



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.passapply.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

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 2

Which of the following is a valid reason to avoid the use of EAP-MD5 in production WLANs?

- A. It does not support a RADIUS server.
- B. It is not a valid EAP type.
- C. It does not support mutual authentication.
- D. It does not support the outer identity.

Correct Answer: C

QUESTION 3

In a security penetration exercise, a WLAN consultant obtains the WEP key of XYZ Corporation's wireless network. Demonstrating the vulnerabilities of using WEP, the consultant uses a laptop running a software AP in an attempt to hijack the authorized user's connections. XYZ's legacy network is using 802.11n APs with 802.11b, 11g, and 11n client devices. With this setup, how can the consultant cause all of the authorized clients to establish Layer 2 connectivity with the software access point?

- A. When the RF signal between the clients and the authorized AP is temporarily disrupted and the consultant's software AP is using the same SSID on a different channel than the authorized AP, the clients will reassociate to the software AP.
- B. If the consultant's software AP broadcasts Beacon frames that advertise 802.11g data rates that are faster rates than XYZ's current 802.11b data rates, all WLAN clients will reassociate to the faster AP.
- C. A higher SSID priority value configured in the Beacon frames of the consultant's software AP will take priority over the SSID in the authorized AP, causing the clients to reassociate.
- D. All WLAN clients will reassociate to the consultant's software AP if the consultant's software AP provides the same SSID on any channel with a 10 dB SNR improvement over the authorized AP.



Correct Answer: A

QUESTION 4

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 5

The IEEE 802.11 Pairwise Transient Key (PTK) is derived from what cryptographic element?

- A. PeerKey (PK)
- B. Group Master Key (GMK)
- C. Key Confirmation Key (KCK)
- D. Pairwise Master Key (PMK)
- E. Phase Shift Key (PSK)
- F. Group Temporal Key (GTK)

Correct Answer: D

[CWSP-206 Practice Test](#)

[CWSP-206 Study Guide](#)

[CWSP-206 Braindumps](#)