9.2 Lab: Analyze a DoS Attack

Candidate: COMPTIA COMPTIA ()
Time Spent: 00:42

Score: 0%

Task Summary

Required Actions and Questions

✗ Filter ICMP packets

✗ Filter SYN packets

✗ Ping CorpTest (192.168.10.19) to test connectivity

✗ Launch an hping3 flood

✗ *Q1*: For the selected packet, what is the Hex value for Flags?

Your answer:

Correct answer: 0x002

Explanation

Complete this lab as follows:

1. Using Wireshark, capture packets on the enp2s0 interface.
   a. From the Favorites bar, select **Wireshark**.
   b. Under Capture, select **enp2s0**.
   c. Select the **blue fin** to begin a Wireshark capture.
2. Using a Terminal, ping CorpTest (192.168.10.19).
   a. From the Favorites bar, select **Terminal**.
   b. At the prompt, type **ping CorpTest** (or 192.168.10.19) and press **Enter**.
   c. In Wireshark, apply a display filter by typing **icmp** (lower case). Note the packets captured in Wireshark.
   d. After a few seconds, type **Ctrl-C** to stop the ping. Clear the display filter.
3. Filter the packet capture to show only SYN packets, then start a SYN flood.
   a. In Wireshare's *Apply a display filter* field, type **tcp.flags.syn==1** and press **Enter**.
   b. From the Terminal, type **hping3 --syn --flood CorpTest** (or 192.168.10.19) and press **Enter** to start a TCP SYN flood against the CorpTest server.
   c. After a few seconds of capturing packets, select the **red box** to stop the Wireshark capture.
4. Examine the captured packets and answer the question.
   a. Maximize the Wireshark window for better viewing.
   b. In the top pane of Wireshark, select one of the *packets* captured with a destination address of 192.168.10.19.
   c. In the middle pane of Wireshark, expand **Transmission Control Protocol**.

d. Scroll down to Flags.
   Notice that the Flags item in this pane and the data in the Info column in the top pane show that this (and all the packets) is a SYN packet.
e. In the top right, select **Questions**.
f. Answer the question.