1. **TCP SYN flood attack.**

In a SYN flood attack, an attacker sends a series of SYN requests to a server requests for connection, and when the server send the SYN+ACK back to the attacker, the attacker does not respond or spoof source IP address, and, thus, results in a series of half-open connections and the server will wait for the acknowledgement of the client. Hence, excessive amount of resources is used and will exceed the maximum amount of resources. Hence, the legitimate connections will be denied.

2. **How SYN cookies work to prevent DOS effect from SYN flood attack.**

A SYN cookie is an initial TCP sequence number that generated by TCP servers which the server's initial sequence number increases faster than the client's initial sequence number. It complies with the basic TCP requirement. When the SYN queue fills up, the server does not need to drop connections but sends SYN+ACK back as if the queue had been grown larger. The server checks if the function of the SYN cookie worked for the recent value of time and rebuilds the SYN queue.

3. **Legitimate client script**

```
#!/bin/bash

   while true; do
      curl –o index.html 5.6.7.8
      sleep 1
   done
```

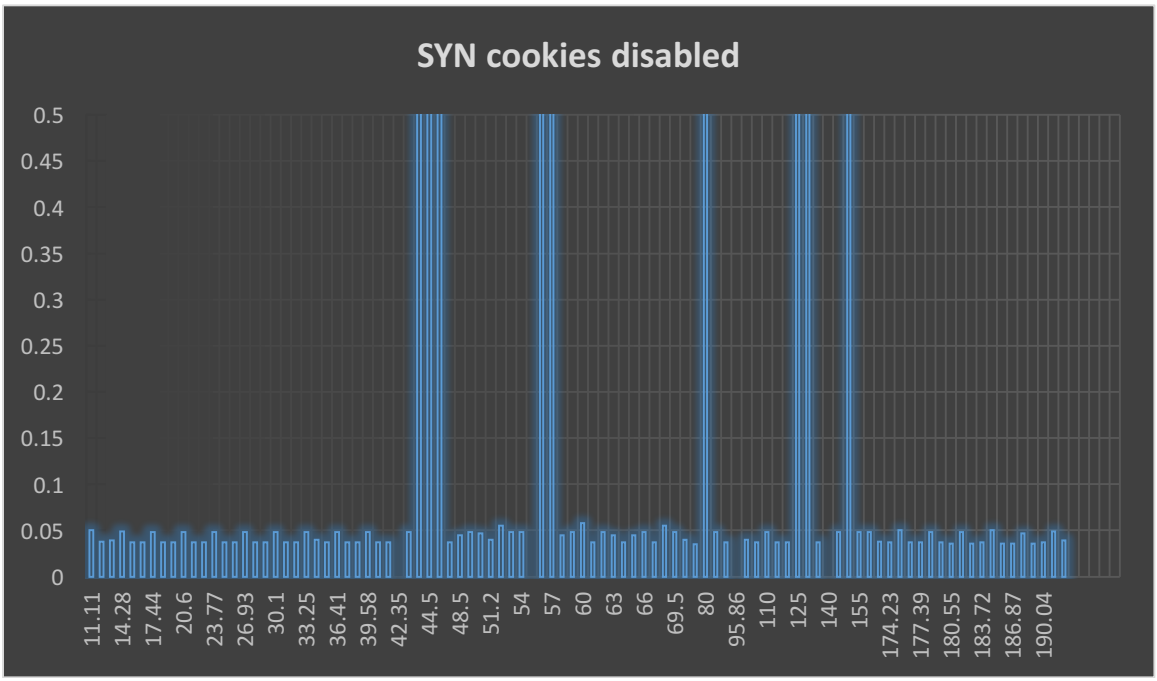
4. **Flooder attack command**

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

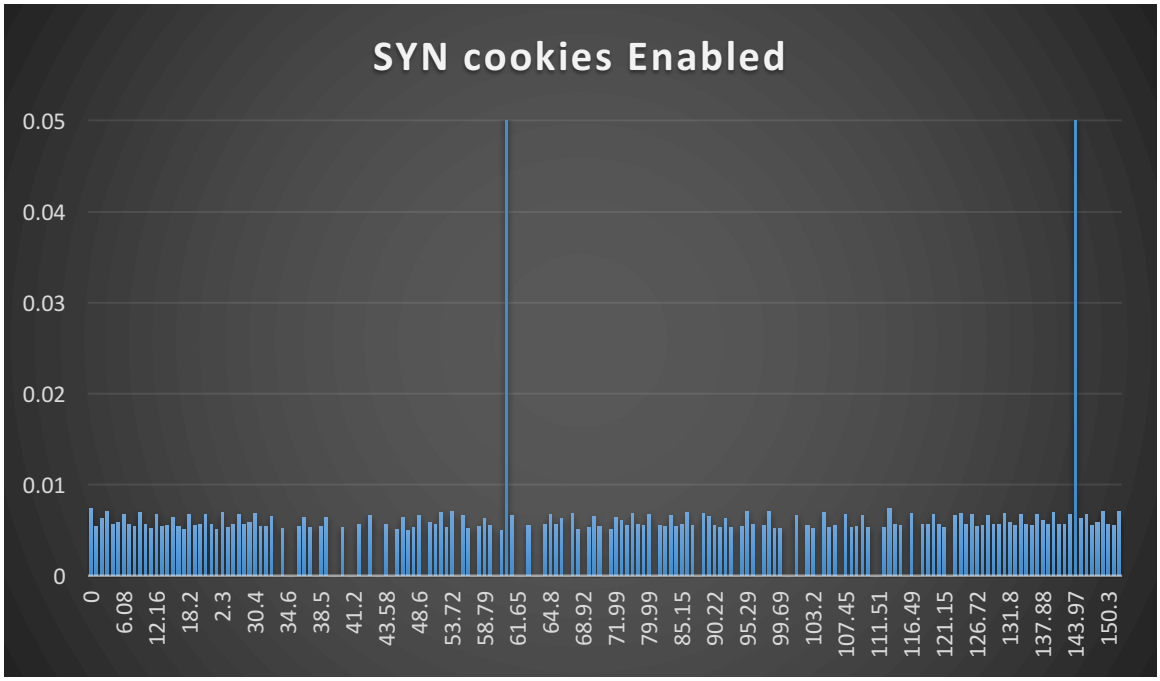
5. **Graph**

The add line didn't work. (1) attack started at 36s and stopped at 128s.
(2) attack started at 40s and stopped at 130s.

(1) SYN cookies Disabled



(2) SYN cookies Enabled



6. **What happens in each case. Attack effectiveness and info**

SYN disabled:

After the flooder in effect, the amount outliers have increased significantly. There you can tell that the attack was effective. That is because without the SYN cookies, the amount of resources used by the spoofed IP addresses has excess the server's limit, and the server had to drop connections which made the legitimate connection wait much longer than usual.

SYN enabled:

The connections were much more stable. Some outliers occurred may due to the network issues, and even when the attack started, all connections were pretty stable, and you can tell that the attack did not work, since the SYN cookies were protecting the legitimate connections by checking if the functions return the correct value. Hence, when the flooder in effect, the server did not have to drop connections but rearrange the queue by not providing any resources those connections that did not have a correct value for recent t.