Free Questions for CWSP-206 by certscare

Shared by Silva on 24-05-2024

For More Free Questions and Preparation Resources

Question 1

You must implement 7 APs for a branch office location in your organizations. All APs will be autonomous and provide the same two SSIDs (CORP1879 and Guest).

Because each AP is managed directly through a web-based interface, what must be changed on every AP before enabling the WLANs to ensure proper staging procedures are followed?

Options:

A- Output power

B- Fragmentation threshold

C- Administrative password

D- Cell radius

Answer:

C

Question 2

What EAP type supports using MS-CHAPv2, EAP-GTC or EAP-TLS for wireless client authentication?

Options:

A- EAP-GTC

B- PEAP

C- EAP-TTLS

D- LEAP

E- H-REAP

Answer:

B

Question 3

What policy would help mitigate the impact of peer-to-peer attacks against wireless-enabled corporate laptop computers when the laptops are also used on public access networks such as wireless hotspots?

Options:

A- Require Port Address Translation (PAT) on each laptop.

B- Require secure applications such as POP, HTTP, and SSH.

C- Require VPN software for connectivity to the corporate network.

D- Require WPA2-Enterprise as the minimal WLAN security solution.

Answer:

C

Question 4

Question Type: MultipleChoice

ABC Hospital wishes to create a strong security policy as a first step in securing their 802.11 WLAN. Before creating the WLAN security policy, what should you ensure you possess?

Question 5

Question Type: MultipleChoice

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?

Options:

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.

Answer:

C

Question 6

Question Type: MultipleChoice

In a security penetration exercise, a WLAN consultant obtains the WEP key of XYZ Corporation's wireless network. Demonstrating the vulnerabilities of using WEP, the consultant uses a laptop running a software AP in an attempt to hijack the authorized user's connections. XYZ's legacy network is using 802.11n APs with 802.11b, 11g, and 11n client devices. With this setup, how can the consultant cause all of the authorized clients to establish Layer 2 connectivity with the software access point?

Options:

A- When the RF signal between the clients and the authorized AP is temporarily disrupted and the consultant's software AP is using the same SSID on a different channel than the authorized AP, the clients will reassociate to the software AP.

B- If the consultant's software AP broadcasts Beacon frames that advertise 802.11g data rates that are faster rates than XYZ's current 802.11b data rates, all WLAN clients will reassociate to the faster AP.

C- A higher SSID priority value configured in the Beacon frames of the consultant's software AP will take priority over the SSID in the authorized AP, causing the clients to reassociate.

D- All WLAN clients will reassociate to the consultant's software AP if the consultant's software AP provides the same SSID on any channel with a 10 dB SNR improvement over the authorized AP.

Answer:

A

Question 7

Question Type: **MultipleChoice**

You perform a protocol capture using Wireshark and a compatible 802.11 adapter in Linux. When viewing the capture, you see an auth req frame and an auth rsp frame. Then you see an assoc req frame and an assoc rsp frame. Shortly after, you see DHCP communications and then ISAKMP protocol packets. What security solution is represented?

Options:

A- 802.1X/EAP-TTLS

B- WPA2-Personal with AES-CCMP

C- 802.1X/PEAPv0/MS-CHAPv2

D- EAP-MD5

E- Open 802.11 authentication with IPSec

Answer:

E

Question 8

Question Type: MultipleChoice

ABC Corporation is evaluating the security solution for their existing WLAN. Two of their supported solutions include a PPTP VPN and 802.1X/LEAP. They have used PPTP VPNs because of their wide support in server and desktop operating systems. While both PPTP and LEAP adhere to the minimum requirements of the corporate security policy, some individuals have raised concerns about MS-CHAPv2 (and similar) authentication and the known fact that MS-CHAPv2 has proven vulnerable in improper implementations. As a consultant, what do you tell ABC Corporation about implementing MS-CHAPv2 authentication?

Options:

A- MS-CHAPv2 is only appropriate for WLAN security when used inside a TLS-encrypted tunnel.

B- When implemented with AES-CCMP encryption, MS-CHAPv2 is very secure.

C- MS-CHAPv2 uses AES authentication, and is therefore secure.

D- MS-CHAPv2 is compliant with WPA-Personal, but not WPA2-Enterprise.

E- LEAP's use of MS-CHAPv2 is only secure when combined with WEP.

Answer:

A