Part One – Lab: SYN Flood Attack (50%)

In this part, you will simulate a SYN Flood network attack on your own computer and implement a defense against it.
For this purpose, we will use the SEED Labs environment, a virtual machine with container-based networking.

Instructions for setting up the working environment can be found at the following link:
https://seedsecuritylabs.org/labsetup.html

Lab instructions:
https://seedsecuritylabs.org/Labs_20.04/Files/TCP_Attacks/TCP_Attacks.pdf

The lab uses a Python library called SCAPY for building and sending network packets with access to lower layers, instead of using sockets, which wrap these layers.
Most of the code that uses this library is provided in advance, but those who wish to read more can find additional background in Chapter 3 of the following document:
https://seedsecuritylabs.org/Labs_20.04/Files/Sniffing_Spoofing/Sniffing_Spoofing.pdf

You must follow the lab instructions and record a video with all group members, presenting the results of your work:

1. Present the `synflood.py` file that you wrote.

2. Show that SYN Cookies protection is disabled in the victim container.

3. Use the `synflood.py` file in the attacker container to attack the victim container.

4. While the attack is running, capture SYN and SYN-ACK packets using `tcpdump` in the victim container.

5. Display the length of the half-open connection queue in the victim container.

6. Attempt to connect to the victim using telnet from another machine on the network and show that the attempt fails.

7. Enable SYN Cookies protection in the victim container, and repeat steps 3–6 to demonstrate that the defense works.

Part Two – Theoretical Questions (50%)

Question 1 – RDT (20%)

In communication between two hosts over a channel, packets are of fixed size 1200 bytes, the transmission rate is 10 Gbps, and the propagation delay is 20 ms.

a) Assume the basic form of rdt 3.0 (stop-and-wait) is used.
What is the channel utilization in the best-case scenario (no packet loss)? Explain.

b) Assume the Go-Back-N algorithm is used, with 8 bits to represent the packet sequence numbers (SEQ).
What is the channel utilization in the best-case scenario? Explain.

Question 2 – TCP (15%)

Suppose a file of size L is transmitted from computer A to computer B.
For the purpose of this exercise, ignore congestion handling and assume that the sending window and receiving window of both sides are fixed at size W.
Recall that in TCP, W is limited to 16 bits and the sequence number is limited to 32 bits.

a) Assume the channel is FIFO, meaning packets arrive in the order they are sent.
Is the size of the sequence number large enough to guarantee correct data transfer for any file size L, or is there a maximum amount of data that can be sent beyond which errors may occur?
Justify your answer.

b) In the real world, the Internet is not a perfect FIFO channel; packets may arrive in arbitrary order.
Explain why the constraints are still sufficient in this reality.

Question 3 – TCP Congestion Control (15%)

This question refers to TCP Reno.
We observe the values of the congestion window cwnd at some random point in the TCP connection.

The following values of CWND are given at two different points in time:

Stage	CWND	SSTHRESH
1	28 MSS	32 MSS
2	???	???
3	???	???
4	???	???
5	8 MSS	???
6	???	???

You may assume that whenever fast recovery is entered, the first ACK received is a new ACK.

Which of the following values cannot be the value of CWND at time 6?

a) 1 MSS

b) 4 MSS
c) 9 MSS
d) 14 MSS
e) 16 MSS

Complete the rest of the table with the remaining values.