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 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

As the primary security engineer for a large corporate network, you have been asked to author a new security policy for the wireless network. While most client devices support 802.1X authentication, some legacy devices still only support passphrase/PSK-based security methods. When writing the 802.11 security policy, what password-related items should be addressed?

A. Certificates should always be recommended instead of passwords for 802.11 client authentication.

B. Password complexity should be maximized so that weak WEP IV attacks are prevented.

C. Static passwords should be changed on a regular basis to minimize the vulnerabilities of a PSK-based authentication.

D. EAP-TLS must be implemented in such scenarios.

E. MS-CHAPv2 passwords used with EAP/PEAPv0 should be stronger than typical WPA2-PSK passphrases.

Correct Answer: C

QUESTION 3

ABC Company is implementing a secure 802.11 WLAN at their headquarters (HQ) building in New York and at each of the 10 small, remote branch offices around the United States. 802.1X/EAP is ABC\\'s preferred security solution, where possible. All access points (at the HQ building and all branch offices) connect to a single WLAN controller located at HQ. Each branch office has only a single AP and minimal IT resources. What security best practices should be followed in this deployment scenario?

A. Remote management of the WLAN controller via Telnet, SSH, HTTP, and HTTPS should be prohibited across the WAN link.

B. RADIUS services should be provided at branch offices so that authentication server and suppliant credentials are not sent over the Internet.

C. An encrypted VPN should connect the WLAN controller and each remote controller-based AP, or each remote site should provide an encrypted VPN tunnel to HQ.

D. APs at HQ and at each branch office should not broadcast the same SSID; instead each branch should have a unique ID for user accounting purposes.

Correct Answer: C

QUESTION 4

While seeking the source of interference on channel 11 in your 802.11n WLAN running within 2.4 GHz, you notice a signal in the spectrum analyzer real time FFT display. The signal is characterized with the greatest strength utilizing only 1-2 megahertz of bandwidth and it does not use significantly more bandwidth until it has weakened by roughly 20 dB. At approximately -70 dB, it spreads across as much as 35 megahertz of bandwidth. What kind of signal is described?

A. A high-power ultra wideband (UWB) Bluetooth transmission.

B. A 2.4 GHz WLAN transmission using transmit beam forming.

C. A high-power, narrowband signal.

D. A deauthentication flood from a WIPS blocking an AP.

E. An HT-OFDM access point.

F. A frequency hopping wireless device in discovery mode.

Correct Answer: C

QUESTION 5

A WLAN consultant has just finished installing a WLAN controller with 15 controller-based APs. Two SSIDs with separate VLANs are configured for this network, and both VLANs are configured to use the same RADIUS server. The SSIDs are configured as follows:

SSID Blue – VLAN 10 – Lightweight EAP (LEAP) authentication – CCMP cipher suite SSID Red – VLAN 20 – PEAPv0/EAP-TLS authentication – TKIP cipher suite

The consultant\\'s computer can successfully authenticate and browse the Internet when using the Blue SSID. The same computer cannot authenticate when using the Red SSID. What is a possible cause of the problem?

A. The consultant does not have a valid Kerberos ID on the Blue VLAN.

B. The client does not have a proper certificate installed for the tunneled authentication within the established TLS tunnel.

C. The TKIP cipher suite is not a valid option for PEAPv0 authentication.

D. The Red VLAN does not use server certificate, but the client requires one.

Correct Answer: B