CWSP-206 Q&As

CWSP Certified Wireless Security Professional

Pass CWNP CWSP-206 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/cwsp-206.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

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 risk is still associated with implementing the guest VLAN without any advanced traffic monitoring or filtering feature enabled?

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

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

Correct Answer: A

QUESTION 2

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?

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.

Correct Answer: B

QUESTION 3

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?

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.

Correct Answer: A

QUESTION 4

In order to acquire credentials of a valid user on a public hotspot network, what attacks may be conducted? Choose the single completely correct answer.

A. MAC denial of service and/or physical theft

B. Social engineering and/or eavesdropping

C. Authentication cracking and/or RF DoS

D. Code injection and/or XSS

E. RF DoS and/or physical theft

Correct Answer: B

QUESTION 5

You manage a wireless network that services 200 wireless users. Your facility requires 20 access points, and you have installed an IEEE 802.11-compliant implementation of 802.1X/LEAP with AES-CCMP as an authentication and encryption solution. In this configuration, the wireless network is initially susceptible to what type of attack?

A. Offline dictionary attacks

B. Application eavesdropping

C. Session hijacking

D. Layer 3 peer-to-peer

E. Encryption cracking

Correct Answer: A