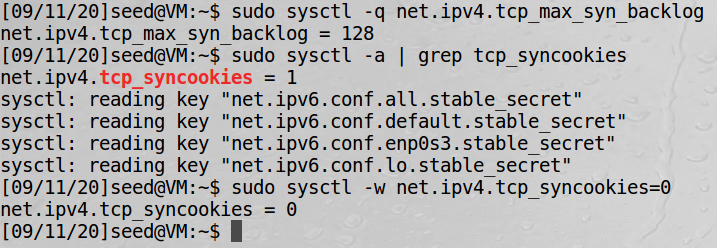
**实验1：TCP/IP Attack Lab**

## Task 1: SYN Flooding Attack

首先在被攻击的主机（10.0.2.8）上检查最大连接数，关闭syn cookie



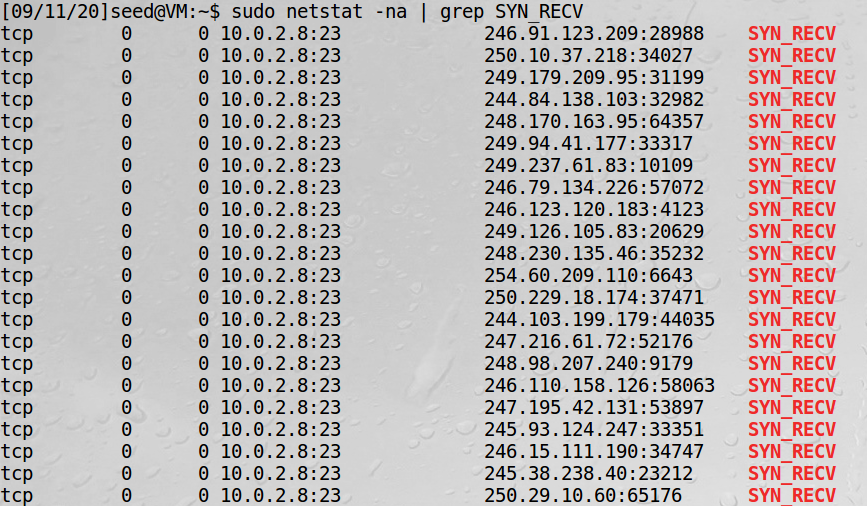
在攻击前，被攻击的主机上没有SYN——RECV状态的连接



在攻击者主机（10.0.2.9）上对10.0.2.8的23端口进行攻击



在被攻击的主机上可以观察到很多半开连接



在将syn cookie打开后，发现被攻击的主机似乎可以支持更多的连接

原理是：使用一种特殊的算法生成Sequence Number，这种算法考虑到了对方的IP、端口、己方IP、端口的固定信息，以及对方无法知道而己方比较固定的一些信息，如MSS、时间等，在收到对方的ACK报文后，重新计算一遍，看其是否与对方回应报文中的（SequenceNumber-1）相同，从而决定是否分配TCB资源。

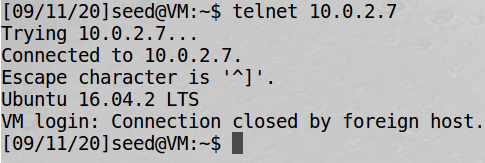
## Task 2: TCP RST Attacks on telnet and ssh Connections

① 使用netwox

在10.0.2.8运行以下命令



这时在10.0.2.9上进行telnet 10.0.2.7时，telnet连接建立的过程会被终止



在10.0.2.8运行以下命令

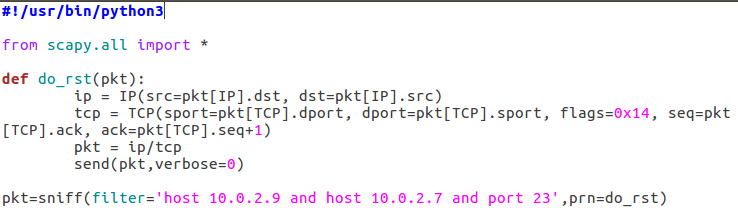


这时在10.0.2.9上进行ssh 10.0.2.7时，ssh连接建立的过程会被终止

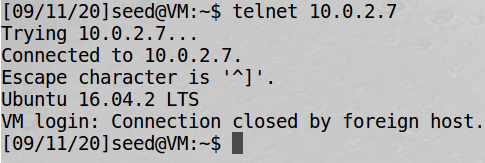


② 使用scapy

在10.0.2.8运行下面的代码



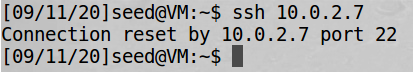
这时在10.0.2.9上进行telnet 10.0.2.7时，telnet连接建立的过程会被终止



将前面的代码最后一行改为



这时在10.0.2.9上进行ssh 10.0.2.7时，ssh连接建立的过程会被终止



## Task 4：TCP Session Hijacking

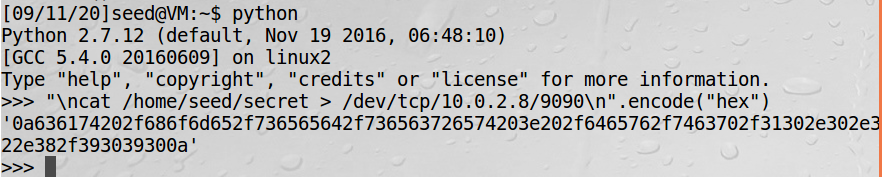
10.0.2.8作为攻击者主机，在这个主机上开一个shell，并监听9090端口



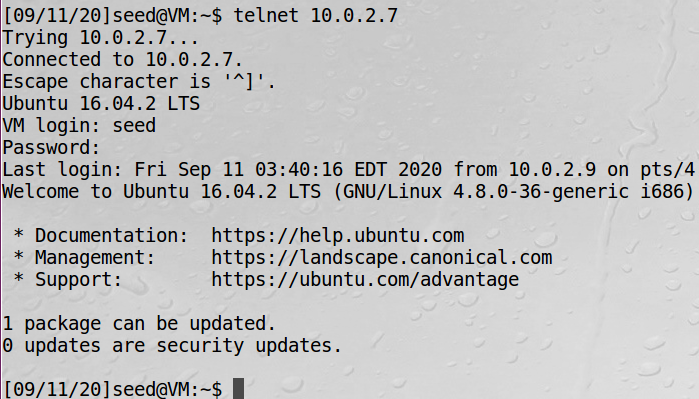
10.0.2.7作为服务器，在服务器上创建一个秘密文件，攻击者的目标是获取服务器上秘密文件的内容



将攻击者要使用的报文负载从字符串编码为16进制

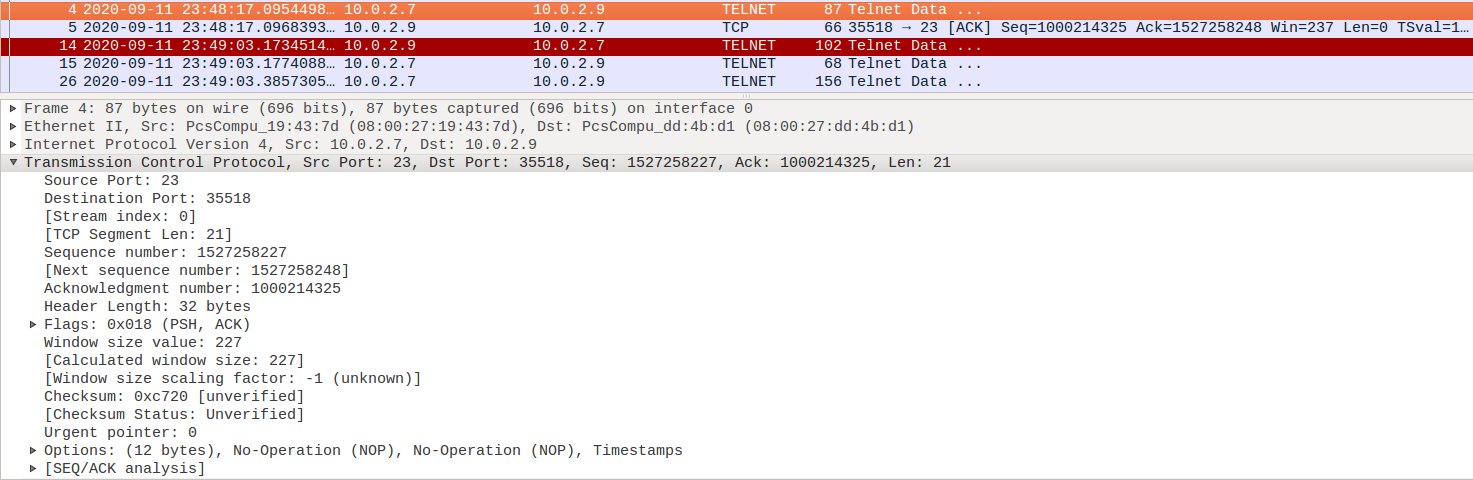


10.0.2.9作为用户，与10.0.2.7服务器建立telnet连接

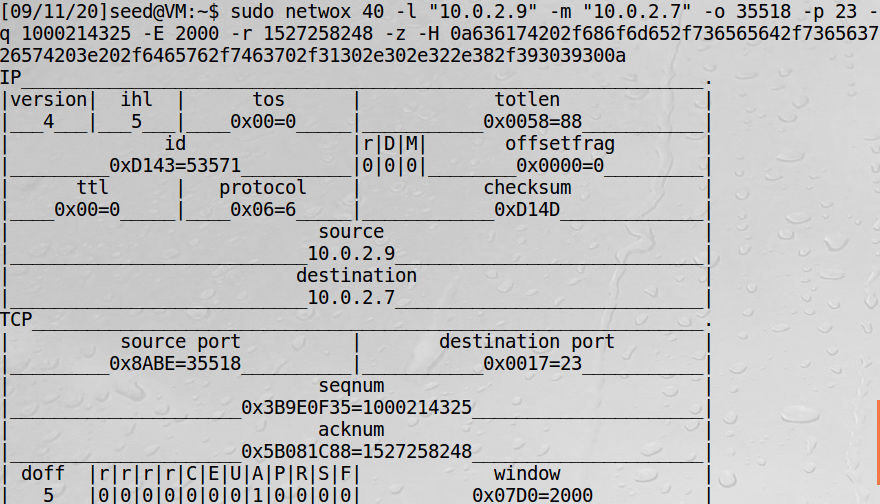


① 使用netwox

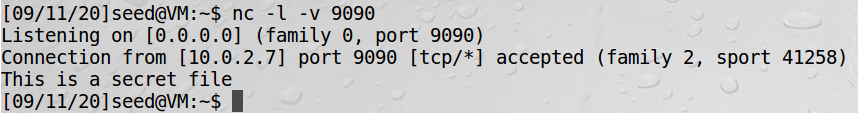
攻击者用wireshark抓包，捕捉服务器发给用户的最后一个tcp报文



从中可以得到源端口、目的端口、seq、ack的值，然后使用netwox进行攻击

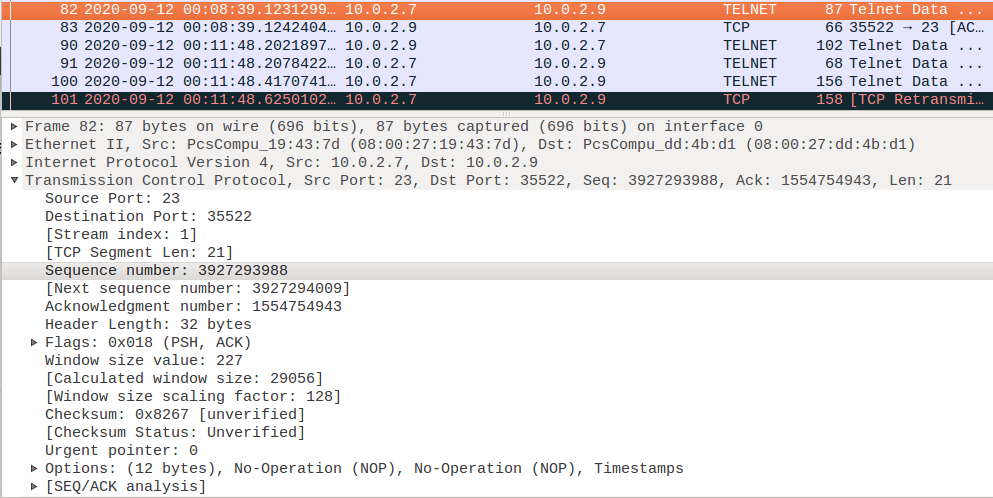


攻击者得到了秘密文件的内容

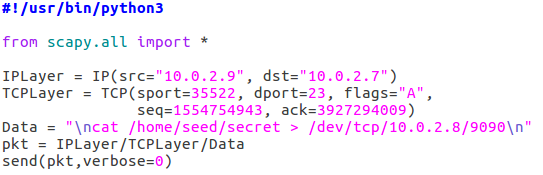


② 使用scapy

同样，我们使用wireshark捕捉最后一个报文



从中可以得到源端口、目的端口、seq、ack的值，然后使用scapy构造攻击报文



攻击成功

