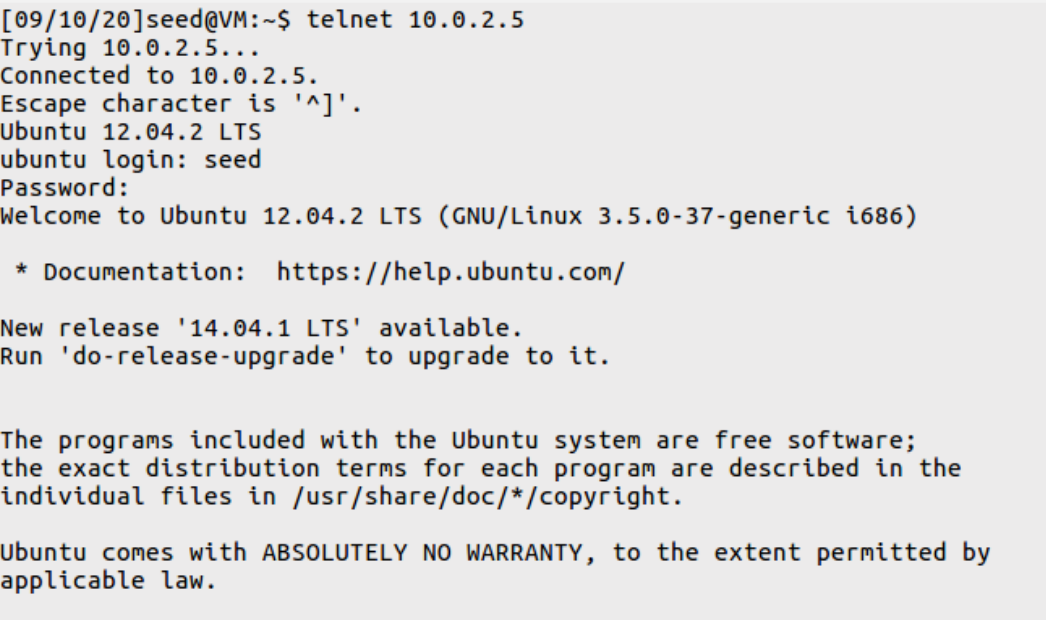
LAB1

TASK1

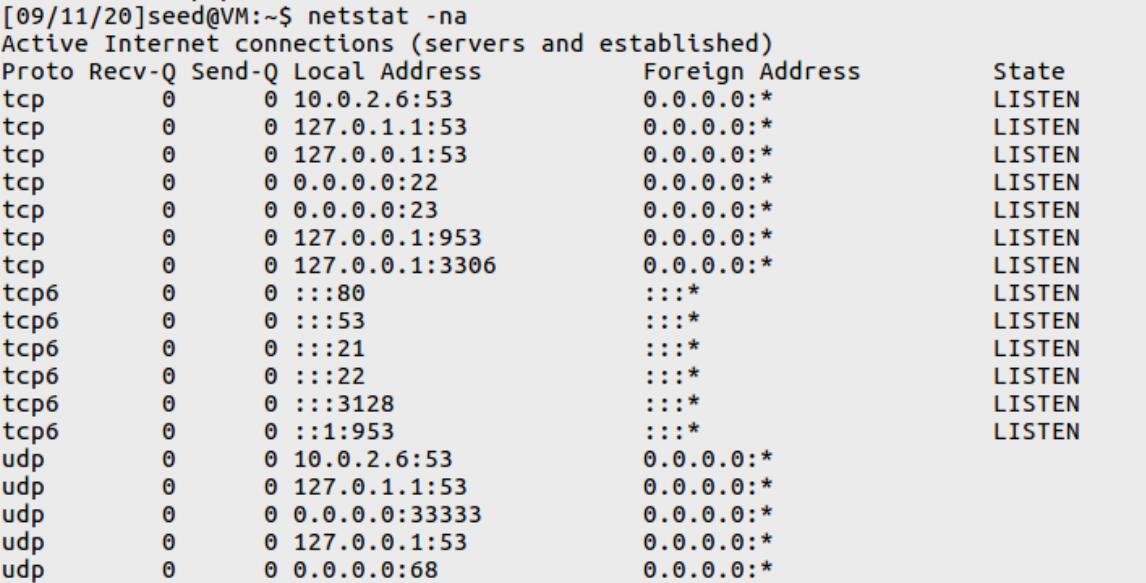
关闭SYN Cookie Countermeasure

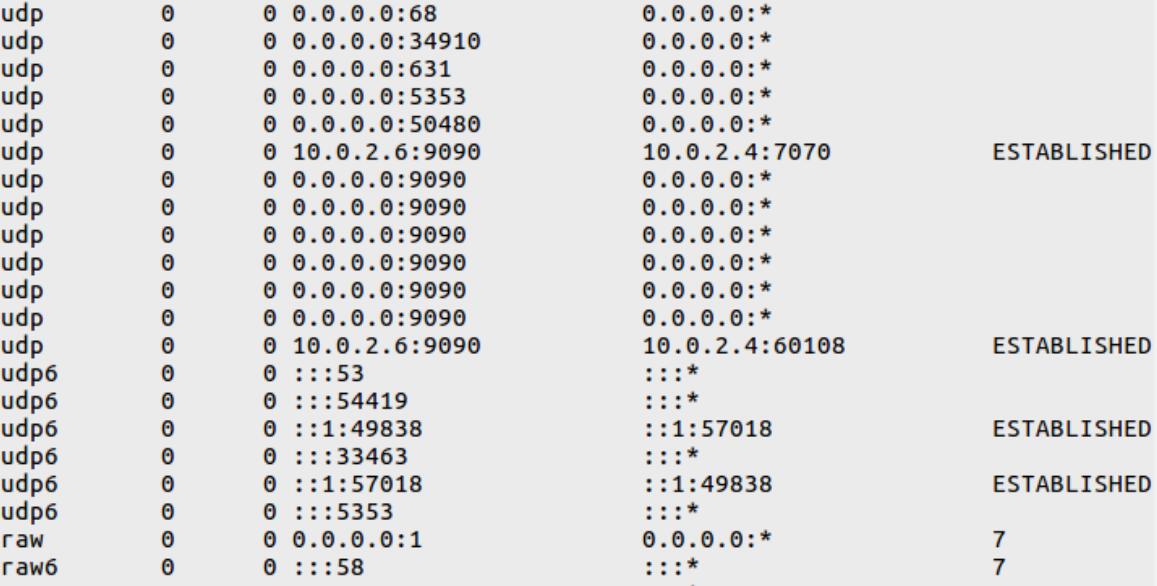
STSH%1Y0Q7%9Y[FPWM1[FPX**观察者测试受害者的telnet连接是否可用，用观察受害者的连接队列**

如上图所示，攻击开始前，观察者VM M可以成功与受害者建立telnet连接。



观察此时受害者的连接队列，发现此时有几个建立的连接，也有的连接处于LISTEN状态。



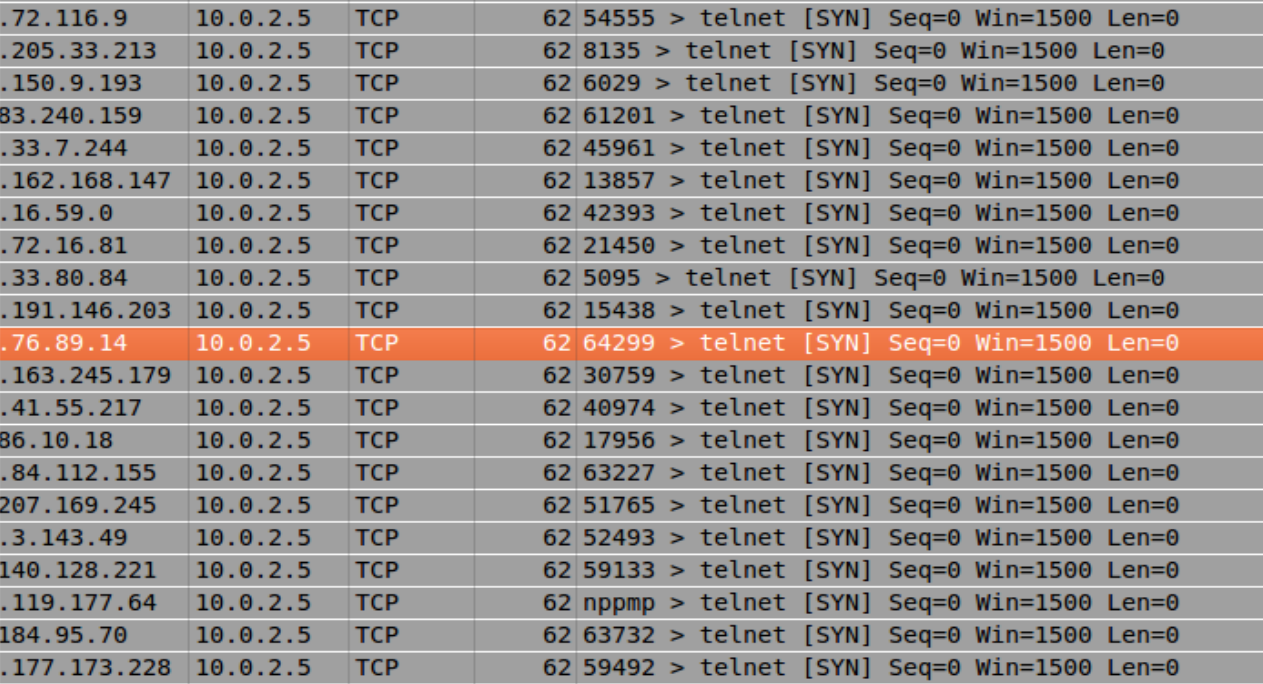
**攻击者利用Netwox 76对受害者进行SYN洪泛攻击**

Netwox编号为76的工具提供了SYN 洪泛攻击的基本功能。

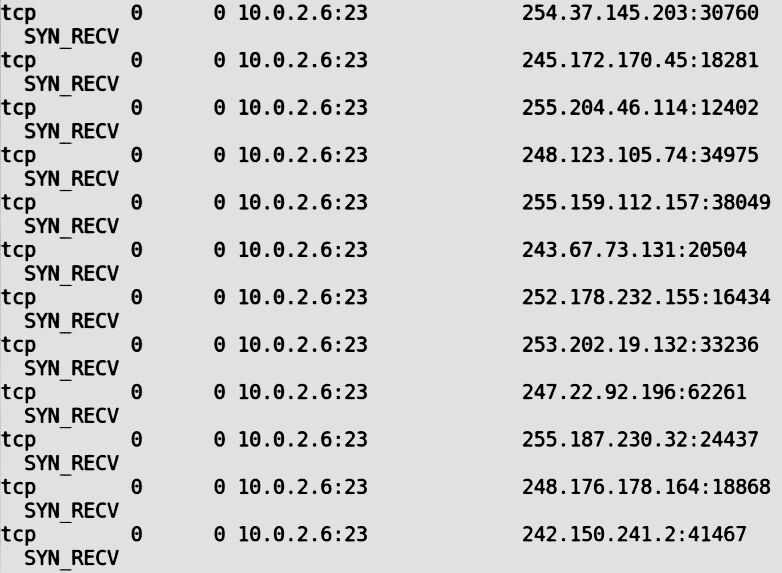
在攻击者VM A上针对受害者的23端口（telnet服务）执行攻击指令：

BM{4AL[WT`BOTHDEW@~2E4H

受害者VM B上打开wireshark抓包，可以看到，受害者收到数量极大的SYN报文，但是并未收到最终的ACK报文，因而其连接队列中有了许多半连接状态的TCP连接。

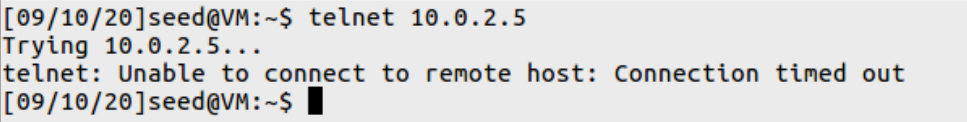


查看受害者当前连接情况，发现有很多半开放连接。



**观察者再次测试受害者的telnet连接是否可用**

观察者VM M再次尝试与受害者建立telnet连接，发现此时无法建立连接。

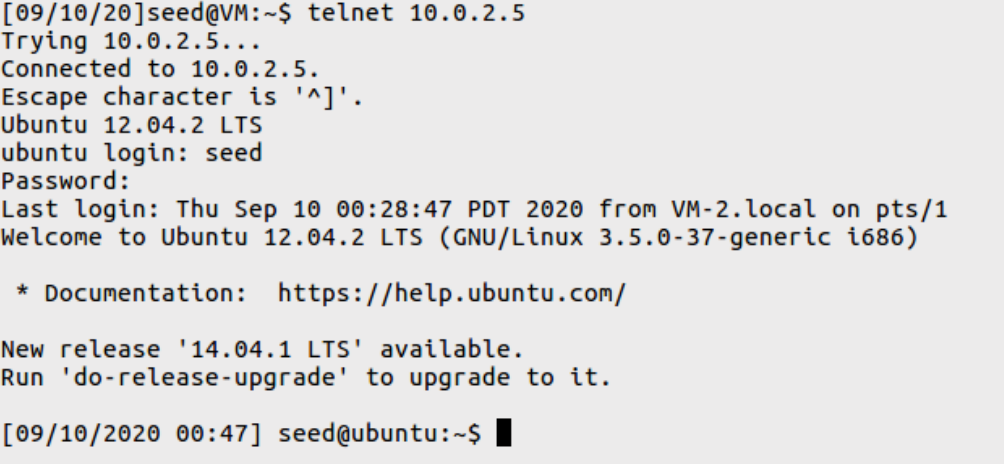


这是因为，被害者的连接队列有固定大小。当这个队列被SYN洪泛攻击造成的半连接填满时，受害者不能再与其他用户建立TCP连接。这说明在SYN cookie Countermeasure机制关闭的前提下，SYN泛洪攻击成功。

TASK2

使用Netwox 78对telnet进行攻击

观察者先与受害者建立telnet连接

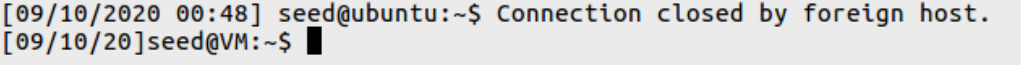


攻击者进行TCP RST攻击

攻击者向受害者发送RST报文，企图中断观察者和受害者间的telnet连接。

UU6BVU4F$G@BS@EOP[{%H~1

观察者与受害者建立的telnet连接被终止

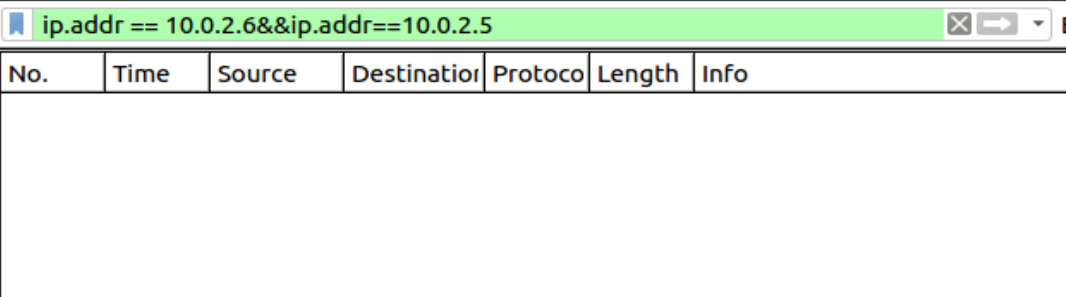


可以看到，攻击者执行攻击指令后，观察者与受害者之间的telnet连接终止，TCP RST攻击成功。

TASK4

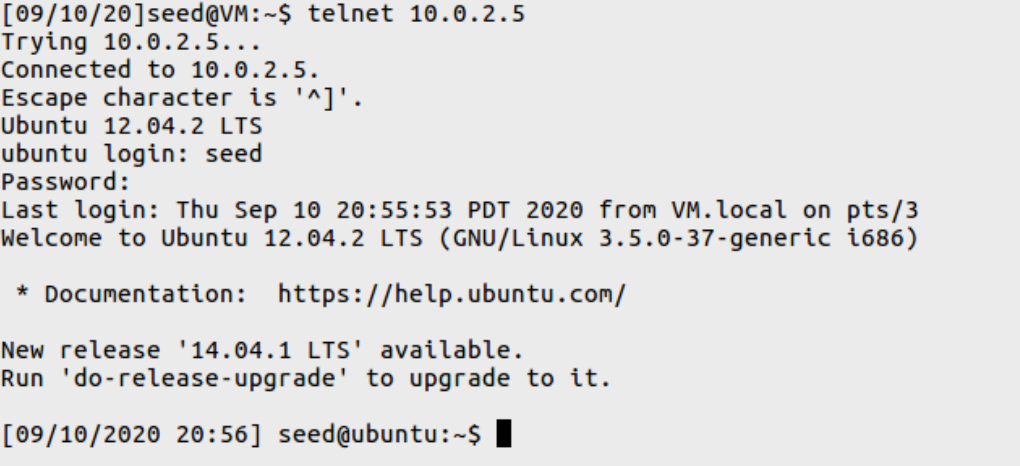
使用Netwox 40进行攻击

首先在攻击者主机VM A上开启wireshark，过滤器设置如下

****

攻击者只抓受害者与观察者之间通信的报文。

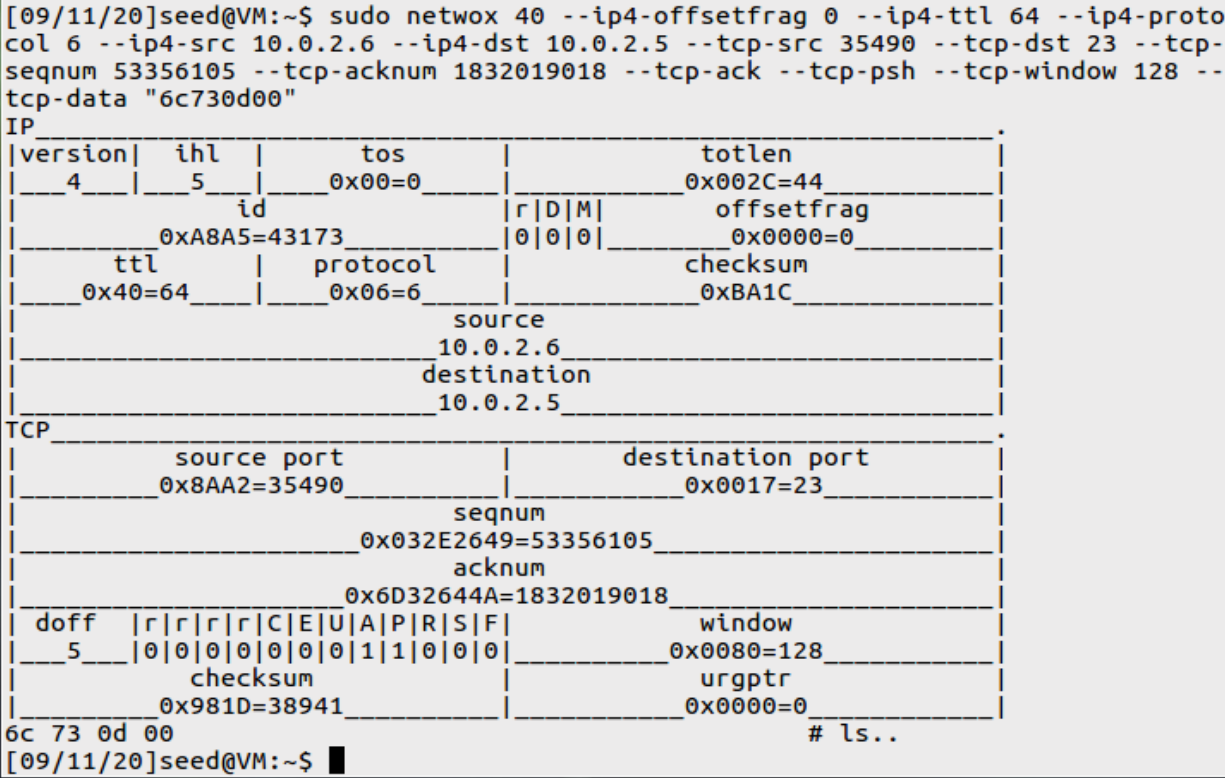
观察者与被害者之间建立telnet会话，同时攻击者抓包

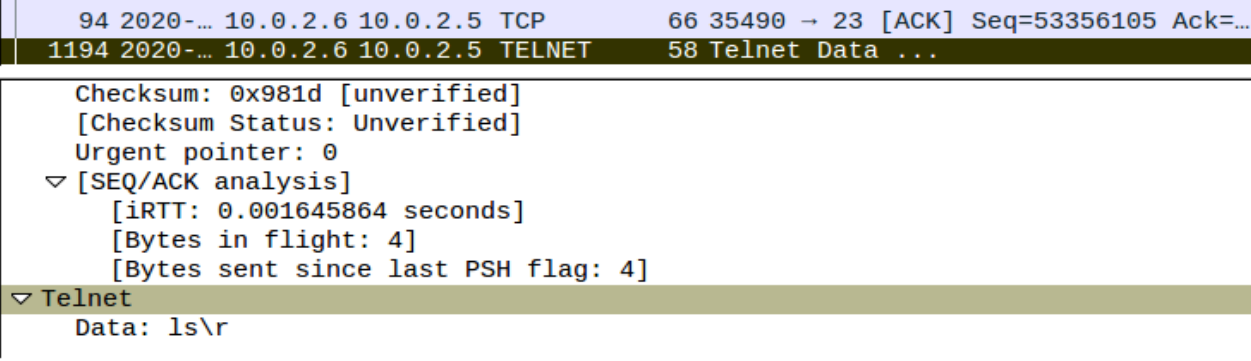


攻击者观察最后一个数据包（从观察者发往受害者）的源ip、目标ip、源端口、目的端口、sequence number和ack number，将它们填入netwox伪造报文的对应位置。

攻击者利用Netwox 40攻击受害者，伪造一个来自于观察者的报文发送给受害者

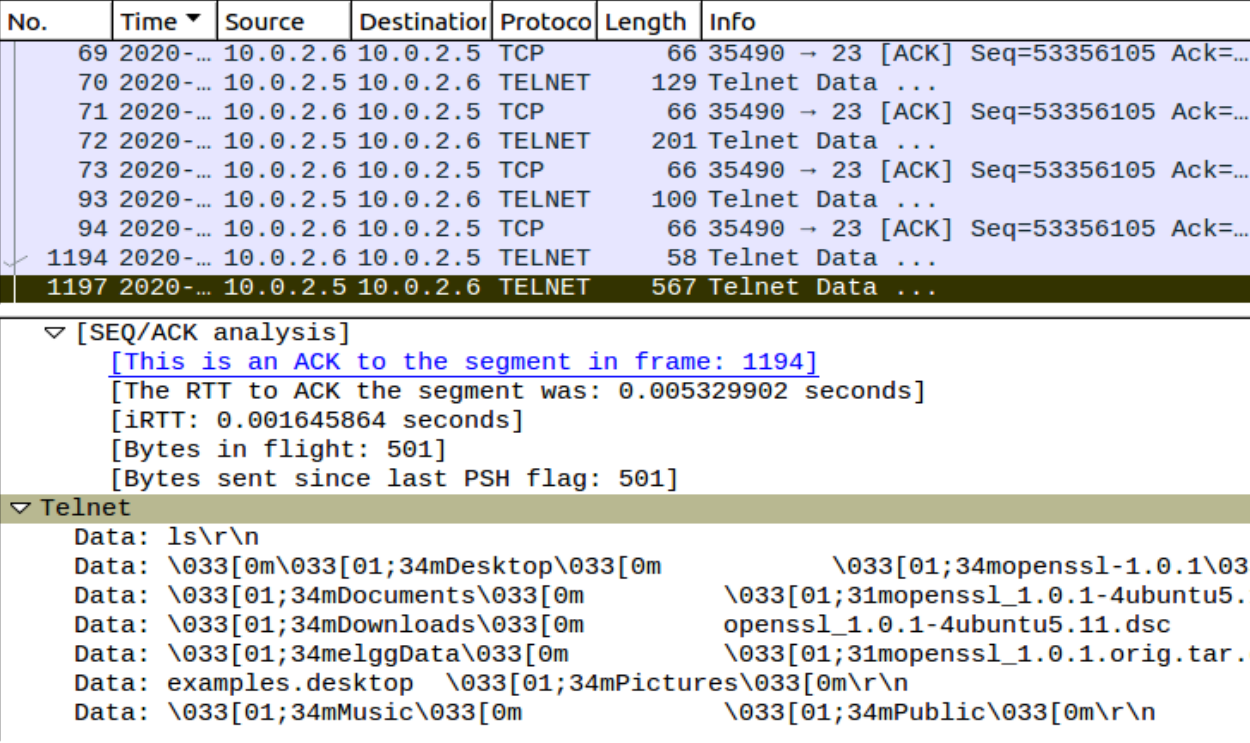
攻击者利用指令sudo netwox 40 --ip4-offsetfrag 0 --ip4-ttl 64 --ip4-protocol 6 --ip4-src 10.0.2.6 --ip4-dst 10.0.2.5 --tcp-src 35490 --tcp-dst 23 --tcp-seqnum 53356105 --tcp-acknum 1832019018 --tcp-ack --tcp-psh --tcp-window 128 --tcp-data "6c730d00"，来伪造一个从观察者发往受害者的包（从而伪装成观察者与受害者通信）。包的data部分为”6c730d00”，是指令”ls\r”的十六进制表示。





上图即为攻击者伪造的报文，可以看到，其数据部分为”ls\r”。

报文发出去后，攻击者在wireshark上抓到了受害者发给观察者（其实是假扮成观察者的攻击者）的响应报文，报文的数据部分是受害者执行指令”ls\r”的结果（输出目录下所有的文件）。



攻击者通过抓包，成功在受害者与观察者都不知道自己存在的情况下，获得了服务器当前目录下所有文件的名称，会话劫持攻击成功。