9.7 Lab: Discover a Rogue DHCP Server

Candidate: COMPTIA COMPTIA ()
Time Spent: 01:00

Score: 0%

Task Summary

Required Actions and Questions

- ✗ Capture and filter DHCP traffic
- ✗ Disable and enable the enp2s0 network interface
- ✗ *Q1*: What is the IP address of the rogue DHCP server?
  Your answer:
  Correct answer: 10.10.10.240
- ✗ *Q2*: What is the IP address of the legitimate DHCP server?
  Your answer:
  Correct answer: 192.168.0.14

Explanation

Complete this lab as follows:

1. Use Wireshark to capture and filter DHCP traffic.
   a. From the Favorites bar, select **Wireshark**.
   b. Under Capture, select **enp2s0**.
   c. Select the **blue fin** to begin a Wireshark capture.
   d. In the *Apply a display filter* field, type **bootp** and press **Enter**.
2. Disable and enable the enp2s0 network interface.
   a. From the Favorites bar, select **Terminal**.
   b. At the prompt, type **ip addr show** and press **Enter** to view the current IP configuration.
   c. Type **ip link set enp2s0 down** and press **Enter**.
   d. Type **ip link set enp2s0 up** and press **Enter** to enable the interface and request an IP address from the DHCP server.
3. Locate the rogue and legitimate DHCP servers.
   a. Maximize the Wireshark window for better viewing.
   b. In Wireshark, under the Source column, find the ***IP addresses*** of the rogue and legitimate DHCP servers that sent the DHCP Offer packets.
   c. Answer the questions.