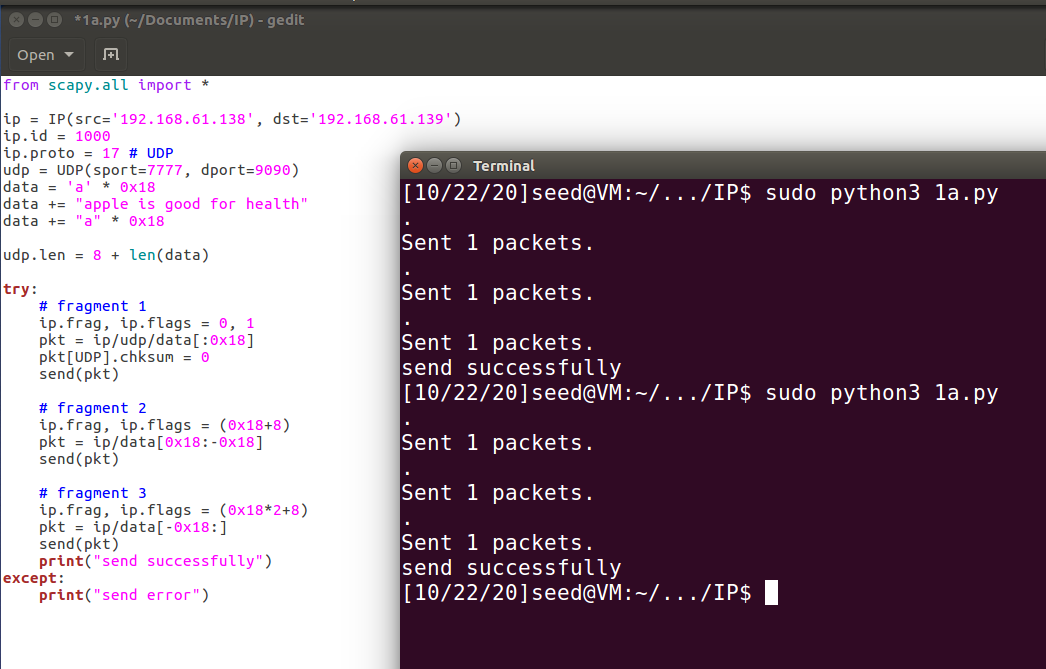
IP/ICMP Attacks Lab Report

管箫 18307130012 2018级信息安全

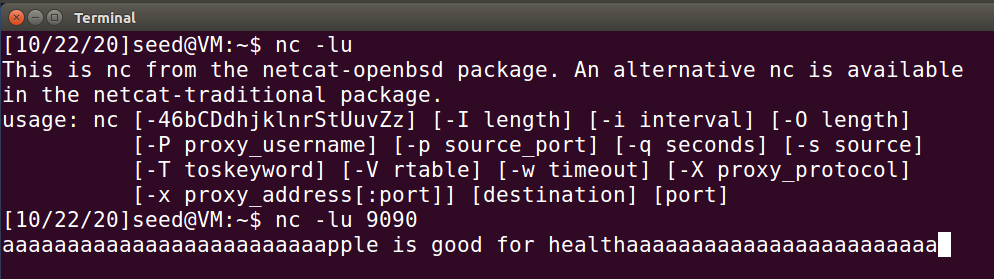
**一、Task Set 1: IP Fragmentation**

1、Task 1.a: Conducting IP Fragmentation

在主机A上构造数据包：



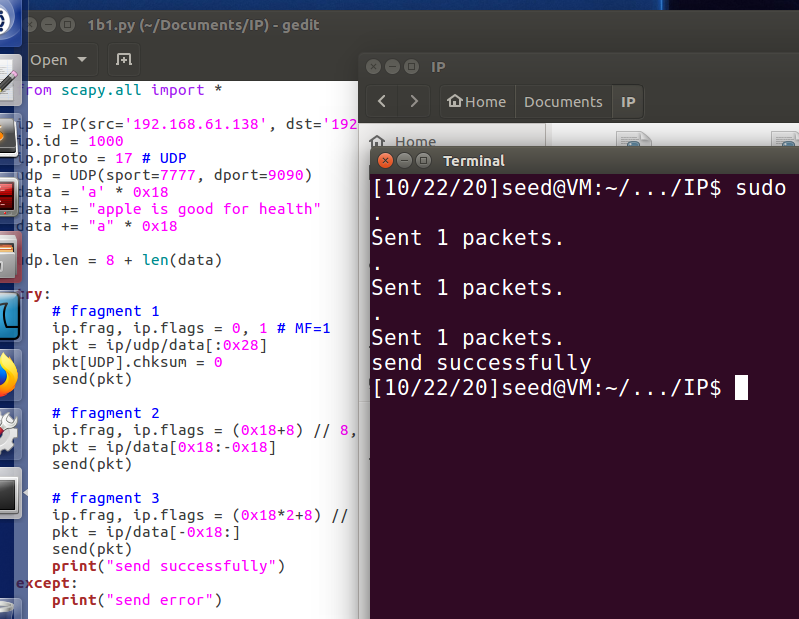
在主机B上观测到正常接收：



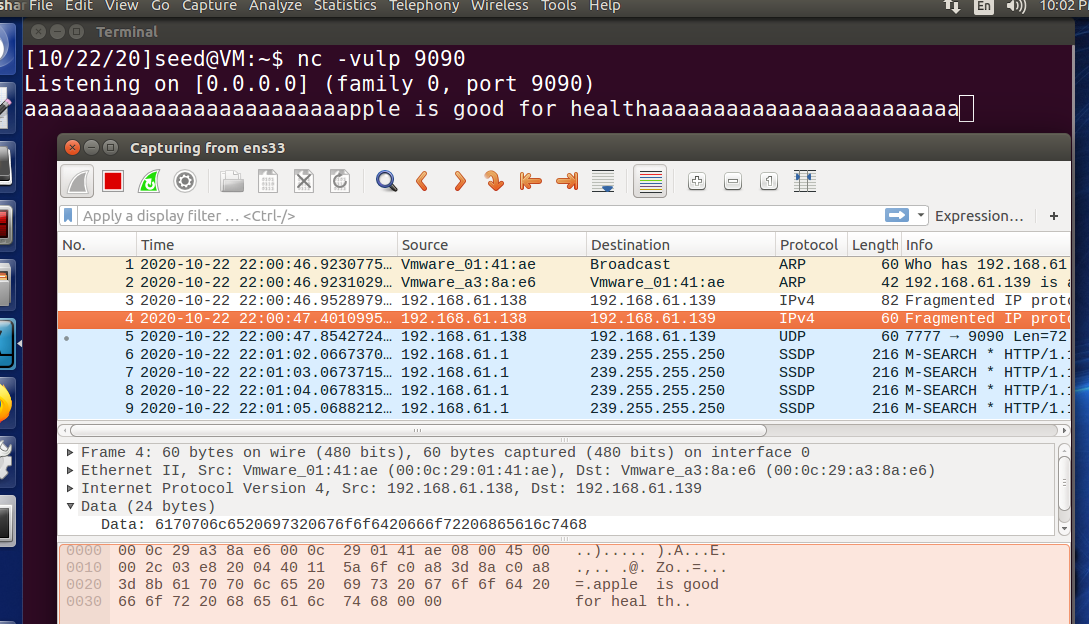
2、Task 1.b: IP Fragments with Overlapping Contents

①第一片的后K字节数据应与第二片中的前K字节数据具有相同的偏移量

取偏移量为0x10

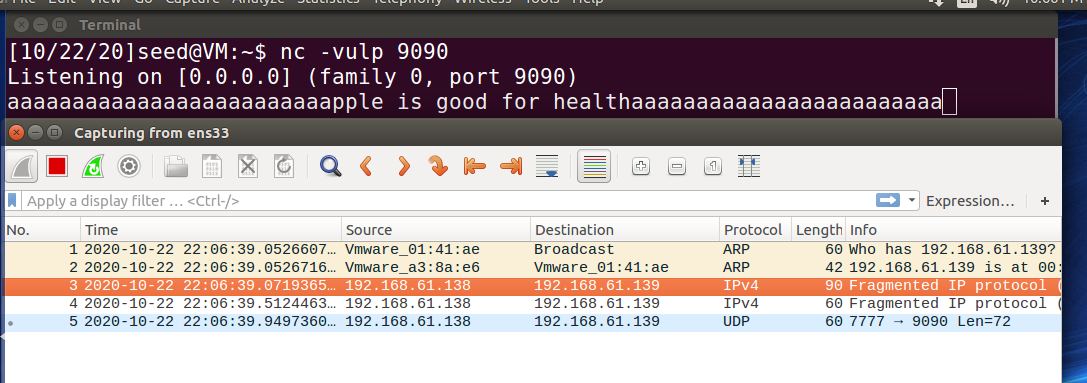


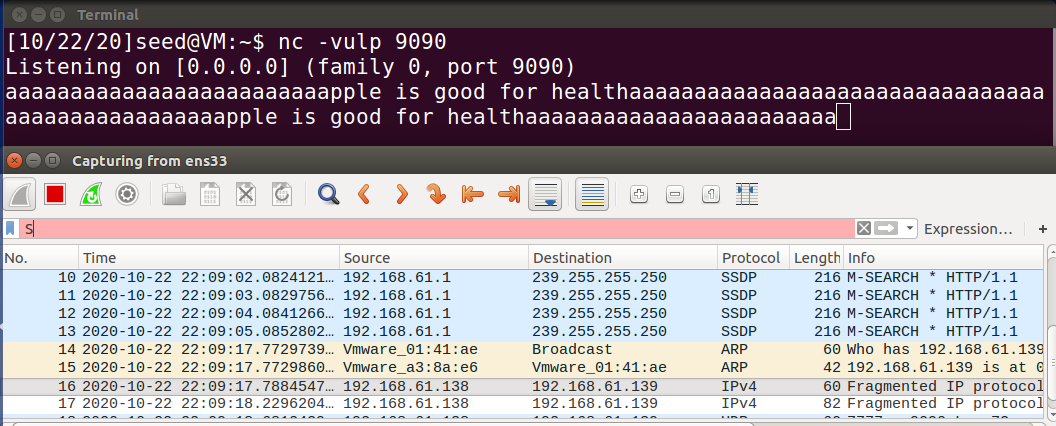
观察到nc正确回显，wireshark正确捕获了三个包。

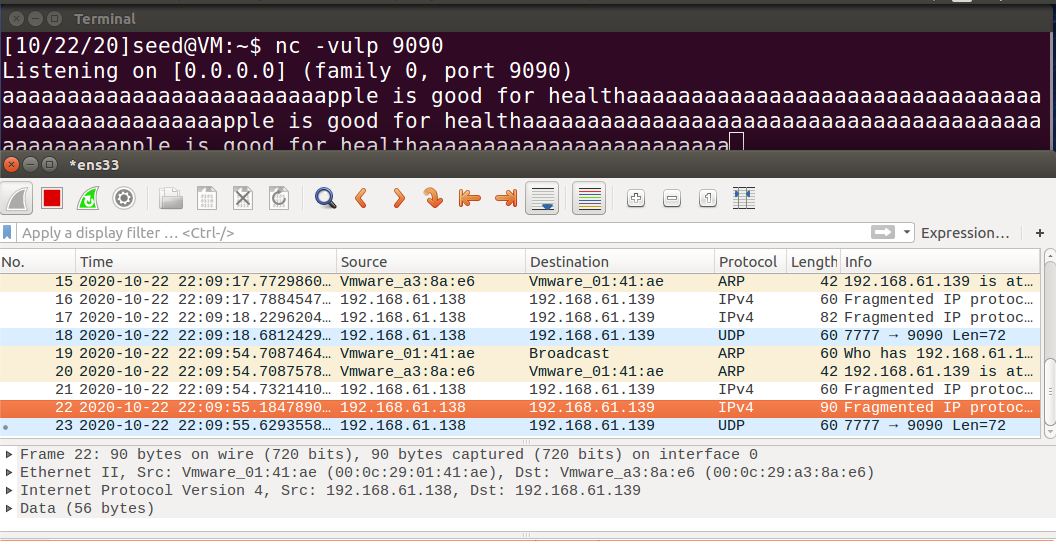


②第一分片完全包含第二分片

仍然正确回显，wireshark捕获到了三个数据包。



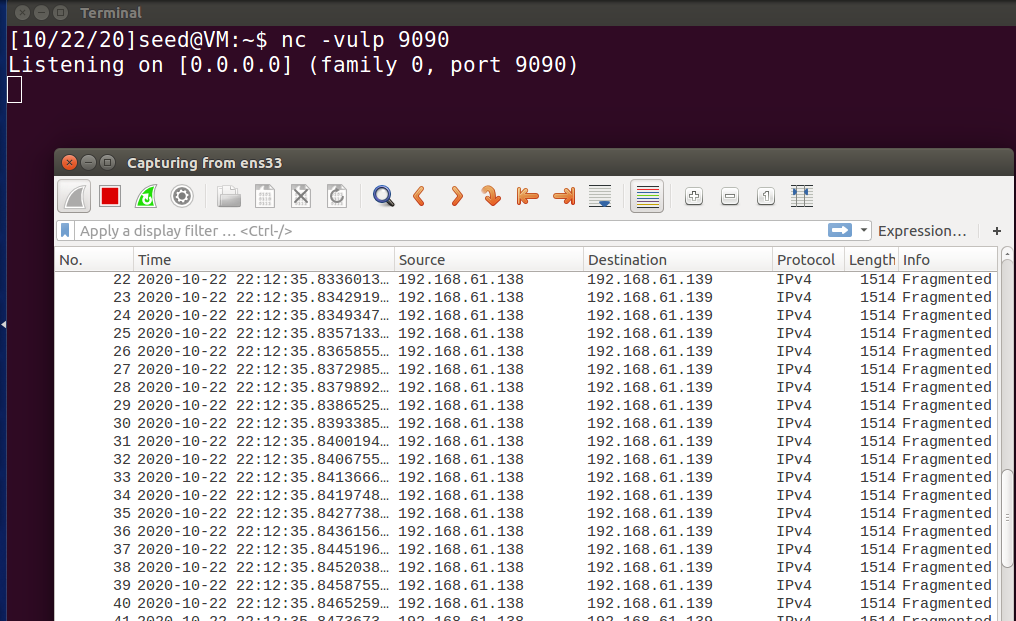
③同①，但第一和第二个发送顺序更换



观察到均正常显示

3、Task 1.c: Sending a Super-Large Packet

我们产生一个大小超过上限65535的包。

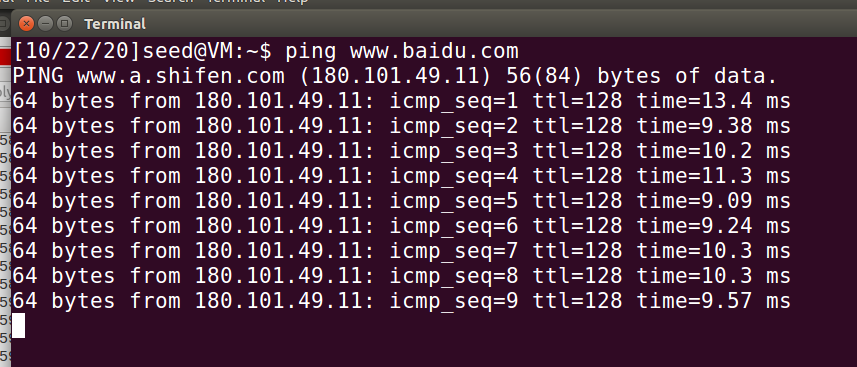


观察到wireshark捕获了大量分片数据包，但nc没有回显。

说明这一方式不符合nc的规则。

4、Task 1.d: Sending Incomplete IP Packet

主机A开启12个线程同时对主机B发送分片数据包。



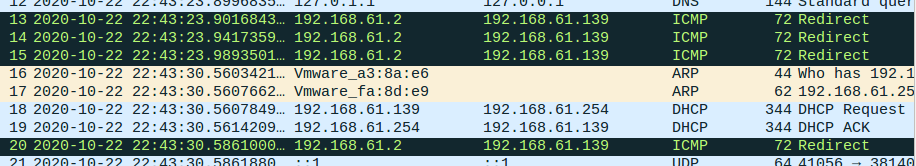
主机B收到了大量数据包，造成ping命令的延时。

未能彻底堵塞主机B的网络的可能性是攻击流量不够大，或者是配置的网络带宽和内存过大。

**二、Task Set 2: ICMP Redirect Attack**

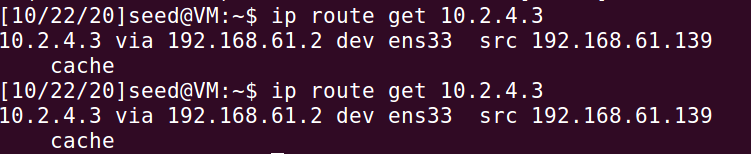
1、重定向

这里实验出现一点偏差，arp命令生成的包会被重定向，但ip route不能很好的识别重定向结果。



2、问题回答

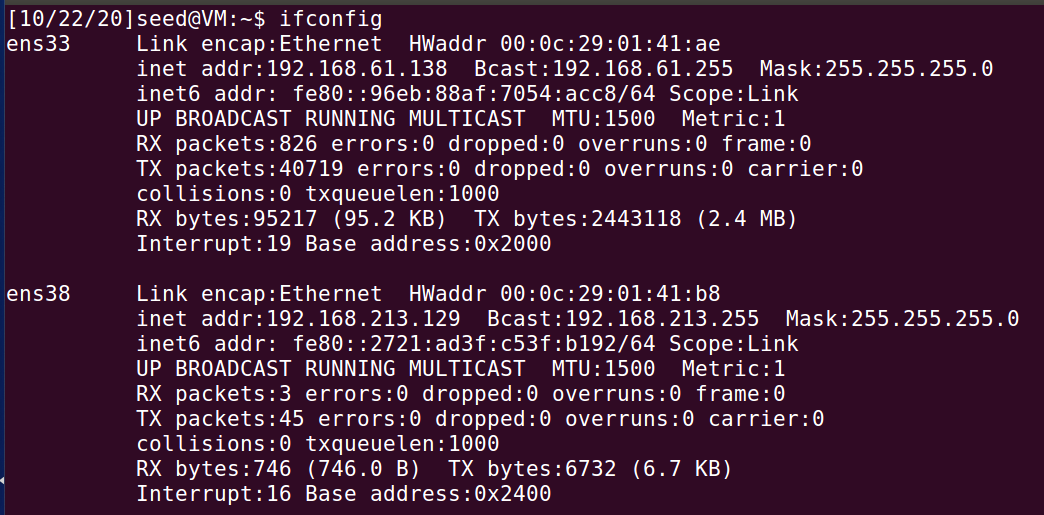
两种情况下均不发生变化，也即不可行。



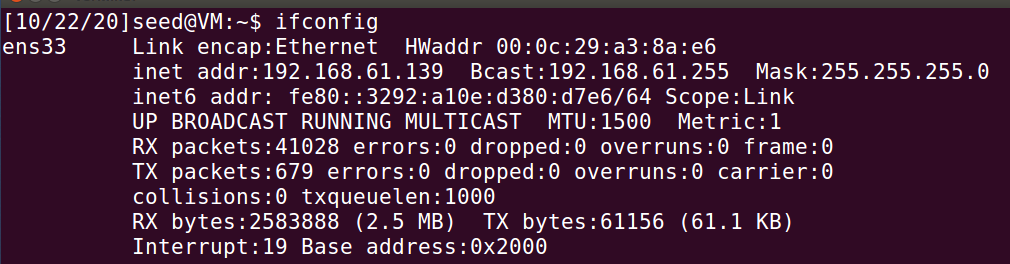
**三、Task Set 3: Routing and Reverse Path Filtering**

1、设立虚拟网络

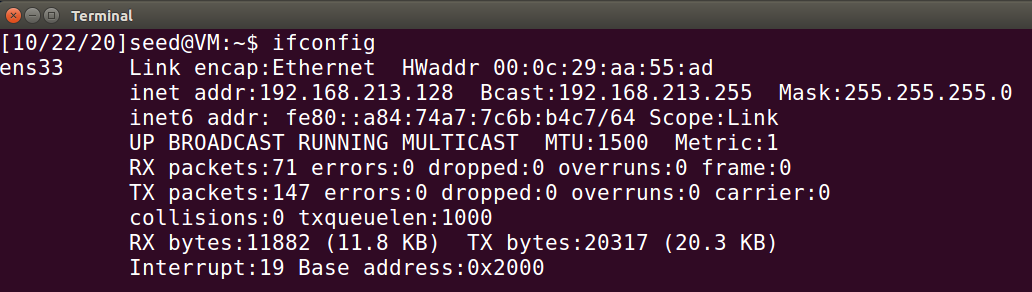
Vm R：



Vm A：

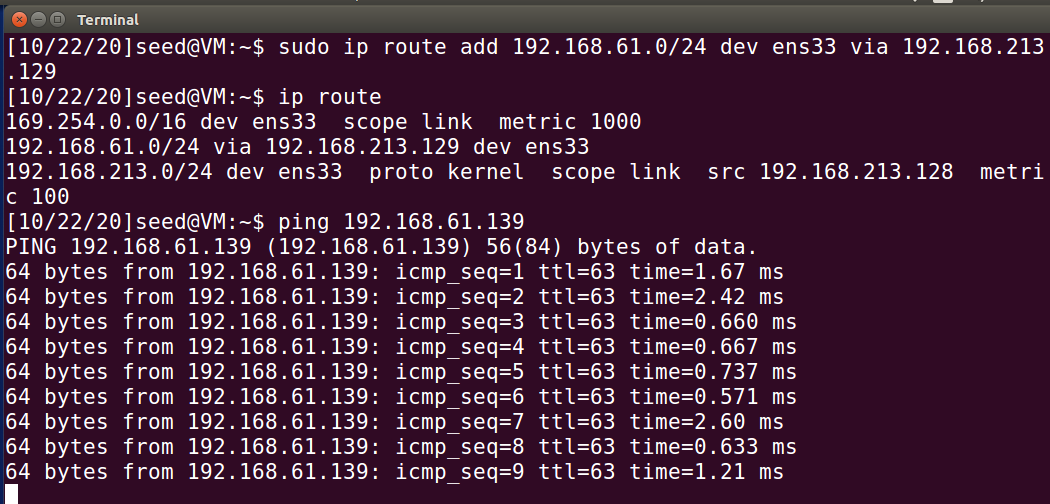


VM B：



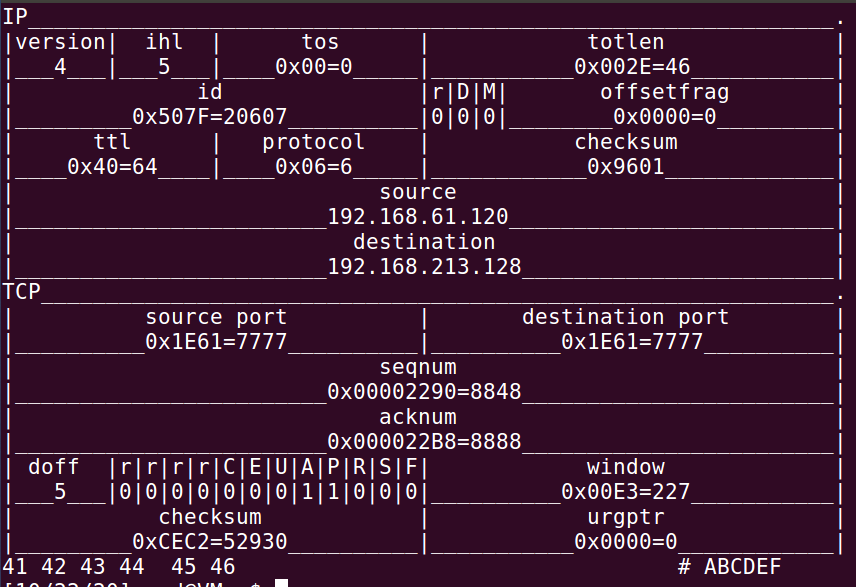
2、配置网络路径

成功ping通VM A与VM B

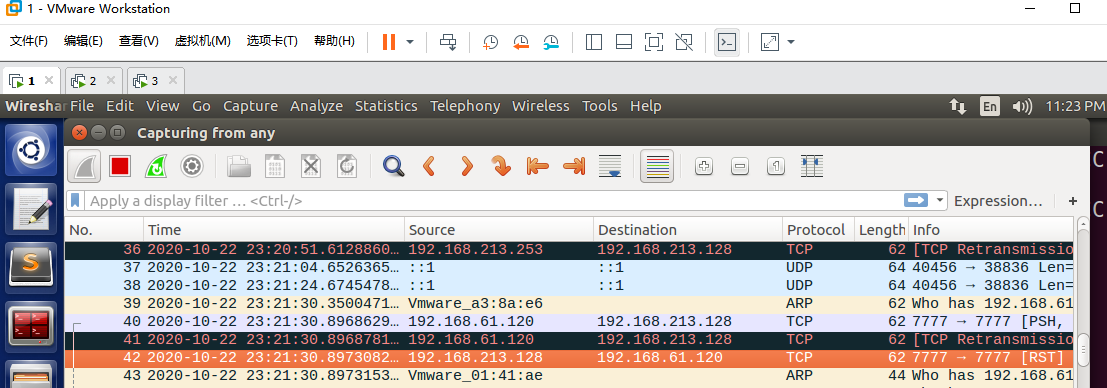


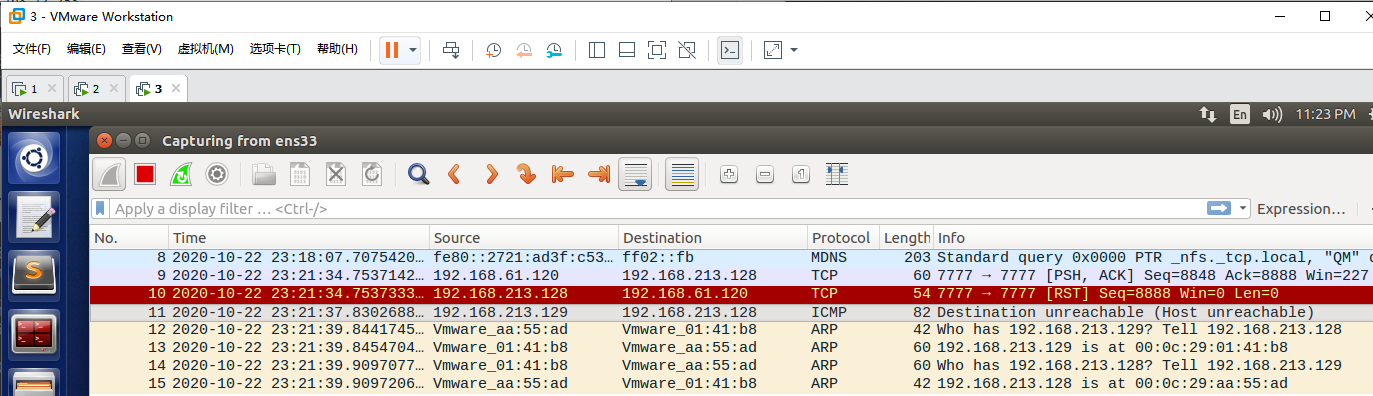
3、发起攻击

1、伪造ip在第一级局域网中

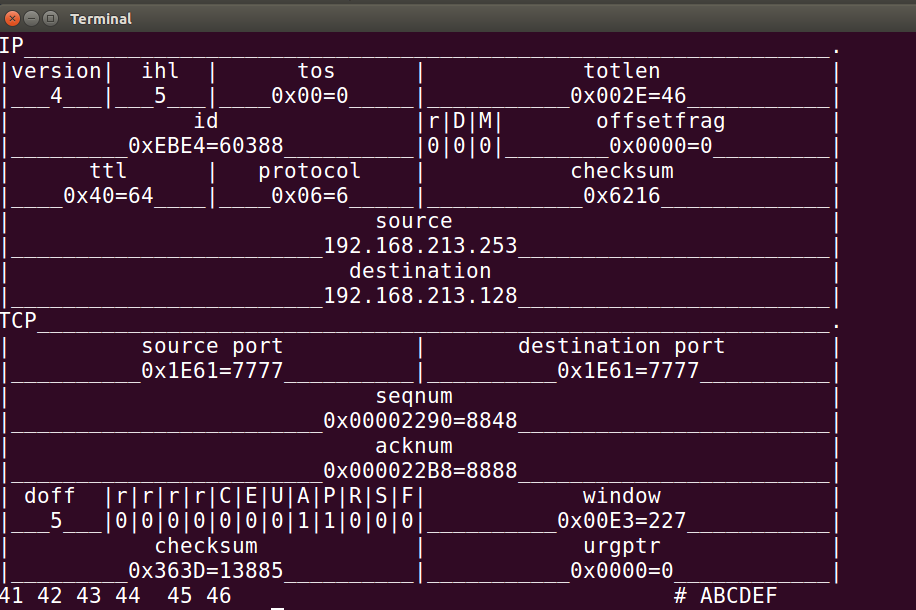


观察到主机R接收到该包，主机B接收到该包并报错

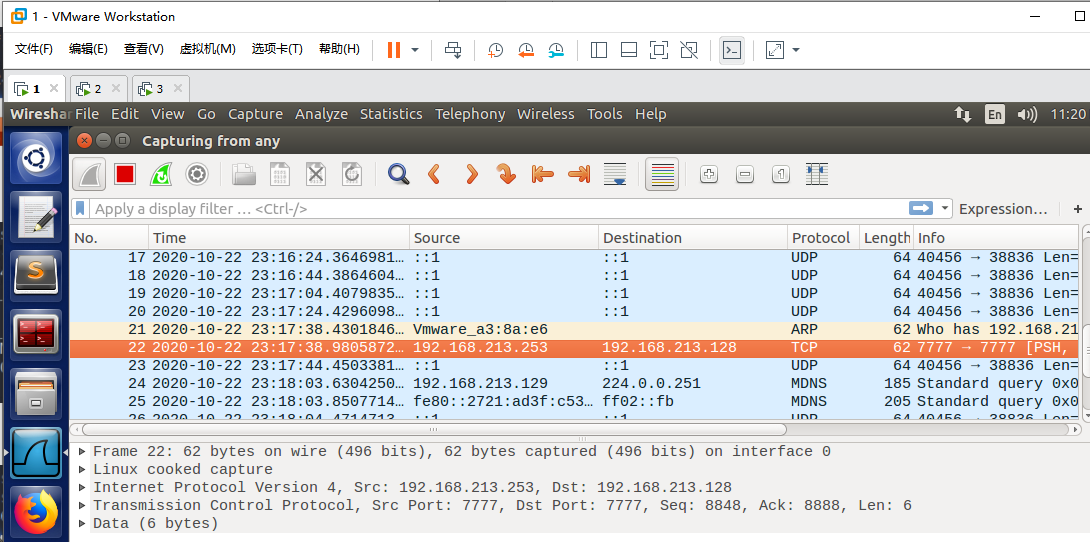




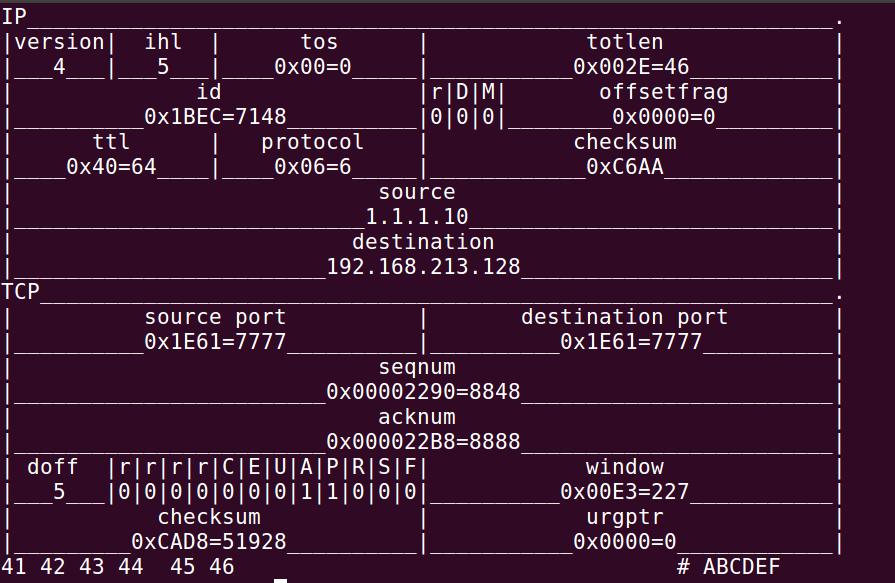
2、伪造ip在第二级局域网中



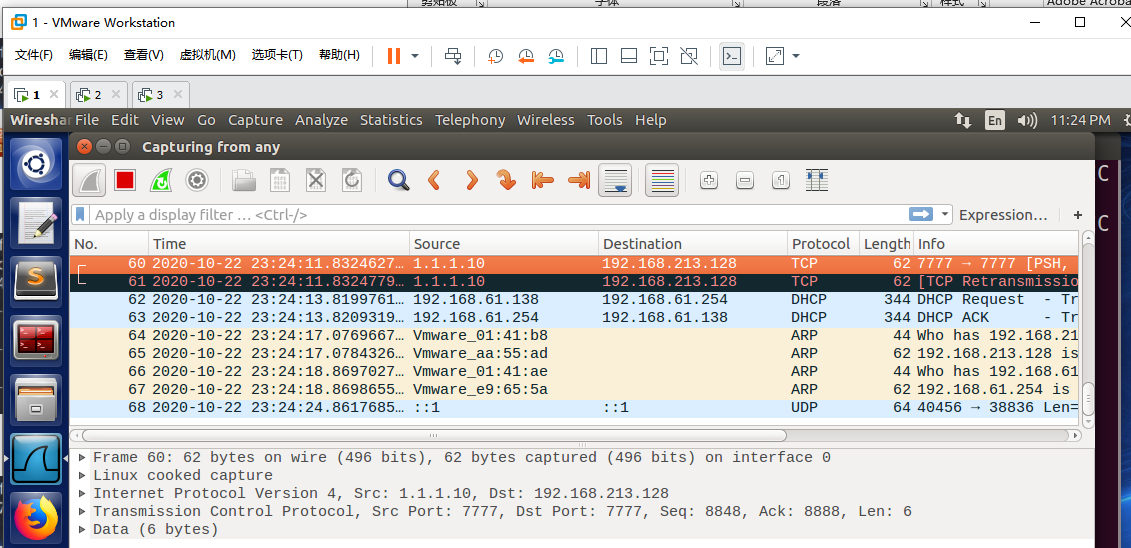
伪造ip为192.168.213.253，观察到主机R接收到了该包，主机B未接收到

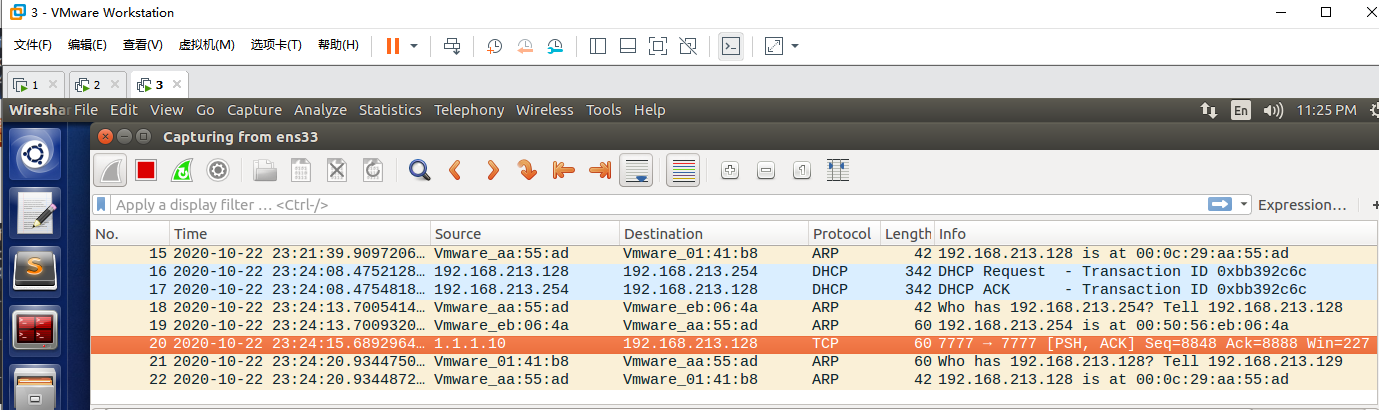


3、伪造ip在互联网中



主机R与主机B均收到该包，并且正常响应。





**四、总结分析**

1、IP层对其信息完全不进行验证，使得我们拥有任意伪造源IP的能力。

2、通过诱导被害主机更改其路由缓存表，攻击发起者可以截获其所有网络流量，并通过精心准备的伪造和欺骗，可以实施中间人攻击。

3、路由会记录ip转发的端口来源，所以若子网和其到来数据包的端口不匹配，就会造成丢包。