

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.pass2lead.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 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

QUESTION 2

What software and hardware tools are used in the process performed to hijack a wireless station from the authorized wireless network onto an unauthorized wireless network?

- A. A low-gain patch antenna and terminal emulation software
- B. MAC spoofing software and MAC DoS software
- C. RF jamming device and a wireless radio card
- D. A wireless workgroup bridge and a protocol analyzer

Correct Answer: C

QUESTION 3

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 4

Many corporations configure guest VLANs on their WLAN controllers that allow visitors to have Internet access only. The guest traffic is tunneled to the DMZ to prevent some security risks. In this deployment, what risk is still associated with implementing the guest VLAN without any advanced traffic monitoring or filtering feature enabled?

- A. Intruders can send spam to the Internet through the guest VLAN.
- B. Peer-to-peer attacks can still be conducted between guest users unless application-layer monitoring and filtering are implemented.
- C. Guest users can reconfigure AP radios servicing the guest VLAN unless unsecure network management protocols (e.g. Telnet, HTTP) are blocked.
- D. Once guest users are associated to the WLAN, they can capture 802.11 frames from the corporate VLANs.

Correct Answer: A

QUESTION 5

In XYZ's small business, two autonomous 802.11ac APs and 12 client devices are in use with WPA2Personal. What statement about the WLAN security of this company is true?

- A. Intruders may obtain the passphrase with an offline dictionary attack and gain network access, but will be unable to decrypt the data traffic of other users.
- B. Because WPA2-Personal uses Open System authentication followed by a 4-Way Handshake, hijacking attacks are easily performed.
- C. A successful attack against all unicast traffic on the network would require a weak passphrase dictionary attack and the capture of the latest 4-Way Handshake for each client.
- D. An unauthorized wireless client device cannot associate, but can eavesdrop on some data because WPA2-Personal does not encrypt multicast or broadcast traffic.
- E. An unauthorized WLAN user with a protocol analyzer can decode data frames of authorized users if he captures the BSSID, client MAC address, and a user's 4-Way Handshake.

Correct Answer: C

[CWSP-206 Practice Test](#)

[CWSP-206 Study Guide](#)

[CWSP-206 Exam Questions](#)