



CWSP-206^{Q&As}

CWSP Certified Wireless Security Professional

Pass CWNP CWSP-206 Exam with 100% Guarantee

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

<https://www.geekcert.com/cwsp-206.html>

100% Passing Guarantee
100% Money Back Assurance

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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

What security vulnerability may result from a lack of staging, change management, and installation procedures for WLAN infrastructure equipment?

- A. The WLAN system may be open to RF Denial-of-Service attacks.
- B. Authentication cracking of 64-bit Hex WPA-Personal PSK.
- C. AES-CCMP encryption keys may be decrypted.
- D. WIPS may not classify authorized, rogue, and neighbor APs accurately.

Correct Answer: D

QUESTION 2

The Aircrack-ng WLAN software tool can capture and transmit modified 802.11 frames over the wireless network. It comes pre-installed on Kali Linux and some other Linux distributions. Which one of the following would not be a suitable penetration testing action taken with this tool?

- A. Auditing the configuration and functionality of a WIPS by simulating common attack sequences.
- B. Transmitting a deauthentication frame to disconnect a user from the AP.
- C. Cracking the authentication or encryption processes implemented poorly in some WLANs.
- D. Probing the RADIUS server and authenticator to expose the RADIUS shared secret.

Correct Answer: D

QUESTION 3

During 802.1X/LEAP authentication, the username is passed across the wireless medium in clear text. From a security perspective, why is this significant?

- A. The username can be looked up in a dictionary file that lists common username/password combinations.
- B. The username is needed for Personal Access Credential (PAC) and X.509 certificate validation.
- C. 4-Way Handshake nonces are based on the username in WPA and WPA2 authentication.
- D. The username is an input to the LEAP challenge/response hash that is exploited, so the username must be known to conduct authentication cracking.

Correct Answer: D

QUESTION 4



In the basic 4-way handshake used in secure 802.11 networks, what is the purpose of the ANonce and SNonce?

- A. They are added together and used as the GMK, from which the GTK is derived.
- B. They are used to pad Message 1 and Message 2 so each frame contains the same number of bytes.
- C. The IEEE 802.11 standard requires that all encrypted frames contain a nonce to serve as a Message Integrity Check (MIC).
- D. They are input values used in the derivation of the Pairwise Transient Key.

Correct Answer: D

QUESTION 5

ABC Company is an Internet Service Provider with thousands of customers. ABC's customers are given login credentials for network access when they become a customer. ABC uses an LDAP server as the central user credential database. ABC is extending their service to existing customers in some public access areas and would like to use their existing database for authentication. How can ABC Company use their existing user database for wireless user authentication as they implement a large-scale WPA2Enterprise WLAN security solution?

- A. Implement a RADIUS server and query user authentication requests through the LDAP server.
- B. Mirror the LDAP server to a RADIUS database within a WLAN controller and perform daily backups to synchronize the user databases.
- C. Import all users from the LDAP server into a RADIUS server with an LDAP-to-RADIUS conversion tool.
- D. Implement an X.509 compliant Certificate Authority and enable SSL queries on the LDAP server.

Correct Answer: A

[CWSP-206 PDF Dumps](#)

[CWSP-206 Practice Test](#)

[CWSP-206 Exam Questions](#)