网络空间安全课程综合设计任务报告四

57117203 姜舒

2020年9月12日

（一）TCP/IP Attack Lab

Task 1: SYN Flooding Attack

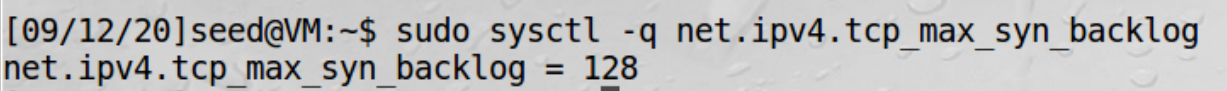
各虚拟机IP地址：

攻击者 虚拟机VA 10.0.2.4

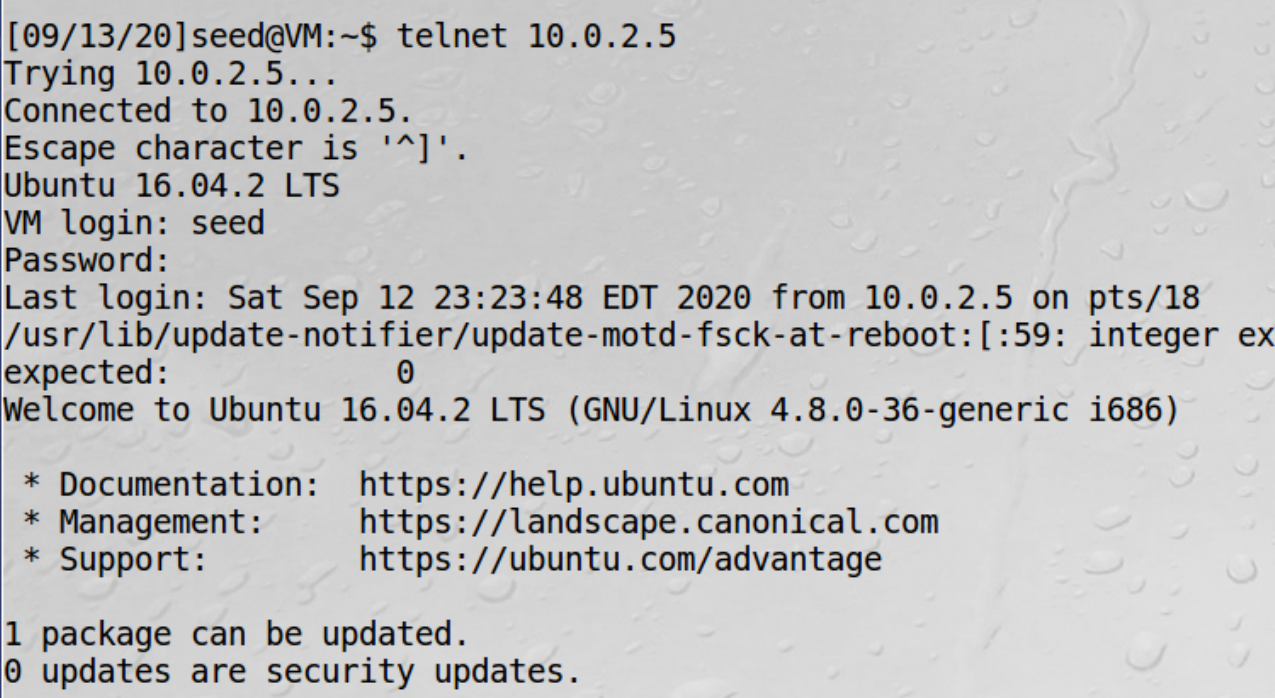
受害者 虚拟机VB 10.0.2.5

观察者 虚拟机VC 10.0.2.6

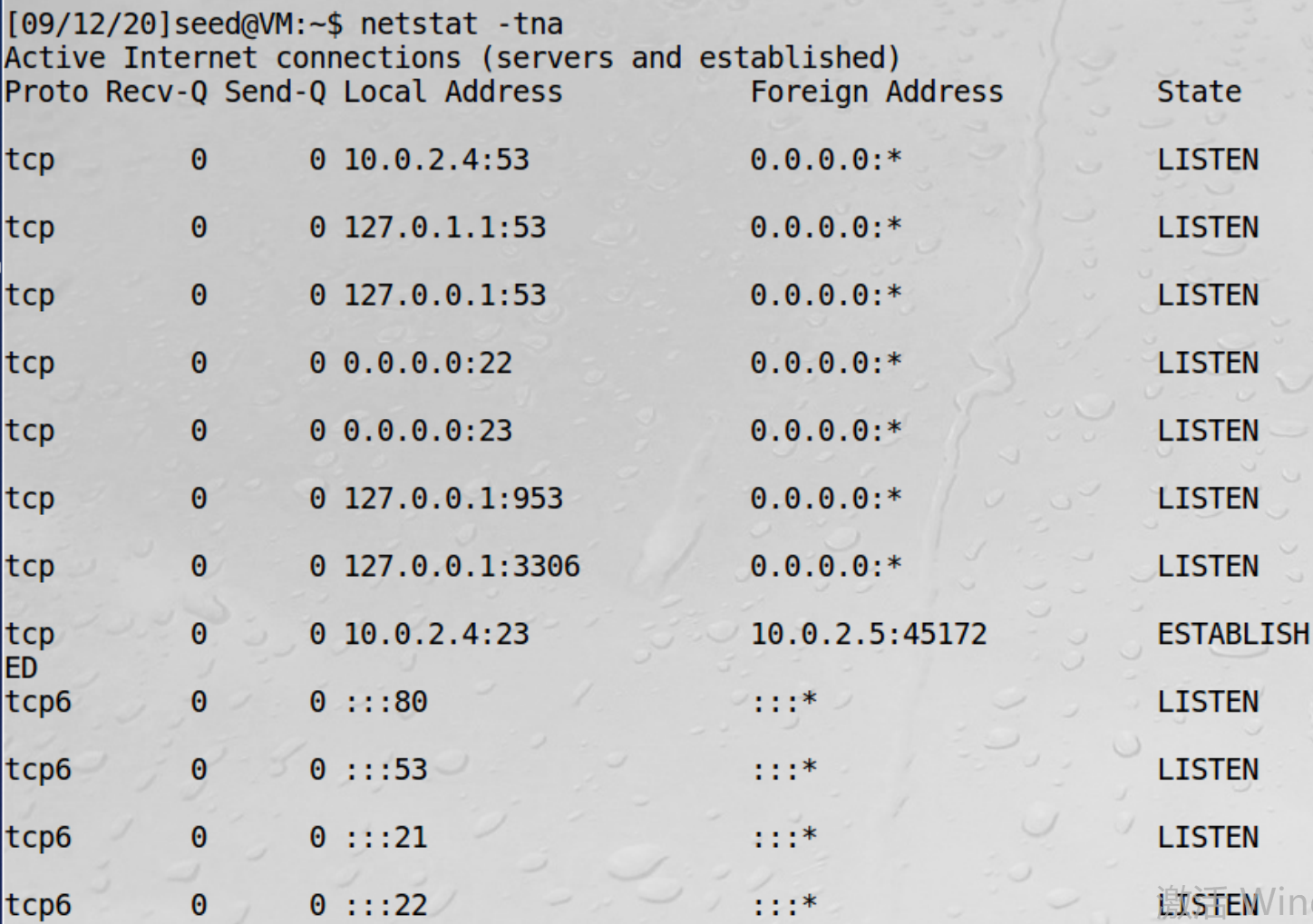
用命令检查受害者虚拟机VB队列的大小，得到结果128

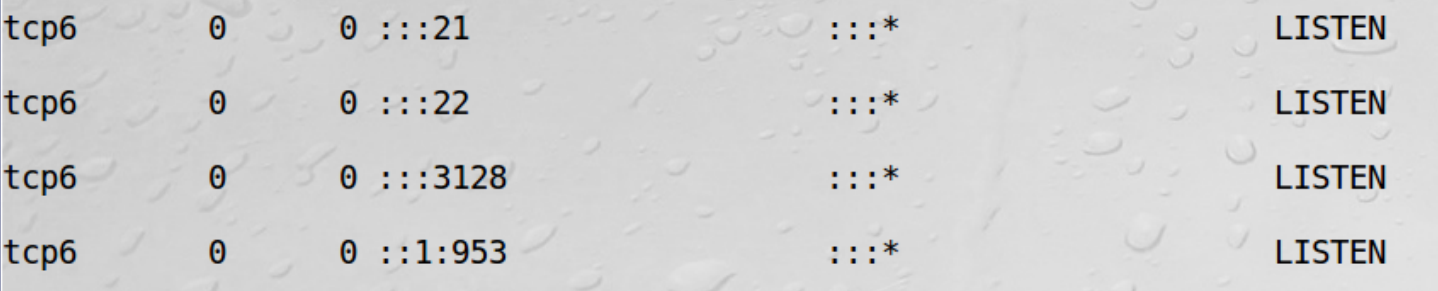


用观察者VC对VB进行telnet连接

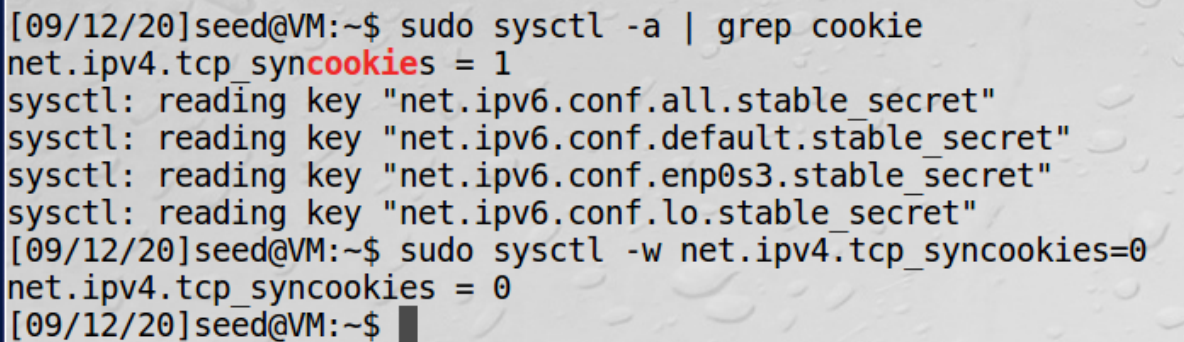


在VB中用$netstat -tna命令查看所有TCP连接。一共十几条连接申请，大多数状态为LISTEN，少量为ESTABLISH

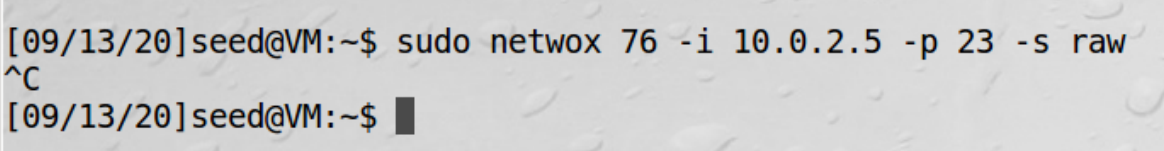




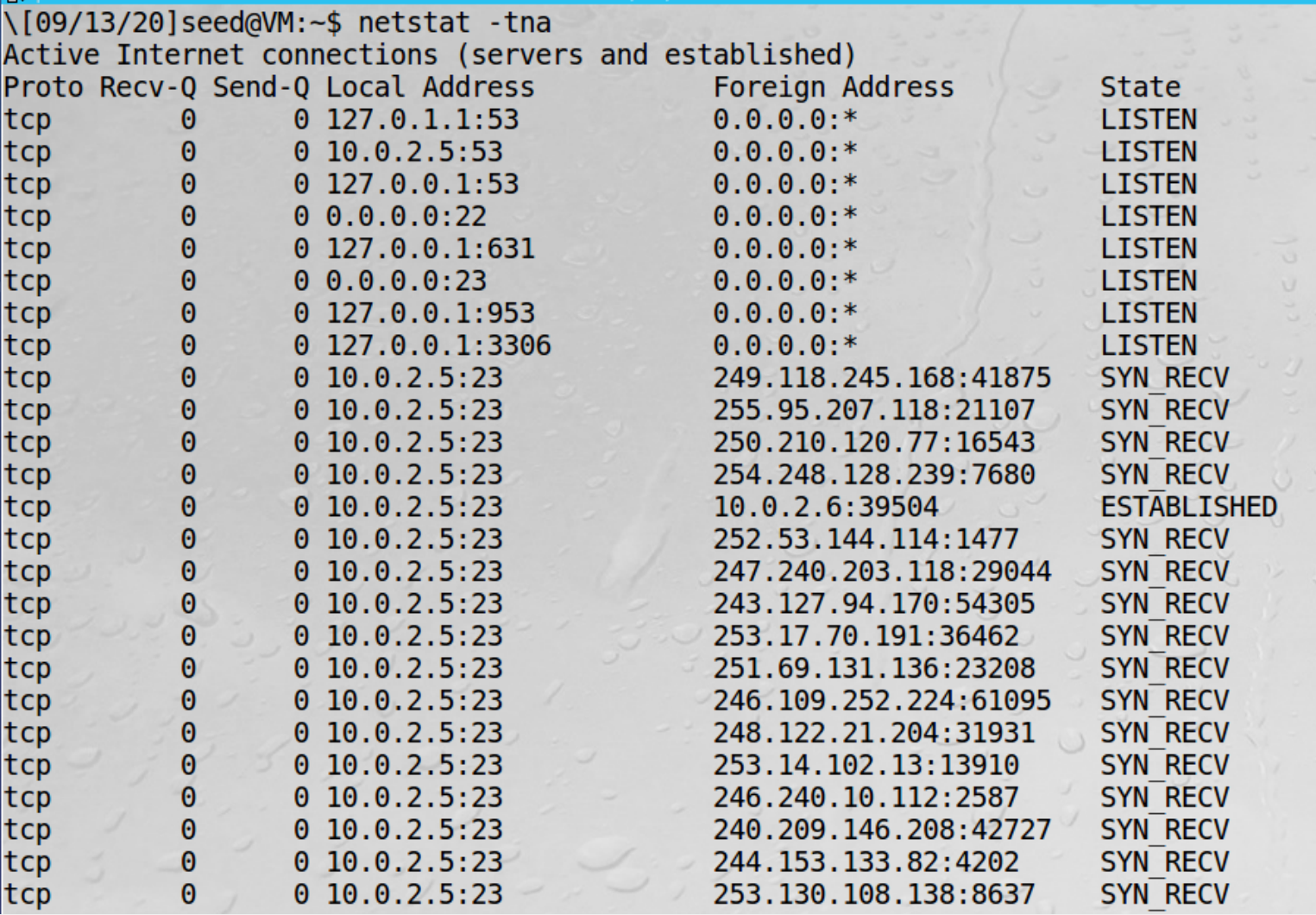
使用命令看到VB的SYN Cookie机制已打开，将其关闭，设置为0。



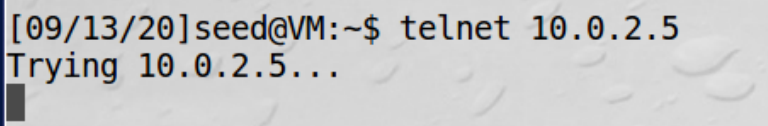
在VA上使用netwox的命令，对VB进行SYN洪泛攻击。



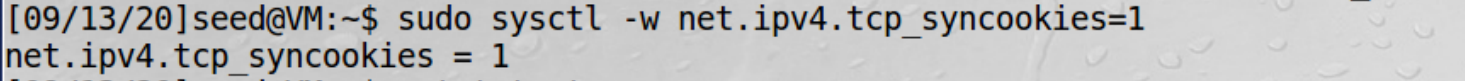
在VB上重新使用netstat命令查看连接，出现了许多状态为SYN\_RECV的连接，攻击成功。

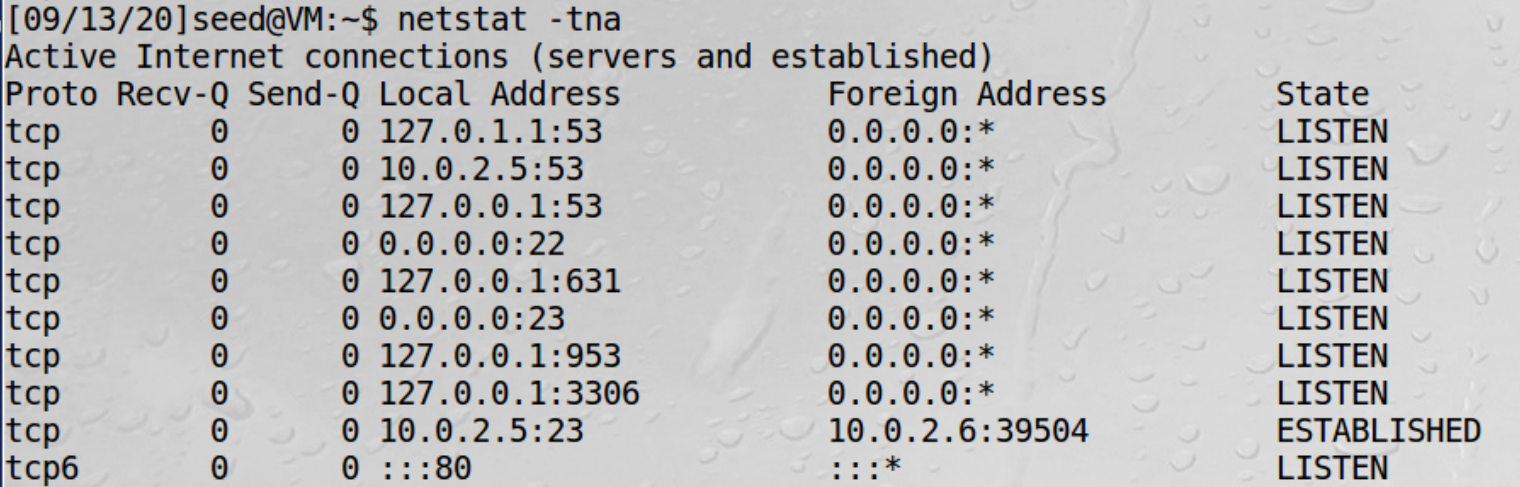


重新在VC上向VB建立连接，连接失败。此时VB被洪泛攻击，队列资源占尽。



将VB的SYN Cookie设为1，开启保护，攻击失败，连接状态恢复正常。



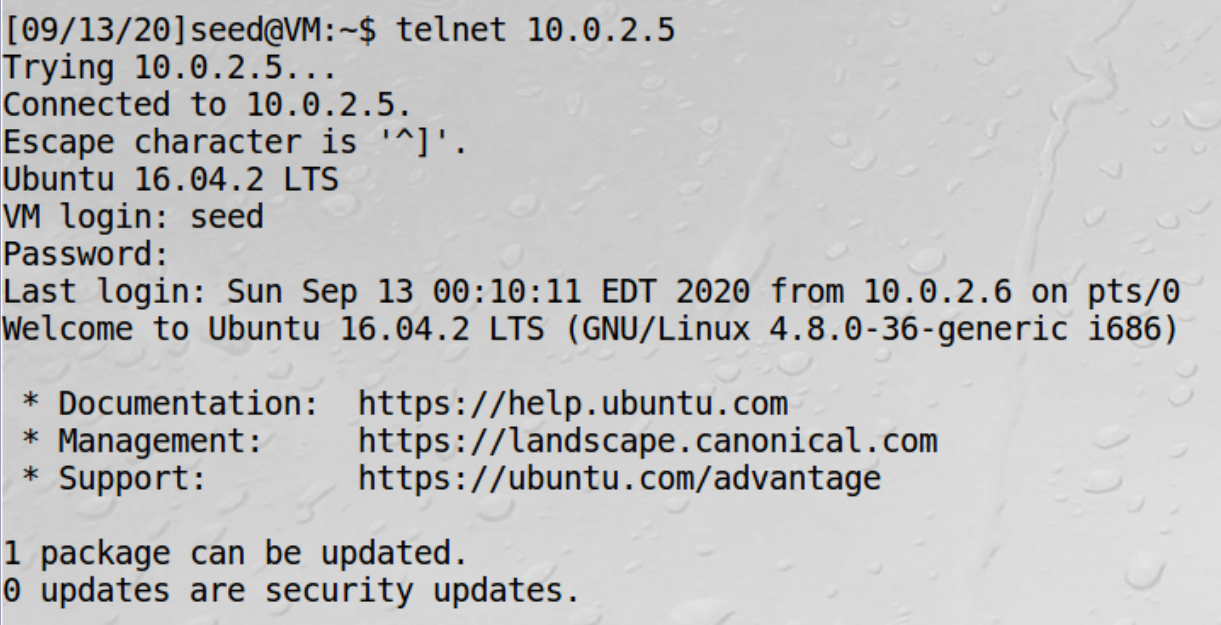


服务器会使用密钥，在接收到SYN包之后根据信息计算一个哈希值H，作为服务器的初始序列号发送到客户端（这个H就是SYN cookie）。

攻击者不会返回ACK报文，没有返回时不会建立socket资源（只损失一些计算资源）；正常的客户端会在ack处填上H+1返回一个ACK报文给服务器，服务器通过重新计算H，来确定ack中的数是否正确，若正确，则再建立合法连接。因而，SYN cookie可以有效防止SYN泛洪攻击。

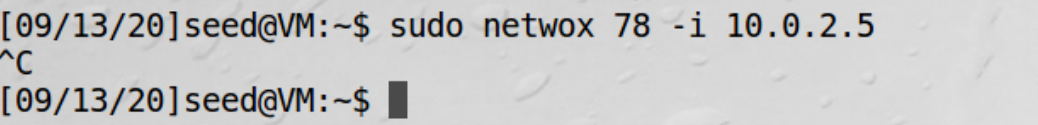
Task 2: TCP RST Attacks on telnet and ssh Connections

先将观察者VC与受害者VB进行telnet连接，连接建立

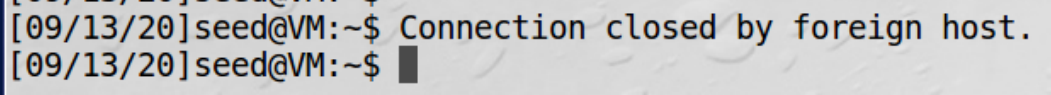


（1）使用netwox攻击

在攻击者VA上使用netwox78的命令，发送攻击报文



在观察者VC上可以看到连接被迫中断。

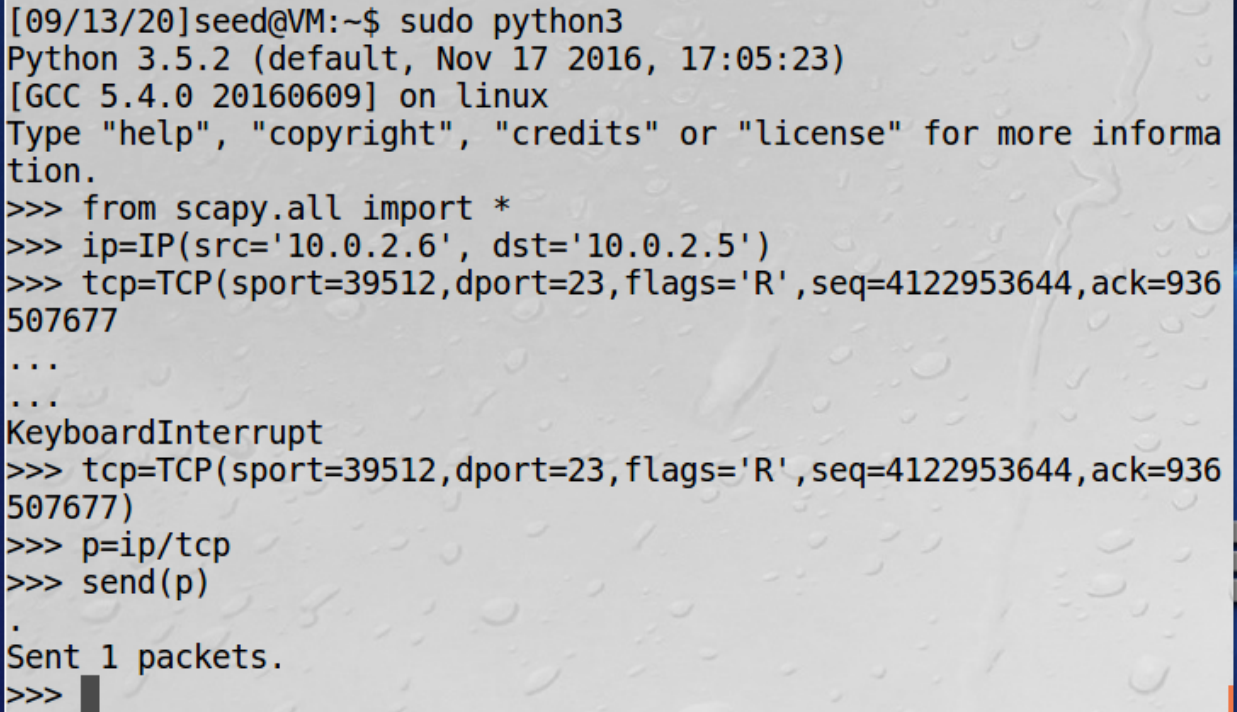


（2）使用scapy攻击

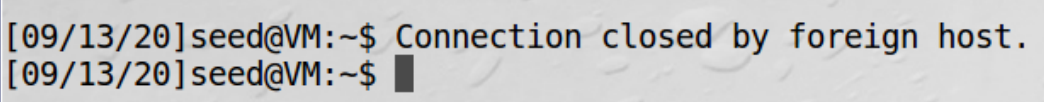
建立telnet连接后，在攻击者VA上打开wireshark抓包，查看TCP连接的报文。最后一条报文信息如下图。获得源端口、目的端口、seq和ack值等关键信息。



使用scapy伪造一条报文，填入获得的src, dst, sport, dport, seq, ack等信息，发送给受害者虚拟机VB



此时在观察者VC上，telnet连接已断开。

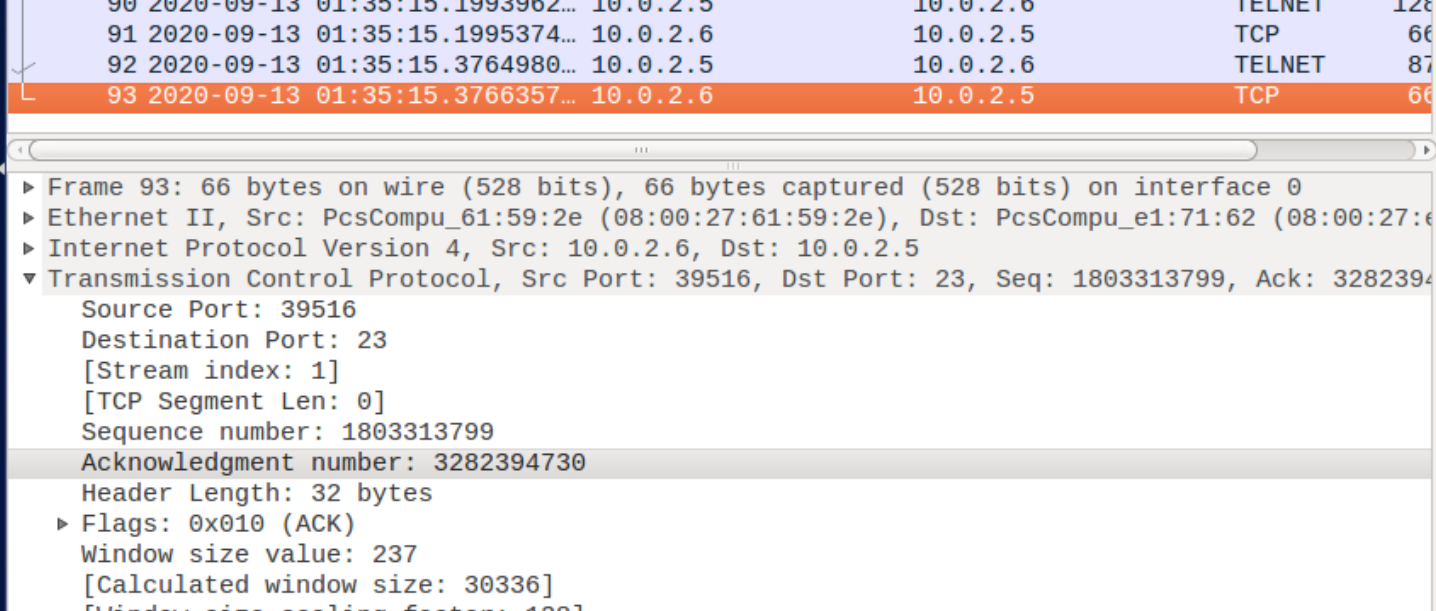


Task 4: TCP Session Hijacking

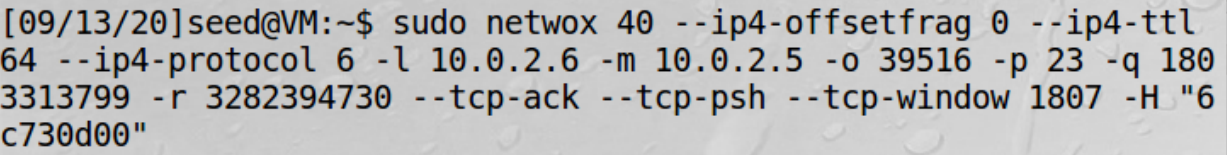
在观察者VC上向受害者VB建立telnet连接

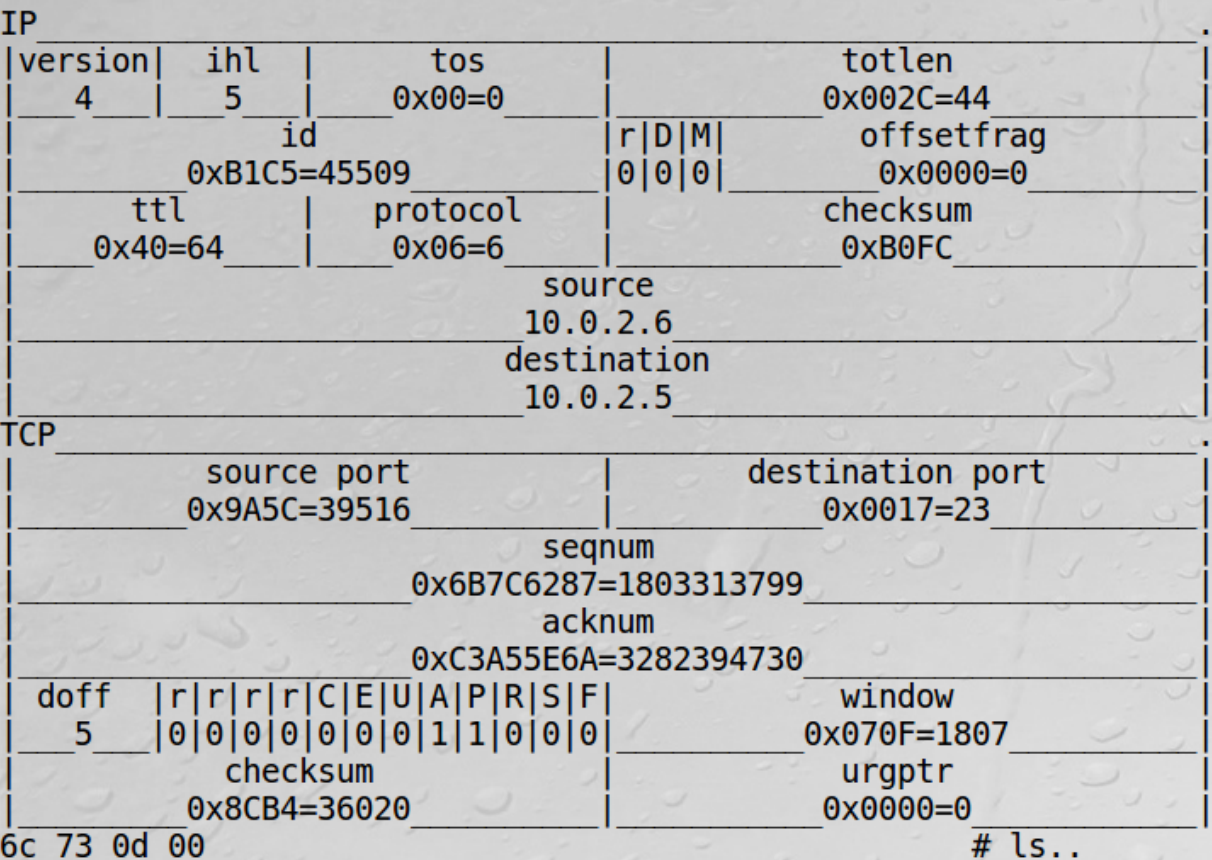
（1）使用netwox40完成攻击

在攻击者VA上打开wireshark抓包VB,VC之间的通信，获得源端口、目的端口、seq和ack值等关键信息。

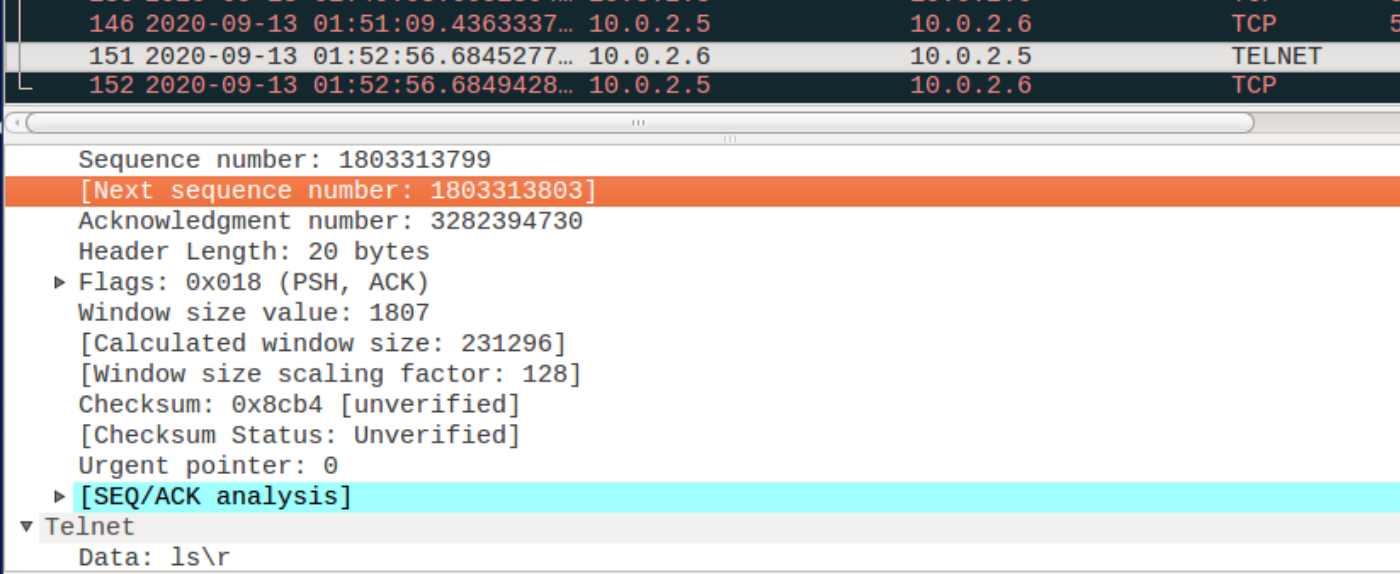


用netwox伪造报文



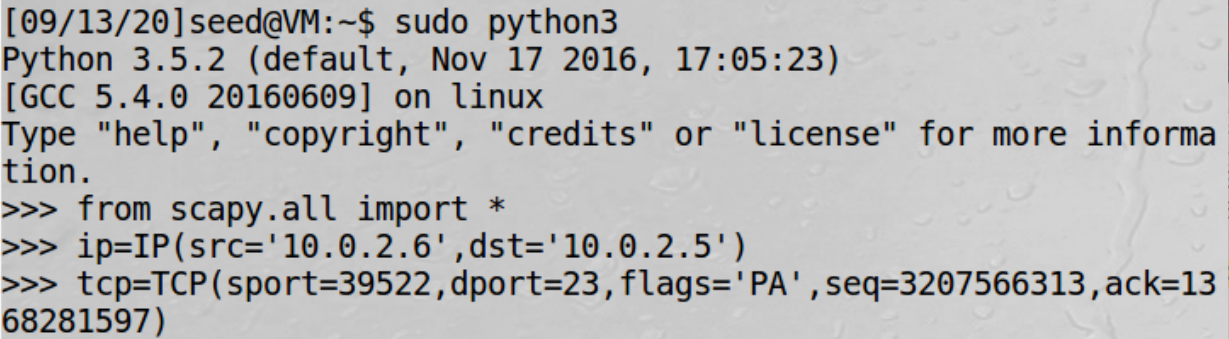


在wireshark上抓博导伪造的报文，看到数据部分为netwox指令中输入的十六进制数字’6c730d00’，表示的实际数据就是ls\r



（2）使用scapy攻击

用scapy伪造一条报文，发送给受害者VB，让VB新建一个att文件





打开VB，看到出现新文件，攻击成功。

