8.13 Lab: Troubleshoot with Wireshark

Candidate: COMPTIA COMPTIA ()
Time Spent: 00:43

Score: 0%

Task Summary

Required Actions and Questions

- ✕ Isolate traffic with the **net 192.168.0.0** filter
- ✕ *Q1*: What is the effect of the **net 192.168.0.0** filter in Wireshark?
  - Your answer:
  - Correct answer: Only packets with either a source or destination address on the 192.168.0.x network are displayed.
- ✕ Isolate traffic with the **host 192.168.0.45** filter
- ✕ *Q2*: What is the effect of the **host 192.168.0.45** filter in Wireshark?
  - Your answer:
  - Correct answer: Only packets with 192.168.0.45 in either the source or destination address are displayed.
- ✕ Isolate traffic with the **ip.src==192.168.0.45** filter
- ✕ *Q3*: What is the effect of the **ip.src==192.168.0.45** filter in Wireshark?
  - Your answer:
  - Correct answer: Only packets with 192.168.0.45 in the source address are displayed.
- ✕ Isolate traffic with the **ip.dst==192.168.0.45** filter
- ✕ *Q4*: What is the effect of the **ip.dst==192.168.0.45** filter in Wireshark?
  - Your answer:
  - Correct answer: Only packets with 192.168.0.45 in the destination address are displayed.
- ✕ Isolate traffic with the **tcp.port==80** filter
- ✕ *Q5*: What is the effect of the **tcp.port==80** filter in Wireshark?
  - Your answer:
  - Correct answer: Only packets with port 80 in either the source or destination port are displayed.
- ✕ Isolate traffic with the **eth contains 11:12:13** filter

✗ *Q6*: What is the effect of the **eth contains 11:12:13** filter in Wireshark?

Your answer:

Correct answer: Only packets with 11:12:13 in either the source or destination MAC address are displayed.

✗ Isolate traffic with the **tcp contains password** filter

✗ *Q7*: What is the captured password?

Your answer:

Correct answer: hippophobia

Explanation

Complete this lab as follows:

1. Begin a Wireshark capture.
   a. From the Favorites bar, select **Wireshark**.
   b. Maximize the window for easier viewing.
   c. Under Capture, select **enp2s0**.
   d. Select the ***blue fin*** to begin a Wireshark capture.
2. Apply the **net 192.168.0.0** filter.
   a. In the *Apply a display filter* field, type **net 192.168.0.0** and press **Enter**.
   Look at the source and destination addresses of the filtered packets.
   b. Select the ***red square*** to stop the Wireshark capture.
   c. In the top right, select **Questions**.
   d. Answer Question 1.
3. Apply the **host 192.168.0.45** filter.
   a. Select the ***blue fin*** to begin a Wireshark capture.
   b. In the *Apply a display filter* field, type **host 192.168.0.45** and press **Enter**.
   Look at the source and destination addresses of the filtered packets.
   c. Answer Question 2.
4. Apply the **ip.src==192.168.0.45** filter.
   a. In the *Apply a display filter* field, type **ip.src==192.168.0.45** and press **Enter**.
   Look at the source and destination addresses of the filtered packets.
   b. Answer Question 3.
5. Apply the **ip.dst==192.168.0.45** filter.
   a. In the *Apply a display filter* field, type **ip.dst==192.168.0.45** and press **Enter**.
   Look at the source and destination addresses of the filtered packets.
   b. Answer Question 4.
6. Apply the **tcp.port==80** filter.
   a. In the *Apply a display filter* field, type **tcp.port==80** and press **Enter**.
   Look in the Info column of the filtered packets.
   b. Answer Question 5.
7. Apply the **eth contains 11:12:13** filter.
   a. In the *Apply a display filter* field, type **eth contains 11:12:13** and press **Enter**.
   Look at the source and destination addresses of the filtered packets.
   b. Answer Question 6.
8. Apply the **tcp contains password** filter.
   a. In the *Apply a display filter* field, type **tcp contains password** and press **Enter**.
   b. Select the ***red box*** to stop the Wireshark capture.
   c. From the bottom pane, locate the password.
   d. Answer Question 7.