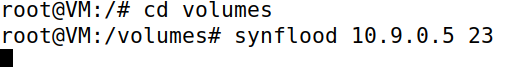
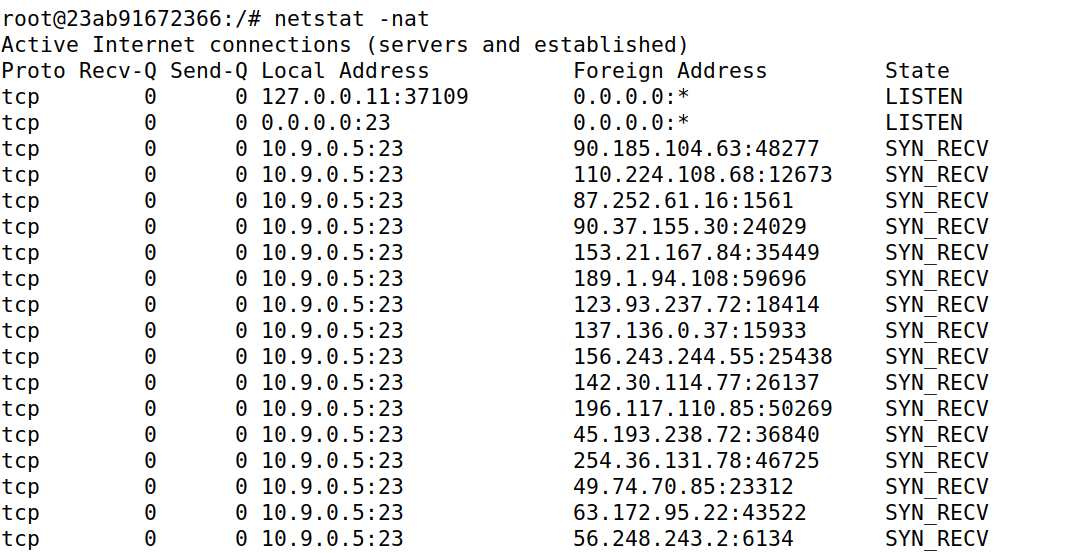
LAB2 57118226 舒钰淇

Task 1: SYN Flooding Attack

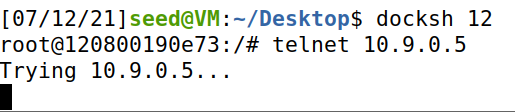
在虚拟机上编译synflood.c，进入攻击者主机运行



可以看到受害主机收到大量SYN\_RECV报文

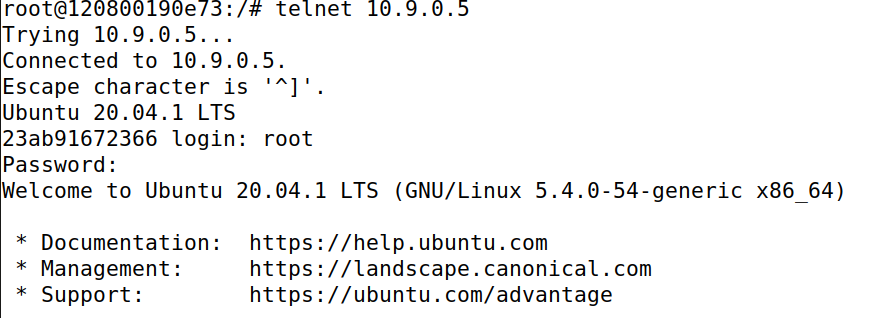


在另一个主机上进行telnet，卡在trying阶段无法连接，攻击成功



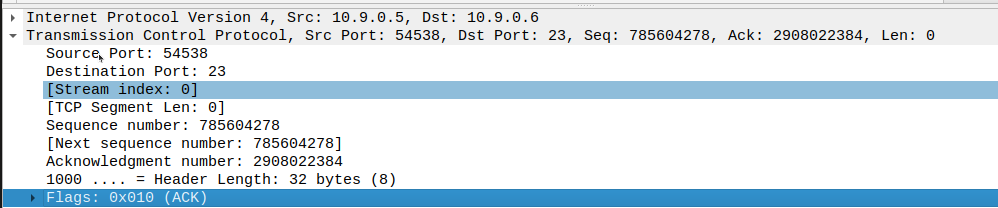
将tcp\_syncookies值改为1，重新运行synflood，再次尝试telnet，telnet成功，攻击失败。



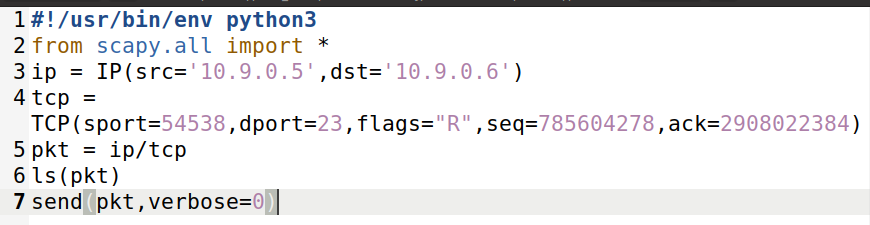


Task 2:TCP RST Attacks on telnet Connections

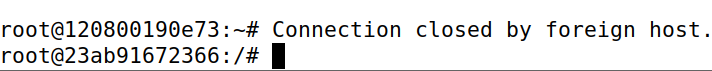
在受害主机（10.9.0.5）上telnet 10.9.0.6，用waireshark找到最后一次ack报文



利用其中的端口和序列号信息编写如下程序

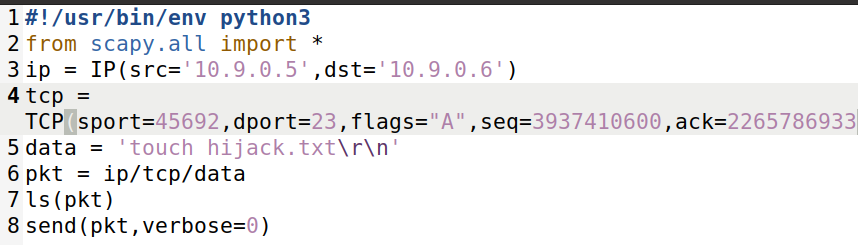


在攻击者主机上运行，可以看到telnet连接被断开



Task 3: TCP Session Hijacking

编写如下程序，劫持TCP会话，在telnet的主机上创建一个名为hijack.txt的文件

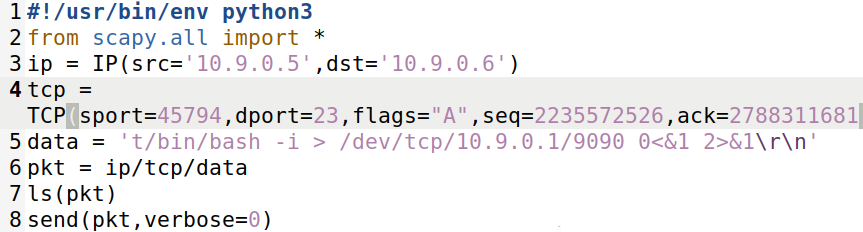


在两个主机已经建立telnet连接时，运行上图所示程序，发出telnet请求的主机卡死，重新telnet后执行ls命令，可以看见TCP会话成功劫持并创建文件。



Task 4: Creating Reverse Shell using TCP Session Hijacking

编写如下程序，劫持会话进行反向shell。



监听9090端口，运行程序，可以看到攻击成功。

