



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 field in the RSN information element (IE) will indicate whether PSK- or Enterprise-based WPA or WPA2 is in use?

- A. Group Cipher Suite
- B. Pairwise Cipher Suite List
- C. AKM Suite List
- D. RSN Capabilities

Correct Answer: C

QUESTION 2

A network security auditor is preparing to perform a comprehensive assessment of an 802.11ac network's security. What task should be performed at the beginning of the audit to maximize the auditor's ability to expose network vulnerabilities?

- A. Identify the IP subnet information for each network segment.
- B. Identify the manufacturer of the wireless infrastructure hardware.
- C. Identify the skill level of the wireless network security administrator(s).
- D. Identify the manufacturer of the wireless intrusion prevention system.
- E. Identify the wireless security solution(s) currently in use.

Correct Answer: E

QUESTION 3

What WLAN client device behavior is exploited by an attacker during a hijacking attack?

- A. After the initial association and 4-way handshake, client stations and access points do not need to perform another 4-way handshake, even if connectivity is lost.
- B. Client drivers scan for and connect to access point in the 2.4 GHz band before scanning the 5 GHz band.
- C. When the RF signal between a client and an access point is disrupted for more than a few seconds, the client device will attempt to associate to an access point with better signal quality.
- D. When the RF signal between a client and an access point is lost, the client will not seek to reassociate with another access point until the 120 second hold down timer has expired.
- E. As specified by the Wi-Fi Alliance, clients using Open System authentication must allow direct client-to-client connections, even in an infrastructure BSS.

Correct Answer: C



QUESTION 4

What attack cannot be detected by a Wireless Intrusion Prevention System (WIPS)?

- A. Deauthentication flood
- B. Soft AP
- C. EAP flood
- D. Eavesdropping
- E. MAC Spoofing
- F. Hotspotter

Correct Answer: D

QUESTION 5

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

[Latest CWSP-206 Dumps](#)

[CWSP-206 VCE Dumps](#)

[CWSP-206 Exam Questions](#)