**TCP/IP Attack Lab**

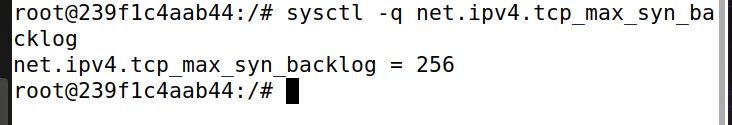
姓名：57118223 姓名：齐天一

Task1：

1. **环境配置**

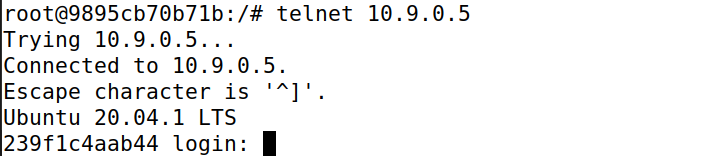
首先创建容器，包括攻击者容器，受害者容器，其它用户容器

在受害者容器输入指令可以查看系统队列的长度：



**（2）在正常情况下远程登录**

在发动泛洪攻击前，先用用户远程登录，发现成功登录了



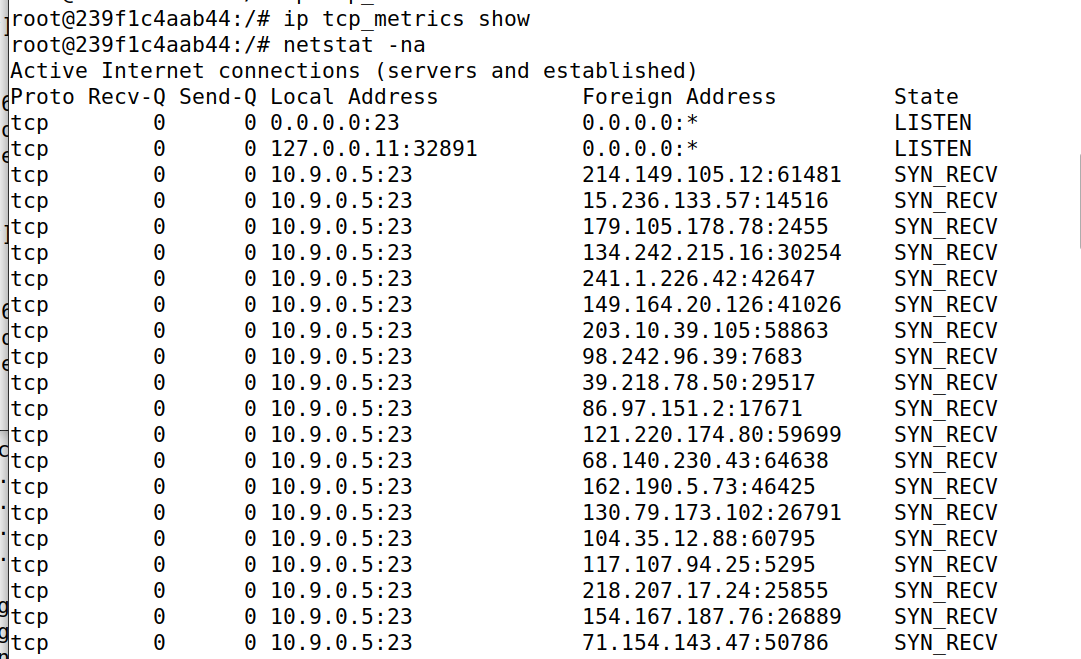
**（3）泛洪攻击下的远程登录**

①首先对攻击程序进行编译（在虚拟机环境下）

在攻击者容器中，输入以下指令，运行synflood程序

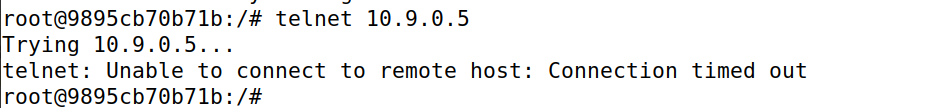
KPRX5]4G2F$D%$MPA4~WFNF

②此时在受害者容器中，输入netstat -na查看信息:



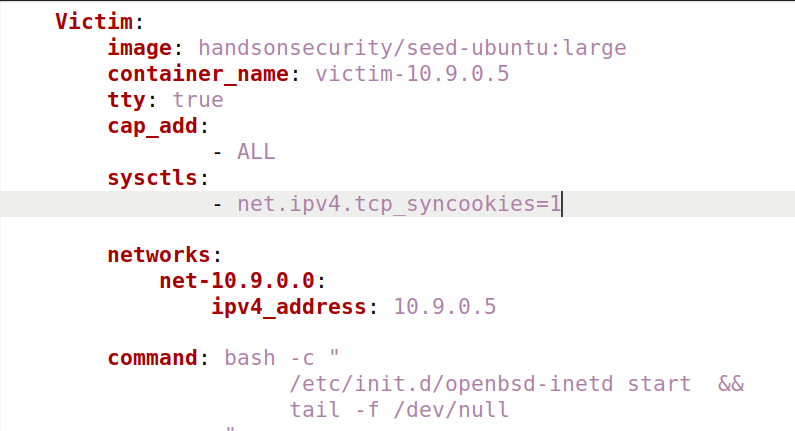
可以看到出现了大量的SYN\_RECV报文，说明只完成了第一次握手,符合泛洪攻击的原理。

③在其它用户容器中，再次尝试登录：

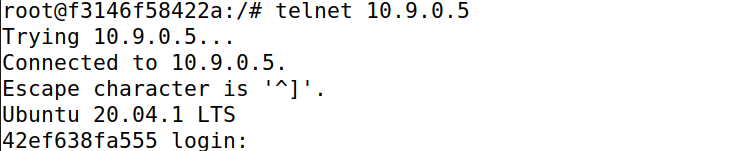
  
可以看到登陆超时，没有成功登录，说明泛洪攻击成功，实现了对其它用户连接的阻碍和干扰。

**（4）打开SYN Cookie后再次进行泛洪攻击**

①首先修改配置文件中syncookies的值，将其修改为1，表示开启：

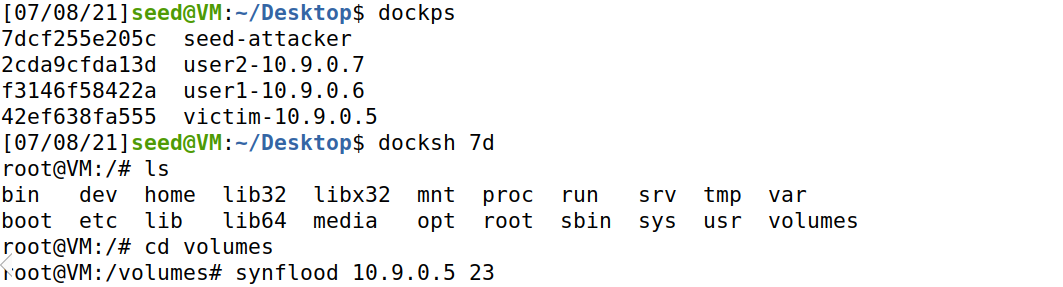


②在不泛洪攻击时，使用用户容器进行登录：

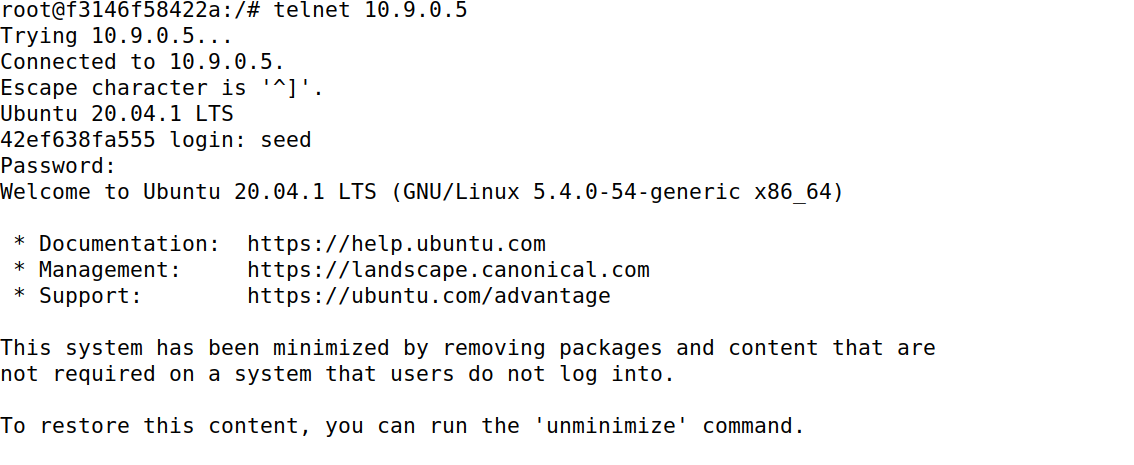


登录成功。

③启动泛洪攻击

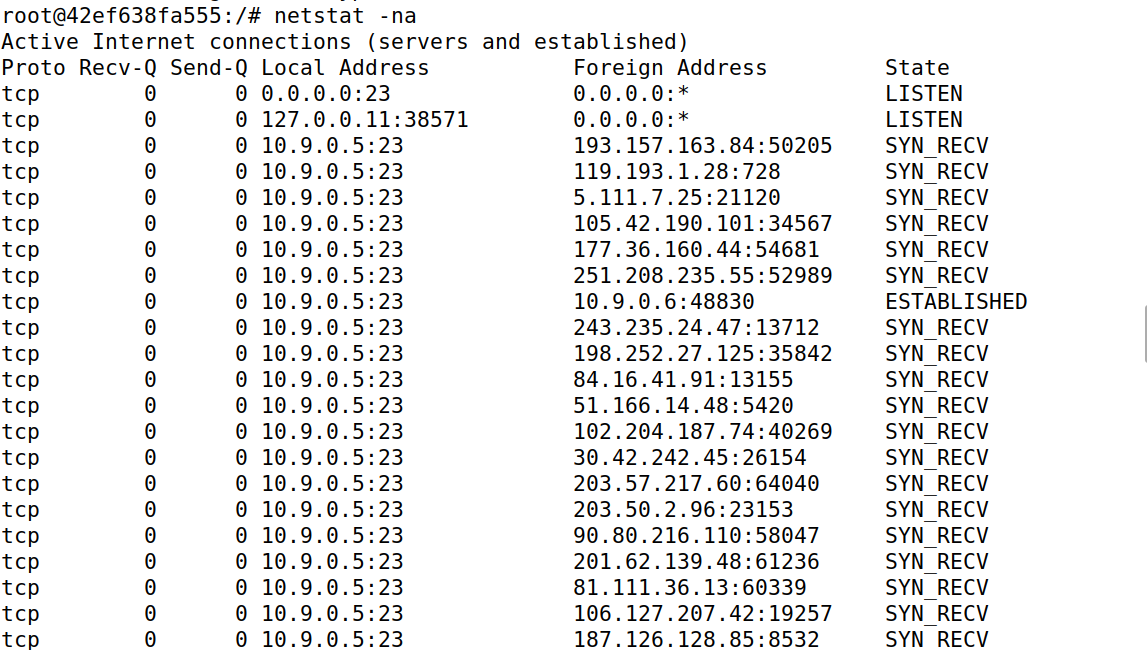


④使用用户进行远程：



可以看到成功实现了登录！成功验证了SYN Cookies对泛洪攻击的防御效果。

在受害者容器中输入netstat -na：



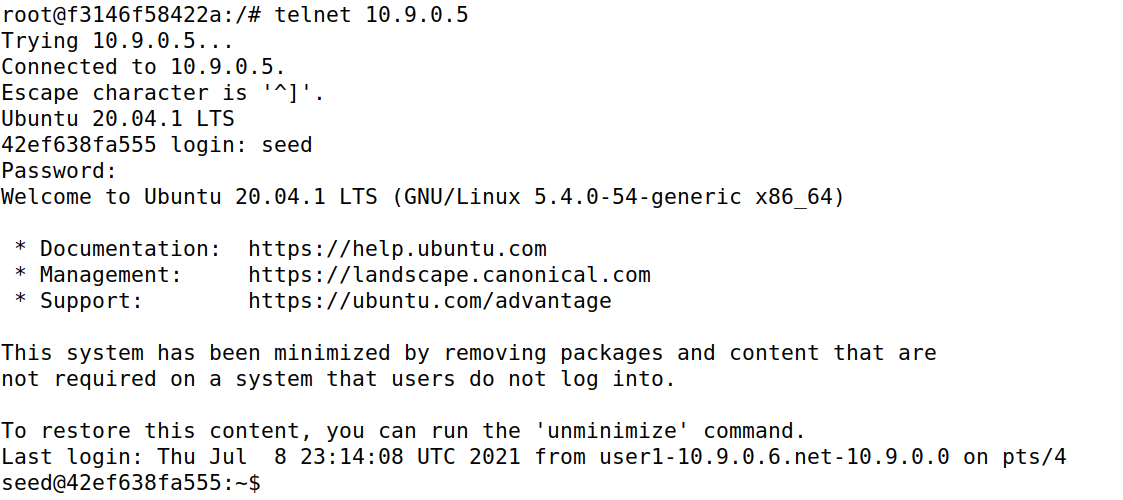
可以看到除了SYN\_RECV，还出现了ESTABLISHED状态，观察ip发现，这个tcp连接对应的就是刚才用户向受害者发起的连接，再次验证了SYN Cookies的效果。

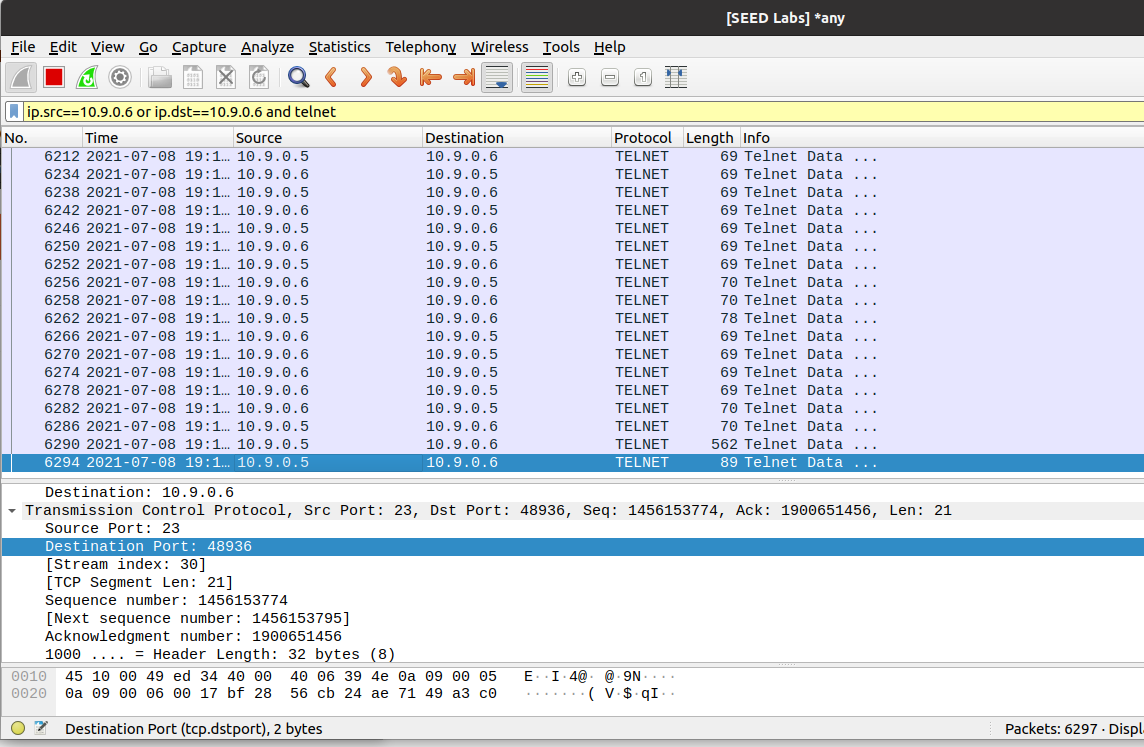
SYN Cookies防范泛洪攻击的原理：

当服务器收到第⼀次握⼿的SYN信息时，它会使用密钥和包中的信息计算一个哈希值，并将哈希值作为服务器的初始序列号发送到客户端，这个H就被称为SYN cookie。当再次收到客户端的请求时，利⽤⾃⼰的密钥校验哈希值的准确性，即可判断这个客户端是否为之前发来第⼀次握⼿的客户端，从而避免了排队问题。

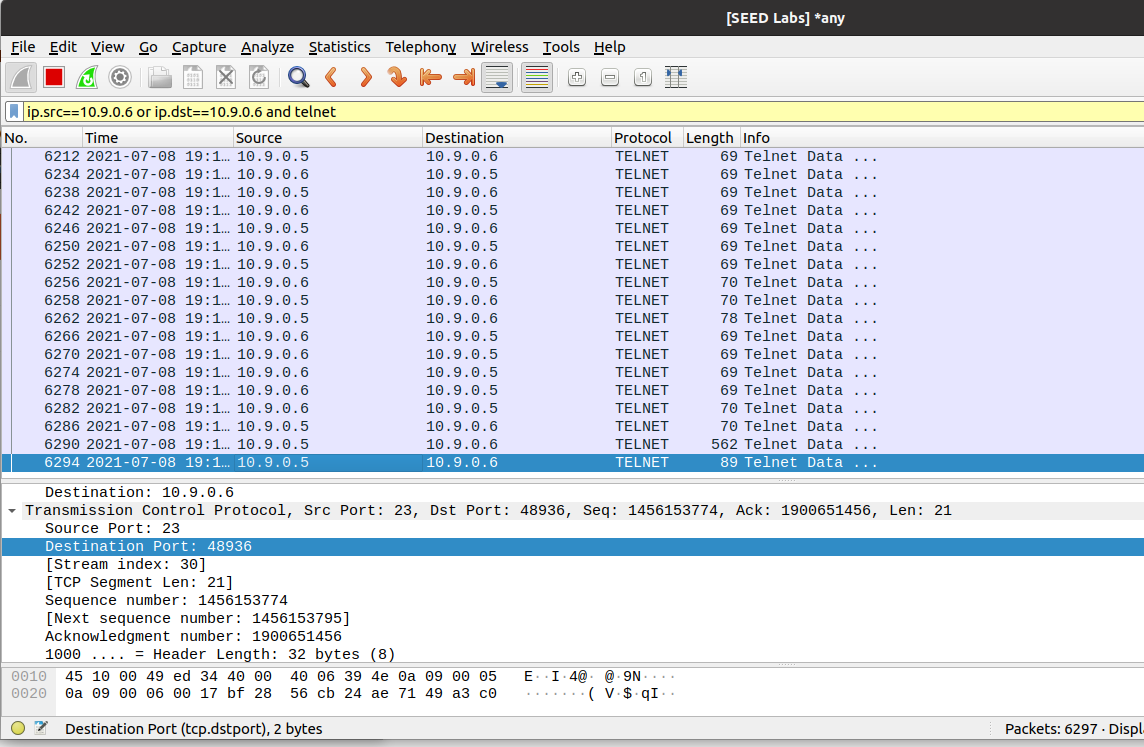
Task2：

①用户容器先向受害者发起talent请求并登录：

  
②打开wireshark检测发动的报文：

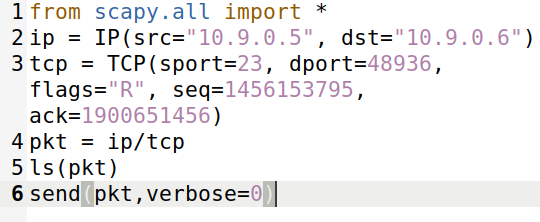


为了找到实验相关的报文，我们使用过滤规则，寻找ip为10.9.0.6(用户ip)且telnet相关报文，找到其中最后一个，查看相应信息：



可以看到目标端口值（48936），下一个seq值（1456153795），ack值（1900651456）。

③将相关信息填入到程序中，用来构造rst报文。



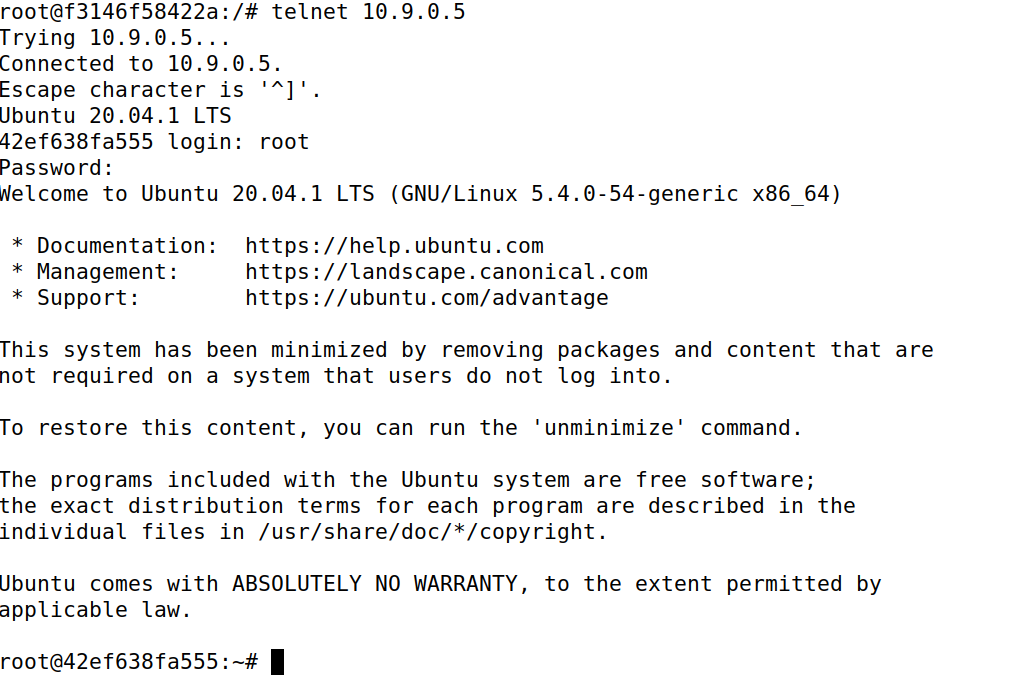
④在攻击者容器运行程序，可以看到，在用户容器中，登录已经断开，说明成功实现了攻击。



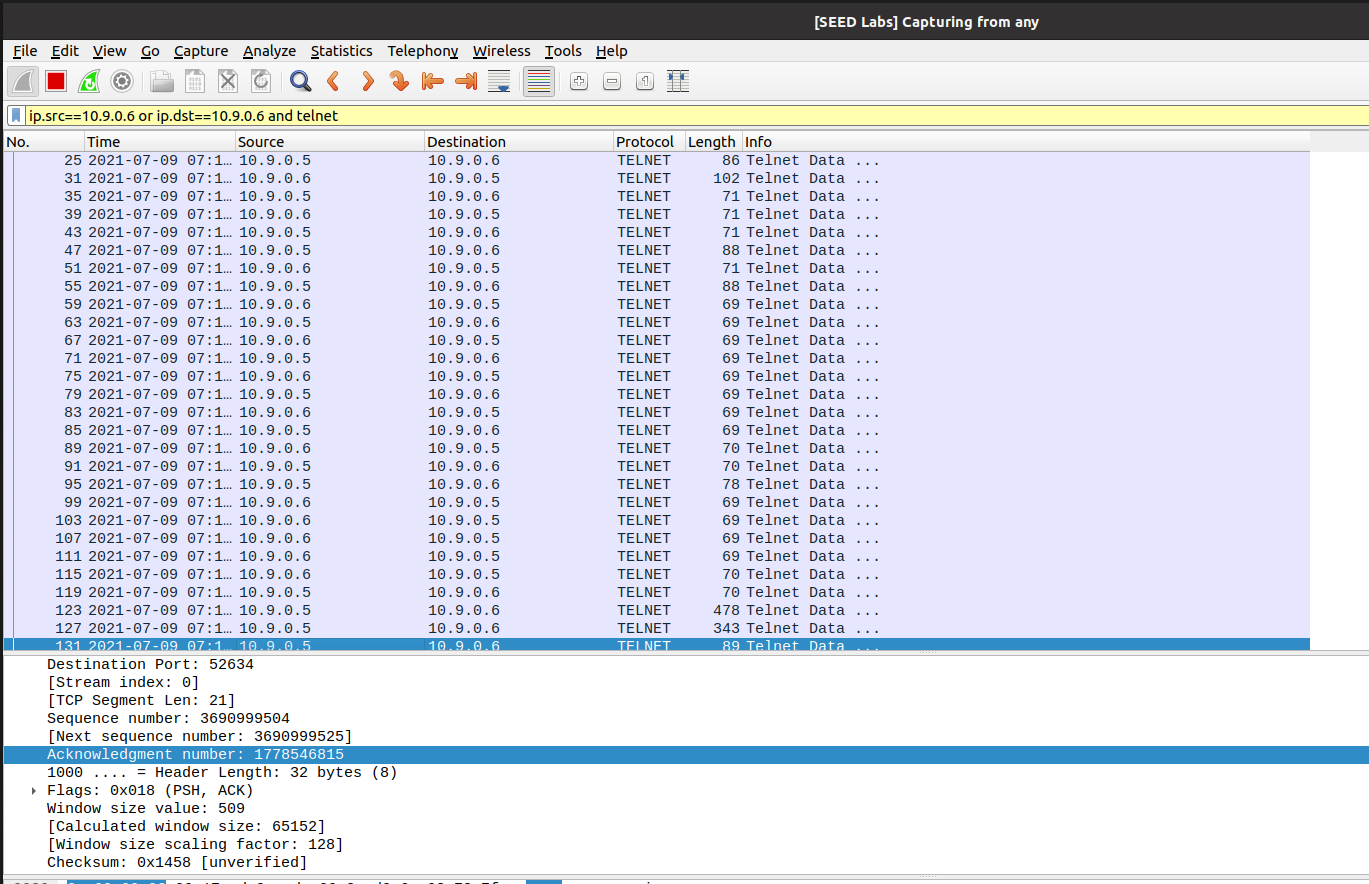
Task3：

在本实验中，由其它用户（10.9.0.6）向受害者发起连接，攻击者截取报文，并将恶意指令放在伪造的用户报文中，发给受害者，从而使受害者执行恶意指令。

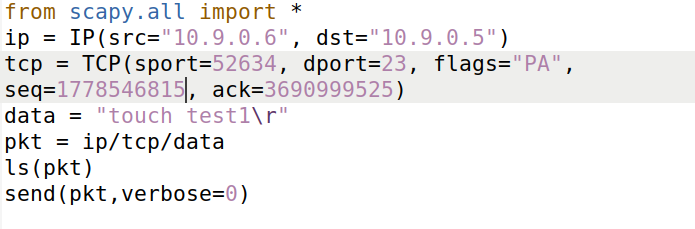
①首先在用户容器中，发起telnet，远程登录受害者：



②使用wireshark观察，用过滤器筛选出本次telnet的报文，选择最后一个报文，根据其信息构造攻击程序。

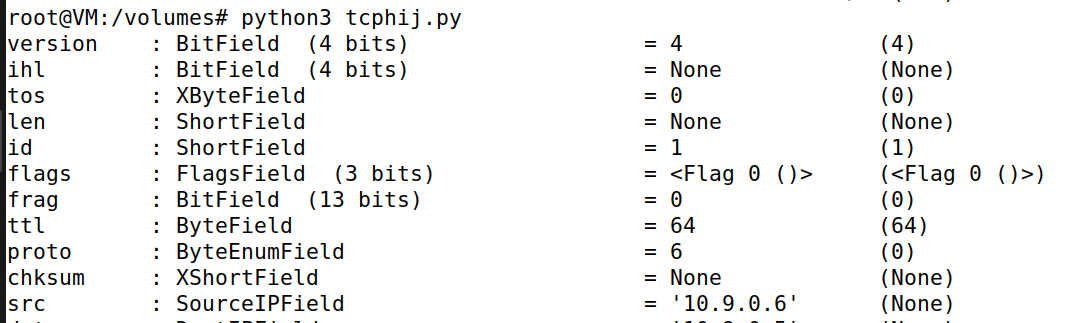


③可以看到，用户的端口为52634，next seq为3690999504，ack为1778546815

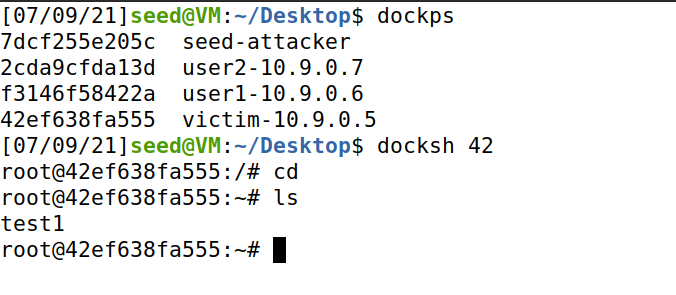
因此构造代码如下：  


其中seq为上一个报文的ack值，ack值为上一个报文的next seq，同时flags设为PA。同时为了体现攻击效果，我们在data中加入一个用于创建文件夹指令“touch test1\r”，由受害者执行。

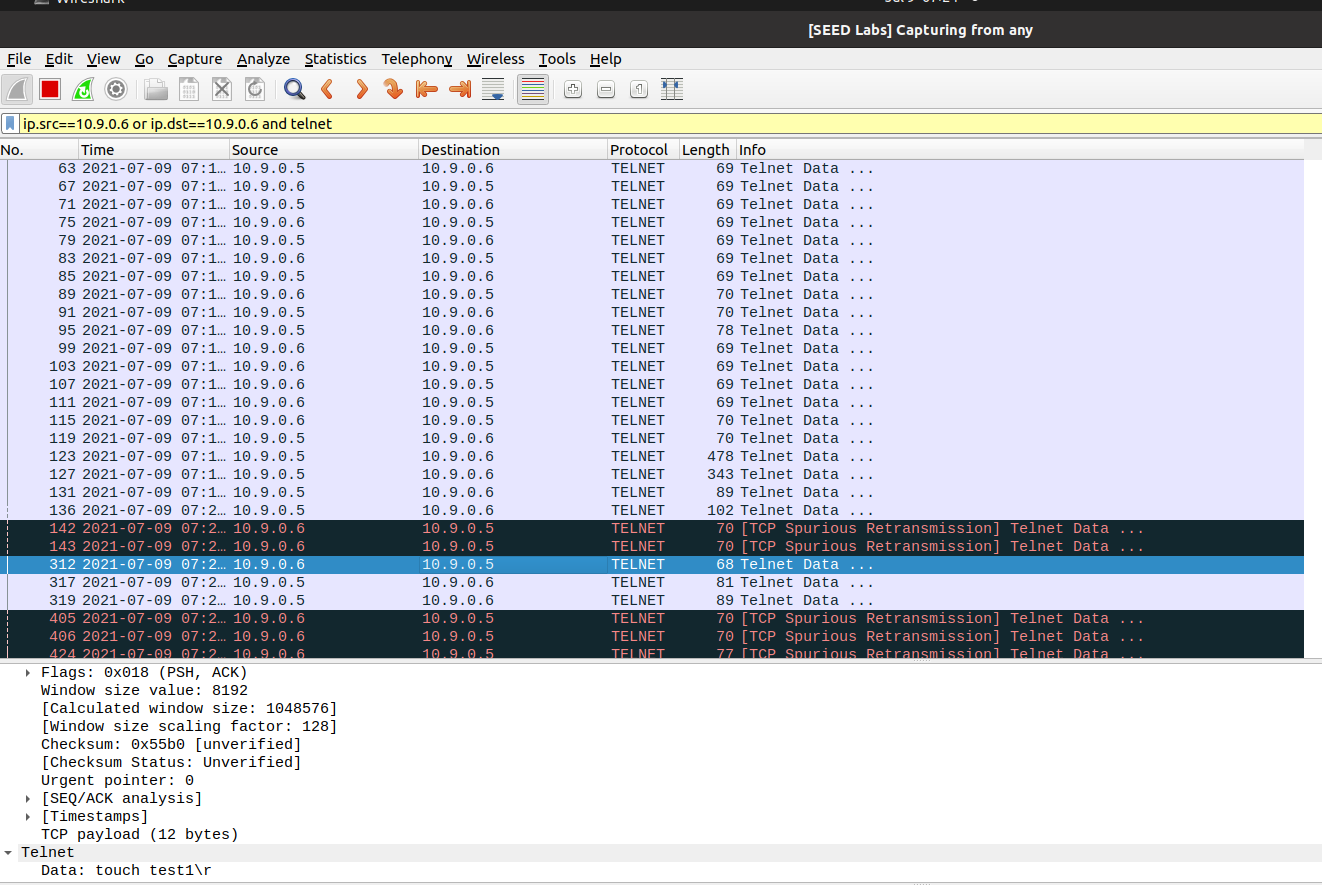
在攻击者容器中运行程序：



④在受害者容器中查看，可以看到出现了一个新的文件夹test1，说明指令执行成功：



打开wireshark，可以看到在原来的报文后面出现了我们构造的报文：

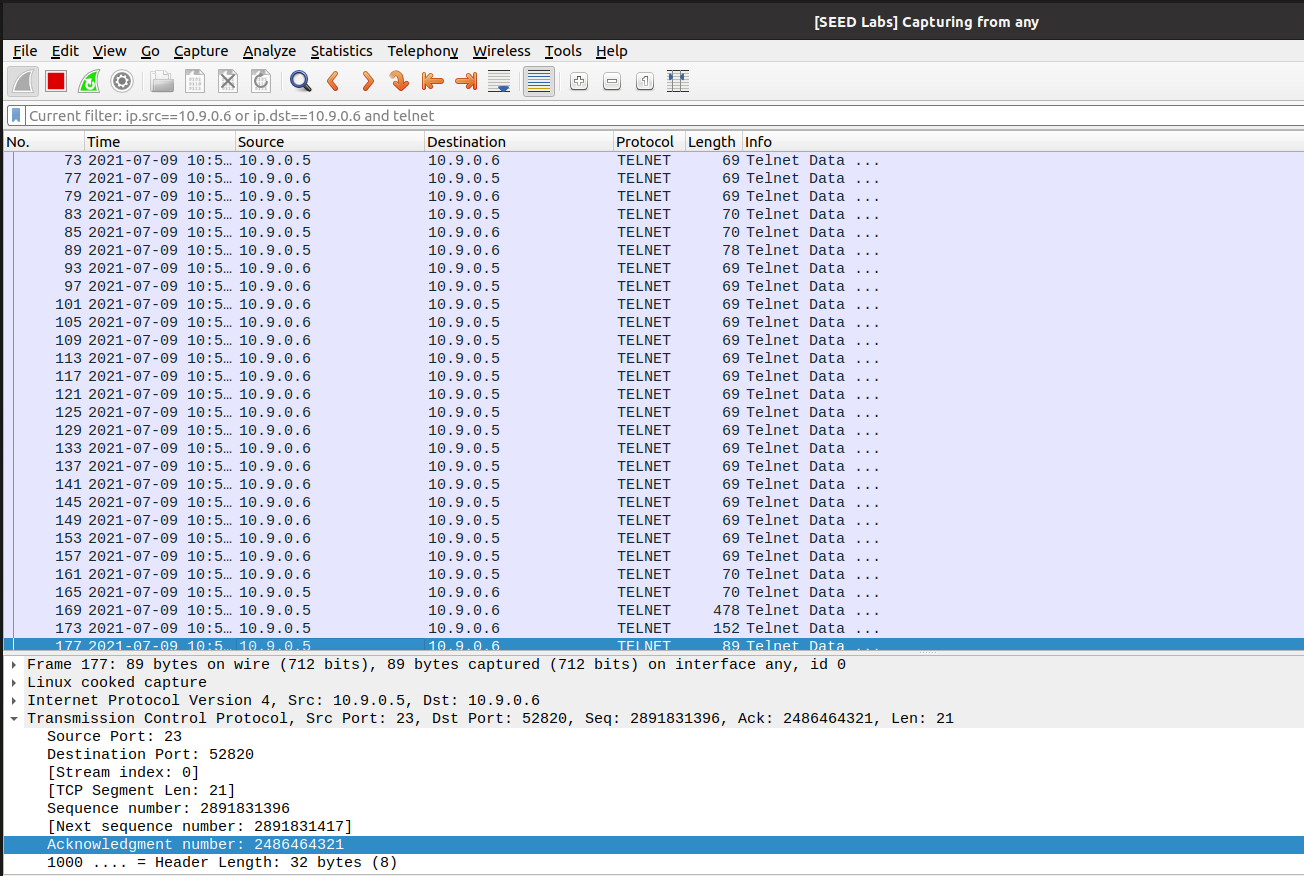


其中data就是我们的指令，这再次证明攻击实施成功.

Task4:

①在用户容器中对受害者发起telnet连接（与Task3相同）

②使用wirkshark抓包，获取最后一次连接的报文：

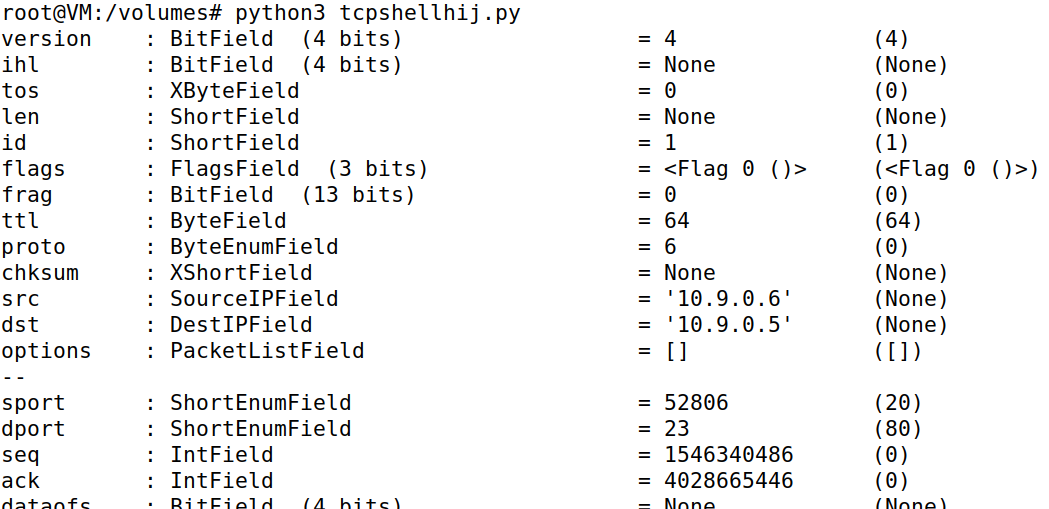
  
可以看到

③根据报文信息构造攻击程序，并在data中加入获取shell的指令

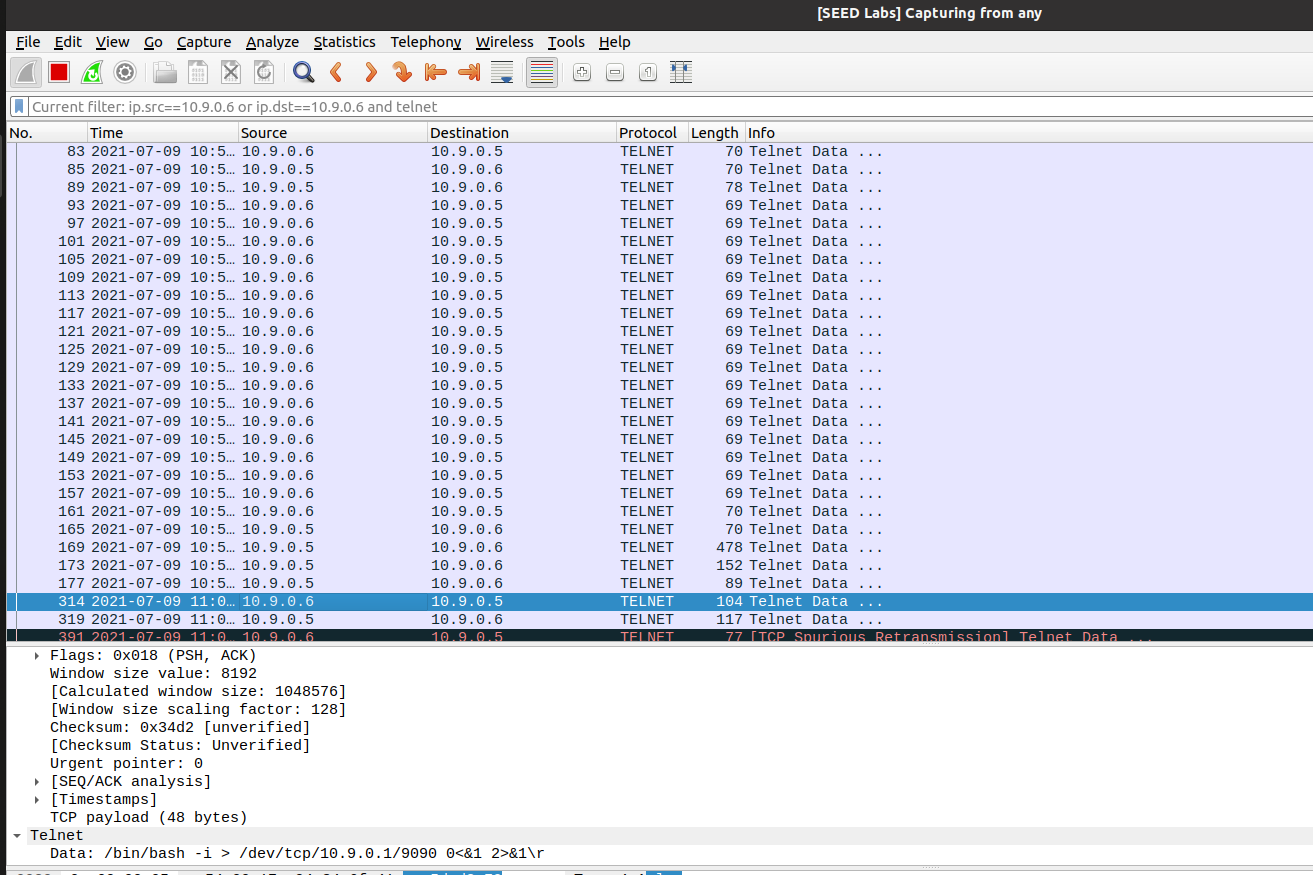
  
④在攻击者容器中，输入listen指令开启监听模式：



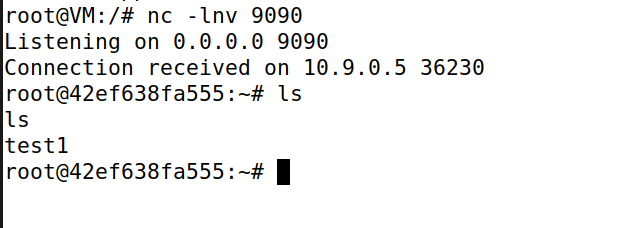
⑤在攻击者容器中运行程序



此时在wireshark中可以看到data为获取shell指令报文：



此时在攻击者容器中，收到了来自10.9.0.5的连接，可以看到成功登陆了受害者主机：



输入ls指令，可以看到命令成功执行，说明获取了shell的权限。