Free Questions for CWSP-207

Shared by Stafford on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

You must support a TSN as you have older wireless equipment that will not support the required processing of AES encryption. Which one of the following technologies will you use on the network so that a TSN can be implemented that would not be required in a network compliant with 802.11-2012 non-deprecated technologies?

Options:

A- WEP

B- RC4

C- CCMP

D- WPA2

Topic 4, Security Lifecycle Management

Answer:

B

Question 2

Question Type: MultipleChoice

Given: The Marketing department's WLAN users need to reach their file and email server as well as the Internet, but should not have access to any other network resources.

What single WLAN security feature should be implemented to comply with these requirements?

Options:

A- Mutual authentication

B- Captive portal

C- Role-based access control

D- Group authentication

E- RADIUS policy accounting

Answer:

C

Question 3

Question Type: MultipleChoice

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?

Options:

A- A high-power, narrowband signal

B- A 2.4 GHz WLAN transmission using transmit beam forming

C- An HT-OFDM access point

D- A frequency hopping wireless device in discovery mode

E- A deauthentication flood from a WIPS blocking an AP

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

Answer:

A

Question 4

Question Type: **MultipleChoice**

Given: Many corporations configure guest VLANs on their WLAN controllers that allow visitors to have Internet access only. The guest traffic is tunneled to the DMZ to prevent some security risks.

In this deployment, what risks are still associated with implementing the guest VLAN without any advanced traffic monitoring or filtering features enabled? (Choose 2)

Options:

A- Intruders can send spam to the Internet through the guest VLAN.

B- Peer-to-peer attacks can still be conducted between guest users unless application-layer monitoring and filtering are implemented.

C- Unauthorized users can perform Internet-based network attacks through the WLAN.

D- Guest users can reconfigure AP radios servicing the guest VLAN unless unsecure network management protocols (e.g. Telnet, HTTP) are blocked.

E- Once guest users are associated to the WLAN, they can capture 802.11 frames from the corporate VLANs.

Answer:

A, C

Question 5

Question Type: MultipleChoice

You are using a utility that takes input and generates random output. For example, you can provide the input of a known word as a secret word and then also provide another known word as salt input. When you process the input it generates a secret code which is a combination of letters and numbers with case sensitivity. For what is the described utility used? (Choose 3)

Options:

A- Generating passwords for WLAN infrastructure equipment logins

B- Generating PMKs that can be imported into 802.11 RSN-compatible devices

C- Generating secret keys for RADIUS servers and WLAN infrastructure devices

D- Generating passphrases for WLAN systems secured with WPA2-Personal

E- Generating dynamic session keys used for IPSec VPNs

Answer:

A, C, D

Question 6

Question Type: **MultipleChoice**

Given: You support a coffee shop and have recently installed a free 802.11ac wireless hot-spot for the benefit of your customers. You want to minimize legal risk in the event that the hot-spot is used for illegal Internet activity.

What option specifies the best approach to minimize legal risk at this public hot-spot while maintaining an open venue for customer Internet access?

Options:

A- Configure WPA2-Enterprise security on the access point

B- Block TCP port 25 and 80 outbound on the Internet router

C- Require client STAs to have updated firewall and antivirus software

D- Allow only trusted patrons to use the WLAN

E- Use a WIPS to monitor all traffic and deauthenticate malicious stations

F- Implement a captive portal with an acceptable use disclaimer

Answer:

F

Question 7

Question Type: **MultipleChoice**

Given: Your company has just completed installation of an IEEE 802.11 WLAN controller with 20 controller-based APs. The CSO has specified PEAPv0/EAP-MSCHAPv2 as the only authorized WLAN authentication mechanism. Since an LDAP-compliant user database was already in use, a RADIUS server was installed and is querying authentication requests to the LDAP server.

Where must the X.509 server certificate and private key be installed in this network?

Options:

A- Supplicant devices

B- LDAP server

C- Controller-based APs

D- WLAN controller

E- RADIUS server

Answer:

E

Question 8

Question Type: MultipleChoice

The IEEE 802.11 standard defined Open System authentication as consisting of two auth frames and two assoc frames. In a WPA2-Enterprise network, what process immediately follows the 802.11 association procedure?

Options:

A- Group Key Handshake

B- 802.1X/EAP authentication

C- DHCP Discovery

D- 4-Way Handshake

E- Passphrase-to-PSK mapping

F- RADIUS shared secret lookup

Answer:

B

Question 9

Question Type: MultipleChoice

Given: ABC Company has a WLAN controller using WPA2-Enterprise with PEAPv0/MS-CHAPv2 and AES-CCMP to secure their corporate wireless dat

a. 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 hot-spot 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- Implement separate controllers for the corporate and guest WLANs.

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

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

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

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

Answer:

D

20%
DISCOUNT