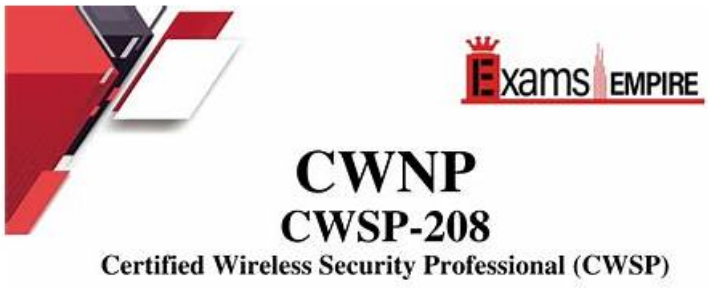
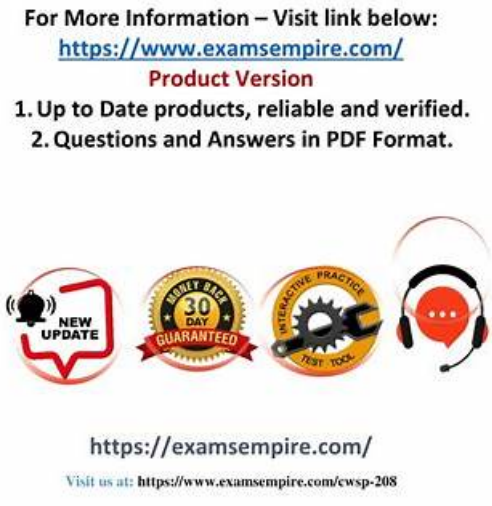
Guaranteed CWSP-208 Questions Answers & CWSP-208 Exam





What's more, part of that PDFDumps CWSP-208 dumps now are free: https://drive.google.com/open?id=1V9I-vMY7K_tNDnVRte4VZMCDwbAd03f1

Three versions of CWSP-208 exam dumps are provided by us. Each version has its own advantages. CWSP-208 PDF version is printable and you can take it with you. CWSP-208 Soft test engine can stimulate the real exam environment, so that it can release your nerves while facing the real exam. CWSP-208 Online Test engine can be used in any web browsers, and it can also record your performance and practicing history. You can continue your practice next time.

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.

CWSP-208 practice materials & CWSP-208 real test & CWSP-208 test prep

Before the clients buy our CWSP-208 guide prep they can have a free download and tryout. The client can visit the website pages of our product and understand our CWSP-208 study materials in detail. You can see the demo, the form of the software and part of our titles. To better understand our CWSP-208 Preparation questions, you can also look at the details and the guarantee. So it is convenient for you to have a good understanding of our CWSP-208 exam questions before you decide to buy our CWSP-208 training materials.

CWNP Certified Wireless Security Professional (CWSP) Sample Questions (Q91-Q96):

NEW QUESTION # 91
What wireless security protocol provides mutual authentication without using an X.509 certificate?

- A. PEAPv0/EAP-MSCHAPv2
- B. EAP-MD5
- C. EAP-FAST
- D. EAP-TTLS
- E. EAP-TLS
- F. PEAPv1/EAP-GTC

Answer: C

Explanation:
EAP-FAST (Flexible Authentication via Secure Tunneling) provides:
Mutual authentication using Protected Access Credentials (PACs).
Does not require X.509 certificates for either client or server (although optional for servers).
Is faster and easier to deploy in environments lacking a PKI.
Incorrect:
B). EAP-MD5 provides no mutual authentication.
C). EAP-TLS requires client and server certificates.

D). PEAPv0/EAP-MSCHAPv2 requires a server certificate.
E). EAP-TTLS requires a server certificate.
F). PEAPv1/EAP-GTC still requires a server certificate.
References:
CWSP-208 Study Guide, Chapter 4 (EAP Method Comparisons)
Cisco EAP-FAST Whitepaper
Wi-Fi Alliance EAP Interoperability Matrix

NEW QUESTION # 92
In what deployment scenarios would it be desirable to enable peer-to-peer traffic blocking?

- A. In corporate Voice over Wi-Fi networks with push-to-talk multicast capabilities
- B. At public hot-spots in which many clients use diverse applications
- C. In home networks in which file and printer sharing is enabled
- D. In university environments using multicast video training sourced from professor's laptops

Answer: B

Explanation:
Peer-to-peer blocking (also called client isolation) is useful in open or public WLANs to prevent devices from communicating directly with each other.
B). In public hot-spots, isolating users helps protect against malware spread, snooping, and attacks from nearby devices.
Incorrect:
A). In home networks, peer-to-peer communication is often desired for file sharing.
C). Voice over Wi-Fi may rely on peer communication (e.g., multicast).
D). In university setups using multicast, peer-to-peer restrictions could hinder functionality.
References:
CWSP-208 Study Guide, Chapter 3 (Access Control and WLAN Policies)
CWNP WLAN Best Practices for Public Networks

NEW QUESTION # 93
After completing the installation of a new overlay WIPS for the purpose of rogue detection and security monitoring at your corporate headquarters, what baseline function MUST be performed in order to identify security threats?

- A. Authorized PEAP usernames must be added to the WIPS server's user database.
- B. Separate security profiles must be defined for network operation in different regulatory domains
- C. Upstream and downstream throughput thresholds must be specified to ensure that service-level agreements are being met.
- D. WLAN devices that are discovered must be classified (rogue, authorized, neighbor, etc.) and a WLAN policy must define how to classify new devices.

Answer: D

Explanation:
After deploying a WIPS, an essential baseline activity is to classify all detected devices in the RF environment. These classifications allow the system to enforce security policies and detect policy violations.
Classifications include:
Authorized (managed devices)
Rogue (unauthorized, possibly dangerous)
Neighbor (not part of your network but legitimate)
External or Ad hoc devices
Without this initial classification, WIPS cannot properly assess threats or trigger alarms.
References:
CWSP-208 Study Guide, Chapter 7 - WIPS Classification and Threat Management CWNP CWSP-208 Objectives: "Device Classification and Policy Enforcement"

NEW QUESTION # 94
Given: Fred works primarily from home and public wireless hot-spots rather than commuting to the office. He frequently accesses

the office network remotely from his Mac laptop using the local 802.11 WLAN.
In this remote scenario, what single wireless security practice will provide the greatest security for Fred?

- A. Use secure protocols, such as FTP, for remote file transfers.
- B. Use an IPSec VPN for connectivity to the office network
- C. Use WIPS sensor software on the laptop to monitor for risks and attacks
- D. Use 802.1X/PEAPv0 to connect to the corporate office network from public hot-spots
- E. Use only HTTPS when agreeing to acceptable use terms on public networks
- F. Use enterprise WIPS on the corporate office network

Answer: B

Explanation:
When connecting over untrusted public networks:
An IPSec VPN provides encryption and authentication from the client to the corporate network.
This protects against eavesdropping, man-in-the-middle attacks, and spoofed hotspots.
Incorrect:
B). HTTPS only protects web sessions-not all traffic.
C). Enterprise WIPS at the office won't protect remote users.
D). Laptop-based WIPS software is rare and less effective than using a VPN.
E). 802.1X/PEAP is not designed for remote use over public hotspots.
F). FTP is not secure; secure alternatives include SFTP or FTPS.
References:
CWSP-208 Study Guide, Chapter 6 (VPNs and Remote Security)
CWNP Remote Access Security Best Practices

NEW QUESTION # 95
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 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.
- B. 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.
- C. 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.
- D. 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.
- E. 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.

Answer: A

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 # 96
.....

If you want to take CWNP CWSP-208 exam, PDFDumps CWNP CWSP-208 exam dumps are your best tools. The dumps can help you pass CWSP-208 test easily. And the dumps are very highly regarded. With our test questions and test answers, you don't need to worry about CWSP-208 Certification. Because our dumps can solve all difficult problems you encounter in the process of preparing for the exam. Before you make a decision, you can download our free demo. For this, you will know whether our questions and answers fit to you or not.

BONUS!!! Download part of PDFDumps CWSP-208 dumps for free: https://drive.google.com/open?id=1V9I-vMY7K_tNDnVRte4VZMCDwbAd03f1