TCP/IP Attack Lab

**Task1: SYN Flooding Attack**

主机A（攻击）：172.20.10.8

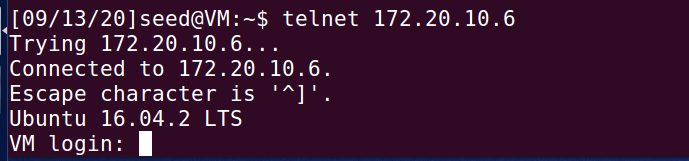
主机B (靶机)：172.20.10.6

主机C (测试)：172.20.10.7

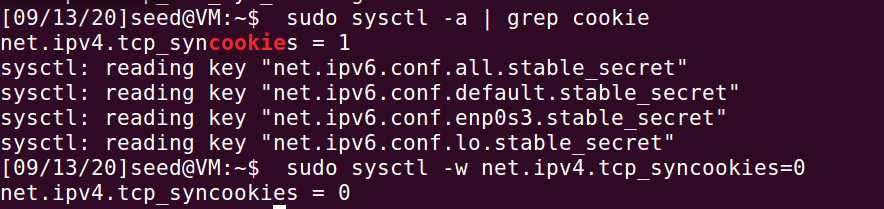
先查看靶机系统的tcp队列的最大容量

****

攻击前，在C主机中，使用telnet连接B，可以成功登陆

****

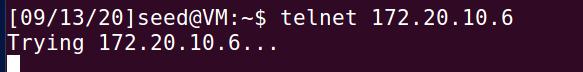
将B主机中的保护措施关掉

****

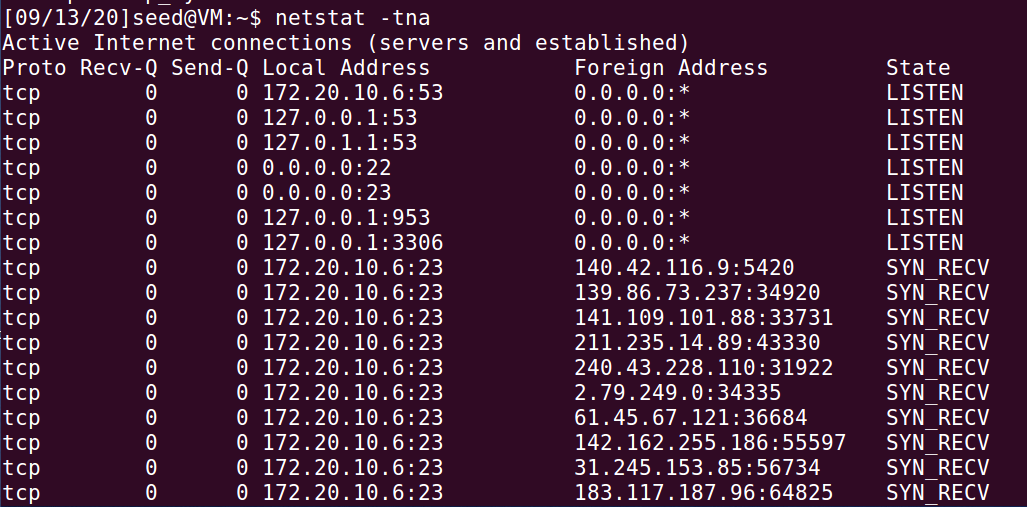
在主机A中对主机B发起攻击

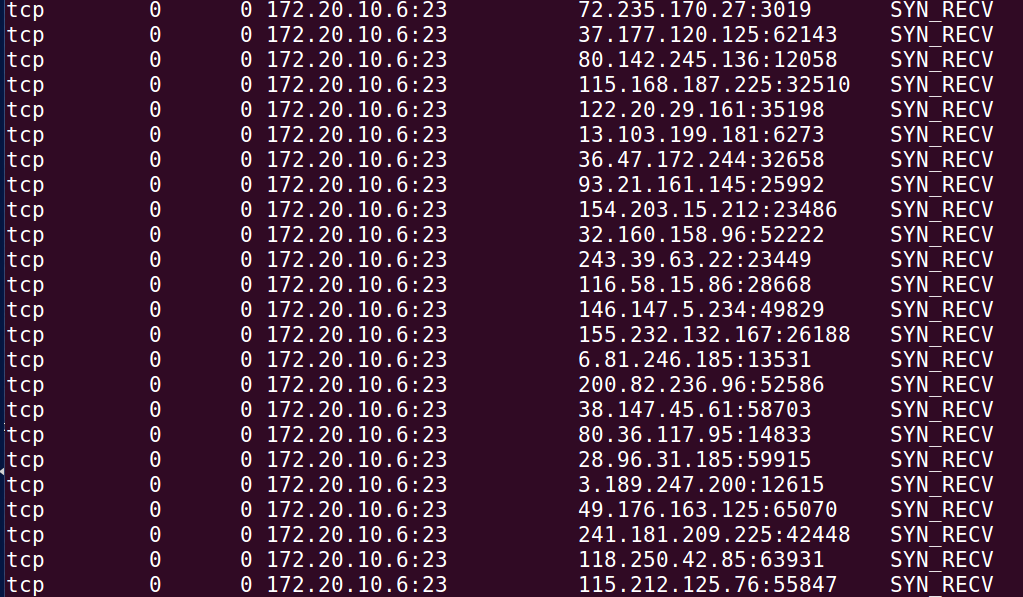
****

在主机c中尝试使用telnet连接主机B,此时已经连接不上

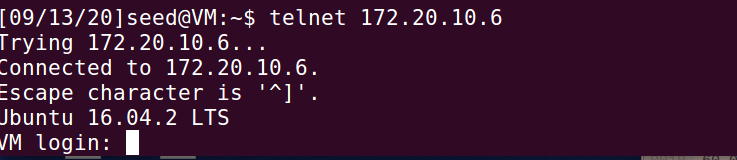
****

在主机B中发现，有大量的由随机地址发送过来的tcp连接请求拥塞在缓存中。

****

****

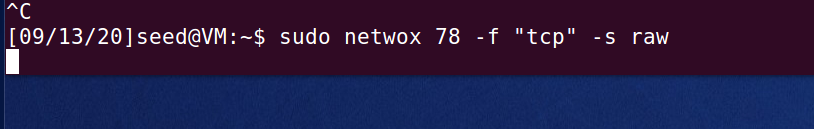
此时打开B主机上的保护，再次使用主机c连接主机B, 发现可以连接上。

****

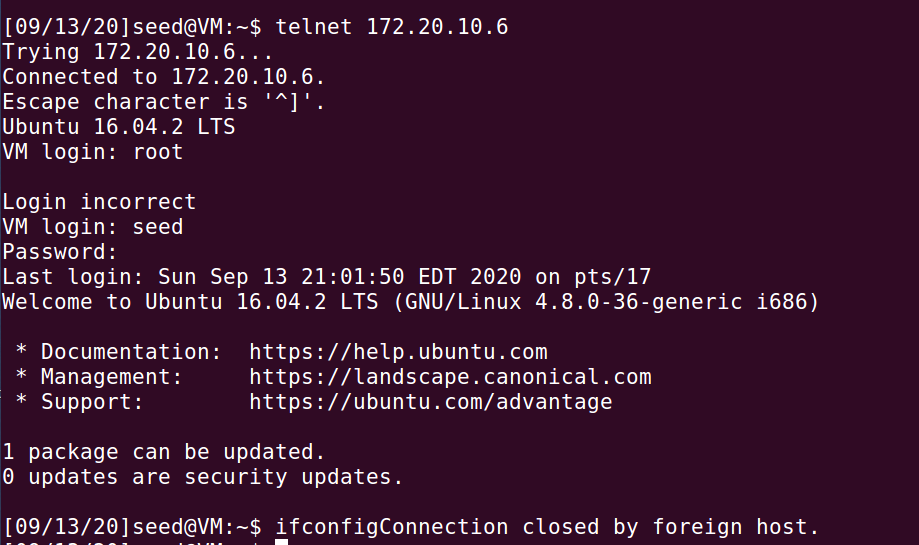
**Task2: TCP RST Attacks on telnet and ssh Connections**

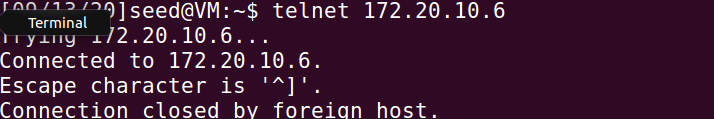
**Using Netwox.**

在主机A中实施攻击

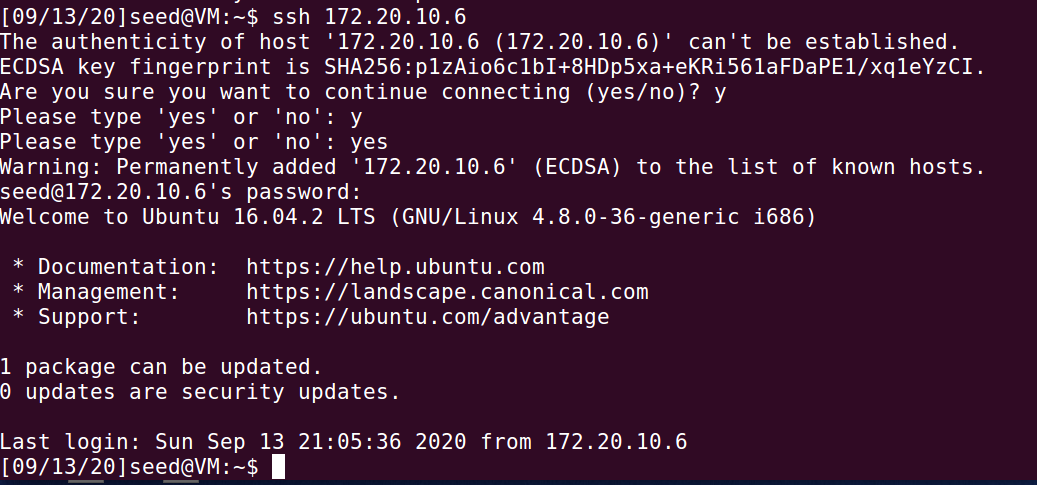
****

发现主机C与主机B的telnet连接被迅速切断，且无法通过多次连接成功登陆

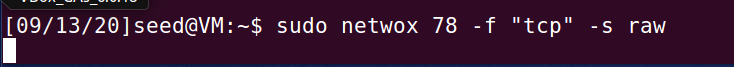
****

****

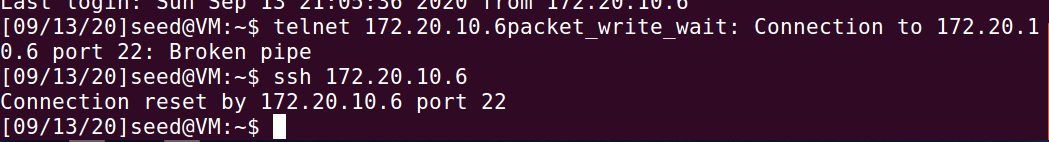
使用主机C SSH服务连接主机B

****

在主机A中使用netwox进行TCP RST攻击

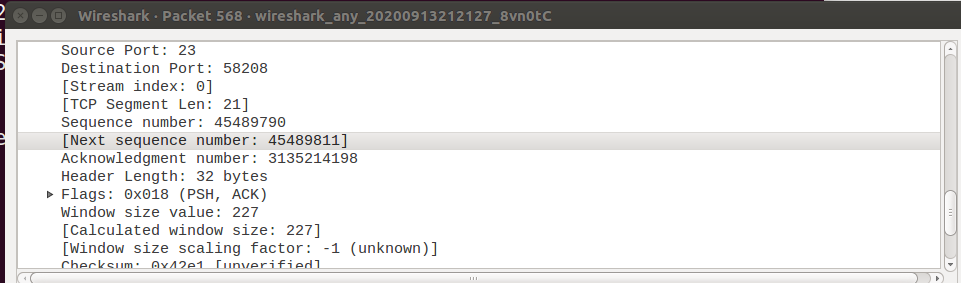


发现主机C上的ssh连接被切断，且无法通过重新连接而恢复

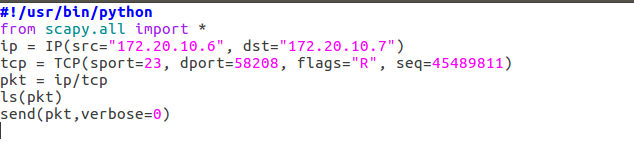
****

**使用scapy**

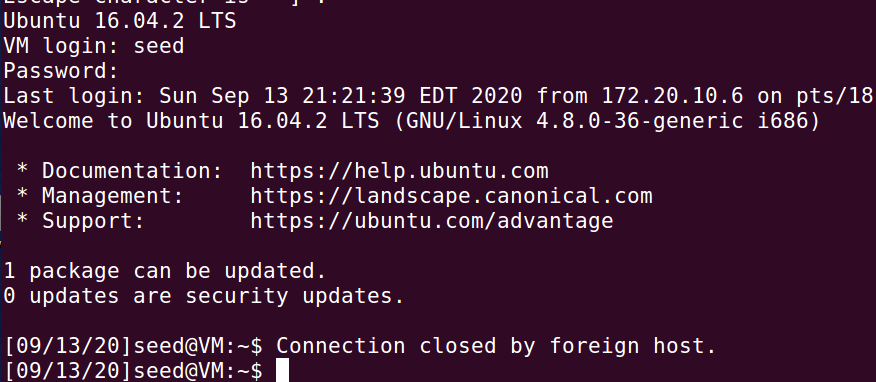
在c主机的wireshark中获取最新的主机B向主机C发送的telnet数据包，找到对应的sport，dport和seq

****

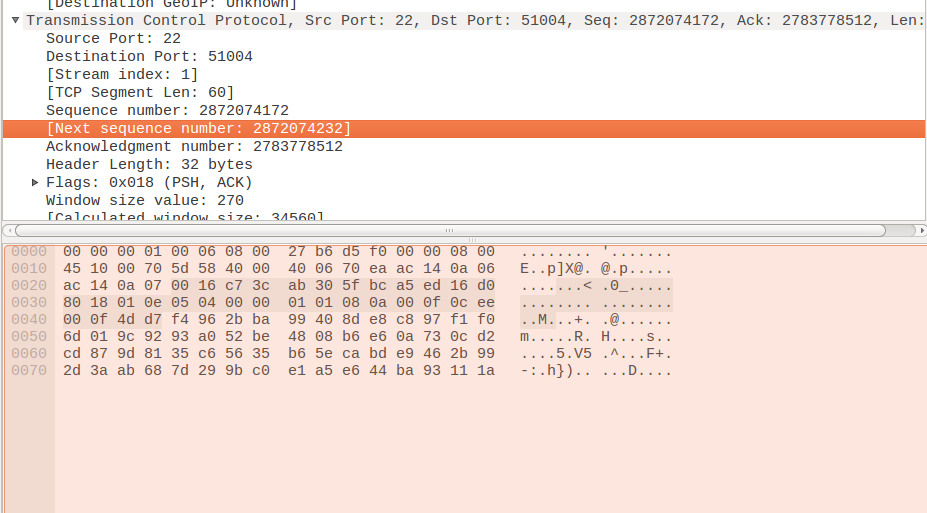
编写攻击代码，并在a中运行

****

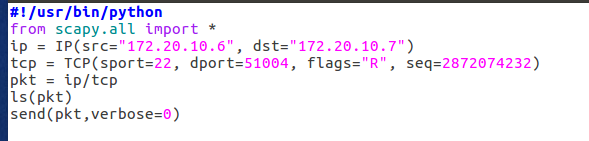
发现主机C与主机B的连接被切断

****

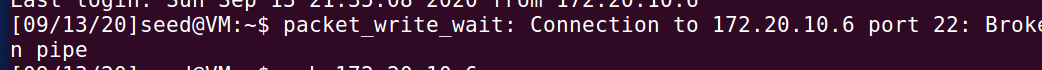
同样，在主机c中获取ssh连接的数据



编写攻击代码并在a中运行



C与B的ssh连接被切断

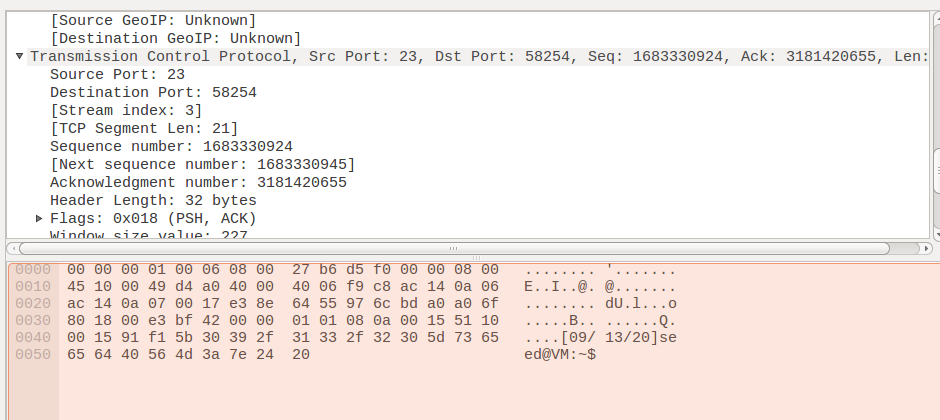


**Task4: TCP Session Hijacking**

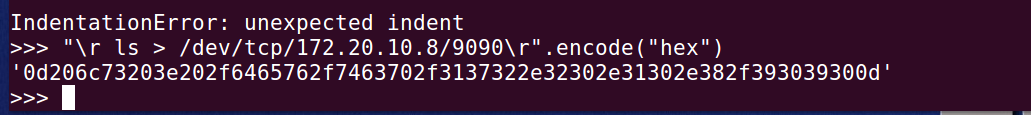
**Using netwox**

C主机使用telnet远程登录B

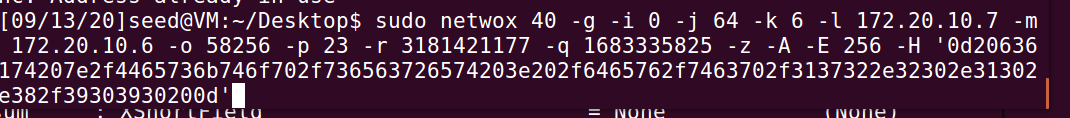
使用wireshark查看B发送给C的最后一个telnet数据包

****

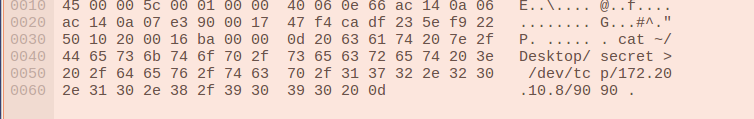
使用python2将命令encode成指定格式

****

根据前面的数据包编写命令



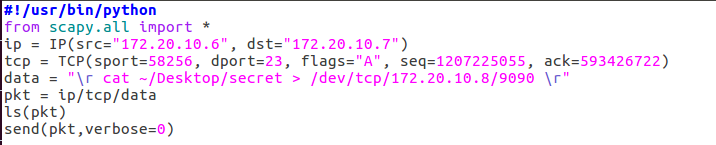
在c中wiresharirk查看伪造数据包发送成功。

****

**使用scapy：**

使用c主机重新连接b主机并查看最后一个数据包

根据数据包内容编写代码

****

运行后重新再c端抓包，可以发现结果与上一个一致（伪造数据包成功）