Labs

back to dashboard

WLAN Protocol Analysis

EXPIRED

Observe the management and data frames exchanges

15-45 Minutes 290 Points 6/10 Difficulty

Start Stop

You have already completed this exercise.

Mission Statement Verify Flags New Terminal

Get yourself familiar with the WLAN protocol and observe the management and data frames exchanges between stations and Access Points in an 802.11 WLAN.

Objectives

1. Scroll down the list of frames and click frame #8, which is an unencrypted simple data frame. Look at the frame body and notice the upper-layer information, such as IP addresses and TCP ports.
2. Click frame #136, which is an encrypted simple data frame. Look at the frame body and notice that WEP encryption is being used and that the upper-layer information cannot be seen.
3. Scroll down the list of frames and observe the EAP frame exchange from frame #209 to frame #246.
4. Scroll down the list of frames and observe the 4-Way Handshake from frame #247 to frame #254.

Labs

back to dashboard

WLAN Protocol Analysis

EXPIRED

Observe the management and data frames exchanges

15-45 Minutes 290 Points 6/10 Difficulty

Start Stop

You have already completed this exercise.

Mission Statement | Verify Flags | New Terminal

Hide Flags

1. Identify the destination Protocol and IP:PORT used in frame #8

Syntax - <Protocol> <IP:PORT>

ftp 192.168.100.52:1105 ✓ 30 Points

2. What are the Initialisation Vector (IV) and Integrity Check Value (ICV) in frame #136?

Syntax - <IV> <ICV>

0x003a27 0x7305864a ✓ 40 Points

3. What is the protocol type shown on the 802.1x authentication frame #209?

EAPOL ✓ 30 Points

4. What is the Source MAC address of the 802.1x client from frame #209?

00:40:96:a2:e1:c2 ✓ 40 Points

5. Is the source MAC is frame #209 same as receiver MAC address in the following frame?

5. Is the source MAC is frame #209 same as receiver MAC address in the following frame?

Hint - Yes/No or Y/N

Yes ✔ 30 Points

6. How many frame exchanged for the entire 802.1x authentication process starting from frame #209?

8 ✔ 40 Points

7. Identify the frame number that holds the third message of the 4-way WPA2 handshake

251 ✔ 40 Points

8. What encryption type is being used for the 4-way handshake?

CCMP ✔ 40 Points