Lab Report

Your Performance

Your Score: 4 of 4 (100%)

Pass Status: Pass

Elapsed Time: 7 minutes 12 seconds

Required Score: 100%

Task Summary

Required Actions & Questions

✓ Filter for ICMP packets

✓ Run ping

✓ Run hping3 for ICMP flood

✓ Q1What is the main difference between a normal icmp (ping) request and an icmp flood? (Select TWO).
Your answer: With the icmp flood, the icmp packets are sent more rapidly., With the flood, all packets come from the source.
Correct answer: With the icmp flood, the icmp packets are sent more rapidly., With the flood, all packets come from the source.

Explanation

In this lab, your task is to create and examine the results of an ICMP flood attack as follows:

- From Kali Linux, start a capture in Wireshark for the esp20 interface.
- Ping CorpDC at 192.168.0.11.
- Examine the ICMP packets captured.
- Use hping3 to launch an ICMP flood attack against CorpDC.
- Examine the ICMP packets captured.
- Answer the questions.

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. From the Favorites bar, open Terminal.
5. At the prompt, type **ping 192.168.0.11** and press **Enter**.
6. After some data exchanges, press **Ctrl** + **c** to stop the ping process.
7. In Wireshark, select the **red box** to stop the Wireshark capture.
8. In the Apply a display filter field, type **icmp** and press **Enter**.
   Notice the number of packets captured and the time between each packet being sent.
9. Select the **blue fin** to begin a new Wireshark capture.
10. In Terminal, type **hping3 --icmp --flood 192.168.0.11** and press **Enter** to start a ping flood against CorpDC.
11. In Wireshark, select the **red box** to stop the Wireshark capture.
    Notice the type, number of packets, and the time between each packet being sent.
12. In Terminal, type **Ctrl** + **c** to stop the ICMP flood.
13. In the top right, select **Answer Questions**.
14. Answer the questions.
15. Select **Score Lab**.