Lab Report

Your Performance

Your Score: 3 of 3 (100%) Pass Status: Pass
Elapsed Time: 2 minutes 22 seconds Required Score: 100%

Task Summary

Required Actions & Questions

- ✓ Filter SYN packets
- ✓ Launch an hping3 flood
- ✓ Q1For the packet selected, what is the hex value for Flags?
  Your answer: 0x002
  Correct answer: 0x002

Explanation

In this lab, your task is to use Wireshark to capture and analyze TCP SYN flood attacks as follows:

- Filter captured packets to show TCP SYN packets for the enp2s0 interface.
- Use **hping3** to launch a SYN flood attack against rmksupplies.com using Terminal.
- Examine a SYN packet with the destination address of 208.33.42.28 after capturing packets for a few seconds.
- Answer the question.

Complete this lab as follows:

1. From the Favorites bar, open Wireshark.
2. Under Capture, select **enp2s0**.
3. Select the **blue fin** to begin a Wireshark capture.
4. In the Apply a display filter field, type **tcp.flags.syn==1** and press **Enter**.
5. From the Favorites bar, open Terminal.
6. At the prompt, type **hping3 --syn --flood rmksupplies.com** and press **Enter** to start a TCP SYN flood against the CorpDC domain controller.
7. After a few seconds of capturing packets, select the **red box** to stop the Wireshark capture
8. In the top pane of Wireshark, select one of the ***packets*** captured with a destination address of 208.33.42.28.
9. In the middle pane of Wireshark, expand **Transmission Control Protocol**.
10. Scroll down to Flags.
    Notice that both Flags in this pane and the Info column in the top pane show this as a SYN packet.
11. In the top right, select **Answer Questions**.
12. Answer the question.
13. Click **Score Lab**.