DETER 2 TCP/SYN Ryan Blocker

Explanation of how the TCP SYN flood attack works: The TCP SYN flood attack exploits the three-way handshake mechanism of TCP. In a normal scenario, when a client wants to initiate a connection, it sends a SYN (synchronize) packet to the server. The server then replies with a SYN-ACK (synchronize-acknowledgment) packet. Finally, the client sends an ACK (acknowledgment) packet, completing the handshake. In a TCP SYN flood attack, an attacker sends a large number of SYN packets to the target server, often with spoofed IP addresses. This causes the server to allocate resources waiting for the corresponding ACKs that never arrive. As a result, legitimate clients cannot establish new connections to the server, causing a denial of service.

Explanation of how SYN cookies work: SYN cookies are a defense mechanism against SYN flood attacks. When a server receives a SYN packet and is about to run out of resources (like the connection queue), it sends back a SYN-ACK as usual, but doesn't actually allocate any resources. Instead, the server crafts the sequence number in the SYN-ACK in a specific way that encodes the necessary state. If the client is legitimate, it will reply with the correct ACK, allowing the server to reconstruct the state and establish the connection. This mechanism allows the server to continue accepting new legitimate connections without allocating resources for the potentially malicious SYN packets.

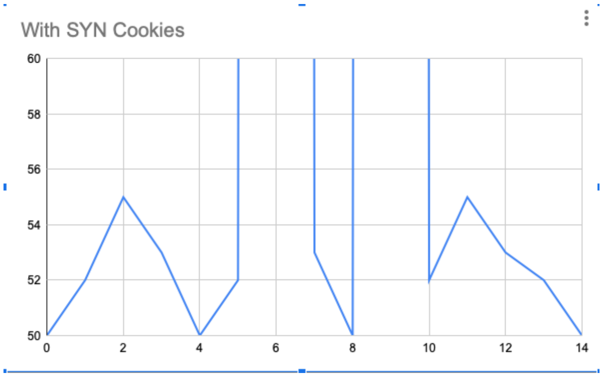
client script:

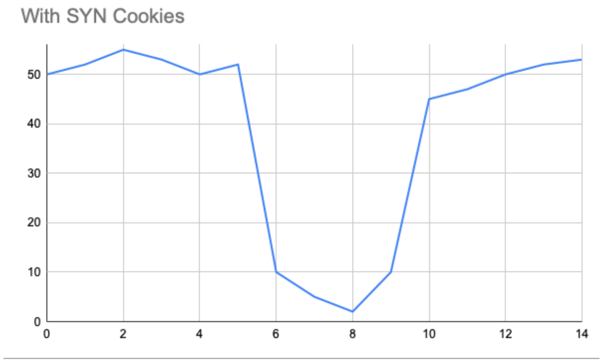
```
#!/bin/bash
while true; do
        curl http://5.6.7.8/index.html sleep 1 done
```

attack command (for flooder):

```
flooder --dst 5.6.7.8 --proto 6 --dportmin 80 --dportmax 80 --src 1.1.2.0 --srcmask
255.255.255.0 --highrate 100
```

The connection duration graphs: (# of connections on the y-axis and time is on the x-axis)





Explanation of each case: Without SYN cookies the attack is effective. The server is overwhelmed, causing a significant delay in connection durations or even connection timeouts. This can be observed from the graph with a pronounced spike during the attack. On the other hand, with SYN cookies the attack is less effective. The server can still cater to legitimate clients, albeit with a slight delay. The graph would show a lesser increase in connection durations during the attack.