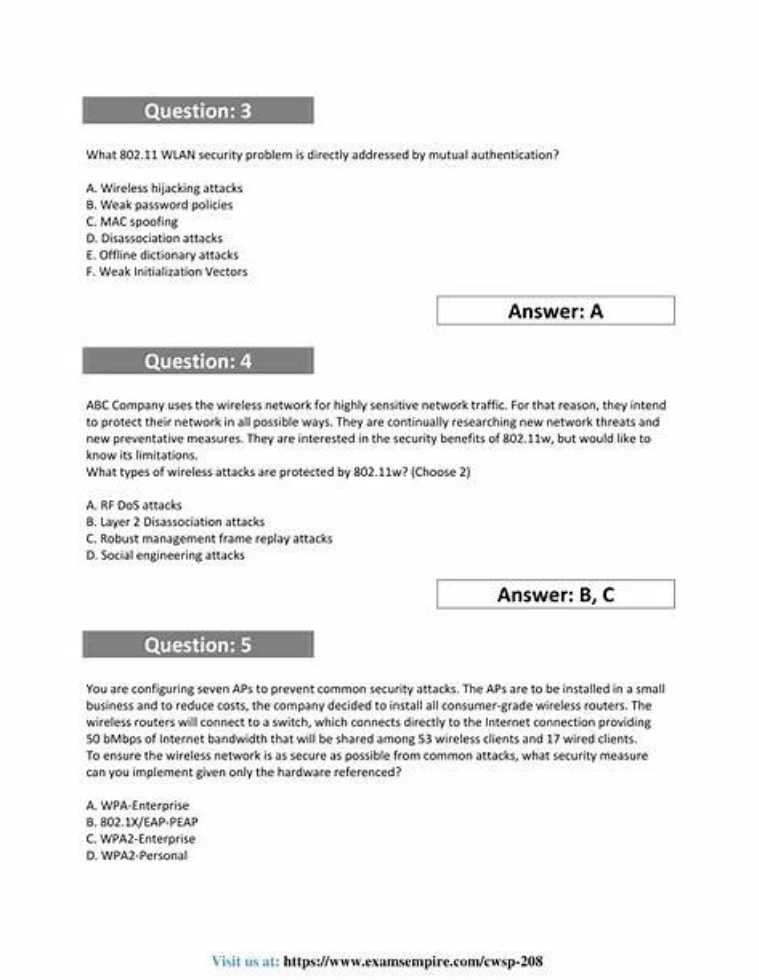
New CWSP-208 Test Format - CWSP-208 Valid Dumps



BTW, DOWNLOAD part of DumpsValid CWSP-208 dumps from Cloud Storage: https://drive.google.com/open?id=1s1BEf-be4Js_-eRz8hjDokDSM25b0QbB

Besides CWNP CWSP-208 exam is popular, Cisco, IBM, HP and so on are also accepted by many people. If you want to get CWSP-208 certificate, DumpsValid dumps can help you to realize your dream. Not having confidence to pass the exam, you give up taking the exam. You can absolutely achieve your goal by DumpsValid test dumps. After you obtain CWSP-208 certificate, you can also attend other certification exams in IT industry. DumpsValid questions and answers are at your hand, all exams are not a problem.

CWNP CWSP-208 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• 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.
Topic 4	• 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.

Free PDF 2026 CWNP Latest New CWSP-208 Test Format

So for this reason, our CWNP CWSP-208 are very similar to the actual exam. With a vast knowledge in this field, DumpsValid always tries to provide candidates with the actual questions so that when they appear in their real CWNP CWSP-208 Exam they do not feel any difference. The Desktop CWNP CWSP-208 Practice Exam Software of DumpsValid arranges a mock exam for the one who wants to evaluate and improve preparation.

CWNP Certified Wireless Security Professional (CWSP) Sample Questions (Q109-Q114):

NEW QUESTION # 109
Given: John Smith uses a coffee shop's Internet hot-spot (no authentication or encryption) to transfer funds between his checking and savings accounts at his bank's website. The bank's website uses the HTTPS protocol to protect sensitive account information. While John was using the hot-spot, a hacker was able to obtain John's bank account user ID and password and exploit this information. What likely scenario could have allowed the hacker to obtain John's bank account user ID and password?

- A. John's bank is using an expired X.509 certificate on their web server. The certificate is on John's Certificate Revocation List (CRL), causing the user ID and password to be sent unencrypted.
- B. The bank's web server is using an X.509 certificate that is not signed by a root CA, causing the user ID and password to be sent unencrypted.
- C. John uses the same username and password for banking that he does for email. John used a POP3 email client at the wireless hot-spot to check his email, and the user ID and password were not encrypted.
- D. John accessed his corporate network with his IPSec VPN software at the wireless hot-spot. An IPSec VPN only encrypts data, so the user ID and password were sent in clear text. John uses the same username and password for banking that he does for his IPSec VPN software.
- E. Before connecting to the bank's website, John's association to the AP was hijacked. The attacker intercepted the HTTPS public encryption key from the bank's web server and has decrypted John's login credentials in near real-time.

Answer: C

Explanation:

In this scenario, although the bank's website uses HTTPS (which encrypts communications between John's browser and the bank's server), the compromise did not occur during the banking session itself. Instead, the attacker exploited a common security mistake: credential reuse.
John reused his email credentials for his bank login, and he accessed his email using a POP3 client without encryption at a public hotspot. This means his username and password were sent in cleartext, which is trivially easy to sniff on an open wireless network. Once an attacker obtained those credentials, they could use them to log into his bank account if the same credentials were used there.
Here's how this aligns with CWSP knowledge domains:
* CWSP Security Threats & Attacks: This is a classic example of credential harvesting via cleartext protocols (POP3), and password reuse, both of which are significant risks in WLAN environments.
* CWSP Secure Network Design: Recommends use of encrypted protocols (e.g., POP3S or IMAPS) and user education against password reuse.
* CWSP WLAN Security Fundamentals: Emphasizes that open Wi-Fi networks offer no encryption by default, leaving unprotected protocols vulnerable to sniffing and interception.
Other answer options and why they are incorrect:
* A & D are invalid because an expired or unsigned certificate may cause browser warnings but won't result in sending credentials unencrypted unless the user bypasses HTTPS (which wasn't stated).
* C is incorrect: IPSec VPNs encrypt all data between the client and VPN endpoint-including credentials.
* E is technically incorrect and misleading: intercepting the public key of an HTTPS session doesn't allow decryption of the credentials due to asymmetric encryption and session key security. Real-time decryption of HTTPS traffic without endpoint compromise is not feasible.
References:
CWSP-208 Study Guide, Chapters 3 (Security Policy) and 5 (Threats and Attacks) CWNP CWSP-208 Official Study Guide CWNP Exam Objectives - WLAN Authentication, Encryption, and VPNs CWNP Whitepapers on WLAN Security Practices

NEW QUESTION # 110
Wireless Intrusion Prevention Systems (WIPS) are used for what purposes? (Choose 3)

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

Answer: A,C,D

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 # 111
A single AP is configured with three separate WLAN profiles, as follows:
1. SSID: ABCData - BSSID: 00:11:22:00:1F:C3 - VLAN 10 - Security: PEAPv0/EAP-MSCHAPv2 with AES-CCMP - 3 current clients
2. SSID: ABCVoice - BSSID: 00:11:22:00:1F:C4 - VLAN 60 - Security: WPA2-Personal with AES-CCMP - 2 current clients
3. SSID: Guest - BSSID: 00:11:22:00:1F:C5 - VLAN 90 - Security: Open with captive portal authentication - 3 current clients
Three STAs are connected to ABCData. Three STAs are connected to Guest. Two STAs are connected to ABCVoice.

How many unique GTKs and PTKs are currently in place in this scenario?

- A. 2 GTKs - 8 PTKs
- B. 2 GTKs - 5 PTKs
- C. 1 GTK - 8 PTKs
- D. 3 GTKs - 8 PTKs

Answer: D

Explanation:
PTK (Pairwise Transient Key) is established per-client, so:
ABCData: 3 clients = 3 PTKs
ABCVoice: 2 clients = 2 PTKs
Guest: 3 clients = 3 PTKs
Total: 8 PTKs
GTK (Group Temporal Key) is shared per SSID, so:
One GTK per SSID (ABCData, ABCVoice, Guest)
Total: 3 GTKs
References:
CWSP-208 Study Guide, Chapter 3 (Key Hierarchy)
IEEE 802.11 Key Management Architecture

NEW QUESTION # 112
What TKIP feature was introduced to counter the weak integrity check algorithm used in WEP?

- A. Sequence counters
- B. 32-bit ICV (CRC-32)
- C. Michael
- D. Block cipher support
- E. RC5 stream cipher

Answer: C

Explanation:
TKIP (used with WPA) introduced "Michael" as a message integrity check (MIC) algorithm to replace the insecure CRC-32 used in WEP. Michael:
Adds tamper protection to each packet.
Helps detect packet forgery.
Incorrect:
A). CRC-32 was used in WEP and proven weak.
B). Sequence counters help prevent replay attacks, not integrity checking.
C). RC5 is not used in WLAN security.
E). TKIP does not support block ciphers-it uses RC4, a stream cipher.
References:
CWSP-208 Study Guide, Chapter 3 (TKIP Security Features)

NEW QUESTION # 113
Given: You are using a Wireless Aggregator utility to combine multiple packet captures. One capture exists for each of channels 1, 6 and 11. What kind of troubleshooting are you likely performing with such a tool?

- A. Wireless adapter failure analysis.
- B. Fast secure roaming problems.
- C. Interference source location.
- D. Narrowband DoS attack detection.

Answer: B

Explanation:
When using a wireless aggregator to combine packet captures from channels 1, 6, and 11 (the three non- overlapping 2.4 GHz

channels), you're most likely analyzing multi-channel behavior. This is particularly relevant when troubleshooting roaming issues, such as fast secure roaming (e.g., 802.11r). These captures help determine whether authentication or association events occur smoothly across APs operating on different channels.
Incorrect:
A). Adapter failure doesn't require multi-channel capture.
B). Interference location is typically single-channel and spectrum-analysis focused.
D). Narrowband DoS attacks are also usually identified using RF spectrum analysis, not packet capture across all channels.
References:
CWSP-208 Study Guide, Chapter 6 (Roaming and Mobility)
CWNP Whitepaper: WLAN Troubleshooting Methodologies
CWNP Learning Portal: 802.11 Roaming and Analysis

NEW QUESTION # 114
.....