11.6.8 Analyze a SYN Flood Attack

Your Performance

Your Score: 1 of 2 (50%)
Pass Status: **Not Passed**
Elapsed Time: 53 seconds
Required Score: 100%

Task Summary

Lab Questions

✗ Filter for SYN and ACK packets

✓ *Q1*: What indicates that this is a distributed denial-of-service (DDoS) attack?

Explanation

Complete this lab as follows:

1. Using Wireshark, only capture packets containing both the SYN flag and ACK flags.
   a. From the Favorites bar, select **Wireshark**.
   b. Under Capture, select **enp2s0**.
   c. From the menu, select the **blue fin** to begin the capture.
   d. In the *Apply a display filter* field, type **tcp.flags.syn==1 and tcp.flags.ack==1** and press **Enter** to filter Wireshark to display only those packets with both the SYN flag and ACK flag.
   You may have to wait up to a minute before any SYN-ACK packets are captured and displayed.
   e. Select the **red square** to stop the capture.
2. Change the filter to only display packets with the SYN flag.
   a. In the *Apply a display filter* field, change the tcp.flags.ack ending from the number **1** to the number **0** and press **Enter**.
   Notice that there are a flood of SYN packets being sent to 198.28.1.1 (www.corpnet.xyz) that are not being acknowledged.
   b. In the top right, select **Answer Questions**.
   c. Answer the question.
   d. Select **Score Lab**.