



CWSP-205^{Q&As}

Certified Wireless Security Professional

Pass CWNP CWSP-205 Exam with 100% Guarantee

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

<https://www.geekcert.com/cwsp-205.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

Which one of the following describes the correct hierarchy of 802.1X authentication key derivation?

- A. The MSK is generated from the 802.1X/EAP authentication. The PMK is derived from the MSK. The PTK is derived from the PMK, and the keys used for actual data encryption are a part of the PTK.
- B. If passphrase-based client authentication is used by the EAP type, the PMK is mapped directly from the user's passphrase. The PMK is then used during the 4-way handshake to create data encryption keys.
- C. After successful EAP authentication, the RADIUS server generates a PMK. A separate key, the MSK, is derived from the AAA key and is hashed with the PMK to create the PTK and GTK.
- D. The PMK is generated from a successful mutual EAP authentication. When mutual authentication is not used, an MSK is created. Either of these two keys may be used to derive the temporal data encryption keys during the 4-way handshake.

Correct Answer: A

QUESTION 2

Given: WLAN protocol analyzers can read and record many wireless frame parameters.

What parameter is needed to physically locate rogue APs with a protocol analyzer?

- A. SSID
- B. IP Address
- C. BSSID
- D. Signal strength
- E. RSN IE
- F. Noise floor

Correct Answer: D

QUESTION 3

In an effort to optimize WLAN performance, ABC Company has upgraded their WLAN infrastructure from 802.11a/g to 802.11n. 802.11a/g clients are still supported and are used throughout ABC's facility. ABC has always been highly security conscious, but due to budget limitations, they have not yet updated their overlay WIPS solution to 802.11n or 802.11ac.

Given ABC's deployment strategy, what security risks would not be detected by the 802.11a/g WIPS?

- A. Hijacking attack performed by using a rogue 802.11n AP against an 802.11a client
- B. Rogue AP operating in Greenfield 40 MHz-only mode



- C. 802.11a STA performing a deauthentication attack against 802.11n APs
- D. 802.11n client spoofing the MAC address of an authorized 802.11n client

Correct Answer: B

QUESTION 4

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

Correct Answer: B

QUESTION 5

Joe's new laptop is experiencing difficulty connecting to ABC Company's 802.11 WLAN using 802.1X/EAP PEAPv0. The company's wireless network administrator assured Joe that his laptop was authorized in the WIPS management console for connectivity to ABC's network before it was given to him. The WIPS termination policy includes alarms for rogue stations, rogue APs, DoS attacks and unauthorized roaming.

What is a likely reason that Joe cannot connect to the network?

- A. Joe disabled his laptop's integrated 802.11 radio and is using a personal PC card radio with a different chipset, drivers, and client utilities.
- B. Joe's integrated 802.11 radio is sending multiple Probe Request frames on each channel.
- C. An ASLEAP attack has been detected on APs to which Joe's laptop was trying to associate. The WIPS responded by disabling the APs.
- D. Joe configured his 802.11 radio card to transmit at 100 mW to increase his SNR. The WIPS is detecting this much output power as a DoS attack.

Correct Answer: A

[Latest CWSP-205 Dumps](#)

[CWSP-205 PDF Dumps](#)

[CWSP-205 Exam Questions](#)