**Lab4 Report**

**TCP/IP Attack Lab**

57117107 赵笛言

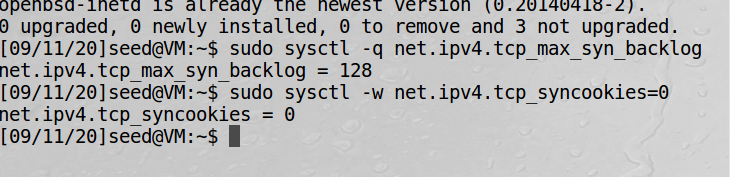
**LabTasks：**

首先进行网络设置。 要进行此实验，需要三台计算机，一台计算机用于攻击，第二台计算机用于受害者，第三台计算机用于观察者。然后将主机用作第三台计算机。将它们放在同一局域网内。

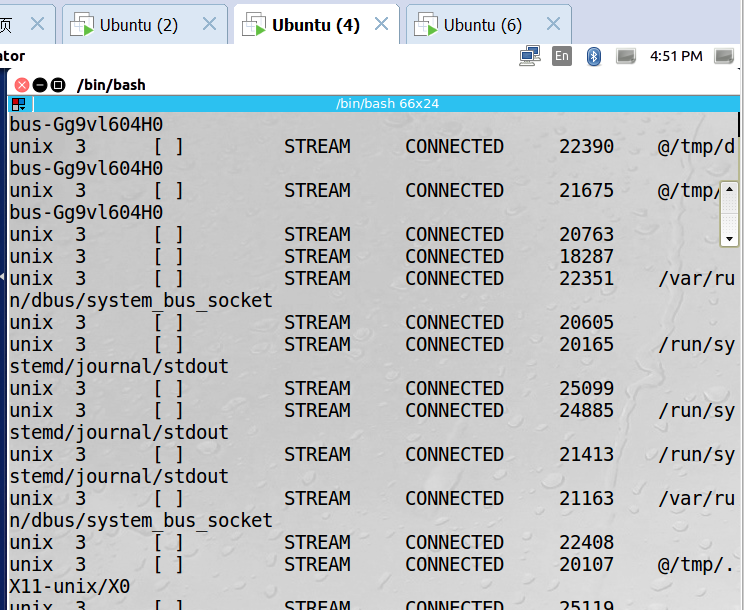
因此有攻击者A(192.168.118.150)，受害者B(192.168.118.151)，观察者C(192.168.118.153)

Task1: SYN Flooding Attack

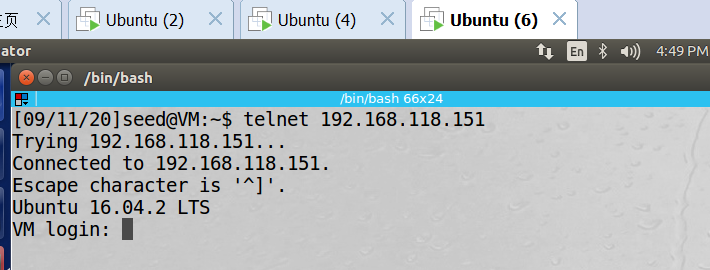
首先关掉防御措施SYN cookies：



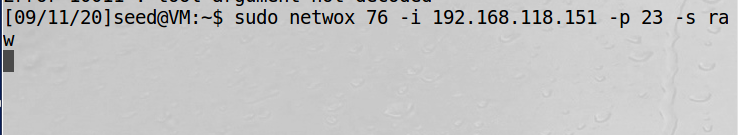
然后通过netstat -a命令查看B主机目前的连接状况，没有半打开链接：



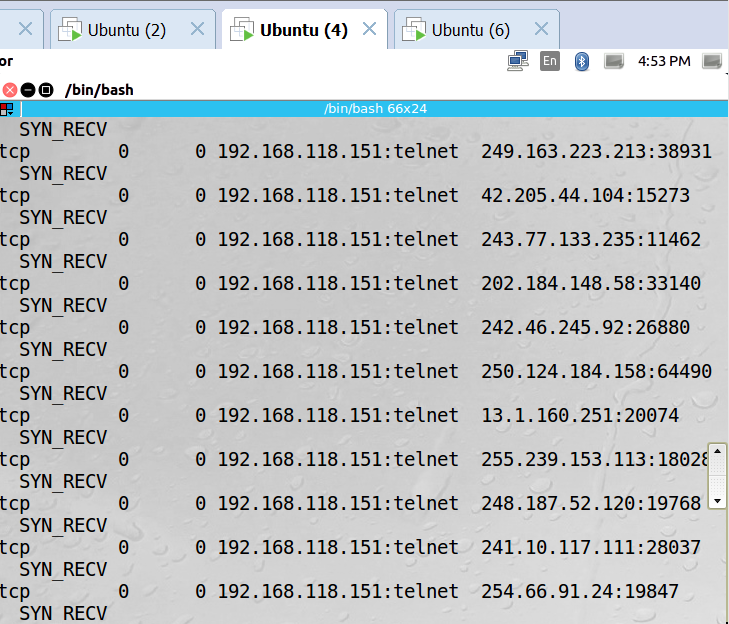
接下来再通过主机C telnet连接B：



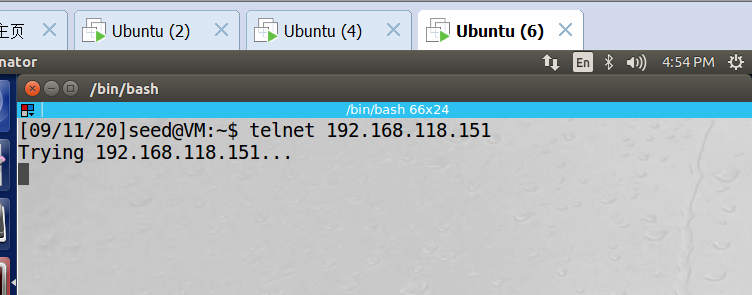
接下来通过A开始攻击：



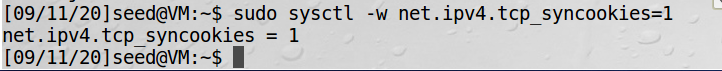
再通过同样的netstat -a命令查看，出现很多半连接：

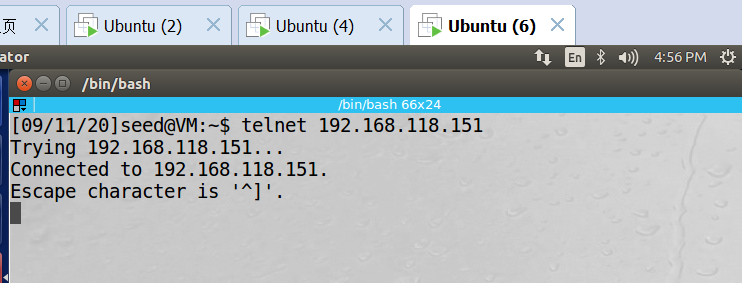


再次使用C来尝试连接：（失败）



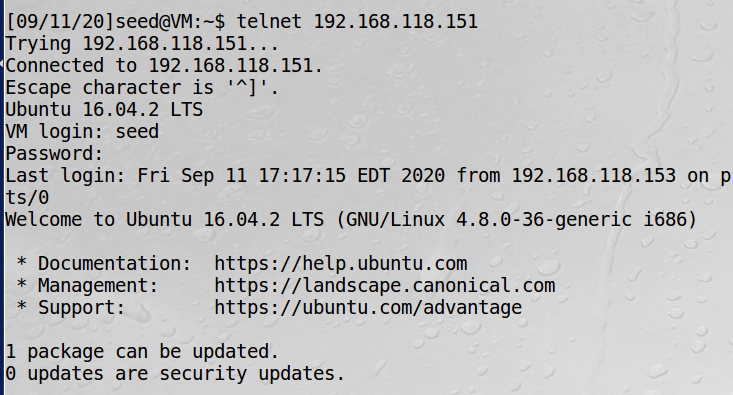
此时打开主机B的SYN cookies：



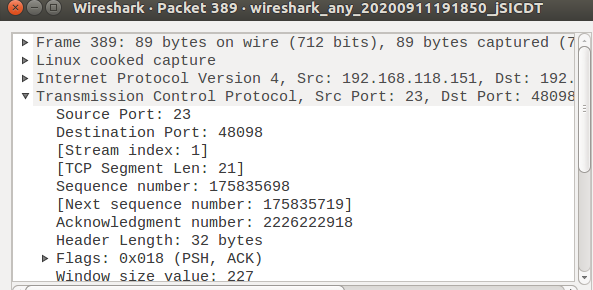
虽然用netstat -a查看B主机还是有很多半连接，但主机C可以进行连接：

Task2: TCP RST Attacks on telnet and ssh Connections

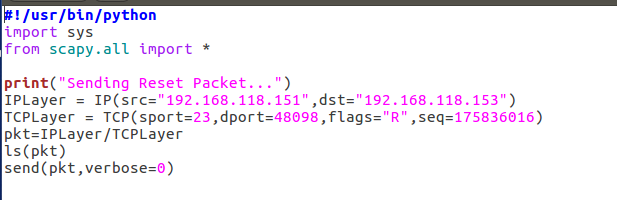
B、C建立telnet连接：



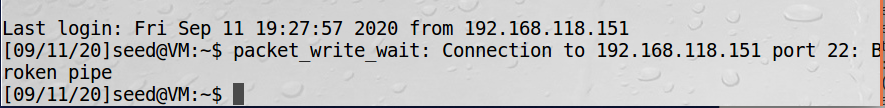
然后利用wireshark查看最后一个数据包信息：



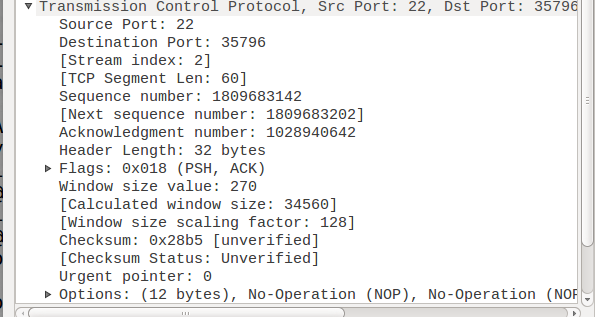
凭此构造reset.py攻击脚本：

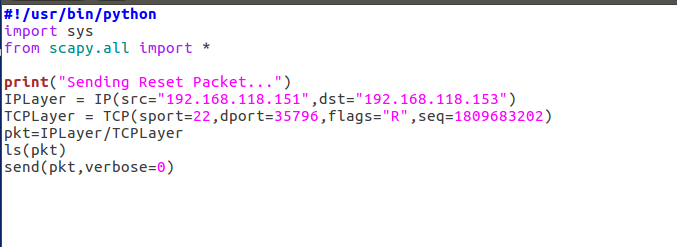


最后可以看见C上显示一下信息攻击成功：

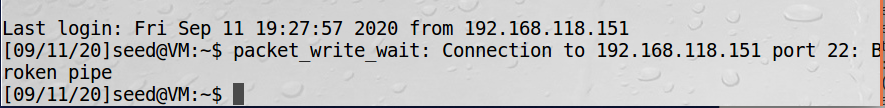


Ssh攻击方式非常类似，同样需要最后一个数据包信息来构造攻击程序：





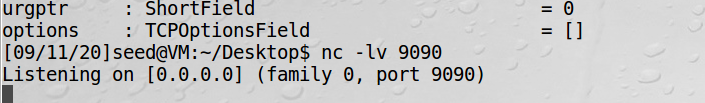
最后攻击成功：



Task4: TCP Session Hijacking

先查看攻击原理：

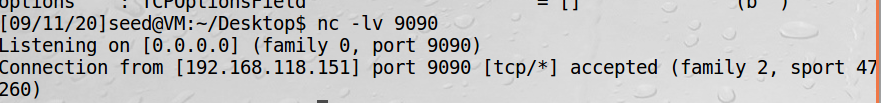
先在A机上输入：



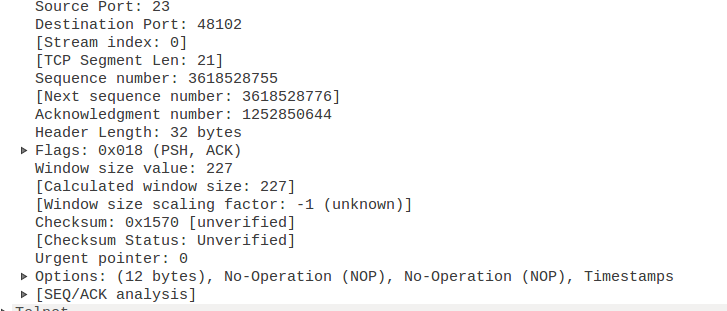
再在B机上输入：



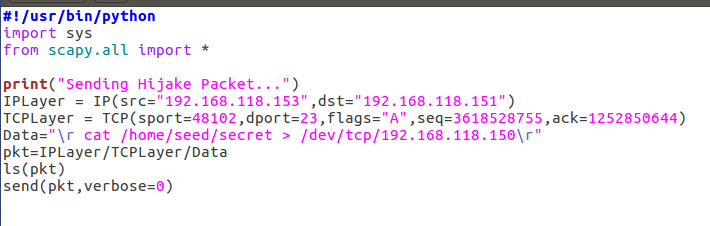
A机可以显示：



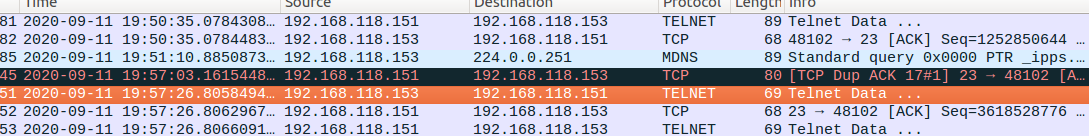
因此可以再根据数据包信息：



构造攻击程序：



攻击结果如下：



总结：感觉Lab4比Lab3好上手，一边看教材一边做比较容易。（还因为只选了90分）。但最后一个会话劫持在攻击数据选择来命中时一直出现问题难以解决。

做安全类的实验真的很需要耐心。