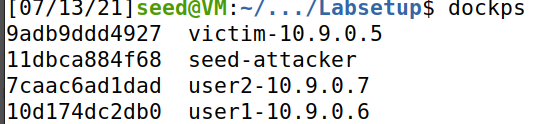
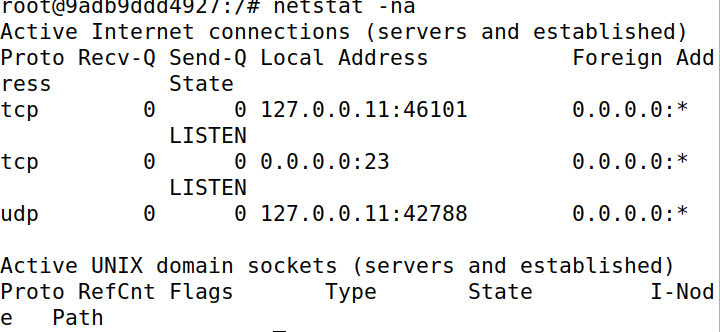
Task1

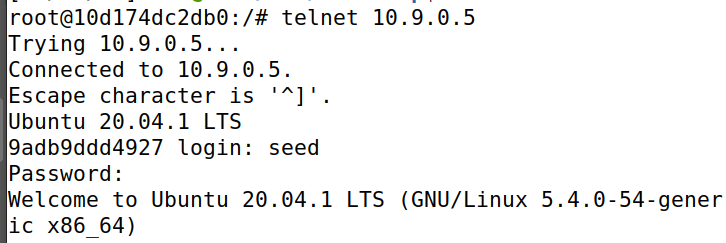
本实验采用受害者和user1两个容器



在攻击之前查看受害者容器的套接字队列



此时可以正常在user1容器中对受害者容器建立telnet连接

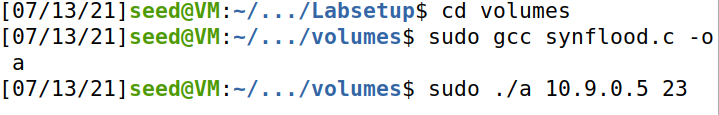


关闭SYNcookie的防御，yml文件中

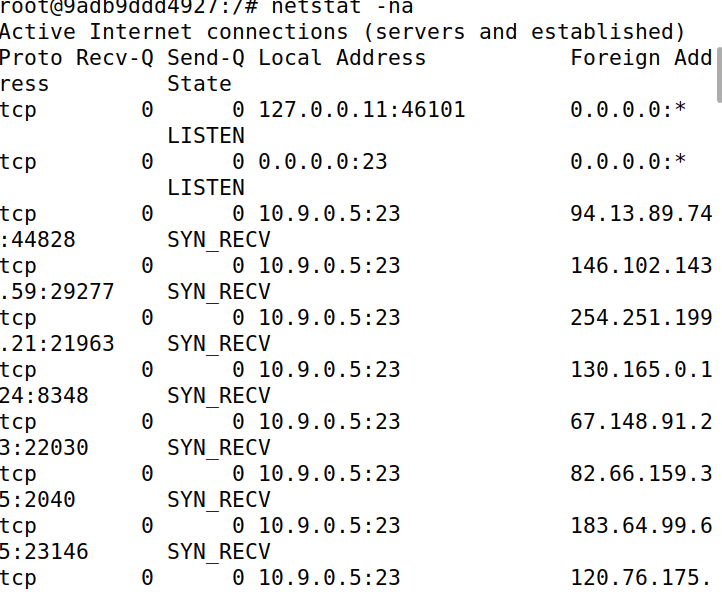


说明已经关闭

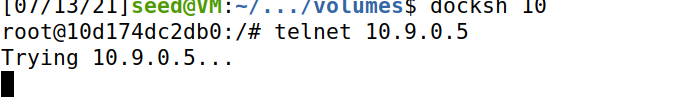
在主机中编译后用root权限下对受害者容器发动洪泛攻击



再查看受害容器的套接字队列



发现有许多状态为SYN\_RECV，也就是仅发出第一次握手，没有后续握手的TCP连接请求。此时在user1容器中向受害者容器发送telnet请求，提示超时。

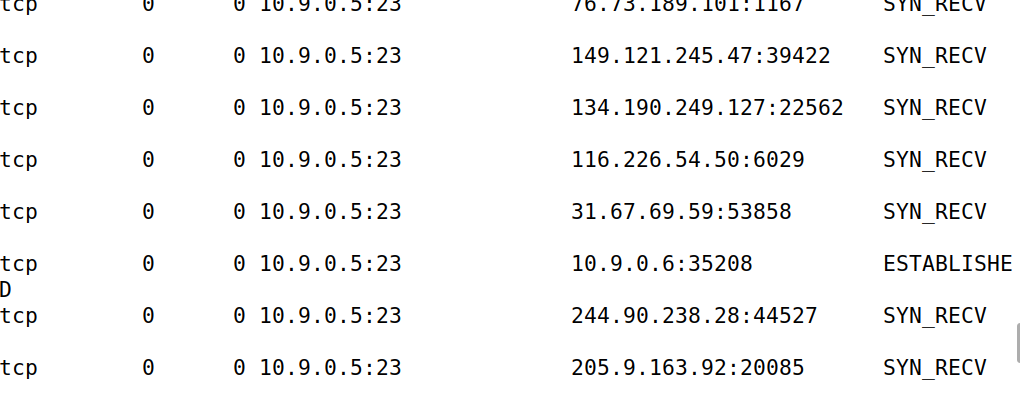


重新开启受害者容器中的SYN Cookie防御



重新发动红洪泛攻击，从user1向受害者发动telnet连接，发现连接成功。

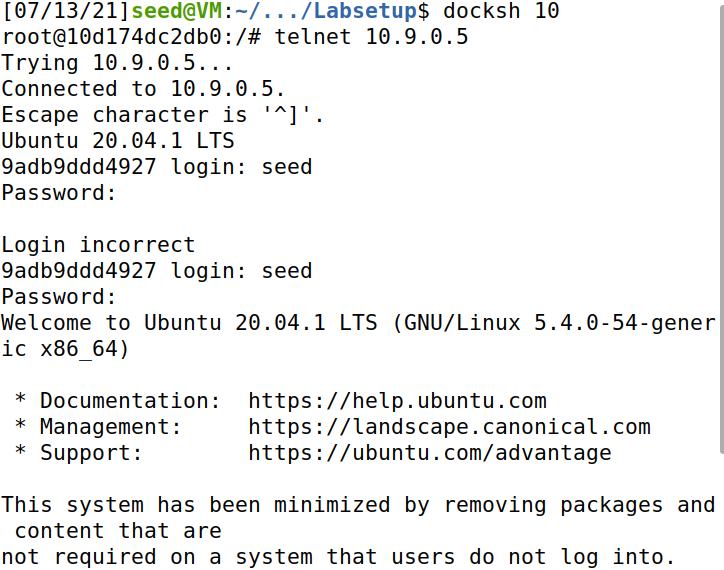
再次查看套接字



发现user1发起的telnet建立成功

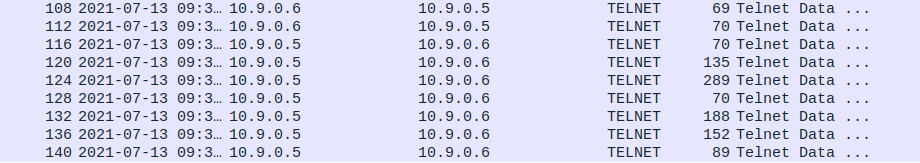
Task2

从IP地址为10.9.0.6的user1容器向IP为10.9.0.5的受害者容器发起telnet请求

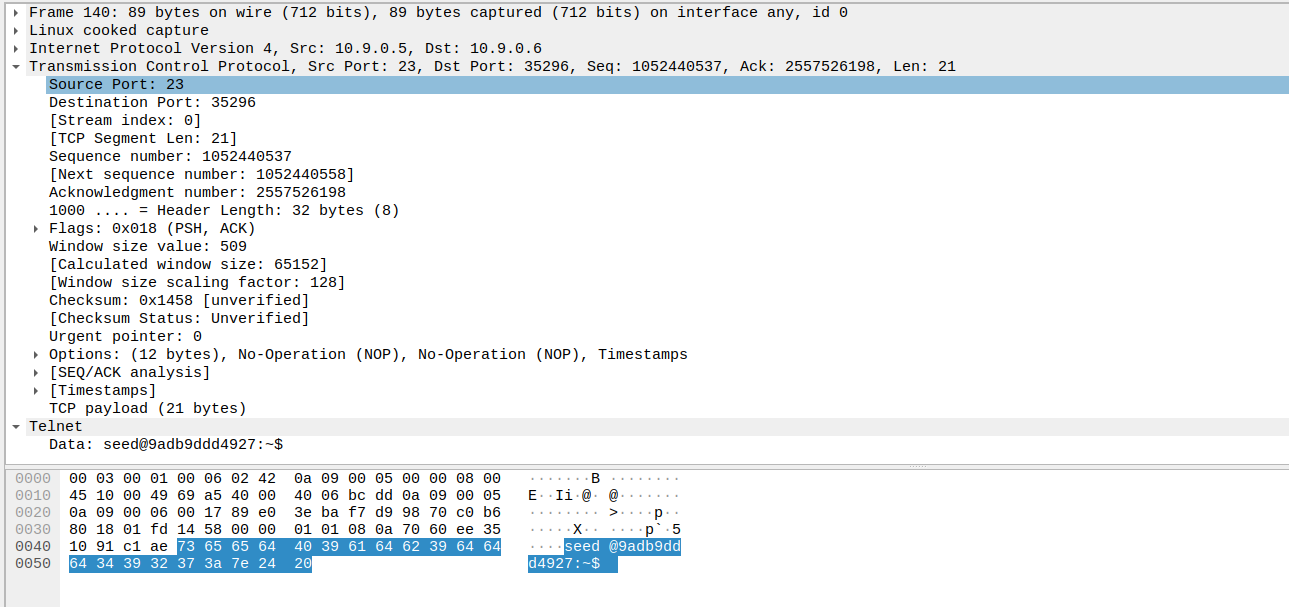


同时用wireshark抓取telnet包

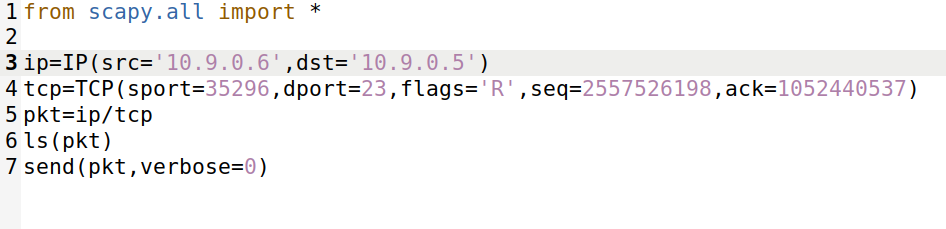
在连接稳定后选取最后一个telnet包



详细信息如下



从中获取源IP/端口，目的IP/端口，seq，ack等信息并补全程序



在root权限下运行该程序



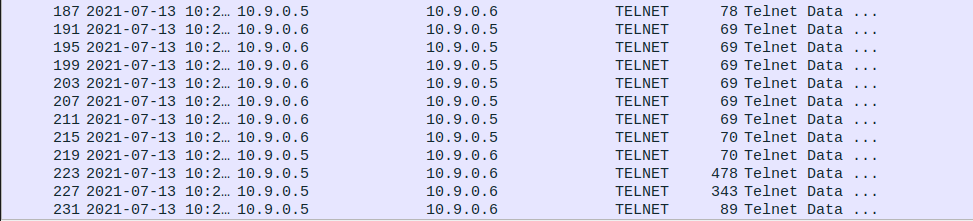
User1容器中telnet连接断开，伪造成功。

Task3

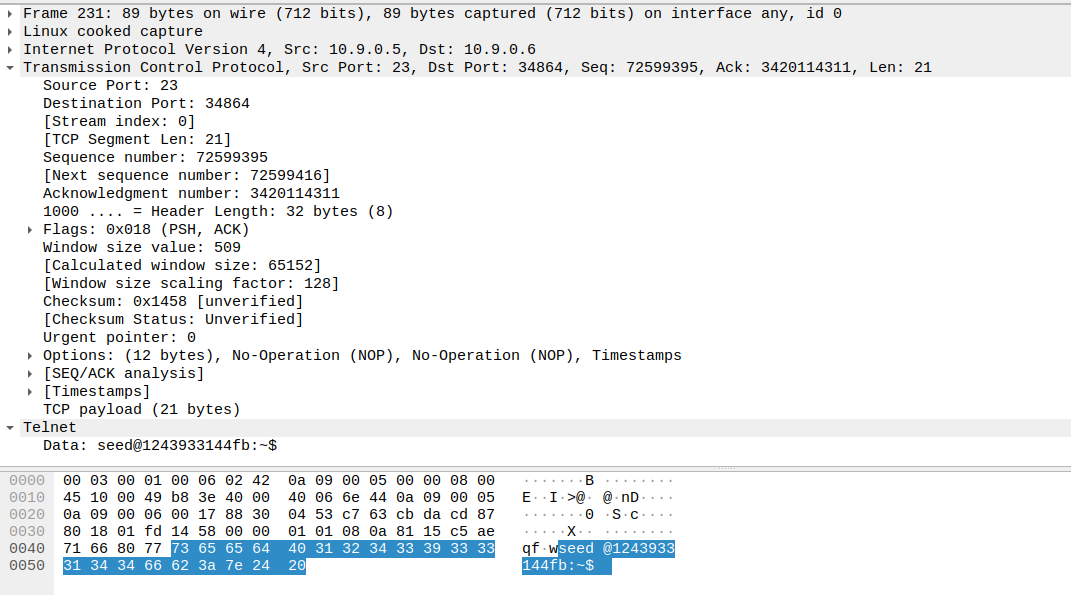
从IP地址为10.9.0.6的user1容器向IP为10.9.0.5的受害者容器发起telnet请求，如task2

同时用wireshark抓取telnet包

在连接稳定后选取最后一个telnet包



详细信息如下

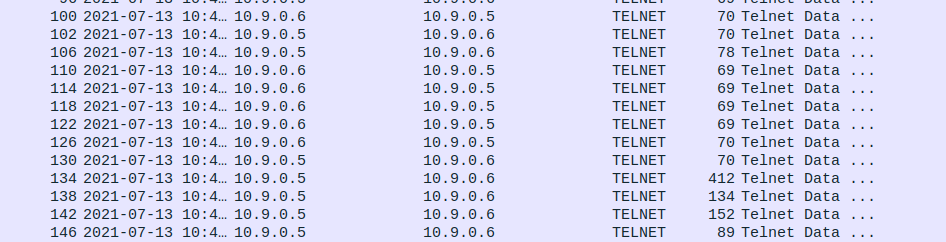


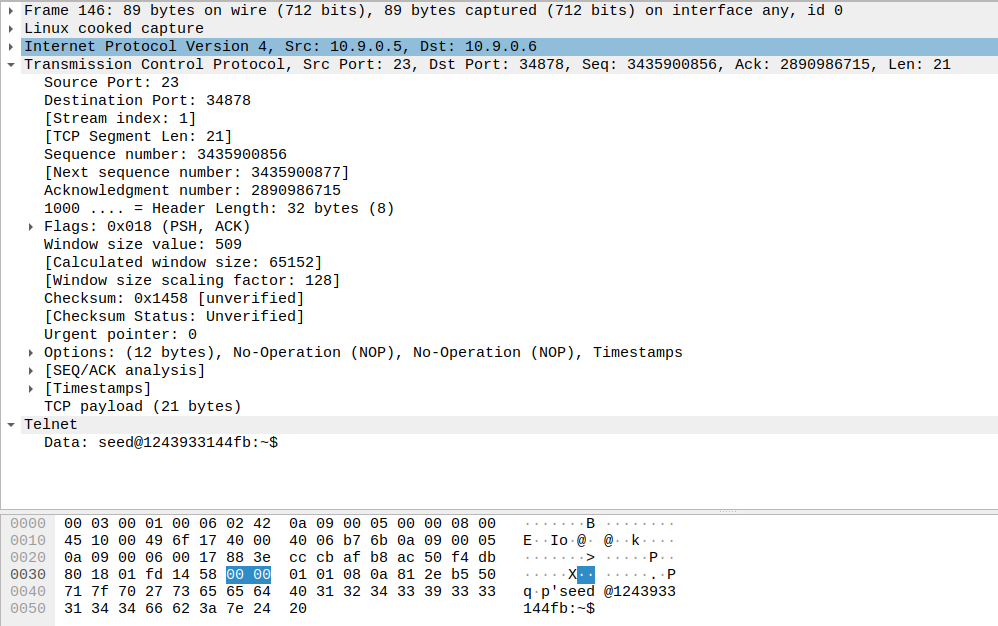
从中获取源IP/端口，目的IP/端口，seq，ack等信息并补全程序，并进行创建1.txt的data操作

在root权限下运行该程序，发现user1容器中远程连接的文件下出现1.txt，操作成功

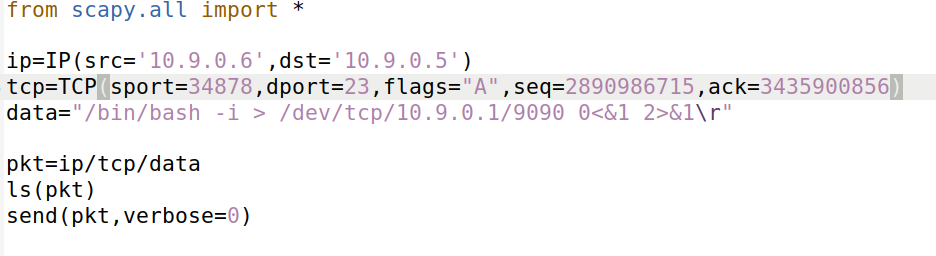


Task4



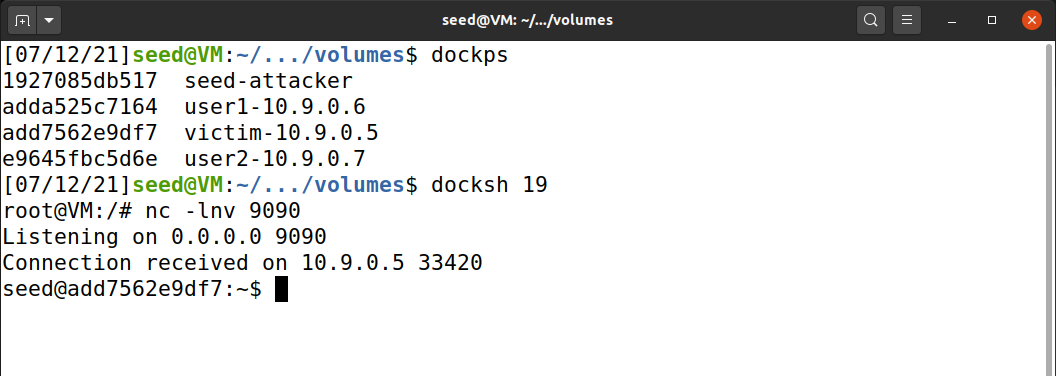


代码如下



Root下运行

攻击者容器监听



Shell建立