9.4 Lab: Poison ARP and Analyze with Wireshark

Candidate: COMPTIA COMPTIA ()
Time Spent: 02:57

Score: 0%

Task Summary

Lab Questions

✕ *Q1*: What is the MAC address of the first responding device?

Your answer:

Correct answer: 00:00:1B:11:22:33

✕ *Q2*: What was the MAC address of the duplicate responding device?

Your answer:

Correct answer: 00:00:1B:33:22:11

Explanation

Complete this lab as follows:

1. Use Wireshark to capture packets on *enp2s0*.
   a. From the Favorites bar, select **Wireshark**.
   b. Maximize the window for better viewing.
   c. Under Capture, select **enp2s0**.
   d. From the menu bar, select the ***blue fin*** to begin a Wireshark capture.
   e. After capturing packets for five seconds, select the ***red box*** to stop the Wireshark capture.
2. Filter for only ARP packets.
   a. In the *Apply a display filter* field, type **arp** and press **Enter** to only show ARP packets.
   b. In the Info column, look for the lines containing the **192.168.0.2** IP address.
3. Answer the questions.