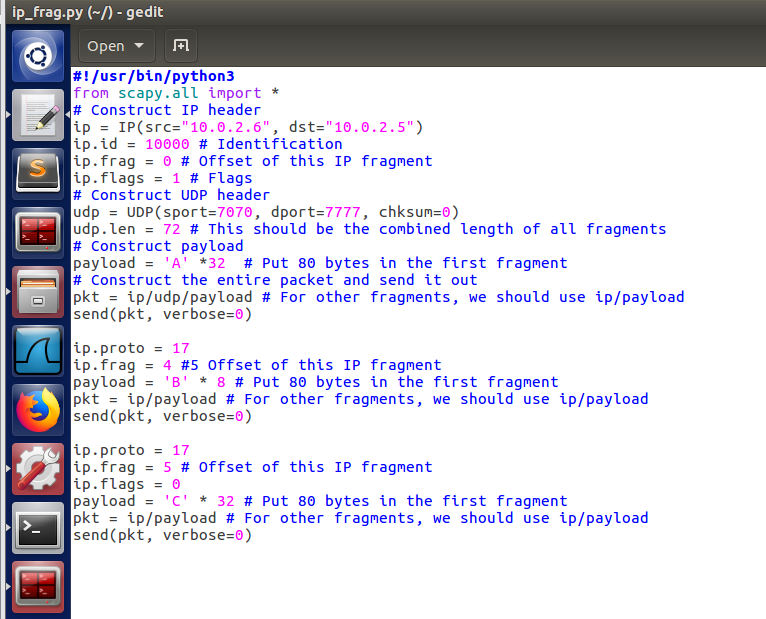


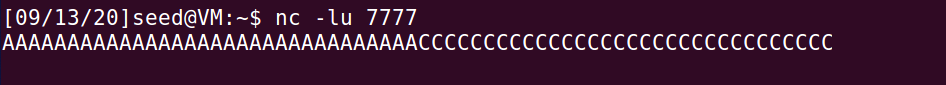


效果是一样的

## 2

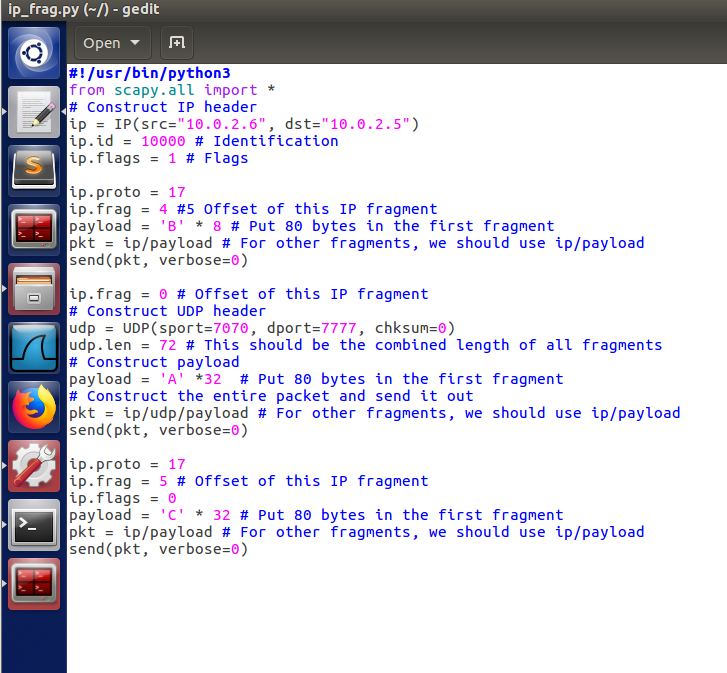
先发第一个：

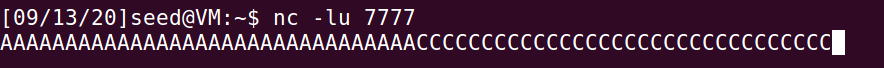




第二片被完全抛弃了

先发第二片：

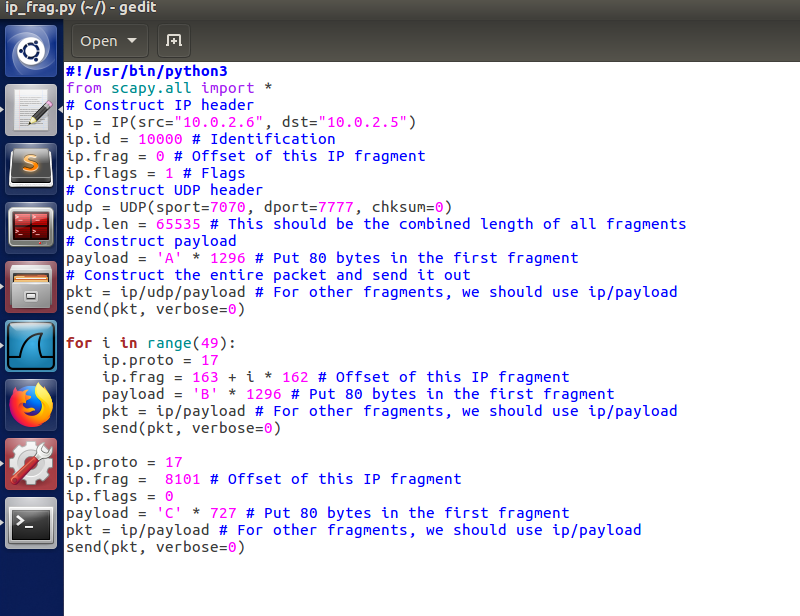




结果还是一样的

# Task1c

程序：

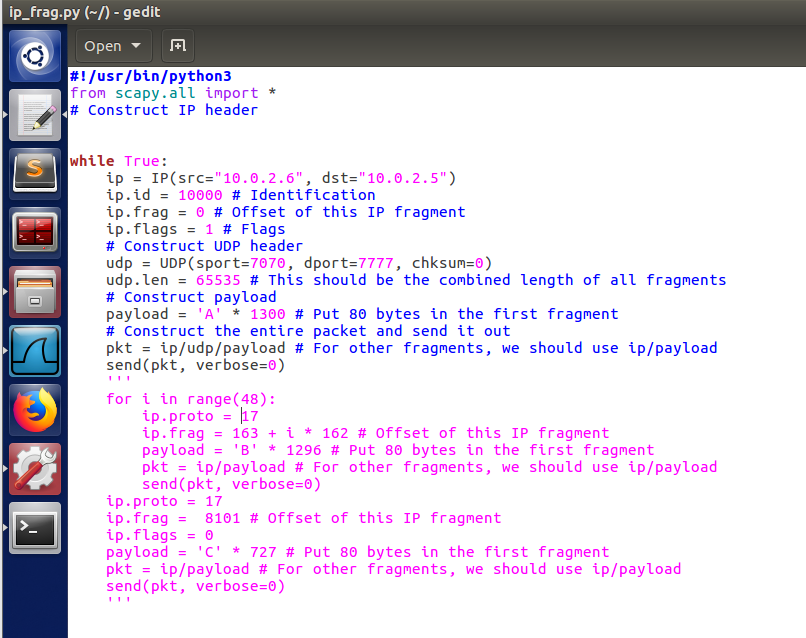


服务器端，使用dmesg查看内核消息：



可以看到收到了oversize的IP包，但是并没有感觉到什么异样（比如崩溃）？UDP服务器也没收到东西

# Task1d

程序：

但是10.0.2.5一直没有什么异样，可能是速度不够快？然后我又用netwox 74 -i 10.0.2.5对10.0.2.5发送大量的不完整分段也并没有反应。