

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 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

The tool has 2 options for detection.

2.1 First Detection Option

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 latest TCP SYN request are saved in a text file 'packet_breakdown.log'. Afterwards, the number of TCP SYN packets received is set to 80% the original threshold, accordingly, if 20% (of the original threshold) 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.

2.2 Second Detection Option

Option 2 is similar to Option 1, except instead of using a TCP SYN packet threshold, it uses the difference between the number of SYN and ACK packets received as the threshold. However, the attacker may easily get around this because the detection tool does not keep track of who transmitted a SYN packet because it would take up too much space and undermine the objective of the detector.

3 Running The Attack and The Detection Tool

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

```
C:\>python TCP-SYN-Detector.py

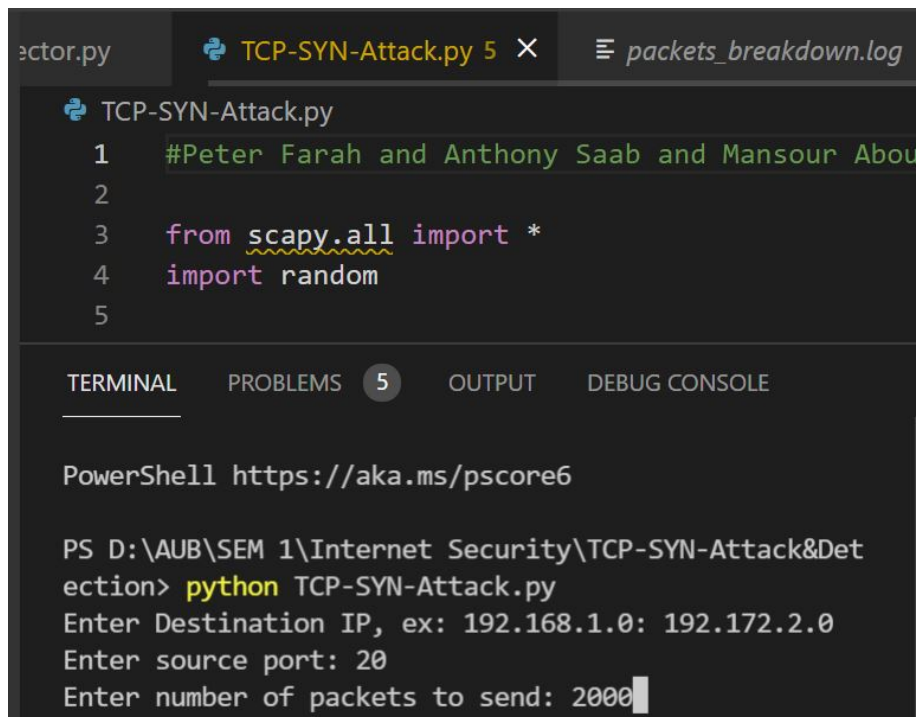
Recommended:(do not enter 0)
Enter threshold for number of SYN/5s. Enter 0 if you prefer to choose a threshold of (SYN-ack)/5s: 100
```

Figure 1: Running TCP-SYN-Detector.py with the threshold specified by the user.

```
C:\>python TCP-SYN-Detector.py

Recommended:(do not enter 0)
Enter threshold for number of SYN/5s. Enter 0 if you prefer to choose a threshold of (SYN-ack)/5s: 100
```

Figure 2: Running TCP-SYN-Detector.py with threshold calculated as the difference between SYN and ACK packets.



The screenshot shows a code editor with a file named `TCP-SYN-Attack.py` open. The script content is as follows:

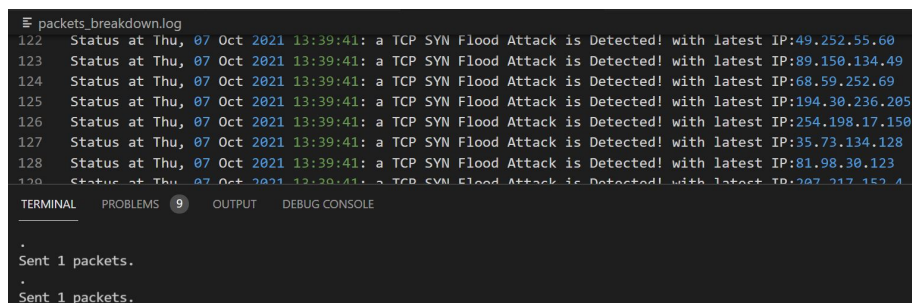
```
1 #Peter Farah and Anthony Saab and Mansour About
2
3 from scapy.all import *
4 import random
5
```

Below the code editor, the `TERMINAL` tab is active, showing the execution of the script. The terminal output is:

```
PowerShell https://aka.ms/pscore6

PS D:\AUB\SEM 1\Internet Security\TCP-SYN-Attack&Detection> python TCP-SYN-Attack.py
Enter Destination IP, ex: 192.168.1.0: 192.172.2.0
Enter source port: 20
Enter number of packets to send: 2000
```

Figure 3: Running TCP-SYN-Attack.py



The screenshot shows a terminal window with a log file named `packets_breakdown.log`. The log contains multiple entries indicating that a TCP SYN Flood Attack has been detected. Each entry includes a timestamp and a list of IP addresses. The terminal output is as follows:

```
122 Status at Thu, 07 Oct 2021 13:39:41: a TCP SYN Flood Attack is Detected! with latest IP:49.252.55.60
123 Status at Thu, 07 Oct 2021 13:39:41: a TCP SYN Flood Attack is Detected! with latest IP:89.150.134.49
124 Status at Thu, 07 Oct 2021 13:39:41: a TCP SYN Flood Attack is Detected! with latest IP:68.59.252.69
125 Status at Thu, 07 Oct 2021 13:39:41: a TCP SYN Flood Attack is Detected! with latest IP:194.30.236.205
126 Status at Thu, 07 Oct 2021 13:39:41: a TCP SYN Flood Attack is Detected! with latest IP:254.198.17.150
127 Status at Thu, 07 Oct 2021 13:39:41: a TCP SYN Flood Attack is Detected! with latest IP:35.73.134.128
128 Status at Thu, 07 Oct 2021 13:39:41: a TCP SYN Flood Attack is Detected! with latest IP:81.98.30.123
129 Status at Thu, 07 Oct 2021 13:39:41: a TCP SYN Flood Attack is Detected! with latest IP:207.217.152.4

TERMINAL PROBLEMS 9 OUTPUT DEBUG CONSOLE

Sent 1 packets.
Sent 1 packets.
```

Figure 4: Attack detection.