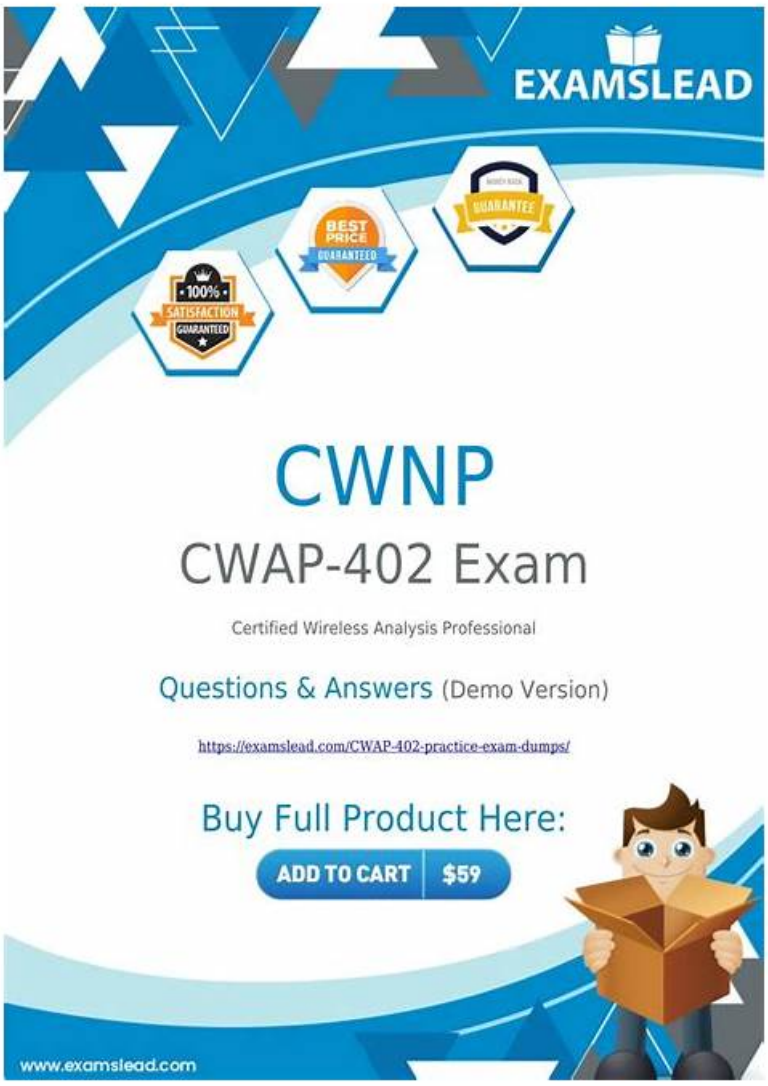
Free PDF Quiz CWNP - Trustable CWSP-208 Test Topics Pdf



2025 Latest PracticeTorrent CWSP-208 PDF Dumps and CWSP-208 Exam Engine Free Share: https://drive.google.com/open?id=1cr3tGq-2JrpXAUNBUOGP8iiwC0VcmlEC

You can run the Certified Wireless Security Professional (CWSP) CWSP-208 PDF Questions file on any device laptop, smartphone or tablet, etc. You just need to memorize all CWSP-208 exam questions in the pdf dumps file. CWNP CWSP-208 practice test software (Web-based and desktop) is specifically useful to attempt the CWSP-208 Practice Exam. It has been a proven strategy to pass professional exams like the CWNP CWSP-208 exam in the last few years. Certified Wireless Security Professional (CWSP) CWSP-208 practice test software is an excellent way to engage candidates in practice.

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	• 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.

Free PDF Quiz 2025 CWNP CWSP-208 High Hit-Rate Test Topics Pdf

Our CWSP-208 study materials have included all significant knowledge about the exam. So you do not need to pick out the important points by yourself. Also, our CWSP-208 practice engine can greatly shorten your preparation time of the exam. So you just need our CWSP-208 learning questions to help you get the certificate. You will find that the coming exam is just a piece of cake in front of you and you will pass it with ease.

CWNP Certified Wireless Security Professional (CWSP) Sample Questions (Q98-Q103):

NEW QUESTION # 98
Which of the following security attacks cannot be detected by a WIPS solution of any kind? (Choose 2)

- A. Social engineering
- B. Eavesdropping
- C. Rogue APs
- D. DoS

Answer: A,B

Explanation:
Wireless Intrusion Prevention Systems (WIPS) are excellent for detecting on-air threats such as rogue APs, DoS attacks, spoofing, and misconfigured devices. However, WIPS cannot detect:
C). Eavesdropping - Passive listening on wireless transmissions cannot be detected because no signal is transmitted by the attacker.
D). Social engineering - Human-based attacks like phishing or pretexting fall outside the scope of wireless monitoring.
Incorrect:
A). Rogue APs can be detected via MAC address comparison, frame analysis, and signal triangulation.
B). DoS attacks, such as deauth floods or RF jamming, can be detected with appropriate WIPS sensors.
References:
CWSP-208 Study Guide, Chapter 5 (WLAN Threats and Attacks)
CWNP WIPS Implementation Guidelines
CWNP Whitepapers on Wireless Threat Detection Capabilities

NEW QUESTION # 99
Given: You are installing 6 APs on the outside of your facility. They will be mounted at a height of 6 feet.
What must you do to implement these APs in a secure manner beyond the normal indoor AP implementations? (Choose the single best answer.)

- A. User external antennas.
- B. Use internal antennas.
- C. Power the APs using PoE.
- D. Ensure proper physical and environmental security using outdoor ruggedized APs or enclosures.

Answer: D

Explanation:
Outdoor APs must be:
Protected from theft or tampering (physical security).
Shielded from weather/environmental conditions (IP-rated enclosures).
Mounted and secured to prevent unauthorized physical access or damage.
Incorrect:
A & B. Antenna type is relevant to RF coverage but does not address outdoor-specific security needs.
C). PoE is useful for power delivery but not a security solution.
References:
CWSP-208 Study Guide, Chapter 7 (Physical Security for Wireless Devices) CWNP Outdoor WLAN Deployment Guidelines

NEW QUESTION # 100
What software and hardware tools are used together to hijack a wireless station from the authorized wireless network onto an unauthorized wireless network? (Choose 2)

- A. A wireless workgroup bridge and a protocol analyzer
- B. RF jamming device and a wireless radio card
- C. DHCP server software and access point software
- D. A low-gain patch antenna and terminal emulation software
- E. MAC spoofing software and MAC DoS software

Answer: B,C

Explanation:
To hijack a wireless client, attackers often use:
An RF jamming device to disconnect the client from the legitimate AP (via deauth attacks or RF disruption) A rogue AP (created using access point software) that impersonates the real network DHCP server software to assign IP addresses and act as a gateway, completing the fake network Incorrect:
B). Terminal emulation is not relevant.
C). Workgroup bridges and protocol analyzers are for monitoring, not attacking.
E). MAC spoofing and DoS do not complete a hijack.
References:
CWSP-208 Study Guide, Chapter 5 (Hijacking Tools and Techniques)
CWNP Practical WLAN Attack Tools Guide

NEW QUESTION # 101
Given: 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?
(Choose 2)

- A. MS-CHAPv2 is compliant with WPA-Personal, but not WPA2-Enterprise.
- B. LEAP's use of MS-CHAPv2 is only secure when combined with WEP.
- C. When implemented with AES-CCMP encryption, MS-CHAPv2 is very secure.
- D. MS-CHAPv2 is only appropriate for WLAN security when used inside a TLS-encrypted tunnel.
- E. MS-CHAPv2 uses AES authentication, and is therefore secure.
- F. MS-CHAPv2 is subject to offline dictionary attacks.

Answer: D,F

Explanation:
MS-CHAPv2 is a widely used authentication protocol, but it has notable weaknesses:
B). MS-CHAPv2 is vulnerable to offline dictionary attacks. Attackers can capture authentication exchanges and attempt password guesses offline due to predictable hashing behavior.
D). The only secure use of MS-CHAPv2 is inside a secure tunnel (e.g., EAP-TTLS or PEAP), where credentials are protected during transmission.
Incorrect:
A). MS-CHAPv2 is used in WPA2-Enterprise, not WPA-Personal, and it is allowed under WPA2-Enterprise via PEAP.
C). WEP does not enhance LEAP's security; it compounds vulnerabilities.
E and F. MS-CHAPv2 does not use AES for authentication. Using AES-CCMP for encryption does not fix MS-CHAPv2's weaknesses.
References:
CWSP-208 Study Guide, Chapter 4 (EAP Methods and Authentication Protocols) CWNP MS-CHAPv2 and PEAP Implementation Guidelines Microsoft MS-CHAPv2 Vulnerability Advisories

NEW QUESTION # 102
Given: 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 features could be used by XYZ to assign the proper network permissions to users during authentication? (Choose 2)

- 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 communicate with the DHCP server to issue the appropriate IP address and VLAN assignment to users.
- C. RADIUS attributes can be used to assign permission levels, such as read-only permission, to users of a particular network resource.
- 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.
- E. The RADIUS server can support vendor-specific attributes in the ACCESS-ACCEPT response, which can be used for user policy assignment.

Answer: C,E

Explanation:
Comprehensive Detailed Explanation:
B). Vendor-Specific Attributes (VSAs) allow integration with WLAN vendors' controllers to assign roles, VLANs, QoS levels, etc., during user authentication.
E). Standard or vendor-specific RADIUS attributes can dynamically assign permission levels based on group membership, department, or role.

Incorrect:
A). RADIUS does not directly manage DHCP functions.
C). SSID is selected by the user's device, not by the RADIUS server.
D). RADIUS uses ACCESS-REJECT, not "DO-NOT-AUTHORIZE," and it is not OS-specific.
References:
CWSP-208 Study Guide, Chapter 4 (RADIUS and Policy Assignment)
CWNP RADIUS Deployment Best Practices

NEW QUESTION # 103
.....

If you feel that you purchase PracticeTorrent CWNP CWSP-208 exam training materials, and use it to prepare for the exam is an adventure, then the whole of life is an adventure. Gone the furthest person is who are willing to do it and willing to take risks. Not to mention that PracticeTorrent CWNP CWSP-208 exam training materials are many candidates proved in practice. It brings the success of each candidate is also real and effective. Dreams and hopes are important, but more important is to go to practice and prove. The PracticeTorrent CWNP CWSP-208 Exam Training materials will be successful, select it, you have no reason unsuccessful !