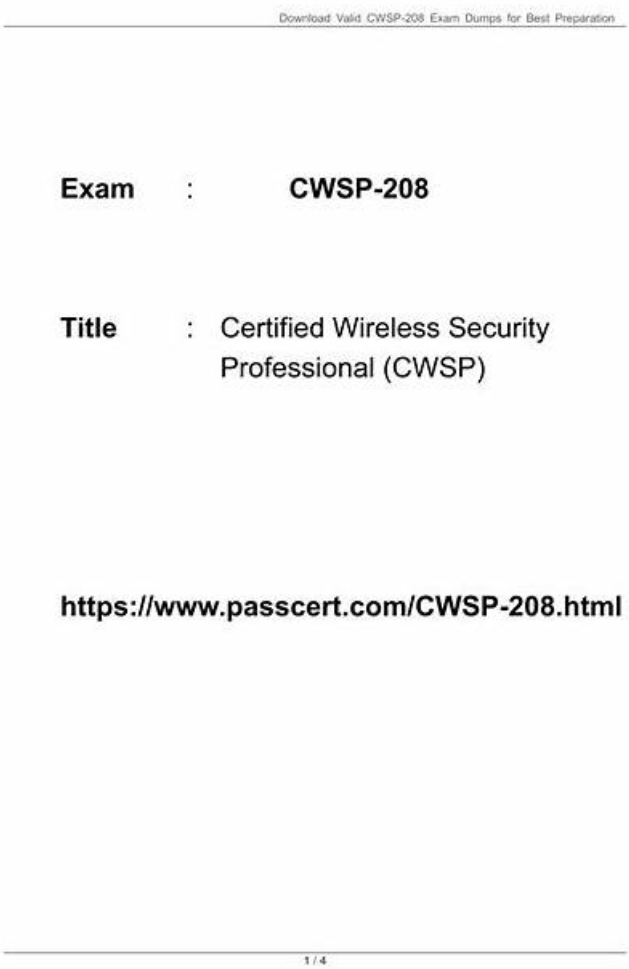
CWSP-208 Reliable Exam Preparation & CWSP-208 New Study Guide



BTW, DOWNLOAD part of ExamDumpsVCE CWSP-208 dumps from Cloud Storage: https://drive.google.com/open?id=1j6E3P88WbhVBT5chAzjpbpIQYTJQI-qx

We have always taken care to provide our customers with the very best. So we provide numerous benefits along with our Certified Wireless Security Professional (CWSP) exam study material. We provide our customers with the demo version of the CWNP CWSP-208 Exam Questions to eradicate any doubts that may be in your mind regarding the validity and accuracy. You can test the product before you buy it.

If you have ExamDumpsVCE's CWNP CWSP-208 exam training materials, we will provide you with one-year free update. This means that you can always get the latest exam information. As long as the Exam Objectives have changed, or our learning material changes, we will update for you in the first time. We know your needs, and we will help you gain confidence to pass the CWNP CWSP-208 Exam. You can be confident to take the exam and pass the exam.

>> CWSP-208 Reliable Exam Preparation <<

Get Real CWNP CWSP-208 Exam Questions By [ExamDumpsVCE]

CWSP-208 questions and answers are written to the highest standards of technical accuracy by our professional experts. With our CWSP-208 free demo, you can check out the questions quality, validity of our CWNP practice torrent before you choose to buy it.

You just need 20-30 hours to study with our CWSP-208 practice dumps, and you can attend the actual test and successfully pass. The CWSP-208 vce torrent will be the best and valuable study tool for your preparation.

CWNP CWSP-208 Exam Syllabus Topics:

Topic	Details
Topic 1	• Security Policy: This section of the exam measures the skills of a Wireless Security Analyst and covers how WLAN security requirements are defined and aligned with organizational needs. It emphasizes evaluating regulatory and technical policies, involving stakeholders, and reviewing infrastructure and client devices. It also assesses how well high-level security policies are written, approved, and maintained throughout their lifecycle, including training initiatives to ensure ongoing stakeholder awareness and compliance.
Topic 2	• WLAN Security Design and Architecture: This part of the exam focuses on the abilities of a Wireless Security Analyst in selecting and deploying appropriate WLAN security solutions in line with established policies. It includes implementing authentication mechanisms like WPA2, WPA3, 802.1X • EAP, and guest access strategies, as well as choosing the right encryption methods, such as AES or VPNs. The section further assesses knowledge of wireless monitoring systems, understanding of AKM processes, and the ability to set up wired security systems like VLANs, firewalls, and ACLs to support wireless infrastructures. Candidates are also tested on their ability to manage secure client onboarding, configure NAC, and implement roaming technologies such as 802.11r. The domain finishes by evaluating practices for protecting public networks, avoiding common configuration errors, and mitigating risks tied to weak security protocols.
Topic 3	• Vulnerabilities, Threats, and Attacks: This section of the exam evaluates a Network Infrastructure Engineer in identifying and mitigating vulnerabilities and threats within WLAN systems. Candidates are expected to use reliable information sources like CVE databases to assess risks, apply remediations, and implement quarantine protocols. The domain also focuses on detecting and responding to attacks such as eavesdropping and phishing. It includes penetration testing, log analysis, and using monitoring tools like SIEM systems or WIPS • WIDS. Additionally, it covers risk analysis procedures, including asset management, risk ratings, and loss calculations to support the development of informed risk management plans.
Topic 4	• Security Lifecycle Management: This section of the exam assesses the performance of a Network Infrastructure Engineer in overseeing the full security lifecycle—from identifying new technologies to ongoing monitoring and auditing. It examines the ability to assess risks associated with new WLAN implementations, apply suitable protections, and perform compliance checks using tools like SIEM. Candidates must also demonstrate effective change management, maintenance strategies, and the use of audit tools to detect vulnerabilities and generate insightful security reports. The evaluation includes tasks such as conducting user interviews, reviewing access controls, performing scans, and reporting findings in alignment with organizational objectives.

CWNP Certified Wireless Security Professional (CWSP) Sample Questions (Q112-Q117):

NEW QUESTION # 112
Given: ABC Company is implementing a secure 802.11 WLAN at their headquarters (HQ) building in New York and at each of the 10 small, remote branch offices around the United States. 802.1X/EAP is ABC's preferred security solution, where possible. All access points (at the HQ building and all branch offices) connect to a single WLAN controller located at HQ. Each branch office has only a single AP and minimal IT resources.
What security best practices should be followed in this deployment scenario?

- A. An encrypted VPN should connect the WLAN controller and each remote controller-based AP, or each remote site should provide an encrypted VPN tunnel to HQ.
- B. Remote management of the WLAN controller via Telnet, SSH, HTTP, and HTTPS should be prohibited across the WAN link.
- C. APs at HQ and at each branch office should not broadcast the same SSID; instead each branch should have a unique ID

for user accounting purposes.
- D. RADIUS services should be provided at branch offices so that authentication server and supplicant credentials are not sent over the Internet.

Answer: A

Explanation:
Because all APs (even those at branch offices) connect to a central controller:
Their control/data traffic must traverse the public internet or WAN.
VPNs (IPSec, GRE, or similar) ensure confidentiality and integrity of authentication traffic and user data over insecure links.
Incorrect:
B). Using different SSIDs complicates management and user experience unnecessarily.
C). Remote RADIUS at small branches contradicts the goal of centralized management.
D). Remote access protocols (SSH, HTTPS) should be secured, not entirely prohibited, to allow remote management.
References:
CWSP-208 Study Guide, Chapter 6 (Remote AP Security)
CWNP Controller-Based Architecture Deployment Guide

NEW QUESTION # 113
Wireless Intrusion Prevention Systems (WIPS) are used for what purposes? (Choose 3)

- A. Security monitoring and notification
- B. Classifying wired client devices
- C. Enforcing wireless network security policy
- D. Detecting and defending against eavesdropping attacks
- E. Performance monitoring and troubleshooting
- F. Preventing physical carrier sense attacks

Answer: A,C,E

Explanation:
WIPS provides multiple functionalities:
B). Policy enforcement - detects and responds to wireless threats such as rogue APs and misconfigurations.
D). Security monitoring - alerts staff when threats like deauth attacks or malware-hosting APs are detected.
A). Performance monitoring - supports diagnostics by capturing information on channel conditions, interference, and device behavior.
Incorrect options:
C). Detecting eavesdropping isn't feasible-passive listening cannot be identified by sensors.
E). Carrier sense DoS and F. Wired device classification are outside WIPS's scope.
References:
CWSP#207 Study Guide, Chapters 5-6 (WIPS Capabilities)

NEW QUESTION # 114
Given: ABC Corporation's 802.11 WLAN is comprised of a redundant WLAN controller pair (N+1) and 30 access points implemented in 2004. ABC implemented WEP encryption with IPSec VPN technology to secure their wireless communication because it was the strongest security solution available at the time it was implemented. IT management has decided to upgrade the WLAN infrastructure and implement Voice over Wi-Fi and is concerned with security because most Voice over Wi-Fi phones do not support IPSec.
As the wireless network administrator, what new security solution would be best for protecting ABC's data?

- A. Migrate corporate data and Voice over Wi-Fi devices to WPA2-Enterprise with fast secure roaming support, and segment Voice over Wi-Fi data on a separate VLAN.
- B. Migrate to a multi-factor security solution to replace IPSec; use WEP with MAC filtering, SSID hiding, stateful packet inspection, and VLAN segmentation.
- C. Migrate corporate data clients to WPA-Enterprise and segment Voice over Wi-Fi phones by assigning them to a different frequency band.
- D. Migrate all 802.11 data devices to WPA-Personal, and implement a secure DHCP server to allocate addresses from a segmented subnet for the Voice over Wi-Fi phones.

Answer: A

Explanation:
Comprehensive Detailed Explanation:
To support real-time applications like Voice over Wi-Fi:
WPA2-Enterprise ensures robust security using 802.1X and AES-CCMP.
Fast secure roaming (802.11r) is essential to maintain voice session quality.
VLAN segmentation improves network performance and security between voice and data devices.
Incorrect:
A). WPA-Enterprise is less secure than WPA2, and frequency band segmentation doesn't address QoS and security together.
C). WEP is deprecated and insecure even with added measures.
D). WPA-Personal lacks centralized authentication and doesn't support enterprise-grade security or fast roaming.
References:
CWSP-208 Study Guide, Chapter 6 (Voice WLAN Security)
CWNP Guide to Secure WLAN Design

NEW QUESTION # 115
In the basic 4-way handshake used in secure 802.11 networks, what is the purpose of the ANonce and SNonce? (Choose 2)

- A. The IEEE 802.11 standard requires that all encrypted frames contain a nonce to serve as a Message Integrity Check (MIC).
- B. They are added together and used as the GMK, from which the GTK is derived.
- C. They are input values used in the derivation of the Pairwise Transient Key.
- D. They allow the participating STAs to create dynamic keys while avoiding sending unicast encryption keys across the wireless medium.
- E. They are used to pad Message 1 and Message 2 so each frame contains the same number of bytes.

Answer: C,D

Explanation:
In the 802.11 4-Way Handshake:
D: The ANonce (from the AP) and SNonce (from the STA) are critical entropy values used along with the PMK, MAC addresses, etc., to derive the PTK securely.
E: This process ensures both parties derive the same PTK without ever transmitting the key over the air, mitigating interception risk.
Incorrect:
A). Nonces are not padding bytes.
B). Nonces are not the MIC; MIC is a separate integrity mechanism.
C). GMK and GTK are for group keys, not derived from nonces.
References:
CWSP-208 Study Guide, Chapter 3 (4-Way Handshake Mechanics)
IEEE 802.11i Specification

NEW QUESTION # 116
Given: ABC Company has a WLAN controller using WPA2-Enterprise with PEAPv0/MS-CHAPv2 and AES- CCMP to secure their corporate wireless data. 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.)

- 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. Require guest users to authenticate via a captive portal HTTPS login page and place the guest WLAN and the corporate WLAN on different VLANs.
- D. Configure access control lists (ACLs) on the guest WLAN to control data types and destinations.
- E. Force all guest users to use a common VPN protocol to connect.

Answer: C

Explanation:
This solution meets all the requirements:
Captive portals allow simple authentication for guest users.
VLAN separation enforces network segmentation.
HTTPS ensures authentication is encrypted.
Incorrect:
A). Separate controllers are unnecessary and costly.
B). WIPS enforcement is reactive, not proactive for normal access control.
C). ACLs alone don't enforce authentication.
E). VPN requirements would be overly complex for guests.
References:
CWSP-208 Study Guide, Chapter 6 (Guest Network Architecture & Captive Portal Authentication)

NEW QUESTION # 117
.....

id=1j6E3P88WbhVBT5chAzjpbpIQYTJQI-qx