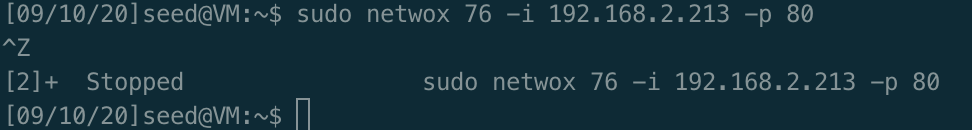
Lab4-report

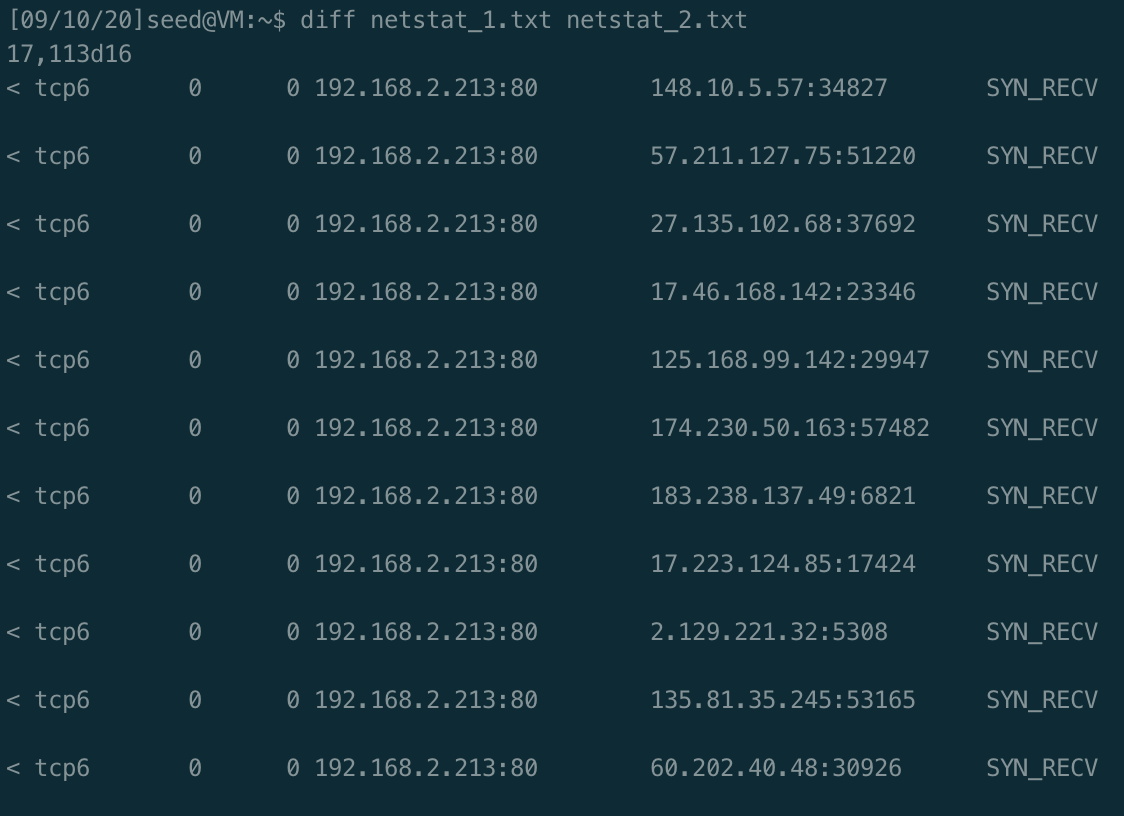
57117139吴星灿

**Task1**

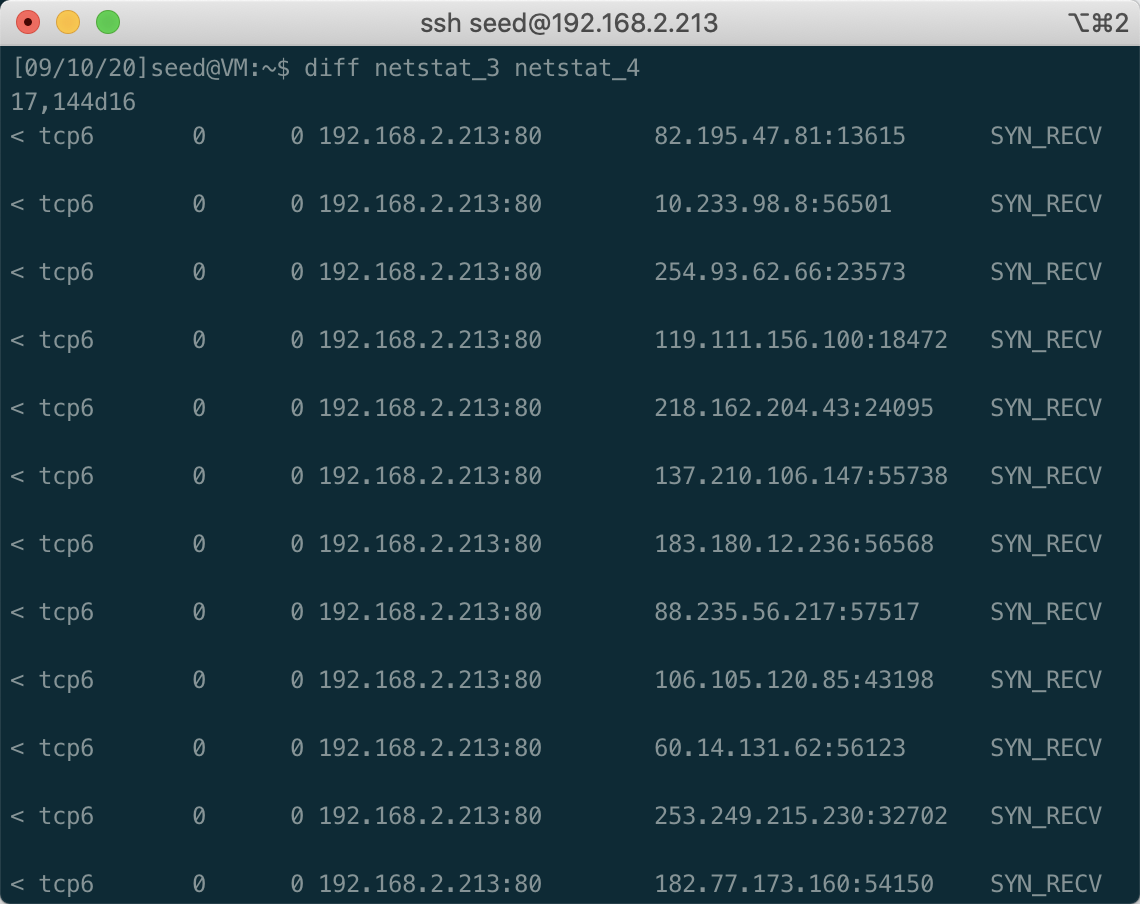
攻击命令如下



攻击成功，被攻击主机连接被中断，下面为被攻击主机前后对比



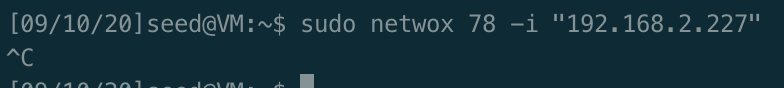
打开syncookies重复攻击，不能中断被攻击主机的网络，但是依然有synrecv，如下图。



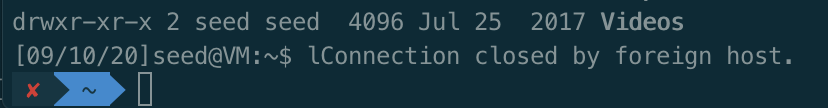
SYN Cookie是对TCP服务器端的三次握手做一些修改，专门用来防范SYN Flood攻击的一种手段。它的原理是，在TCP服务器接收到TCP SYN包并返回TCP SYN + ACK包时，不分配一个专门的数据区，而是根据这个SYN包计算出一个cookie值。这个cookie作为将要返回的SYN ACK包的初始序列号。当客户端返回一个ACK包时，根据包头信息计算cookie，与返回的确认序列号(初始序列号 + 1)进行对比，如果相同，则是一个正常连接，然后，分配资源，建立连接。实现的关键在于cookie的计算，cookie的计算应该包含本次连接的状态信息，使攻击者不能伪造。

**Task2**

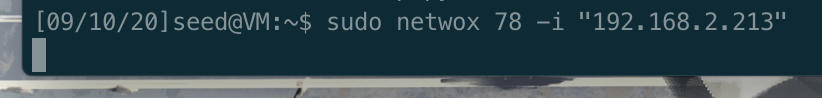
攻击语句如下

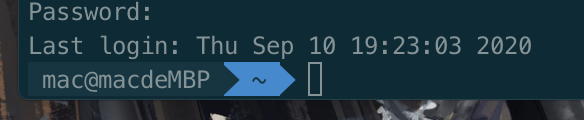


攻击成功，切断了telnet的连接。

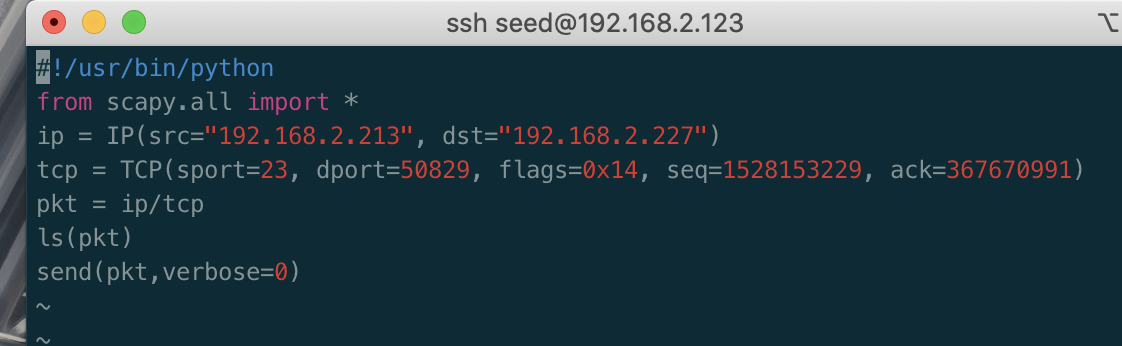


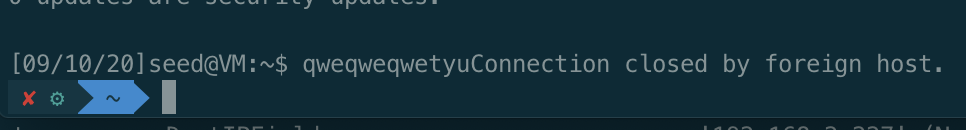
换成ssh连接则无法切断。

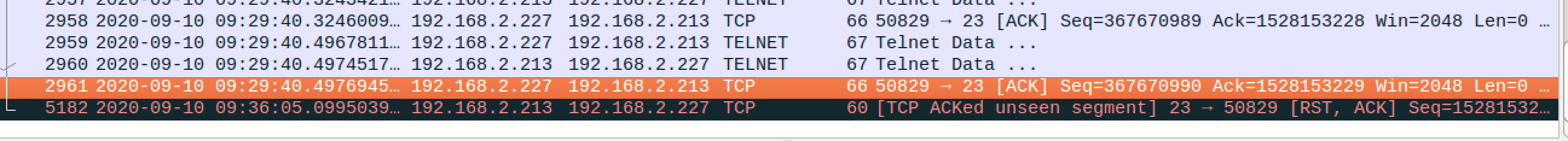




使用python scapy重复上次实验，成功切断telnet连接。



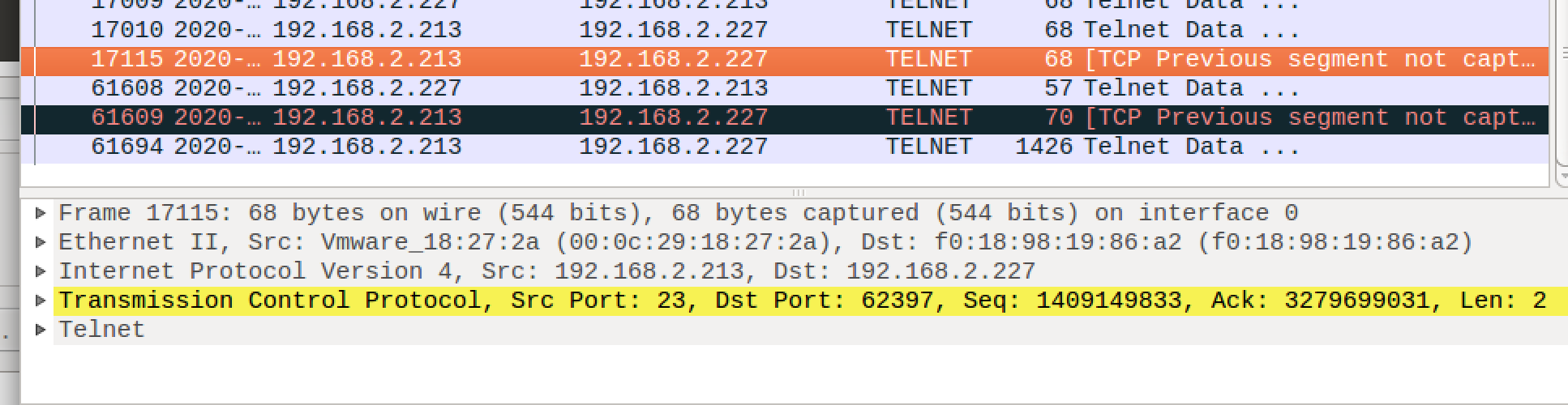




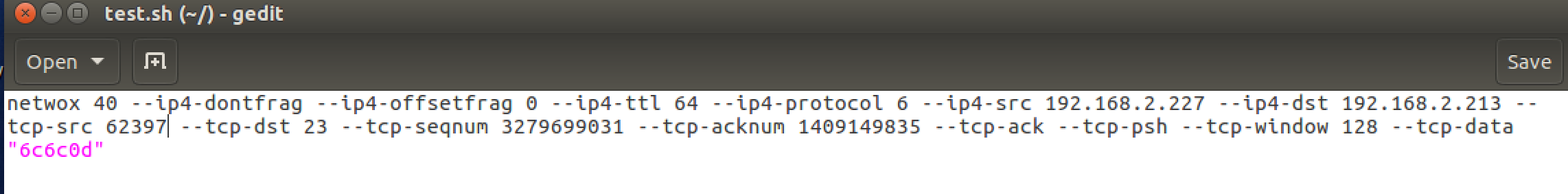
**Task5**

**Netwox攻击**

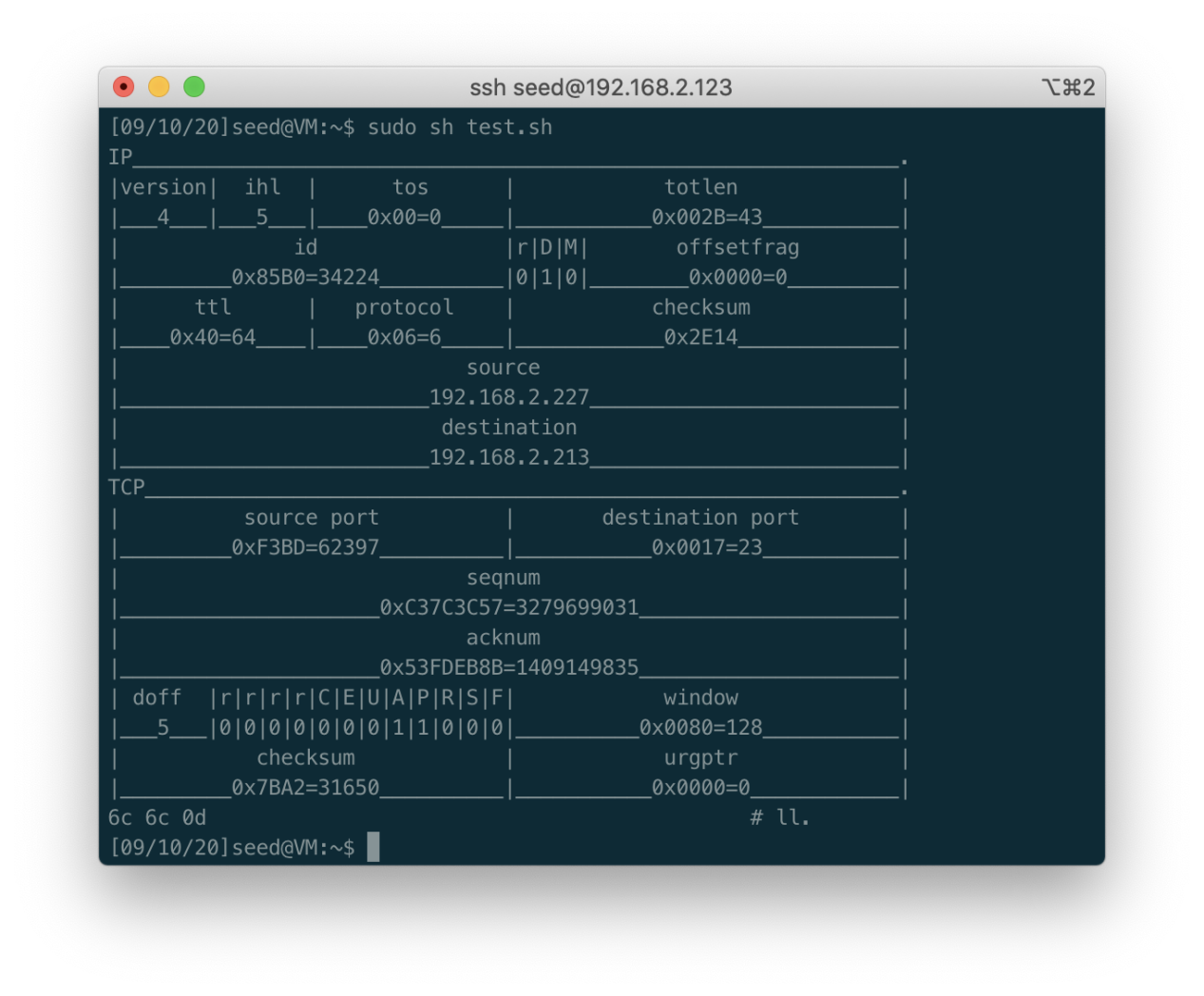
连接上telnet之后，用wireshark抓包，从返回213主机返回的ACK报文中找到端口号，Seq字段，Ack字段，Len字段，ttl字段



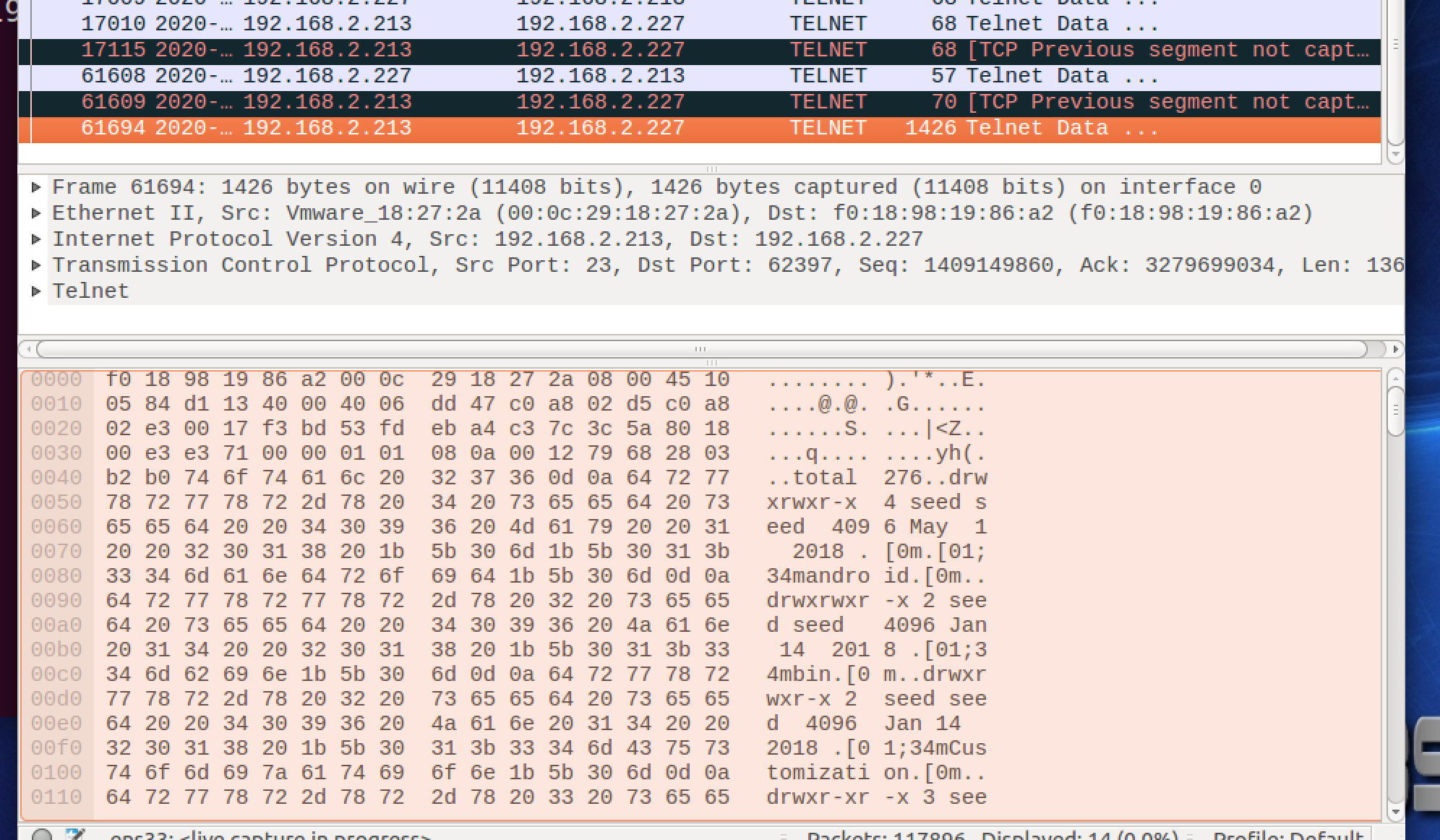
将netwox的参数设置好，其中端口号与ACK报文中一样，seqnum等于ACK报文的Ack值，acknum等于ACK报文的Seq值加上Len值，其他参数与ACK报文保持一致。



攻击的报文如下，注入了一个ll命令。



从wiresharks的捕捉包中看出，被攻击主机213返回了一个对ll命令的回应，攻击成功。



**python攻击**

报文设置方式与netwox一样，同样看到返回对ll的应答，攻击成功。

