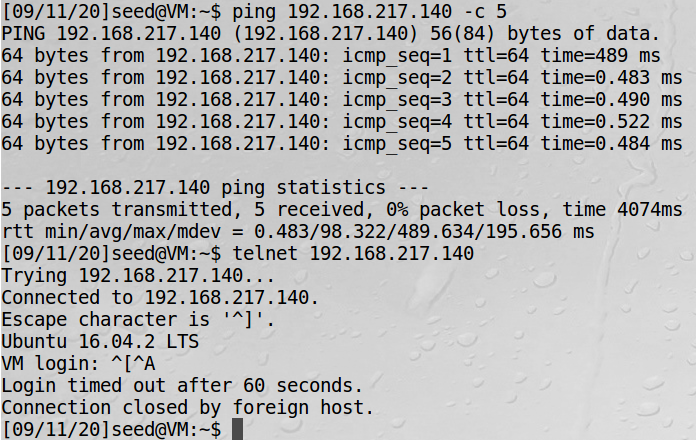
**Task 1: SYN Flooding Attack**

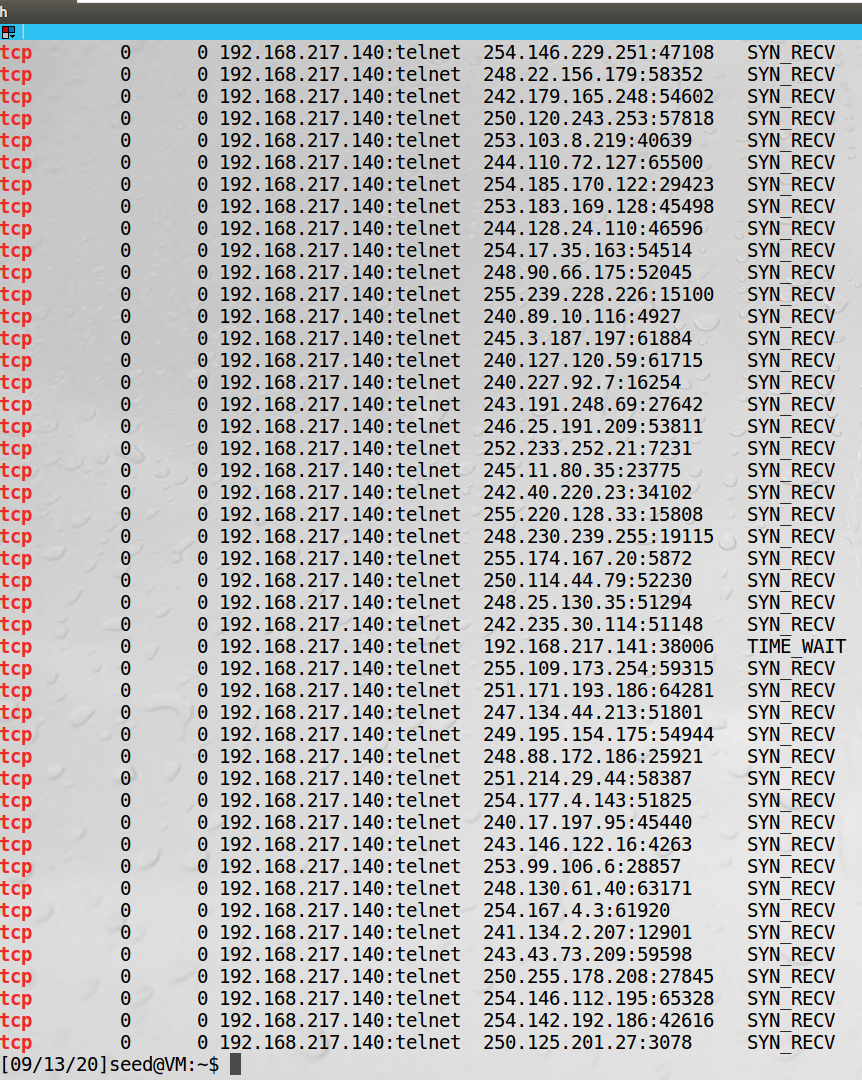
一共设三台VM虚拟机，A（192.168.217.140），B（192.168.217.141）和C（192.168.217.142）



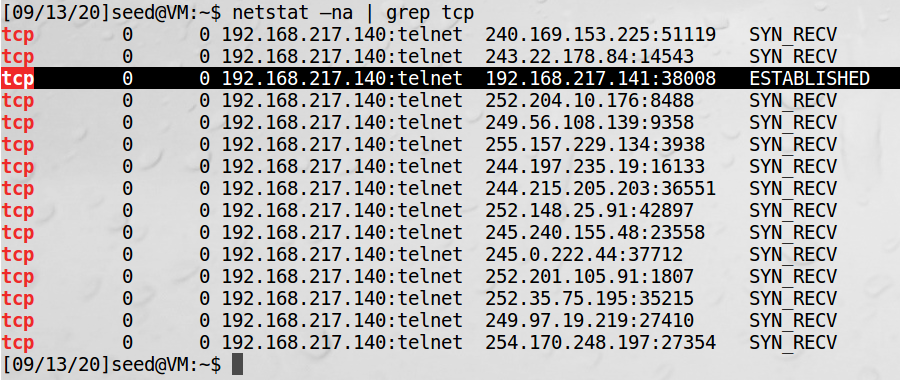
尝试在主机B上telnet登陆A，telnet端口默认是23，正常情况下是可以完成操作的。



当A关闭SYN　cookie时，并进行SYN攻击，可以发现存在大量处于SYN\_RECV状态的连接，而B主机的连接被阻塞了。

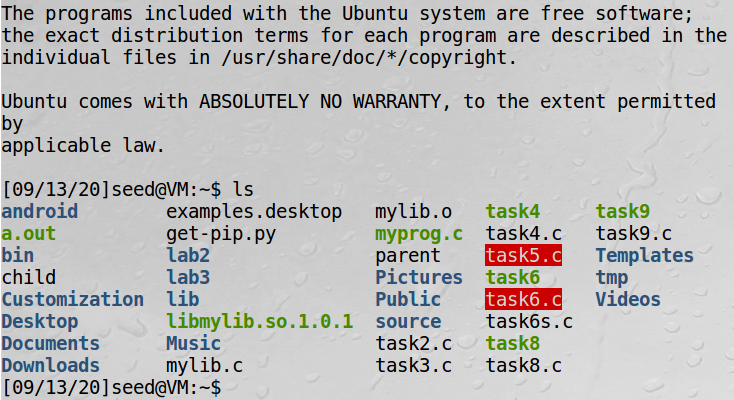


当A打开SYN　cookie时，进行SYN攻击，可以发现处于SYN\_RECV状态的连接大大减少，而B主机的连接也正常建立了。

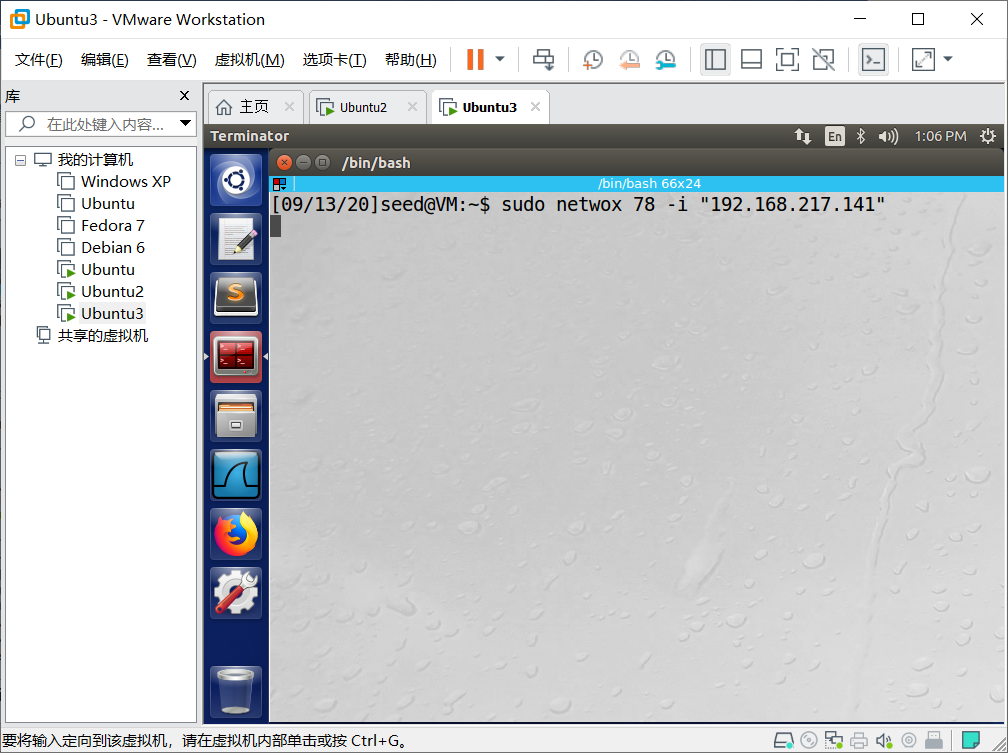


**Task 2: TCP RST Attacks on telnet and ssh Connections**

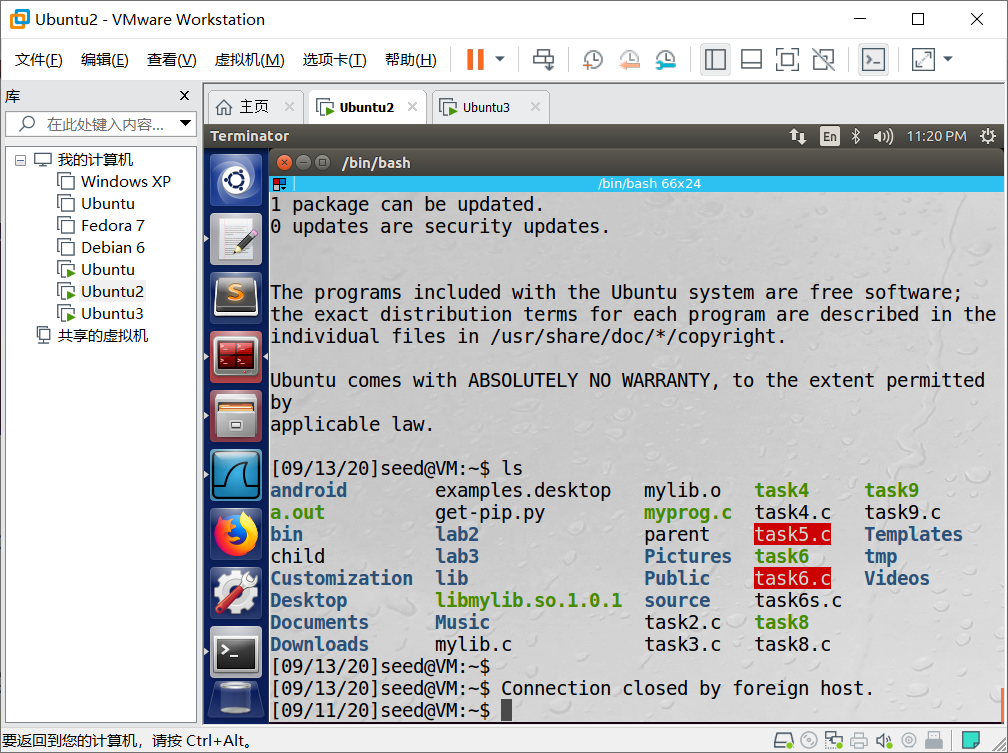




B使用telnet远程登录A虚拟机，正常情况下可以完成一些操作（ls）。

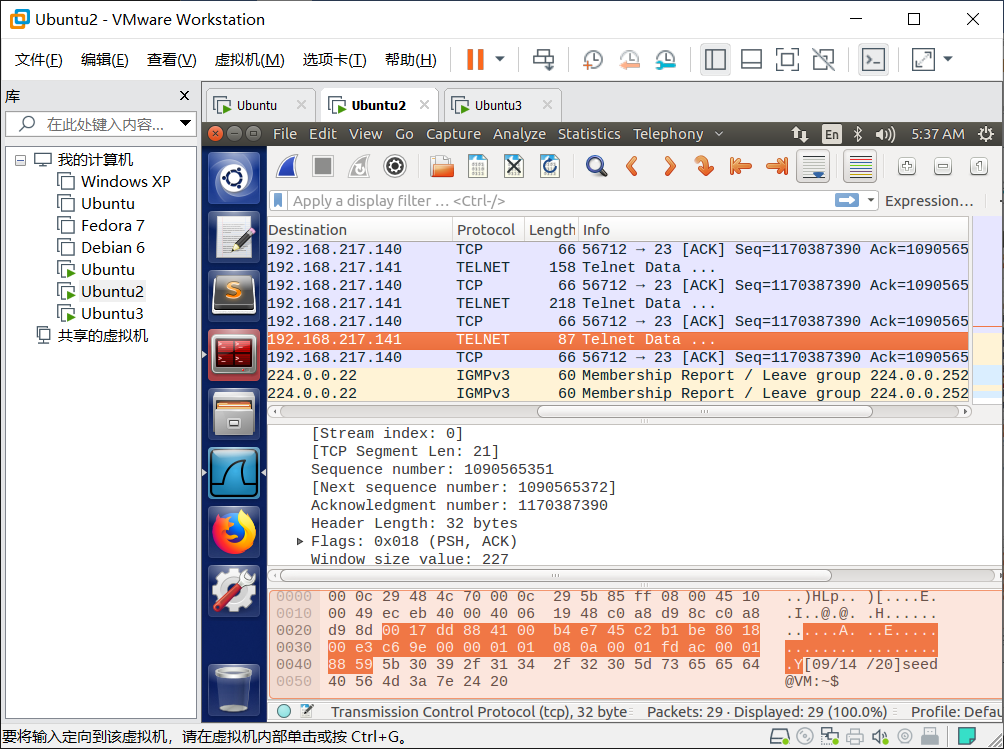


在C上对B进行TCP RST攻击。可以发现A与B的连接被中断了。

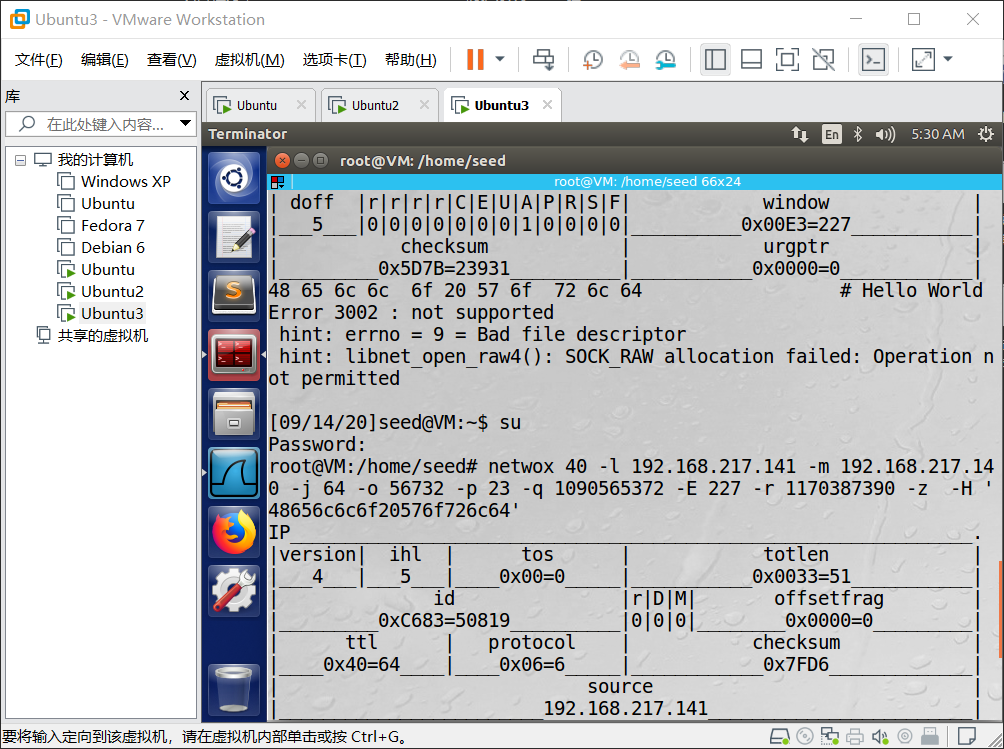


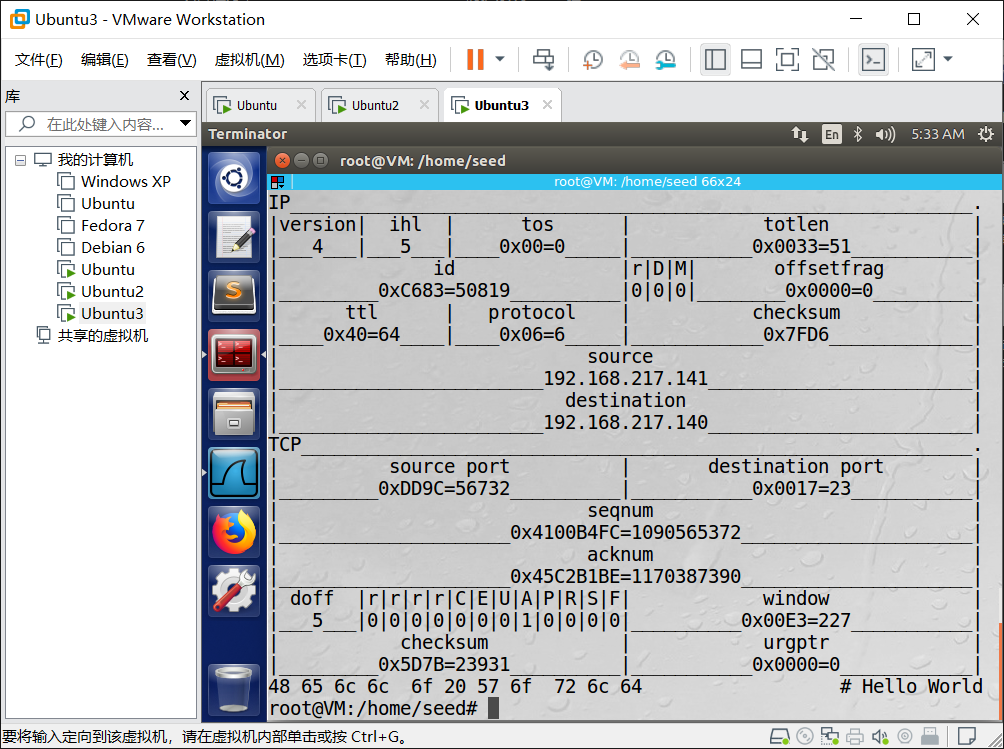
**Task 4: TCP Session Hijacking**

在B上远程登陆A，建立telnet连接。截获连接的报文分析，尝试构建攻击报文。



在攻击者C上使用netwox 40命令进行攻击。设置源地址、目的地址等必要的参数，这里尤其要注意的是攻击报文seq和ack字段的选择，seq字段和ack字段分别是最近一次的回复报文的ack字段和seq字段。发送的数据是hello world。





可以看到已成功伪造TELNET连接欺骗了目的主机A。

