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.passapply.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

What is a primary criteria for a network to qualify as a Robust Security Network (RSN)?

A. Token cards must be used for authentication.

B. Dynamic WEP-104 encryption must be enabled.

C. WEP may not be used for encryption.

D. WPA-Personal must be supported for authentication and encryption.

E. WLAN controllers and APs must not support SSHv1.

Correct Answer: C

QUESTION 3

What drawbacks initially prevented the widespread acceptance and use of Opportunistic Key Caching (OKC)?

A. Sharing cached keys between controllers during inter-controller roaming created vulnerabilities that exposed the keys to attackers.

B. Because OKC is not defined by any standards or certification body, client support was delayed and sporadic early on.

C. Key exchanges during fast roams required processor-intensive cryptography, which was prohibitive for legacy devices supporting only TKIP.

D. The Wi-Fi Alliance continually delayed the creation of a client certification for OKC, even though it was defined by IEEE 802.11r.

Correct Answer: B

QUESTION 4

While performing a manual scan of your environment using a spectrum analyzer on a laptop computer, you notice a signal in the real time FFT view. The signal is characterized by having peak power centered on channel 11 with an approximate width of 20 MHz at its peak. The signal widens to approximately 40 MHz after it has weakened by about 30 dB.

What kind of signal is displayed in the spectrum analyzer?

A. A frequency hopping device is being used as a signal jammer in 5 GHz

B. A low-power wideband RF attack is in progress in 2.4 GHz, causing significant 802.11 interference

C. An 802.11g AP operating normally in 2.4 GHz

D. An 802.11a AP operating normally in 5 GHz

Correct Answer: C

QUESTION 5

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