Lab Report

Your Performance

Your Score: 2 of 2 (100%) Pass Status: Pass
Elapsed Time: 6 minutes 30 seconds Required Score: 100%

Task Summary

Lab Questions

- ✓ Filter for SYN and ACK packets
- ✓ Q1What indicates that this is a distributed denial-of-service (DDoS) attack?
  Your answer: There are multiple source addresses for the SYN packets with the destination address 198.28.1.1.
  Correct answer: There are multiple source addresses for the SYN packets with the destination address 198.28.1.1.

Explanation

In this lab, your task is to:

- Capture packets from the network segment on www_stage using Wireshark.
- Analyze the attack using the following filters:
  - tcp.flags.syn==1 and tcp.flags.ack==1
  - tcp.flags.syn==1 and tcp.flags.ack==0
- Answer the question.

Complete this lab as follows:

1. From the Favorites bar, open Wireshark.
2. Under Capture, select **enp2s0**.
3. From the menu, select the **blue fin** to begin the capture.
4. In the Apply a display filter field, type **tcp.flags.syn==1 and tcp.flags.ack==1** and press **Enter** to filter the Wireshark display to only those packets with both the SYN flag and ACK flag.
   You may have to wait several seconds before any SYN-ACK packets are captured and displayed.
5. Select the **red square** to stop the capture.
6. In the Apply a display filter field, change the tcp.flags.ack ending from **1** to **0** and press **Enter** to filter the Wireshark display to packets with only the SYN flag.
   Notice that there are a flood of SYN packets being sent to 198.28.1.1 (www.corpnet.xyz) that were not being acknowledged.
7. In the top right, select **Answer Questions**.
8. Answer the question.
9. Select **Score Lab**.