Lab Report

Your Performance

Your Score: 4 of 4 (100%) Pass Status: Pass
Elapsed Time: 5 minutes 3 seconds Required Score: 100%

Task Summary

Required Actions & Questions

- ✓ Capture and filter DHCP traffic
- ✓ Disable and enable the enp2s0 network interface
- ✓ Q1What is the IP address of the rogue DHCP server?
  Your answer: 10.10.10.240
  Correct answer: 10.10.10.240
- ✓ Q2What is the IP address of the legitimate DHCP server?
  Your answer: 192.168.0.14
  Correct answer: 192.168.0.14

Explanation

In this lab, your task is to identify the rogue DHCP server using Wireshark:

- Use Wireshark to capture and filter DHCP traffic.
- Disable and enable the enp2s0 network interface to request a new IP address from the DHCP server.
- Find the rogue DHCP server.
- Answer the questions.

Complete this lab as follows:

1. Use Wireshark to capture and filter DHCP traffic as follows:
   a. From the Favorites bar, open 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 as follows:
   a. From the Favorites bar, open 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. Maximize the window for easier viewing.
4. In Wireshark, under the Source column, find the ***IP addresses*** of the rogue and legitimate DHCP servers that sent the DHCP Offer packets.
5. In the top right, select **Answer Questions**.
6. Answer the questions.
7. Select **Score Lab**.