EECE Assignment 1 Report

TCP SYN Flood Attack and Detection

Prof. Imad ElHajj

Peter Farah, Mariam Safieldin, Anthony Saab, and Mansour Abou Shaar

7th October 2021

Abstract

In this assignment, we implemented a TCP SYN Flood attack and a detection tool to detect the attack performed.

1 TCP SYN Flood Attack

Attack is developed by Peter Farah, Anthony Saab, and Mansour Abou Shaar. Details on contribution of each team member is available in the code documentation

The attack consist of sending many packets(number of packets sent chosen by user) over TCP with the SYN flag set over port 80 as destination port. The source IP chosen at random (spoofed) and the destination IP and source port chosen by the user.

2 TCP SYN Flood Detection Tool

Detection tool is developed by Peter Farah and Mariam Safieldin. Details on contribution of each team member is available in the code documentation

By measuring the amount of SYN requests received within a short period of time, the tool identifies potential TCP SYN flood attacks. The program observes a TCP SYN flood attack when it reaches a certain number of connections in a particular amount of time.

Firstly, the tool sniffs packets and passes them through an analyzer function. The analyzer then checks if the packet is a TCP SYN packet, and it stores and accumulates the number of SYN requests received every time a TCP SYN request is sent within a time frame of 5 seconds.

The number of TCP SYN packets received within this time frame are compared to a certain threshold. This threshold is a required input from the user, in order to accommodate the user's demand. If the number of TCP SYN packets received exceeds this threshold in a period of time less than 5 seconds, it is declared as a TCP SYN flood attack, and the time of attack along with the IP source sending the TCP SYN request are saved in a text file 'packet_breakdown.log'. Afterwards, the number of TCP SYN packets received is set to 80, accordingly, if 20 new TCP SYN requests are received during this time frame (period of 5 seconds), it is registered as a TCP SYN flood attack since the threshold is reached. The number of TCP SYN requests received is set to 0 every 5 seconds.

3 Running The Attack and The Detection Tool

To run the attack and the detection tools, follow the following set of instructions:

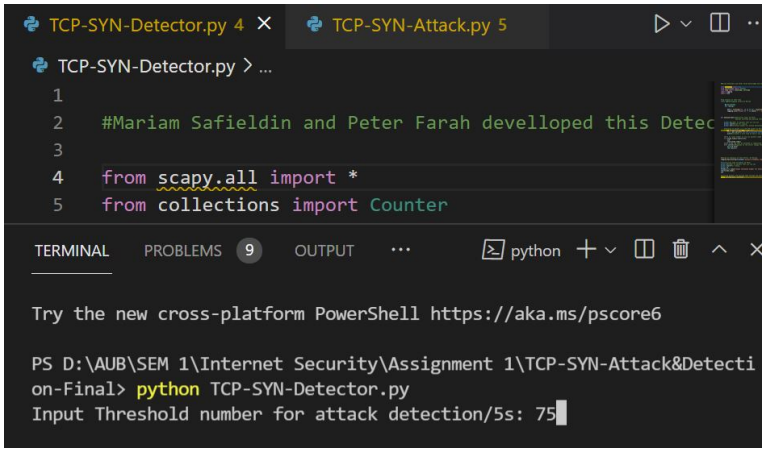

Figure 1: Running TCP-SYN-Detector.py

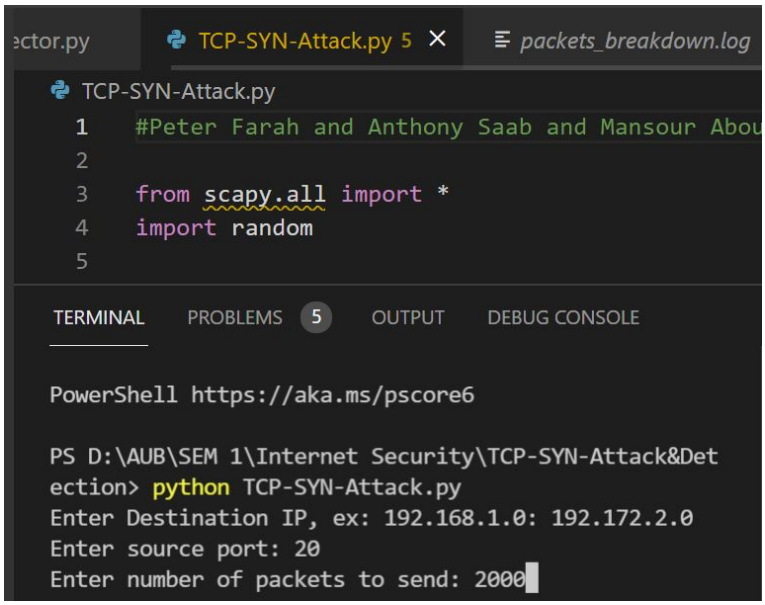

Figure 2: Running TCP-SYN-Attack.py

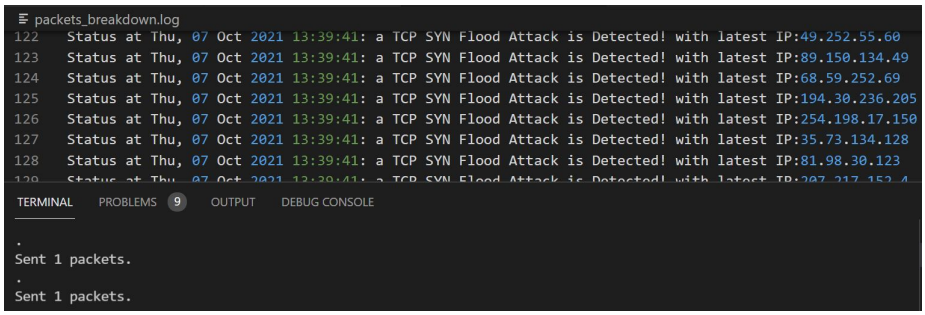

Figure 3: Attack detection.