**Lab16-1: TCP/IP Attack Lab**

实验环境：攻击者192.168.43.166，被攻击者192.168.43.139，观察者192.168.43.85。

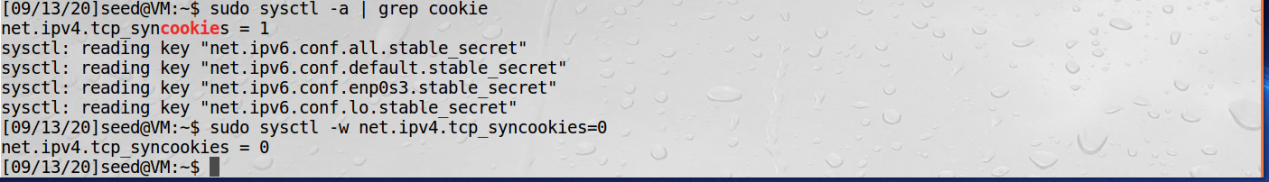
**Task 1: SYN Flooding Attack**

检查被攻击者存放SYN请求的队列大小：



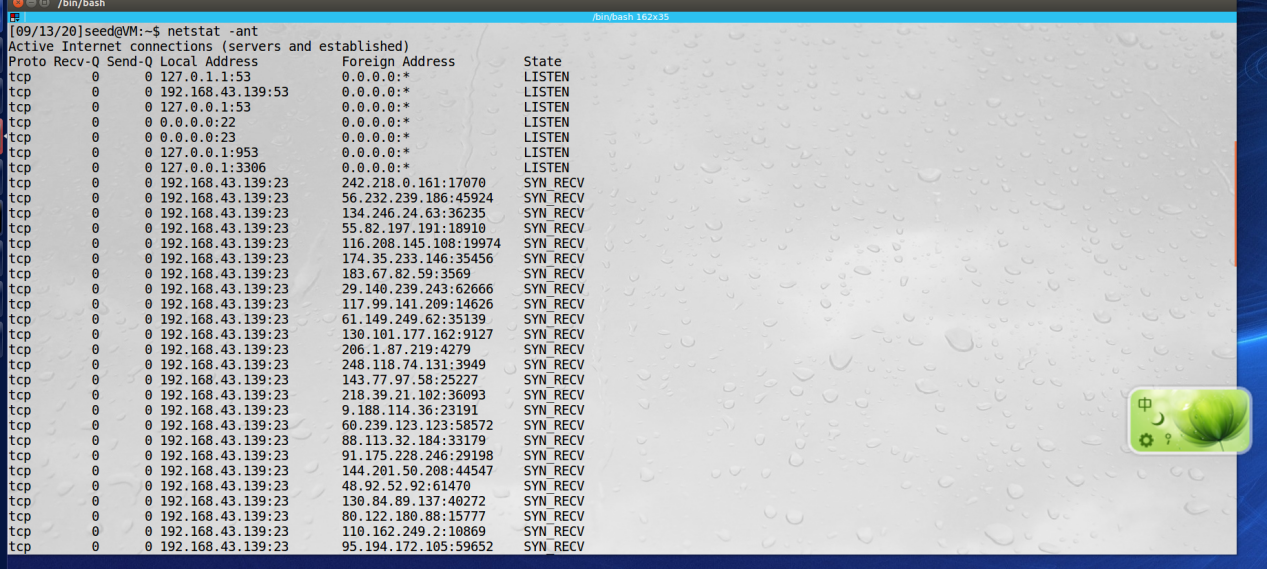
在攻击前，观察者可以远程登录被攻击者的主机；关闭被攻击者的SYN cookie机制并进行攻击：

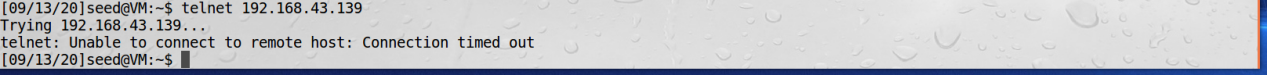


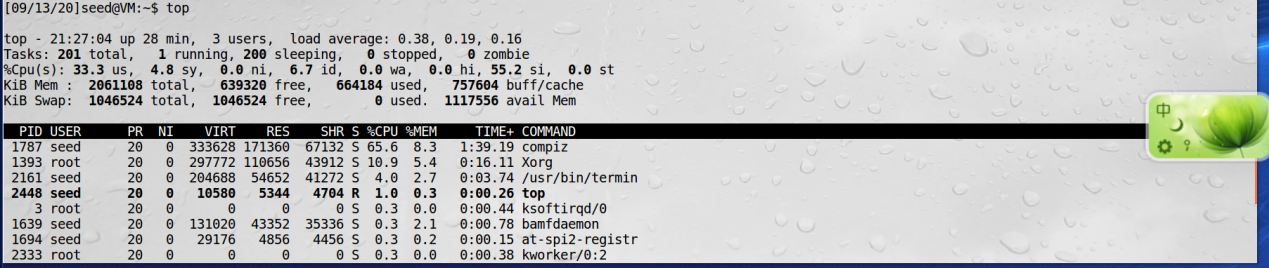




攻击后，被攻击者的23号端口上有大量源IP地址随机的半开放连接，此时观察者无法再登录被攻击者的主机，但被攻击者的CPU使用率没有很高，还有很多其他功能可以正常执行：

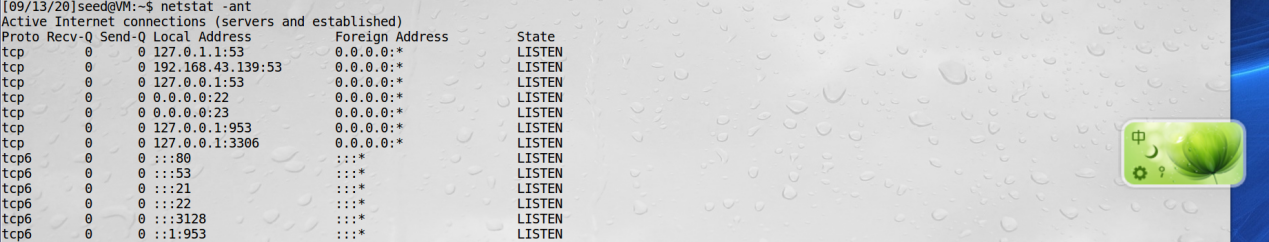




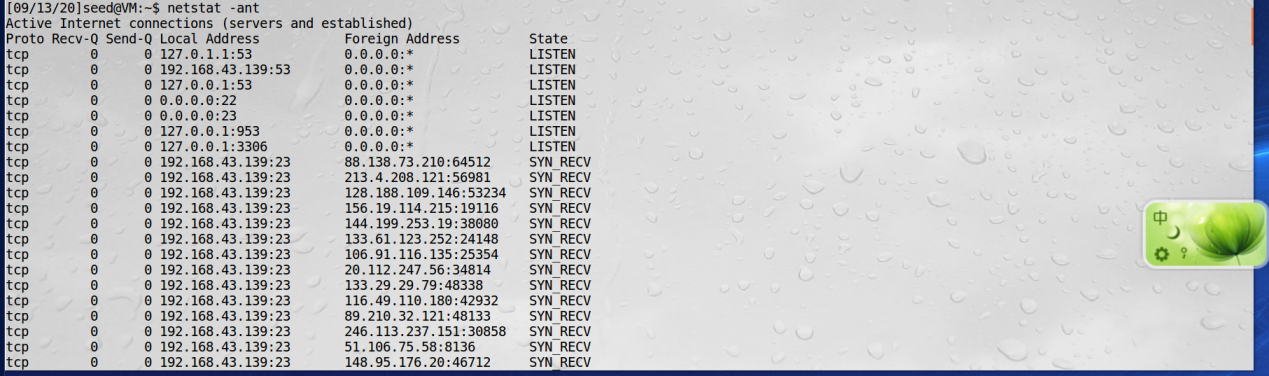


关闭攻击，打开被攻击者的SYN cookie机制，被攻击者的队列状态恢复后，重复上述攻击：

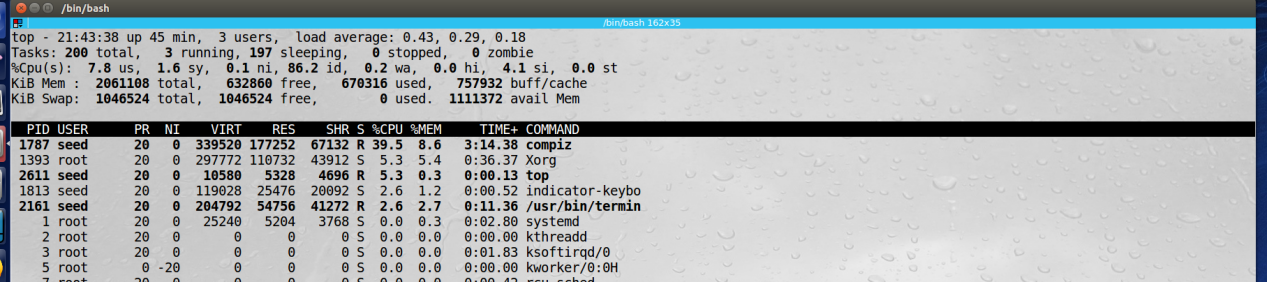




攻击后，被攻击者的23号端口上依然有大量源IP地址随机的半开放连接，但此时观察者可以远程登录被攻击者的主机；同样的，被攻击者的CPU使用率没有很高：

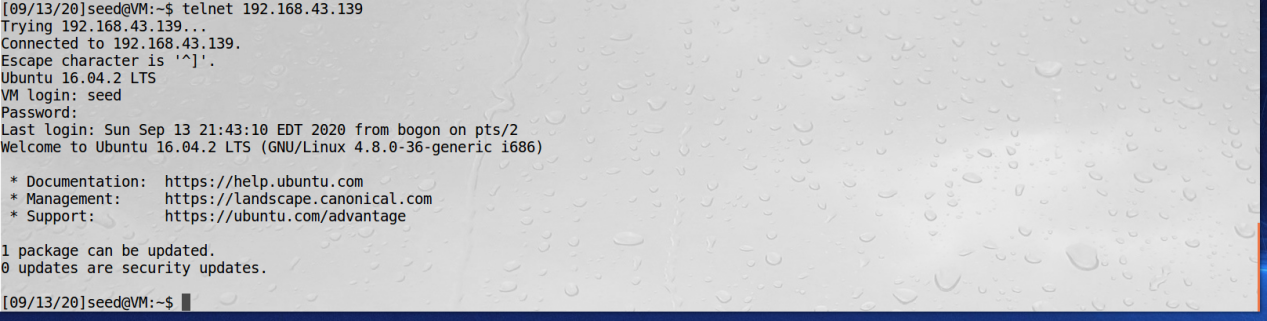






**Task 2: TCP RST Attacks on telnet and ssh Connections**

观察者远程登录被攻击者主机，即在观察者和被攻击者之间建立telnet连接：

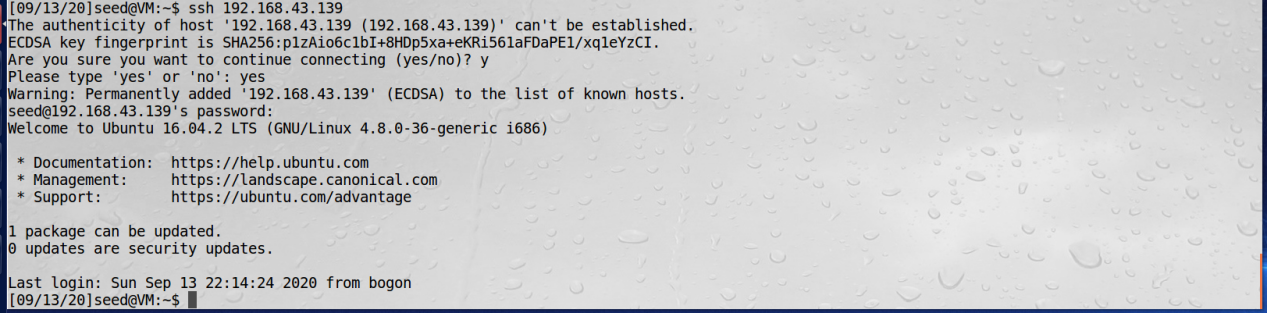


攻击者进行TCP RST攻击，攻击后观察者与被攻击者之间的连接断开：





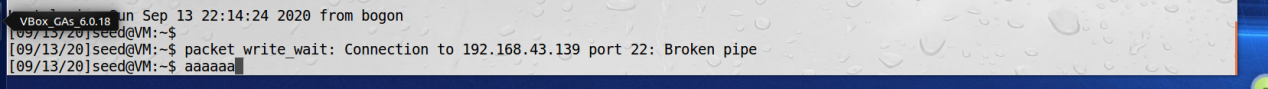
使用ssh连接观察者主机和被攻击者主机，该连接的端口号为22：





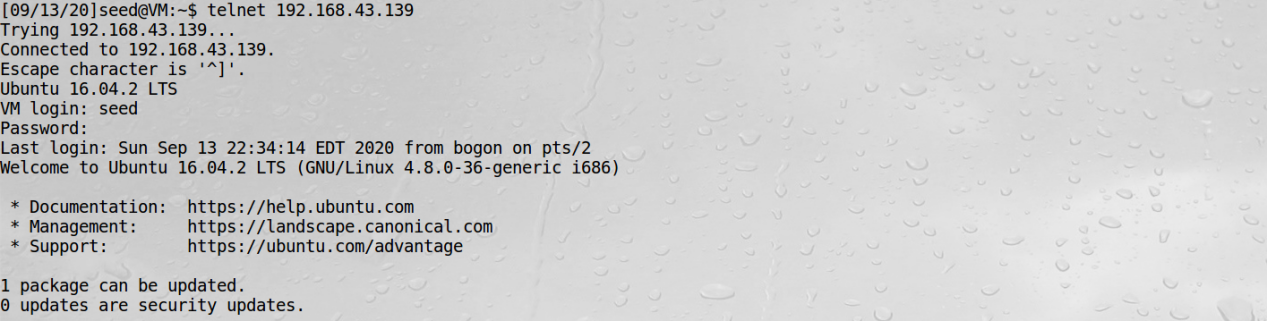
在ssh连接上尝试相同的攻击；连接断开，攻击成功：





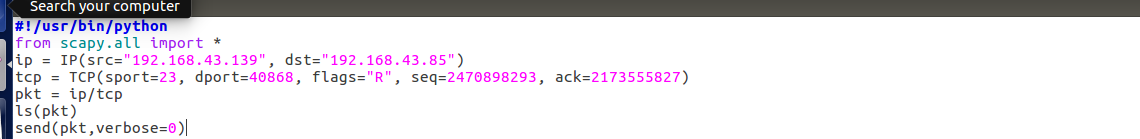
下面，使用Scapy进行TCP RST攻击：

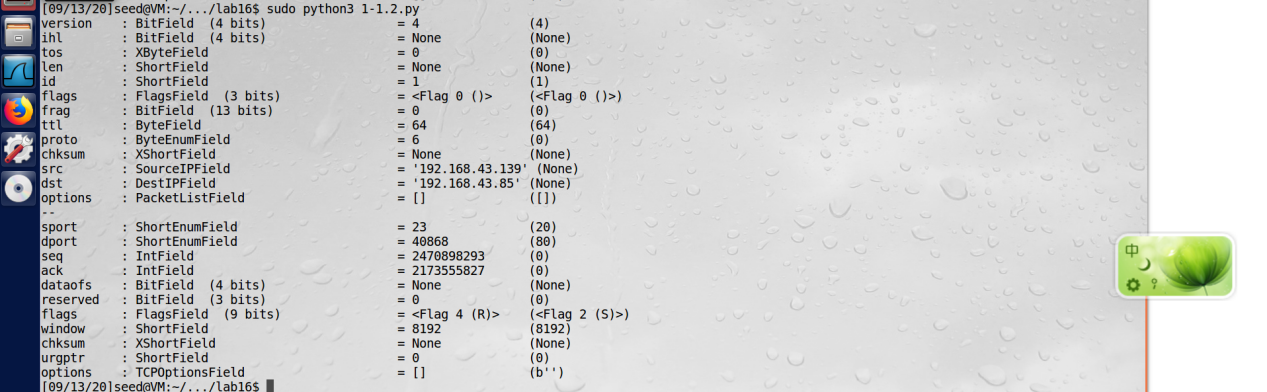
建立连接，捕获连接过程中的最后一个telnet数据包，获得端口号、下一个分段号等信息：



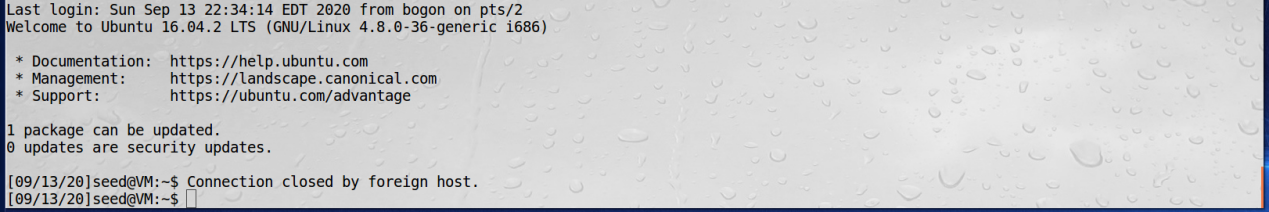


使用获得的信息构造伪造的数据包，进行攻击：





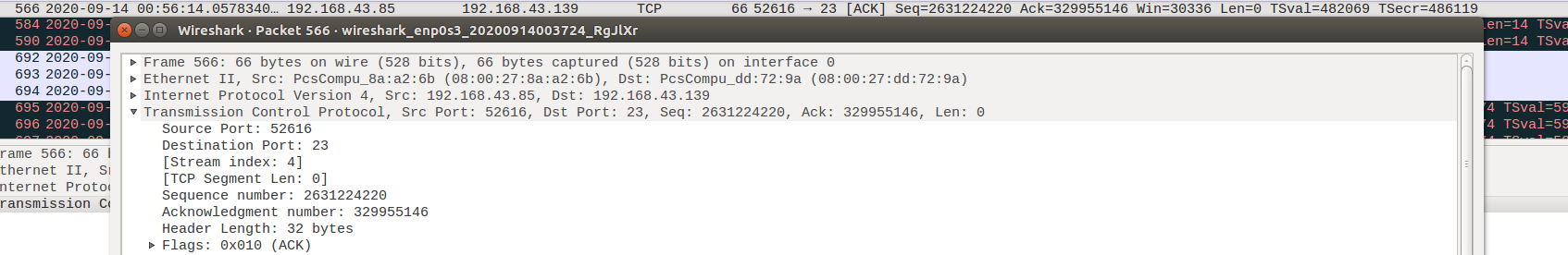
连接被停止，攻击成功：



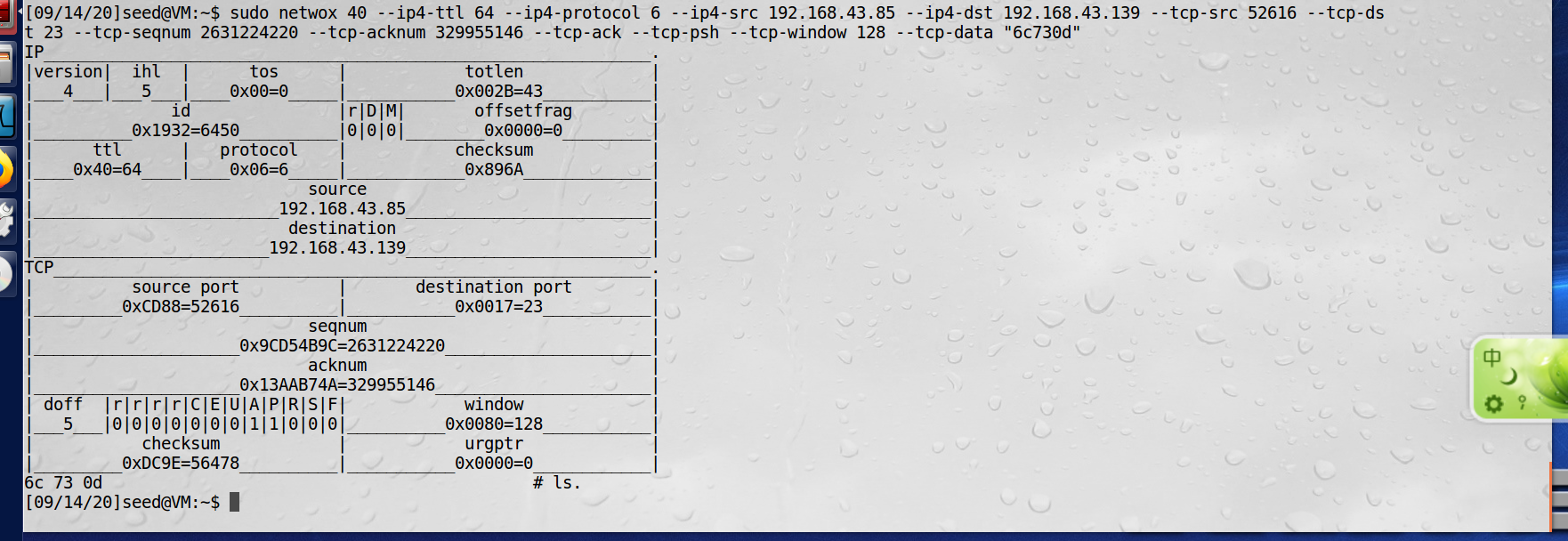
**Task 4: TCP Session Hijacking**

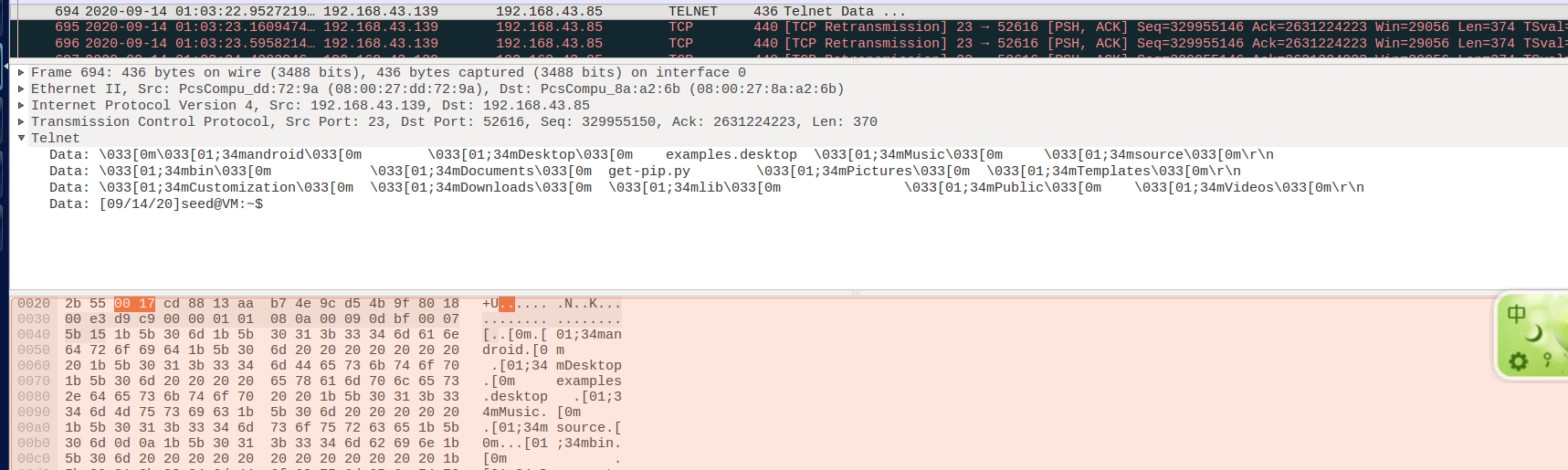
获得攻击所需的十六进制形式语句、端口号、分段号等信息：



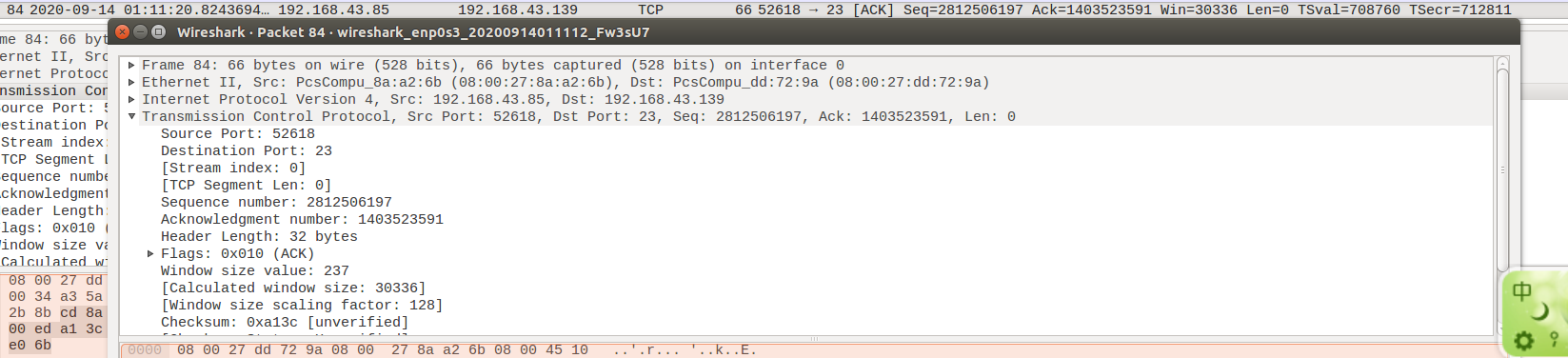


使用netwox进行TCP劫持攻击；攻击成功，被攻击者执行了攻击者伪造报文中的“ls”指令：





重新获取相关信息：



使用scapy进行TCP劫持攻击；攻击成功，被攻击者执行了攻击者伪造报文中的“ls”指令：

