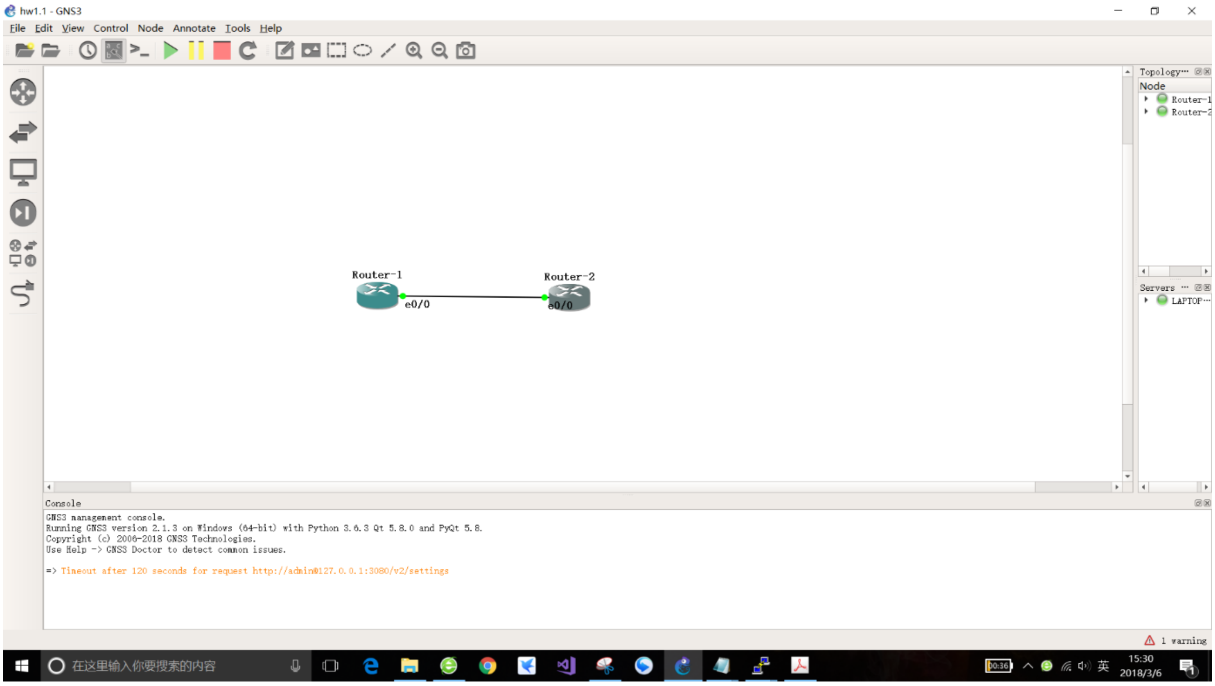
HOME ASSIGNMENT 1   Deadline: 6. March.

YOUR NAME: Liu Shuaishuai

NEPTUN CODE: DK584O

Task 1

Construct a TCP port scanner from TCP port 1 to TCP port 2000 and observe which ports are open. Verify your findings also with the *netstat* command!



```
GNS3 management console.
Running GNS3 version 2.1.3 on Windows (64-bit) with Python 3.6.3 Qt 5.8.0 and PyQt 5.8.
Copyright (c) 2006-2018 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=> Timeout after 120 seconds for request http://admin@127.0.0.1:3080/v2/settings
```

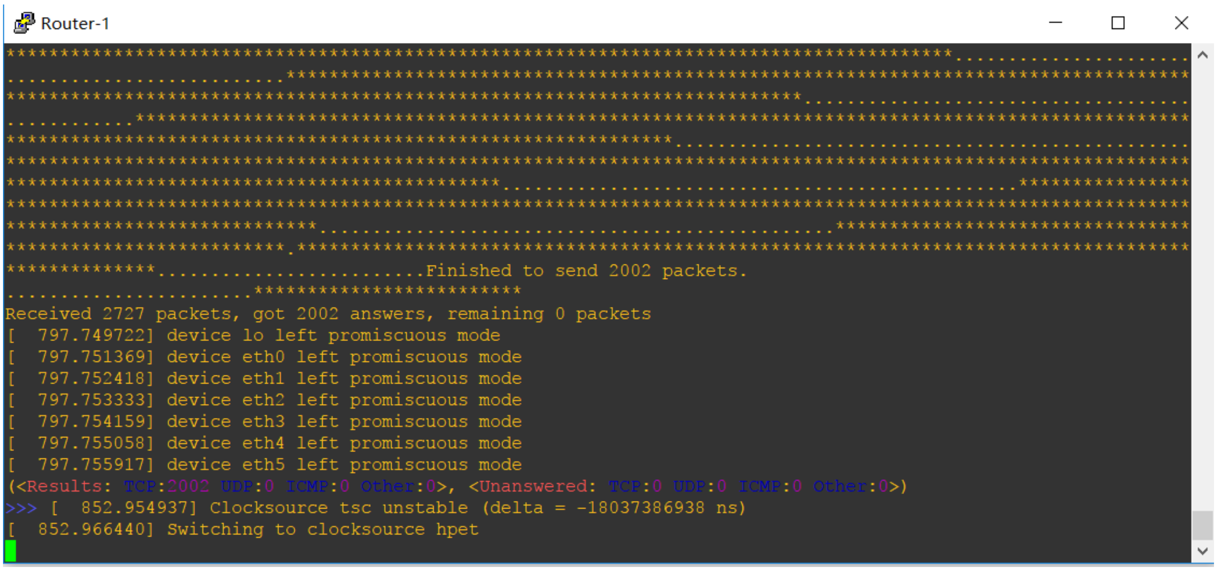
Router1-10.0.1.1

Router2-10.0.1.2

1.   use command from scapy

```
sr(IP(dst="10.1.0.2")/TCP(dport=(0,2001),flags="S"))
```

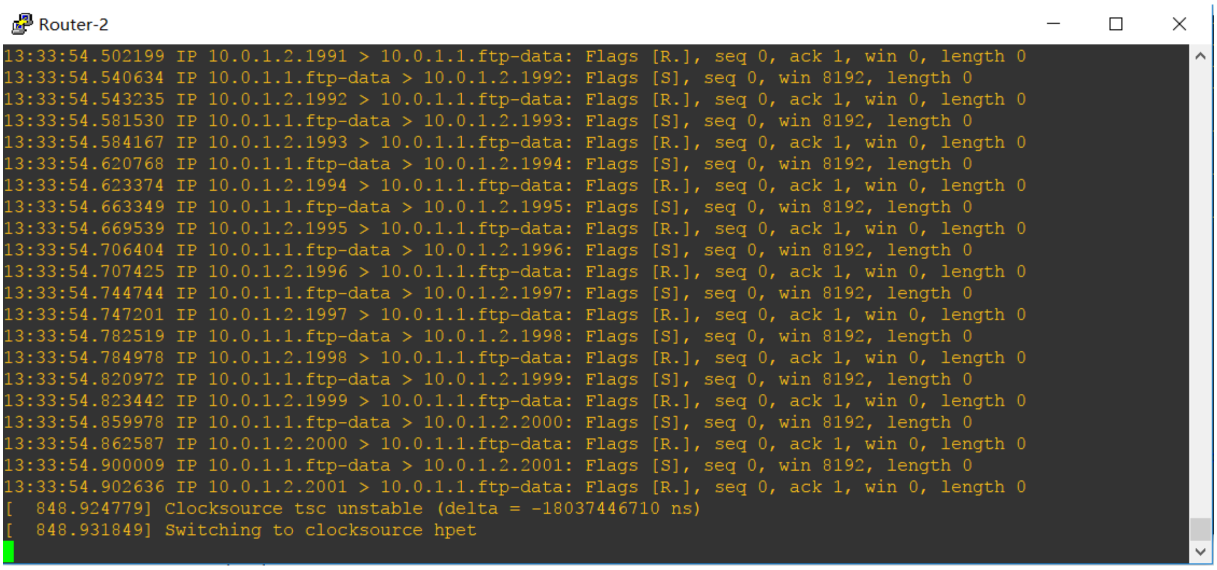
result of router1:



```
************************************************************************************************......................
..........................************************************************************************************
**************************************************************************....................................
............**************************************************************************************************
**************************************************************................................................
**************************************************************************************************************
**********************************************................................................****************
**************************************************************************************************************
*****************************................................................*********************************
**************************.***********************************************************************************
**************.........................Finished to send 2002 packets.
.......................*************************
Received 2727 packets, got 2002 answers, remaining 0 packets
[  797.749722] device lo left promiscuous mode
[  797.751369] device eth0 left promiscuous mode
[  797.752418] device eth1 left promiscuous mode
[  797.753333] device eth2 left promiscuous mode
[  797.754159] device eth3 left promiscuous mode
[  797.755058] device eth4 left promiscuous mode
[  797.755917] device eth5 left promiscuous mode
(<Results: TCP:2002 UDP:0 ICMP:0 Other:0>, <Unanswered: TCP:0 UDP:0 ICMP:0 Other:0>)
>>> [  852.954937] Clocksource tsc unstable (delta = -18037386938 ns)
[  852.966440] Switching to clocksource hpet
```

2.Use tcpdump command in R2

result of router 2:

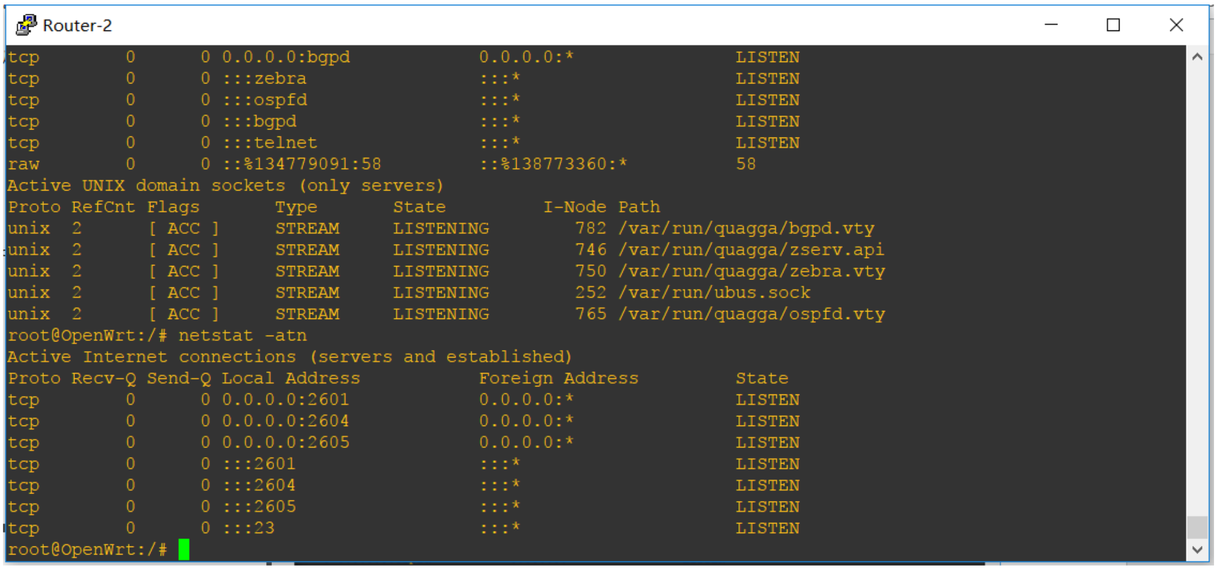


```
13:33:54.502199 IP 10.0.1.2.1991 > 10.0.1.1.ftp-data: Flags [R.], seq 0, ack 1, win 0, length 0
13:33:54.540634 IP 10.0.1.1.ftp-data > 10.0.1.2.1992: Flags [S], seq 0, win 8192, length 0
13:33:54.543235 IP 10.0.1.2.1992 > 10.0.1.1.ftp-data: Flags [R.], seq 0, ack 1, win 0, length 0
13:33:54.581530 IP 10.0.1.1.ftp-data > 10.0.1.2.1993: Flags [S], seq 0, win 8192, length 0
13:33:54.584167 IP 10.0.1.2.1993 > 10.0.1.1.ftp-data: Flags [R.], seq 0, ack 1, win 0, length 0
13:33:54.620768 IP 10.0.1.1.ftp-data > 10.0.1.2.1994: Flags [S], seq 0, win 8192, length 0
13:33:54.623374 IP 10.0.1.2.1994 > 10.0.1.1.ftp-data: Flags [R.], seq 0, ack 1, win 0, length 0
13:33:54.663349 IP 10.0.1.1.ftp-data > 10.0.1.2.1995: Flags [S], seq 0, win 8192, length 0
13:33:54.669539 IP 10.0.1.2.1995 > 10.0.1.1.ftp-data: Flags [R.], seq 0, ack 1, win 0, length 0
13:33:54.706404 IP 10.0.1.1.ftp-data > 10.0.1.2.1996: Flags [S], seq 0, win 8192, length 0
13:33:54.707425 IP 10.0.1.2.1996 > 10.0.1.1.ftp-data: Flags [R.], seq 0, ack 1, win 0, length 0
13:33:54.744744 IP 10.0.1.1.ftp-data > 10.0.1.2.1997: Flags [S], seq 0, win 8192, length 0
13:33:54.747201 IP 10.0.1.2.1997 > 10.0.1.1.ftp-data: Flags [R.], seq 0, ack 1, win 0, length 0
13:33:54.782519 IP 10.0.1.1.ftp-data > 10.0.1.2.1998: Flags [S], seq 0, win 8192, length 0
13:33:54.784978 IP 10.0.1.2.1998 > 10.0.1.1.ftp-data: Flags [R.], seq 0, ack 1, win 0, length 0
13:33:54.820972 IP 10.0.1.1.ftp-data > 10.0.1.2.1999: Flags [S], seq 0, win 8192, length 0
13:33:54.823442 IP 10.0.1.2.1999 > 10.0.1.1.ftp-data: Flags [R.], seq 0, ack 1, win 0, length 0
13:33:54.859978 IP 10.0.1.1.ftp-data > 10.0.1.2.2000: Flags [S], seq 0, win 8192, length 0
13:33:54.862587 IP 10.0.1.2.2000 > 10.0.1.1.ftp-data: Flags [R.], seq 0, ack 1, win 0, length 0
13:33:54.900009 IP 10.0.1.1.ftp-data > 10.0.1.2.2001: Flags [S], seq 0, win 8192, length 0
13:33:54.902636 IP 10.0.1.2.2001 > 10.0.1.1.ftp-data: Flags [R.], seq 0, ack 1, win 0, length 0
[  848.924779] Clocksource tsc unstable (delta = -18037446710 ns)
[  848.931849] Switching to clocksource hpet
```

When R2 replies to R1 by the packet with flags[R], it means the port is close.

On the contrary, When the R2 replies to R1 by the packet with flags[S], it means the port is open.

3.use netstat -atn command in router2



```
tcp        0      0 0.0.0.0:bgpd            0.0.0.0:*               LISTEN
tcp        0      0 :::zebra                :::*                    LISTEN
tcp        0      0 :::ospfd                :::*                    LISTEN
tcp        0      0 :::bgpd                 :::*                    LISTEN
tcp        0      0 :::telnet               :::*                    LISTEN
raw        0      0 ::%134779091:58         ::%138773360:*          58
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING        782 /var/run/quagga/bgpd.vty
unix  2      [ ACC ]     STREAM     LISTENING        746 /var/run/quagga/zserv.api
unix  2      [ ACC ]     STREAM     LISTENING        750 /var/run/quagga/zebra.vty
unix  2      [ ACC ]     STREAM     LISTENING        252 /var/run/ubus.sock
unix  2      [ ACC ]     STREAM     LISTENING        765 /var/run/quagga/ospfd.vty
root@OpenWrt:/# netstat -atn
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:2601            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:2604            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:2605            0.0.0.0:*               LISTEN
tcp        0      0 :::2601                 :::*                    LISTEN
tcp        0      0 :::2604                 :::*                    LISTEN
tcp        0      0 :::2605                 :::*                    LISTEN
tcp        0      0 :::23                   :::*                    LISTEN
root@OpenWrt:/#
```

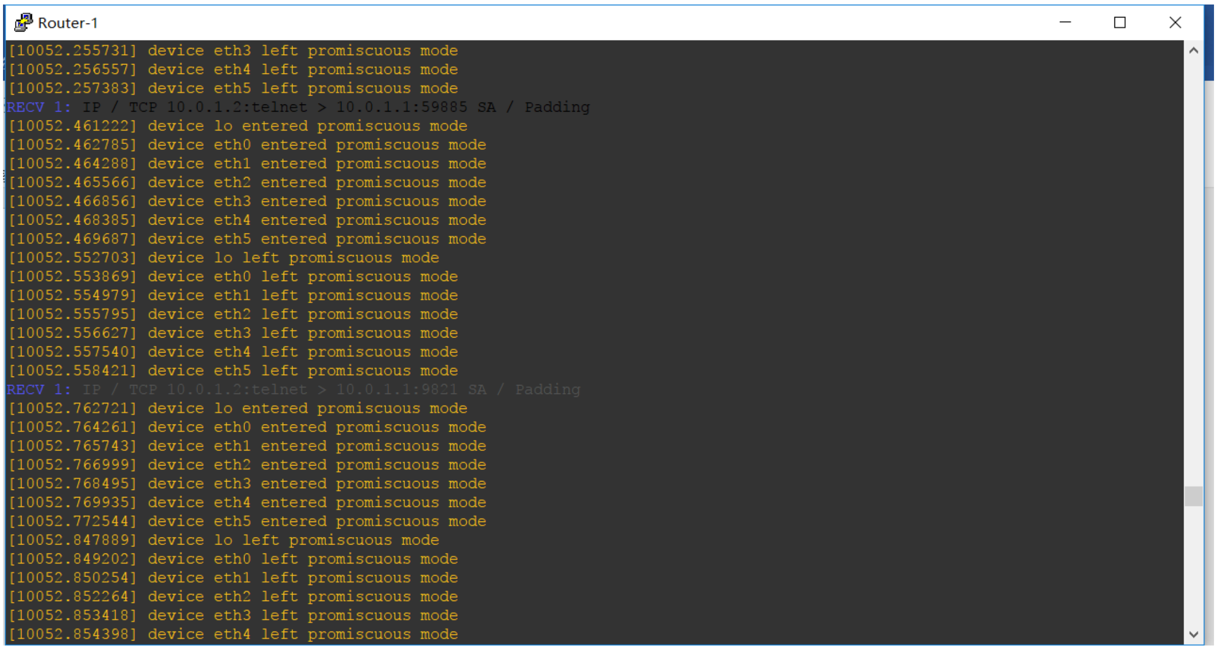
Now we can see which port is open. The 23 port is the only port in open state from 1-2000.

Task 2

Perform a TCP SYN attack against another computer in GNS3. Analyze the packet using the tools *tcpdump* and *netstat*!

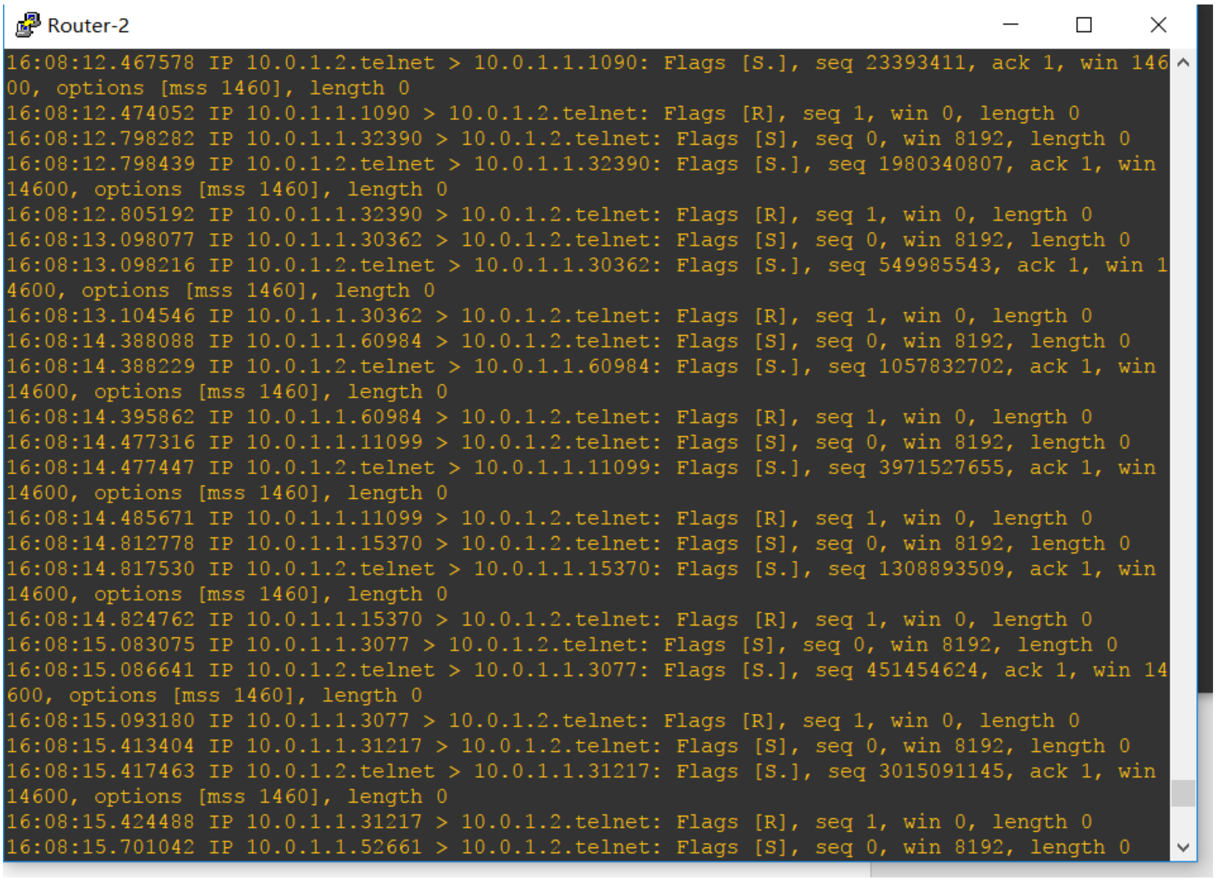
1. use the 2 routers in task1.
2. From task 1 we know that 23 port is open.or use netstat -atn command to check it.
3. Then we send packages by random port from R1 to 23port in R2.

p = IP(dst="10.0.1.2")/TCP(sport=RandShort(),dport=23,flags="S")



```
[10052.255731] device eth3 left promiscuous mode
[10052.256557] device eth4 left promiscuous mode
[10052.257383] device eth5 left promiscuous mode
RECV 1: IP / TCP 10.0.1.2:telnet > 10.0.1.1:59885 SA / Padding
[10052.461222] device lo entered promiscuous mode
[10052.462785] device eth0 entered promiscuous mode
[10052.464288] device eth1 entered promiscuous mode
[10052.465566] device eth2 entered promiscuous mode
[10052.466856] device eth3 entered promiscuous mode
[10052.468385] device eth4 entered promiscuous mode
[10052.469687] device eth5 entered promiscuous mode
[10052.552703] device lo left promiscuous mode
[10052.553869] device eth0 left promiscuous mode
[10052.554979] device eth1 left promiscuous mode
[10052.555795] device eth2 left promiscuous mode
[10052.556627] device eth3 left promiscuous mode
[10052.557540] device eth4 left promiscuous mode
[10052.558421] device eth5 left promiscuous mode
RECV 1: IP / TCP 10.0.1.2:telnet > 10.0.1.1:9821 SA / Padding
[10052.762721] device lo entered promiscuous mode
[10052.764261] device eth0 entered promiscuous mode
[10052.765743] device eth1 entered promiscuous mode
[10052.766999] device eth2 entered promiscuous mode
[10052.768495] device eth3 entered promiscuous mode
[10052.769935] device eth4 entered promiscuous mode
[10052.772544] device eth5 entered promiscuous mode
[10052.847889] device lo left promiscuous mode
[10052.849202] device eth0 left promiscuous mode
[10052.850254] device eth1 left promiscuous mode
[10052.852264] device eth2 left promiscuous mode
[10052.853418] device eth3 left promiscuous mode
[10052.854398] device eth4 left promiscuous mode
```

4. Then we use tcpdump to check the situation in R2



```
16:08:12.467578 IP 10.0.1.2.telnet > 10.0.1.1.1090: Flags [S.], seq 23393411, ack 1, win 146
00, options [mss 1460], length 0
16:08:12.474052 IP 10.0.1.1.1090 > 10.0.1.2.telnet: Flags [R], seq 1, win 0, length 0
16:08:12.798282 IP 10.0.1.1.32390 > 10.0.1.2.telnet: Flags [S], seq 0, win 8192, length 0
16:08:12.798439 IP 10.0.1.2.telnet > 10.0.1.1.32390: Flags [S.], seq 1980340807, ack 1, win
14600, options [mss 1460], length 0
16:08:12.805192 IP 10.0.1.1.32390 > 10.0.1.2.telnet: Flags [R], seq 1, win 0, length 0
16:08:13.098077 IP 10.0.1.1.30362 > 10.0.1.2.telnet: Flags [S], seq 0, win 8192, length 0
16:08:13.098216 IP 10.0.1.2.telnet > 10.0.1.1.30362: Flags [S.], seq 549985543, ack 1, win 1
4600, options [mss 1460], length 0
16:08:13.104546 IP 10.0.1.1.30362 > 10.0.1.2.telnet: Flags [R], seq 1, win 0, length 0
16:08:14.388088 IP 10.0.1.1.60984 > 10.0.1.2.telnet: Flags [S], seq 0, win 8192, length 0
16:08:14.388229 IP 10.0.1.2.telnet > 10.0.1.1.60984: Flags [S.], seq 1057832702, ack 1, win
14600, options [mss 1460], length 0
16:08:14.395862 IP 10.0.1.1.60984 > 10.0.1.2.telnet: Flags [R], seq 1, win 0, length 0
16:08:14.477316 IP 10.0.1.1.11099 > 10.0.1.2.telnet: Flags [S], seq 0, win 8192, length 0
16:08:14.477447 IP 10.0.1.2.telnet > 10.0.1.1.11099: Flags [S.], seq 3971527655, ack 1, win
14600, options [mss 1460], length 0
16:08:14.485671 IP 10.0.1.1.11099 > 10.0.1.2.telnet: Flags [R], seq 1, win 0, length 0
16:08:14.812778 IP 10.0.1.1.15370 > 10.0.1.2.telnet: Flags [S], seq 0, win 8192, length 0
16:08:14.817530 IP 10.0.1.2.telnet > 10.0.1.1.15370: Flags [S.], seq 1308893509, ack 1, win
14600, options [mss 1460], length 0
16:08:14.824762 IP 10.0.1.1.15370 > 10.0.1.2.telnet: Flags [R], seq 1, win 0, length 0
16:08:15.083075 IP 10.0.1.1.3077 > 10.0.1.2.telnet: Flags [S], seq 0, win 8192, length 0
16:08:15.086641 IP 10.0.1.2.telnet > 10.0.1.1.3077: Flags [S.], seq 451454624, ack 1, win 14
600, options [mss 1460], length 0
16:08:15.093180 IP 10.0.1.1.3077 > 10.0.1.2.telnet: Flags [R], seq 1, win 0, length 0
16:08:15.413404 IP 10.0.1.1.31217 > 10.0.1.2.telnet: Flags [S], seq 0, win 8192, length 0
16:08:15.417463 IP 10.0.1.2.telnet > 10.0.1.1.31217: Flags [S.], seq 3015091145, ack 1, win
14600, options [mss 1460], length 0
16:08:15.424488 IP 10.0.1.1.31217 > 10.0.1.2.telnet: Flags [R], seq 1, win 0, length 0
16:08:15.701042 IP 10.0.1.1.52661 > 10.0.1.2.telnet: Flags [S], seq 0, win 8192, length 0
```

For now we perform a TCP SYN attack against another computer.