CWAP-404^Q&As^

Certified Wireless Analysis Professional

Pass CWNP CWAP-404 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/cwap-404.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CWNP Official Exam Center

QUESTION 1

In a Spectrum Analyzer the Swept Spectrogram plot displays what information?

A. RF power present at a particular frequency over the course of time

B. Reductions in frame transmissions

C. Wi-Fi Device information

D. The RF time domain

Correct Answer: A

Explanation: The Swept Spectrogram plot is a spectrum analysis plot that shows the RF power present at a particular frequency over the course of time. It can help identify trends and patterns in the RF spectrum over a longer period of time. It can also show how the RF environment changes over time and how different sources of RF signals affect each other. The other options are not correct, as they describe different types of plots or information that are not related to the Swept Spectrogram plot. References: [Wireless Analysis Professional Study Guide], Chapter 3: Spectrum Analysis, page 72-73

QUESTION 2

Given a protocol analyzer can decrypt WPA2-PSK data packets providing the PSK and SSID are configured in the analyzer software. When performing packet capture (in a non- FT environment) which frames are required in order for PSK frame decryption to be possible?

A. Authentication

B. 4-Way Handshake

C. Reassociation

D. Probe Response

Correct Answer: B

Explanation: The 4-way handshake is the process that establishes the pairwise transient key (PTK) between the client and the AP in WPA2-PSK. The PTK is derived from the PSK, the SSID, and some random numbers exchanged in the handshake frames. The PTK is used to encrypt and decrypt the data frames between the client and the AP. Therefore, in order to decrypt WPA2-PSK data packets, a protocol analyzer needs to capture the 4-way handshake frames and have the PSK and SSID configured in the analyzer software12 References: CWAP-404 Study Guide, Chapter 3: 802.11 MAC Layer Frame Formats and Technologies, page 87 CWAP-404 Objectives, Section 3.5: Analyze security exchanges

QUESTION 3

How many frames are exchanged for 802.11 authentication in the 6 GHz band when WPA3-Enterprise is not used, and a passphrase is used instead?

A. 1

B. 2

C. 3

D. 4

Correct Answer: B

Explanation: Two frames are exchanged for 802.11 authentication in the 6 GHz band when WPA3-Enterprise is not used, and a passphrase is used instead. Authentication is a process that establishes an identity relationship between a STA (station) and an AP (access point) before joining a BSS (Basic Service Set). There are two types of authentication methods defined by 802.11: Open System Authentication and Shared Key Authentication. Open System Authentication does not require any credentials or security information from a STA to join a BSS, and it consists of two frames: an Authentication Request frame sent by the STA to the AP, and an Authentication Response frame sent by the AP to the STA. Shared Key Authentication requires a shared secret key from a STA to join a BSS, and it consists of four frames: two challenge-response frames in addition to the request-response frames. However, Shared Key Authentication uses WEP (Wired Equivalent Privacy) as its encryption algorithm, which is insecure and deprecated. In the 6 GHz band, which is a newly available frequency band for WLANs, Shared Key Authentication is prohibited by the 802.11 standard, as it poses security and interference risks for other users and services in the band. The 6 GHz band requires all WLANs to use WPA3-Personal or WPA3-Enterprise encryption methods, which are more secure and robust than previous encryption methods such as WPA2 or WEP. WPA3-Personal uses a passphrase to derive a PMK (Pairwise Master Key), while WPA3-Enterprise uses an authentication server to obtain a PMK. Both methods use SAE (Simultaneous Authentication of Equals) as their authentication protocol, which replaces PSK (Pre-Shared Key) or EAP (Extensible Authentication Protocol). SAE consists of two frames: an SAE Commit frame sent by both parties to exchange elliptic curve parameters and nonces, and an SAE Confirm frame sent by both parties to verify each other\\'s identities and generate a PMK. Therefore, when WPA3-Enterprise is not used, and a passphrase is used instead in the 6 GHz band, only two frames are exchanged for 802.11 authentication: an SAECommit frame and an SAE Confirm frame. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 8: Security Analysis, page 220-221

QUESTION 4

What is the default 802.11 authentication method for a STA when using Pre-RSNA?

A. Open System

B. Shared Key

C. 4-Way Handshake

D. PSK

Correct Answer: A

Explanation: The default 802.11 authentication method for a STA when using Pre-RSNA is Open System. This is the simplest and most common authentication method, which does not provide any security or encryption. In Open System authentication, the STA sends an Authentication Request frame to the AP, and the AP responds with an Authentication Response frame with a status code of success. After this, the STA can proceed to association with the AP . References: CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 6: MAC Sublayer Frame Exchanges, page 181; CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter

6: MAC Sublayer Frame Exchanges, page 183.

QUESTION 5

How many frames make up the Group Key Handshake excluding any Ack frames that may be required?

A. 1

B. 2

C. 3

D. 4

Correct Answer: B

Explanation: The Group Key Handshake consists of two frames excluding any Ack frames that may be required. The Group Key Handshake is used to distribute and update the Group Temporal Key (GTK) for encrypting broadcast and multicast traffic. The AP initiates the Group Key Handshake by sending a Group Key Message 1 frame to a STA, which contains the new GTK and other information. The STA responds with a Group Key Message 2 frame to the AP, which confirms the receipt of the GTK and other information. After this, both the AP and the STA can use the new GTK for encryption and decryption of broadcast and multicast traffic . References: CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 7: 802.11 Security, page 246; CWAP- 404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 7:

802.11 Security, page 247.