6.1 Lab: Explore Three-Way Handshake in Wireshark

Candidate: COMPTIA COMPTIA ()
Time Spent: 01:03

Score: 0%

Task Summary

Required Actions and Questions

- ✗ Isolate traffic with the **tcp and host 192.168.0.45** filter
- ✗ *Q1*: Which computer (ip address) is the sender of the [SYN] packet?
  Your answer:
  Correct answer: 192.168.0.45
- ✗ *Q2*: What is the value of the [SYN] flag in Wireshark?
  Your answer:
  Correct answer: 0x002
- ✗ *Q3*: Which computer (ip address) is the sender of the [ACK, SYN] packet?
  Your answer:
  Correct answer: 192.168.0.16
- ✗ *Q4*: What is the destination port for the [ACK, SYN] packet in Wireshark?
  Your answer:
  Correct answer: 5049
- ✗ *Q5*: Which computer (ip address) is the sender of the [ACK] packet?
  Your answer:
  Correct answer: 192.168.0.45
- ✗ *Q6*: What is the Acknowledgement number for the [ACK] packet in Wireshark?
  Your answer:
  Correct answer: 2

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.
e. Wait about 5 seconds, then select the ***red square*** to stop the Wireshark capture.

2. Apply a filter for tcp traffic from the computer at 192.168.0.45 and examine a [SYN] packet.
   a. In the *Apply a display filter* field, type **tcp and host 192.168.0.45** and press **Enter**.
   b. Look at the source and destination addresses of the filtered packets.
3. Examine a [SYN] packet
   a. Select a packet that includes [SYN] in the Info column.
   b. In the center pane, expand **Internet Protocol Version 4** and **Transmission Control Protocol**.
   c. Select **Questions**, then answer Questions 1 and 2.
   d. Minimize the **Lab Questions** dialog.
4. Examine an [ACK, SYN] Packet.
   a. Select a packet that includes [ACK, SYN] in the Info column.
   b. Select **Questions**, then answer Questions 3 and 4.
   c. Minimize the **Lab Questions** dialog.
5. Examine an [ACK] Packet.
   a. Select a packet that includes [ACK] in the Info column.
   b. Select **Questions**, then answer Questions 5 and 6.