Free Questions for CWSP-206 by actualtestdumps

Shared by Harrison on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

ABC Company has a WLAN controller using WPA2-Enterprise with PEAPv0/MS-CHAPv2 and AES-CCMP to secure their corporate wireless data. They wish to implement a guest WLAN for guest users to have Internet access, but want to implement some security controls. The security requirements for the hotspot include:

* Cannot access corporate network resources

* Network permissions are limited to Internet access

* All stations must be authenticated

What security controls would you suggest? (Choose the single best answer.)

Options:

A- Configure access control lists (ACLs) on the guest WLAN to control data types and destinations.

B- Require guest users to authenticate via a captive portal HTTPS login page and place the guest WLAN and the corporate WLAN on different VLANs.

C- Implement separate controllers for the corporate and guest WLANs.

D- Use a WIPS to deauthenticate guest users when their station tries to associate with the corporate WLAN.

E- Force all guest users to use a common VPN protocol to connect.

Answer:

B

Question 2

Question Type: MultipleChoice

In the basic 4-way handshake used in secure 802.11 networks, what is the purpose of the ANonce and SNonce?

Options:

A- They are added together and used as the GMK, from which the GTK is derived.

B- They are used to pad Message 1 and Message 2 so each frame contains the same number of bytes.

C- The IEEE 802.11 standard requires that all encrypted frames contain a nonce to serve as a Message Integrity Check (MIC).

D- They are input values used in the derivation of the Pairwise Transient Key.

Answer:

D

Question 3

Question Type: MultipleChoice

The IEEE 802.11 Pairwise Transient Key (PTK) is derived from what cryptographic element?

Options:

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)

Answer:

D

Question 4

Question Type: MultipleChoice

ABC Company is deploying an IEEE 802.11-compliant wireless security solution using 802.1X/EAP authentication. According to company policy, the security solution must prevent an eavesdropper from decrypting data frames traversing a wireless connection. What security characteristic and/or component plays a role in preventing data decryption?

Options:

A- 4-Way Handshake

B- PLCP Cyclic Redundancy Check (CRC)

C- Multi-factor authentication

D- Encrypted Passphrase Protocol (EPP)

E- Integrity Check Value (ICV)

Answer:

A

Question 5

Question Type: MultipleChoice

ABC Company has recently installed a WLAN controller and configured it to support WPA2-Enterprise security. The administrator has configured a security profile on the WLAN controller for each group within the company (Marketing, Sales, and Engineering). How are authenticated users assigned to groups so that they receive the correct security profile within the WLAN controller?

Options:

A- The RADIUS server sends the list of authenticated users and groups to the WLAN controller as part of a 4-Way Handshake prior to user authentication.

B- The WLAN controller polls the RADIUS server for a complete list of authenticated users and groups after each user authentication.

C- The RADIUS server sends a group name return list attribute to the WLAN controller during every successful user authentication.

D- The RADIUS server forwards the request for a group attribute to an LDAP database service, and LDAP sends the group attribute to the WLAN controller.

Answer:

C

Question 6

Question Type: MultipleChoice

ABC Company is an Internet Service Provider with thousands of customers. ABC's customers are given login credentials for network access when they become a customer. ABC uses an LDAP server as the central user credential database. ABC is extending their service to existing customers in some public access areas and would like to use their existing database for authentication. How can ABC Company use their existing user database for wireless user authentication as they implement a large-scale WPA2-Enterprise WLAN security solution?

Options:

A- Implement a RADIUS server and query user authentication requests through the LDAP server.

B- Mirror the LDAP server to a RADIUS database within a WLAN controller and perform daily backups to synchronize the user databases.

C- Import all users from the LDAP server into a RADIUS server with an LDAP-to-RADIUS conversion tool.

D- Implement an X.509 compliant Certificate Authority and enable SSL queries on the LDAP server.

Answer:

A

Question 7

Question Type: **MultipleChoice**

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?

Options:

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.

Answer:

C

Question 8

Question Type: MultipleChoice

A large enterprise is designing a secure, scalable, and manageable 802.11n WLAN that will support thousands of users. The enterprise will support both 802.1X/EAP-TTLS and PEAPv0/MSCHAPv2. Currently, the company is upgrading network servers as well and will replace their existing Microsoft IAS implementation with Microsoft NPS, querying Active Directory for user authentication. For this organization, as they update their WLAN infrastructure, what WLAN controller feature will likely be least valuable?

Options:

A- SNMPv3 support

B- 802.1Q VLAN trunking

C- Internal RADIUS server

D- WIPS support and integration

E- WPA2-Enterprise authentication/encryption

Answer:

C

Question 9

Question Type: MultipleChoice

Role-Based Access Control (RBAC) allows a WLAN administrator to perform what network function?

Options:

A- Provide two or more user groups connected to the same SSID with different levels of network privileges.

B- Allow access to specific files and applications based on the user's WMM access category.

C- Allow simultaneous support for multiple EAP types on a single access point.

D- Minimize traffic load on an AP by requiring mandatory admission control for use of the Voice access category.

Answer:

A

Question 10

Question Type: MultipleChoice

XYZ Company has recently installed a controller-based WLAN and is using a RADIUS server to query authentication requests to an LDAP server. XYZ maintains user-based access policies and would like to use the RADIUS server to facilitate network authorization.

What RADIUS feature could be used by XYZ to assign the proper network permissions to users during authentications?

Options:

A- RADIUS can reassign a client's 802.11 association to a new SSID by referencing a username-to-SSID mapping table in the LDAP user database.

B- The RADIUS server can support vendor-specific attributes in the ACCESS-ACCEPT response, which can be used for user policy assignment.

C- The RADIUS server can communicate with the DHCP server to issue the appropriate IP address and VLAN assignment to users.

D- RADIUS can send a DO-NOT-AUTHORIZE demand to the authenticator to prevent the STA from gaining access to specific files, but may only employ this in relation to Linux servers.

Answer:

B

Question 11

Question Type: MultipleChoice

What protocol, listed here, allows a network manager to securely administer the network?

Options:

A- TFTP

B- Telnet

C- HTTPS

D- SNMPv2

Answer:

C