BrainDumps Collection

Free Questions for CWSP-206 by braindumpscollection

Shared by Cobb on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

When using a tunneled EAP type, such as PEAP, what component is protected inside the TLS tunnel so that it is not sent in clear text across the wireless medium?

Options:

A- Server credentials

B- User credentials

C- RADIUS shared secret

D- X.509 certificates

Answer:

B

Question 2

Question Type: **MultipleChoice**

In an IEEE 802.11-compliant WLAN, when is the 802.1X Controlled Port placed into the unblocked state?

Options:

A- After EAP authentication is successful

B- After Open System authentication

C- After the 4-Way Handshake

D- After any Group Handshake

Answer:

A

Question 3

Question Type: **MultipleChoice**

Your network implements an 802.1X/EAP-based wireless security solution. A WLAN controller is installed and manages seven APs. FreeRADIUS is used for the RADIUS server and is installed on a dedicated server named SRV21. One example client is a MacBook Pro with 8 GB RAM. What device functions as the 802.1X/EAP Authenticator?

Options:

A- WLAN Controller/AP

B- MacBook Pro

C- SRV21

D- RADIUS server

Answer:

A

Question 4

Question Type: MultipleChoice

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:

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?

Options:

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.

Answer:

B

Question 5

Question Type: **MultipleChoice**

Your organization is using EAP as an authentication framework with a specific type that meets the requirements of your corporate policies. Which one of the following statements is true related to this implementation?

Options:

A- The client STAs may communicate over the controlled port in order to authenticate as soon as the Open System authentication completes.

B- The client STAs may communicate over the uncontrolled port in order to authenticate as soon as the Open System authentication completes.

C- The client STAs may use a different, but complementary, EAP type than the AP STAs.

D- The client will be the authenticator in this scenario.

Answer:

B

Question 6

Question Type: **MultipleChoice**

Which of the following is a valid reason to avoid the use of EAP-MD5 in production WLANs?

Options:

A- It does not support a RADIUS server.

B- It is not a valid EAP type.

C- It does not support mutual authentication.

D- It does not support the outer identity.

Answer:

C

Question 7

Question Type: MultipleChoice

What TKIP feature was introduced to counter the weak integrity check algorithm used in WEP?

Options:

A- RC5 stream cipher

B- Block cipher support

C- Sequence counters

D- 32-bit ICV (CRC-32)

E- Michael

Answer:

E

Question 8

Question Type: **MultipleChoice**

Which one of the following is not a role defined in the 802.1X authentication procedures used in 802.11 and 802.3 networks for port-based authentication?

Options:

A- AAA Server

B- Authentication Server

C- Supplicant

D- Authenticator

Answer:

A

Question 9

Question Type: MultipleChoice

Fred works primarily from home and public wireless hotspots rather than commuting to office. He frequently accesses the office network remotely from his Mac laptop using the local 802.11 WLAN. In this remote scenario, what single wireless security practice will provide the greatest security for Fred?

Options:

A- Use enterprise WIPS on the corporate office network.

B- Use 802.1X/PEAPv0 to connect to the corporate office network from public hotspots.

C- Use secure protocols, such as FTP, for remote file transfers.

D- Use an IPSec VPN for connectivity to the office network.

E- Use only HTTPS when agreeing to acceptable use terms on public networks.

F- Use WIPS sensor software on the laptop to monitor for risks and attacks.

Answer:

D

Question 10

Question Type: MultipleChoice

You are installing 6 APs on the outside of your facility. They will be mounted at a height of 6 feet. What must you do to implement these APs in a secure manner beyond the normal indoor AP implementations? (Choose the single best answer.)

Options:

A- Ensure proper physical and environmental security using outdoor ruggedized APs or enclosures.

B- Use internal antennas.

C- Use external antennas.

D- Power the APs using PoE.

Answer:

A

20%
DISCOUNT