To: Frobozz CEO

From: Francisco Manuel Colmenar Lamas

Subject: TCP SYN Flood.

Date: October 26, 2020

At this memo a brief answer to the different questions for the TCP SYN Flood exercise are going to be provided.

To start with, it is needed to explain what a TCP SYN flood attack is and how it works in order to ensure that the entire memo is correctly understood. A SYN flood attack is a type of DoS attack in which the attacker initiates a large number of connections in a short time, usually using spoofed ip addresses, to the server.

An important remark is that the connections are not finished by the attacker. The server sends the SYN-ACK back but the server does not response. Therefore, the server wastes resources waiting for the ACK to established the connection, which does not happen.

The consequence is that legitimate users cannot connect to the server as the server's resources are being exhausted by the attacker.

One approach to avoid the TCP SYN flood attack is to use SYN cookies. In this case, the server encodes the SYN queue entry into sequence numbers which are then sent to the clients by the SYN ACK response. Then, if the server receives the sequence number correctly incremented, the server creates the SYN queue entry for that connection and finally it allocates the resources following the normal procedure.

As a consequence, due to the fact that the resources are not allocated until the sequence number is correctly received by the server, in the case that the SYN TCP flood attack is performed using spoofed IP, the server will not be as damaged as it was in the scenario without the SYN cookies. This is mainly because the server will not receive a response from the spoofed IPs.

Regarding to the connection duration graphs from the attack, with and without the use of SYN cookies, they can be seen in the pictures below.

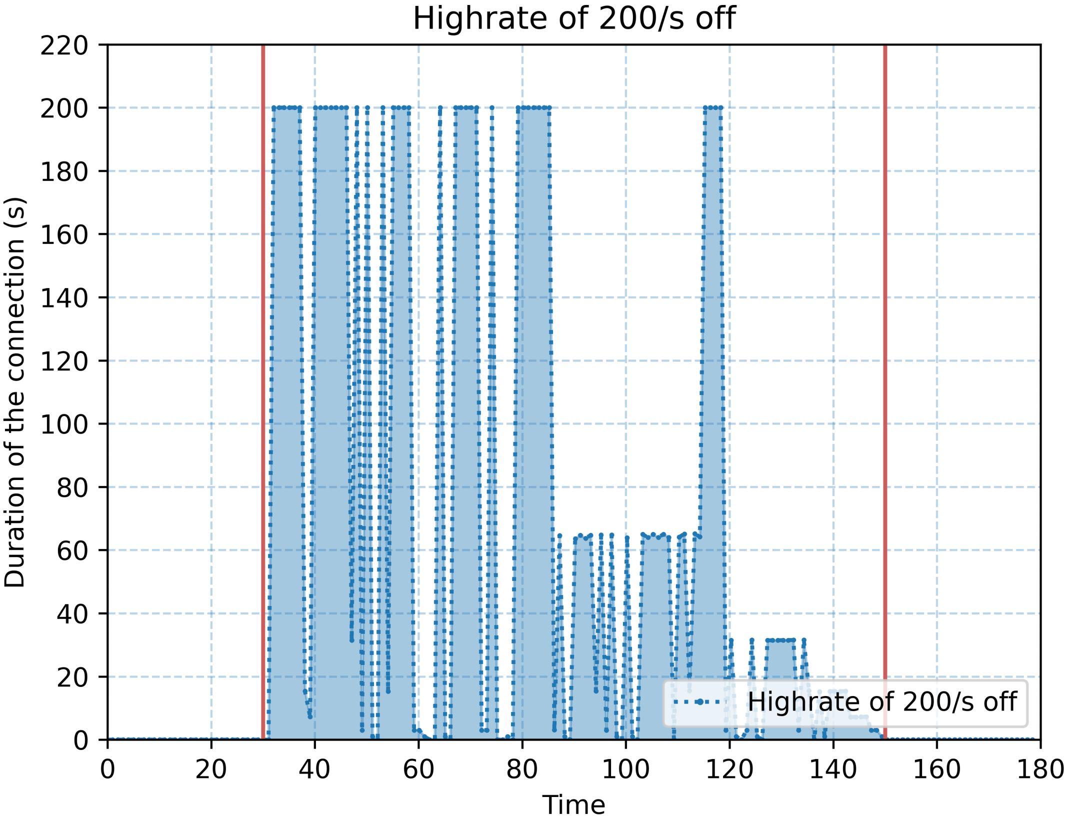

Figure 1: Connection duration graphs with SYN cookies off.

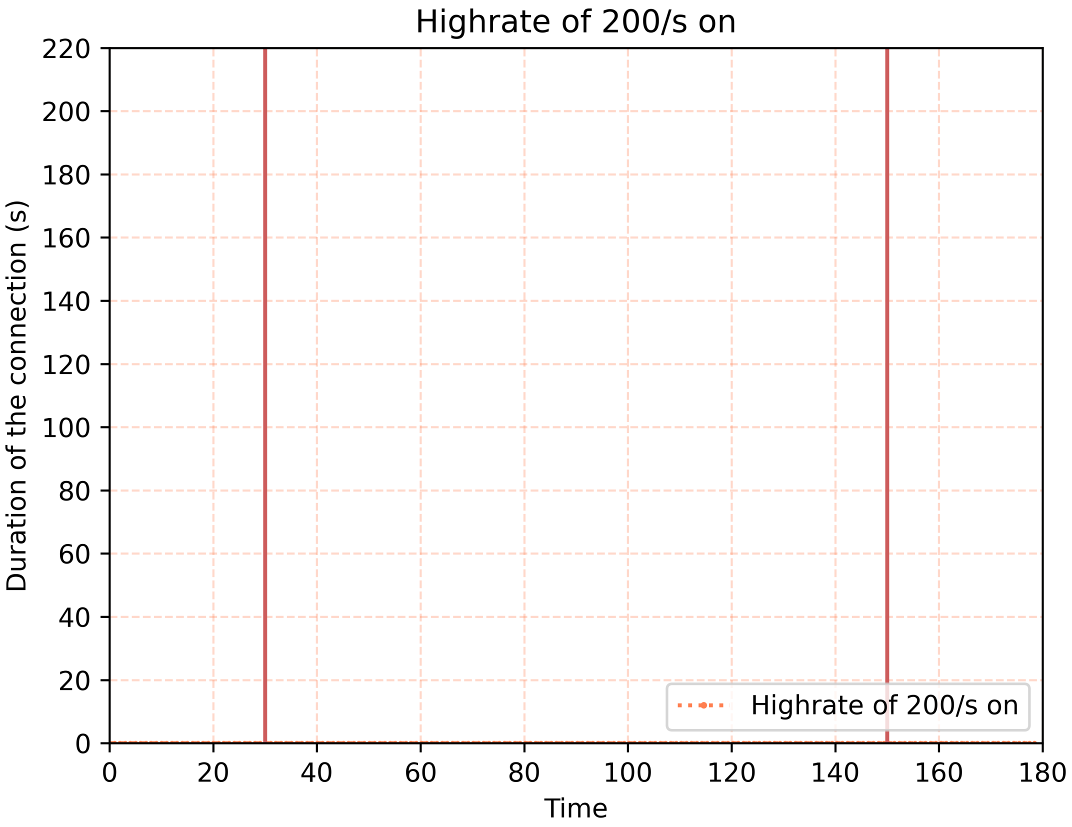

Figure 2: Connection duration graphs with SYN cookies on.

As it can be seen, in the case in which the SYN cookies are not active, when the attack stars at the second 30 the amount of time which takes for creating the connection raises drastically. Note that before that point, the time to create the connection is not clearly visible because it is in the order of 0.002 - 0.004 seconds, which in this graph is too small to see, which at the same time says much about the consequence of the attack.

On the other hand, when the SYN cookies are activated, the effect of the attack has no consequence. This is based on the previously explained description of SYN cookies, as the server does not reserve resources for the client until the last message of the handshake is received, which the attacker does not send, the server does not experiment the denial of service.