Jonathan Nguy

Lab 5 – TCP SYN Flood

1. TCP SYN flood attacks work when the attacker sends multiple SYN requests to a target so that the target's resources are all used up trying to handle that traffic. As a result, the target is unable to respond to legitimate traffic.

More technically:

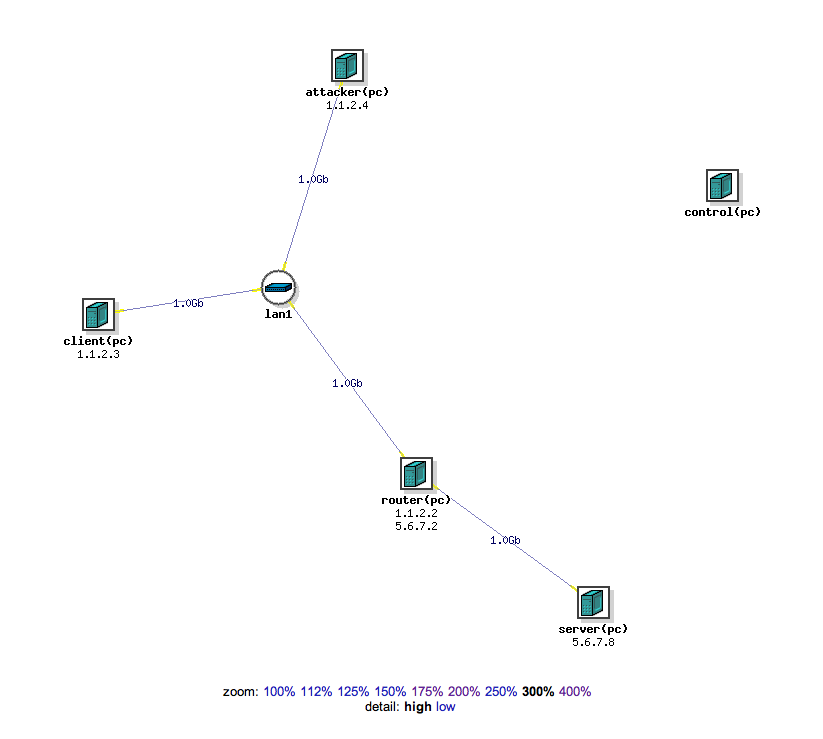
1. The client sends SYN messages to the server.

2. The server responds with SYN-ACKs

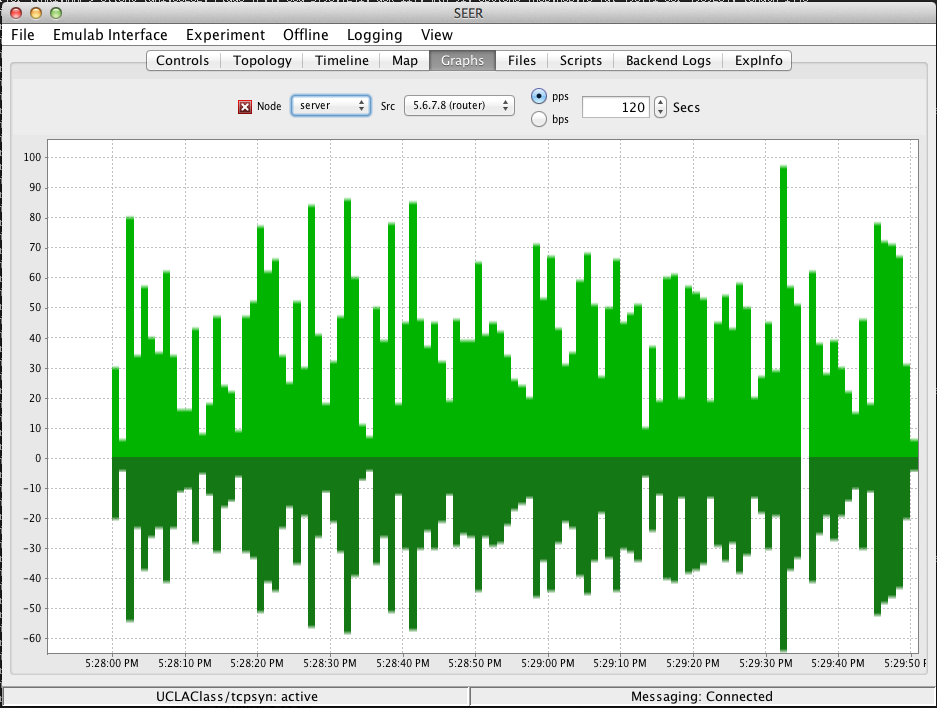
3. The client doesn't respond to those SYN-ACKs, so the server's resources are all used up waiting for the proper response.

2. SYN cookies eliminate the resources allocated when the SYN messages come to a server. From 1, SYN cookies allow the target/server to discard the SYN queue entry, so it won't get filled if there are a lot of SYN messages.

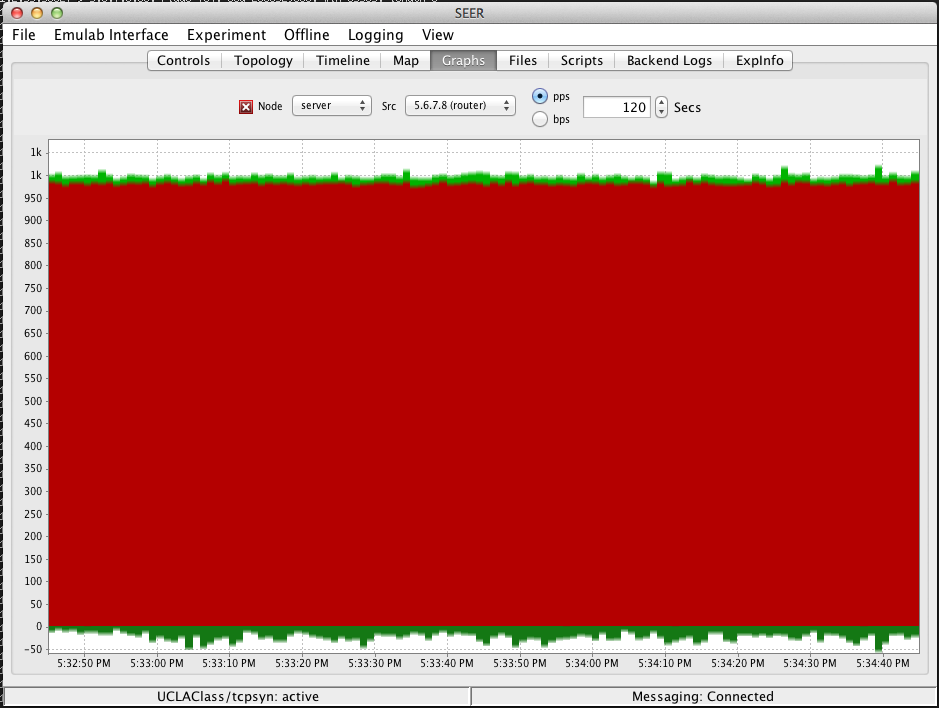
3.



4. Legitimate traffic

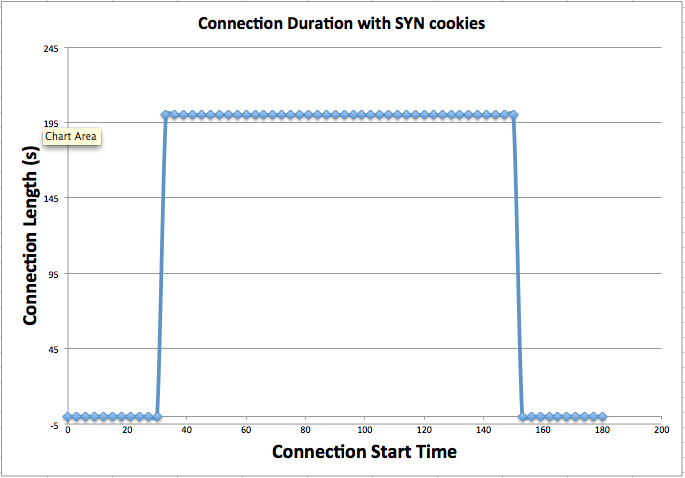


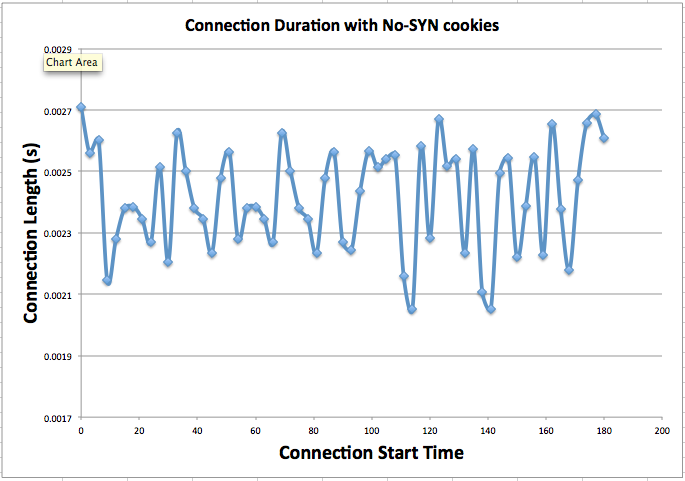
5. Attack traffic



The legitimate traffic doesn’t seem to increase during this time.

6.





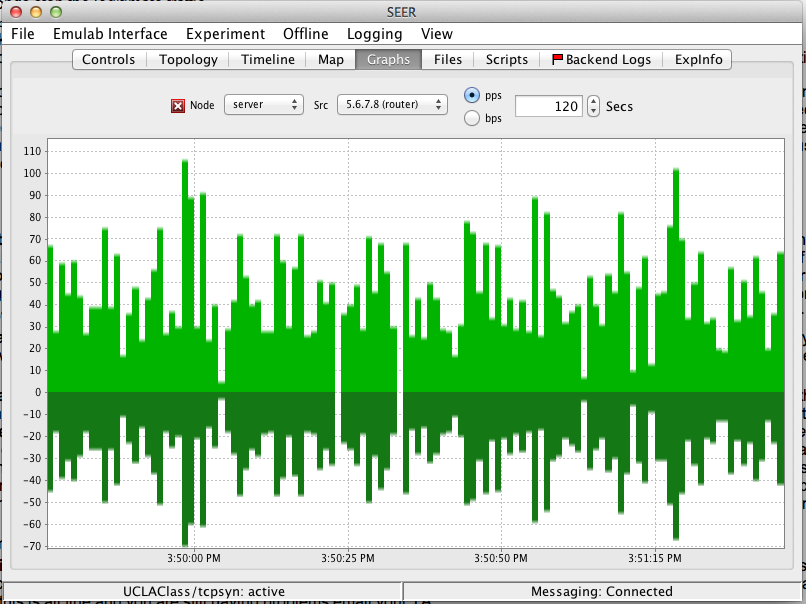
For the no-SYN-cookies graph, there’s a 30 second period where the connections are quick and normal. When the attack occurs, the next 120 seconds shows mostly long connections due to the server being able to respond to all the requests quick enough. The last 30 seconds after the attack is similar to the beginning, where the server is able to handle the load it is receiving.

For the SYN-cookies graph, the whole graph shows as if there’s no delay, due to the fact that SYN-cookies helps prevent the SYN flood attack. Throughout the whole 3 minutes, the server is never flooded with requests, so the connection durations for each SYN is very small.

From the graph, it can be seen that the attack is effective because during the time of the attack, there is a connection duration of 200 seconds (the default). Because of this long connection, we can see that the server’s sources are being used up for a long time, and the server is unable to respond to all the SYN’s it is receiving.

7.1.

Remove spoofing, the server looks like this:



The traffic is pretty much all legitimate, so without spoofing, we can see that the attack isn’t very effective. This happens because without spoofing, the target knows the source of the attack and can easily prevent the SYN flood. To do this attack effectively, we can use a botnet to attack the server. We do not have to spoof the IP address when we have multiple computers, so a SYN flood would be possible if we had many different computers with their own IP addresses.