www.CERTBUS.com

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.certbus.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

SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

What software and hardware tools are used in the process performed to hijack a wireless station from the authorized wireless network onto an unauthorized wireless network?

A. A low-gain patch antenna and terminal emulation software

B. MAC spoofing software and MAC DoS software

C. RF jamming device and a wireless radio card

D. A wireless workgroup bridge and a protocol analyzer

Correct Answer: C

QUESTION 2

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?

A. Controller-based APs

B. WLAN controller

C. RADIUS server

D. Supplicant devices

E. LDAP server

Correct Answer: C

QUESTION 3

What field in the RSN information element (IE) will indicate whether PSK- or Enterprise-based WPA or WPA2 is in use?

A. Group Cipher Suite

B. Pairwise Cipher Suite List

C. AKM Suite List

D. RSN Capabilities

Correct Answer: C

QUESTION 4

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?

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.

Correct Answer: C

QUESTION 5

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 6

A network security auditor is preparing to perform a comprehensive assessment of an 802.11ac network\\'s security. What task should be performed at the beginning of the audit to maximize the auditor\\'s ability to expose network vulnerabilities?

A. Identify the IP subnet information for each network segment.

B. Identify the manufacturer of the wireless infrastructure hardware.

C. Identify the skill level of the wireless network security administrator(s).

D. Identify the manufacturer of the wireless intrusion prevention system.

E. Identify the wireless security solution(s) currently in use.

Correct Answer: E

QUESTION 7

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

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.

Correct Answer: D

QUESTION 8

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?

A. Output power

B. Fragmentation threshold

C. Administrative password

D. Cell radius

Correct Answer: C

QUESTION 9

During 802.1X/LEAP authentication, the username is passed across the wireless medium in clear text. From a security perspective, why is this significant?

A. The username can be looked up in a dictionary file that lists common username/password combinations.

B. The username is needed for Personal Access Credential (PAC) and X.509 certificate validation.

C. 4-Way Handshake nonces are based on the username in WPA and WPA2 authentication.

D. The username is an input to the LEAP challenge/response hash that is exploited, so the username must be known to conduct authentication cracking.

Correct Answer: D

QUESTION 10

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

A. TFTP

B. Telnet

C. HTTPS

D. SNMPv2

Correct Answer: C

CWSP-206 VCE Dumps   CWSP-206 Study Guide   CWSP-206 Braindumps