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.leads4pass.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

When used as part of a WLAN authentication solution, what is the role of LDAP?

A. A data retrieval protocol used by an authentication service such as RADIUS

B. An IEEE X.500 standard compliant database that participates in the 802.1X port-based access control process

C. A SQL compliant authentication service capable of dynamic key generation and distribution

D. A role-based access control protocol for filtering data to/from authenticated stations.

E. An Authentication Server (AS) that communicates directly with, and provides authentication for, the Supplicant.

Correct Answer: A

QUESTION 2

Given: XYZ Hospital plans to improve the security and performance of their Voice over Wi-Fi implementation and will be upgrading to 802.11n phones with 802.1X/EAP authentication. XYZ would like to support fast secure roaming for the phones and will require the ability to troubleshoot reassociations that are delayed or dropped during inter-channel roaming.

What portable solution would be recommended for XYZ to troubleshoot roaming problems?

A. WIPS sensor software installed on a laptop computer

B. Spectrum analyzer software installed on a laptop computer

C. An autonomous AP mounted on a mobile cart and configured to operate in monitor mode

D. Laptop-based protocol analyzer with multiple 802.11n adapters

Correct Answer: D

QUESTION 3

What statement accurately describes the functionality of the IEEE 802.1X standard?

A. Port-based access control with EAP encapsulation over the LAN (EAPoL)

B. Port-based access control with dynamic encryption key management and distribution

C. Port-based access control with support for authenticated-user VLANs only

D. Port-based access control with mandatory support of AES-CCMP encryption

E. Port-based access control, which allows three frame types to traverse the uncontrolled port: EAP, DHCP, and DNS.

Correct Answer: A

QUESTION 4

Given: ABC Company has 20 employees and only needs one access point to cover their entire facility. Ten of ABC Company\\'s employees have laptops with radio cards capable of only WPA security. The other ten employees have laptops with radio cards capable of WPA2 security. The network administrator wishes to secure all wireless communications (broadcast and unicast) for each laptop with its strongest supported security mechanism, but does not wish to implement a RADIUS/AAA server due to complexity.

What security implementation will allow the network administrator to achieve this goal?

A. Implement an SSID with WPA2-Personal that allows both AES-CCMP and TKIP clients to connect.

B. Implement an SSID with WPA-Personal that allows both AES-CCMP and TKIP clients to connect.

C. Implement two separate SSIDs on the AP--one for WPA-Personal using TKIP and one for WPA2Personal using AES-CCMP.

D. Implement an SSID with WPA2-Personal that sends all broadcast traffic using AES-CCMP and unicast traffic using either TKIP or AES-CCMP.

Correct Answer: C

QUESTION 5

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