Emma Stensland

Reese Pearsall

CSCI 476

October 19, 2025

Seedlabs: TCP/IP Attacks

Task 1: SYN Flooding Attack

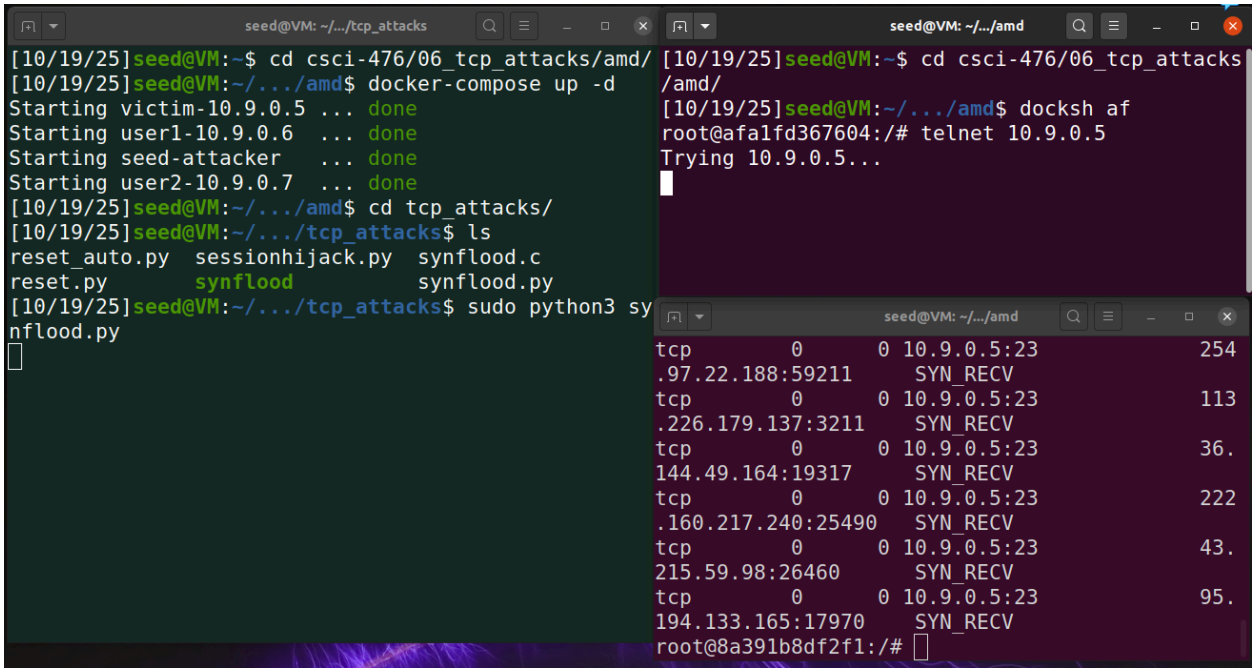
SYN Cookies were disabled, and the SYN/ACK Retries and SYN Backlog options were set.

```
[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

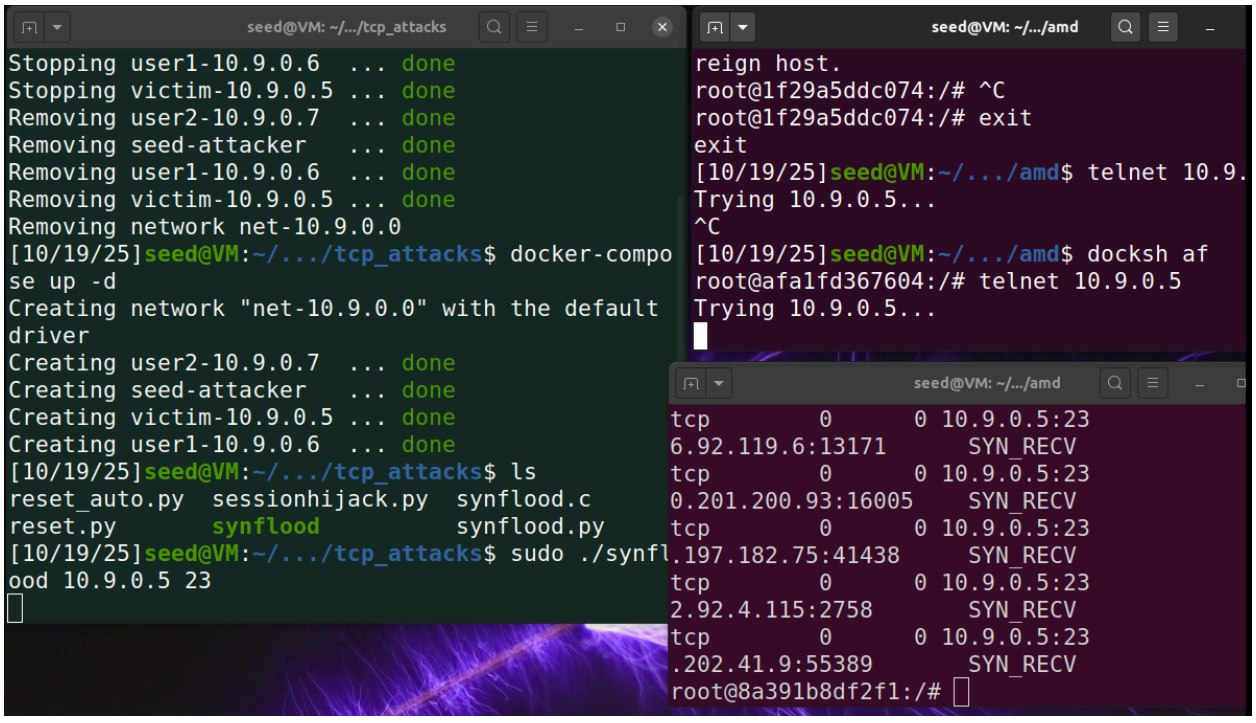
A python script was used to spoof SYN packets and was sent to the IP address of the victim.



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

1.2

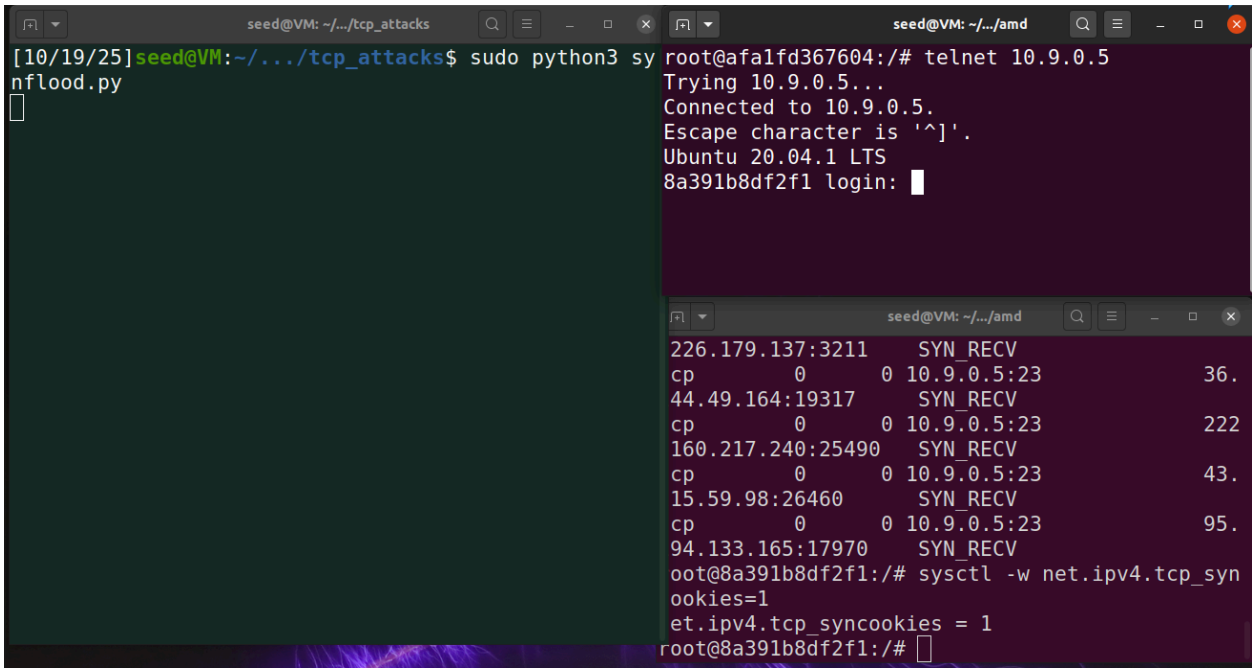
The containers were restarted to refresh them, and the C program was run to spoof packets.



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

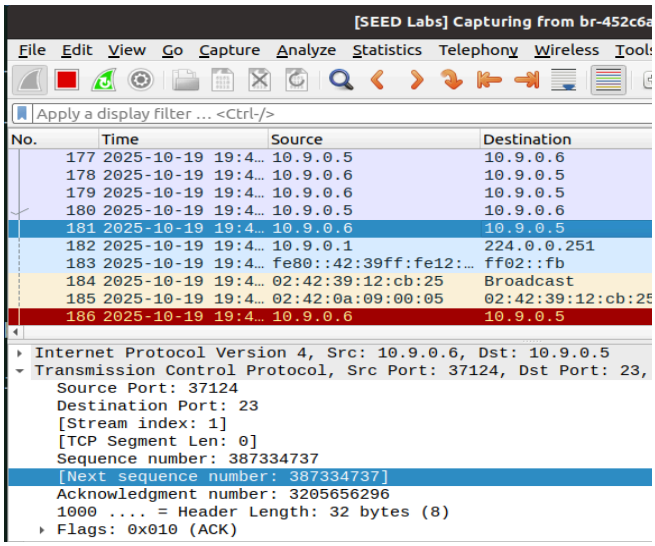
The attack was attempted while SYN cookies were on.

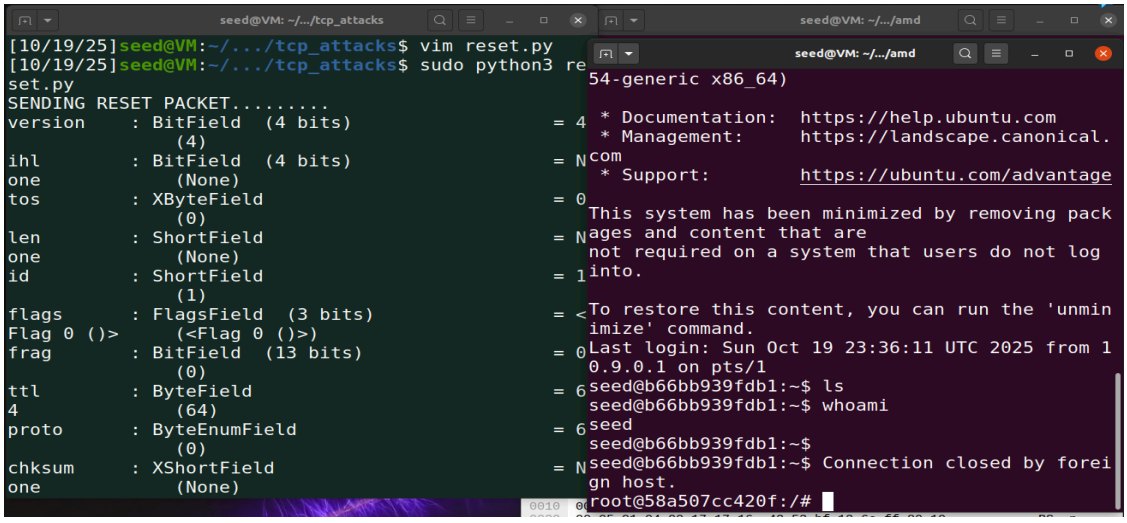


Observations: The attack failed, as no SYN-ACKs with cookies were received, so the SYN requests were dropped.

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.

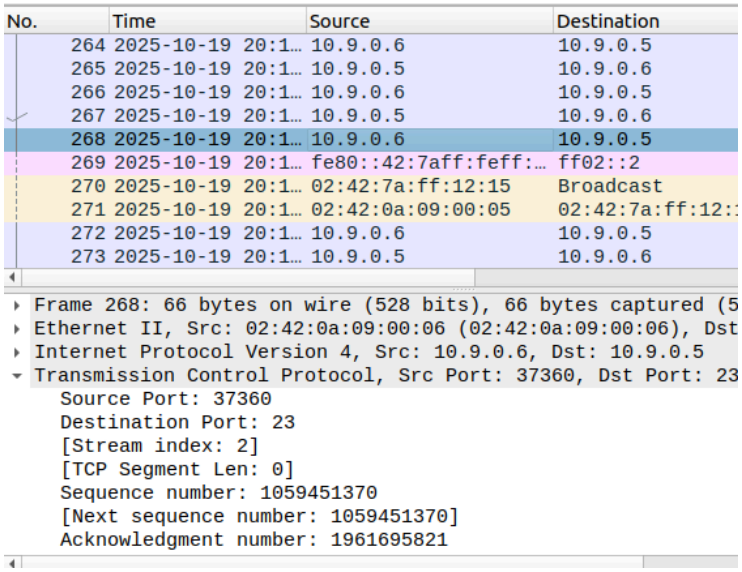


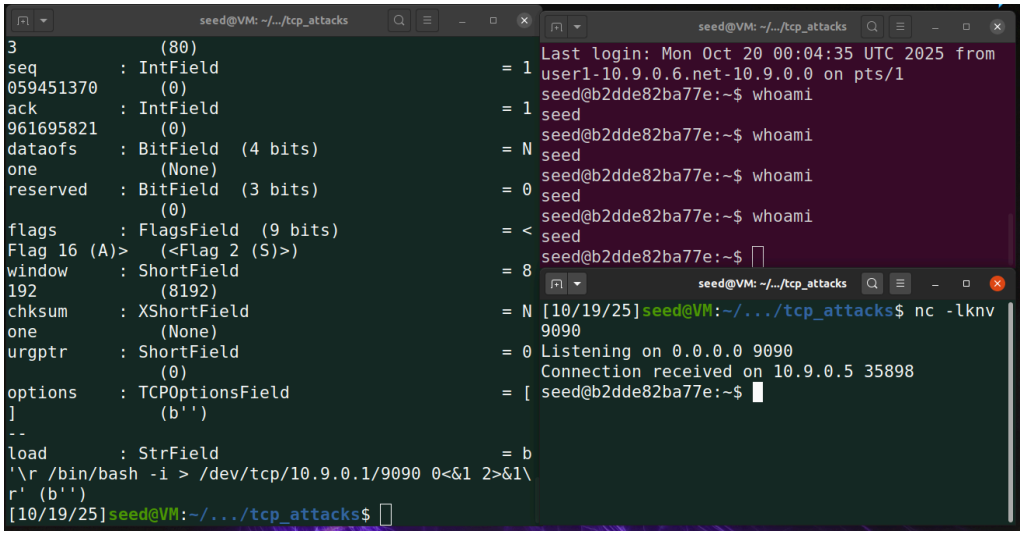


Observations: The attack was successful, and the reset was sent, which terminated the client-server connection.

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.





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