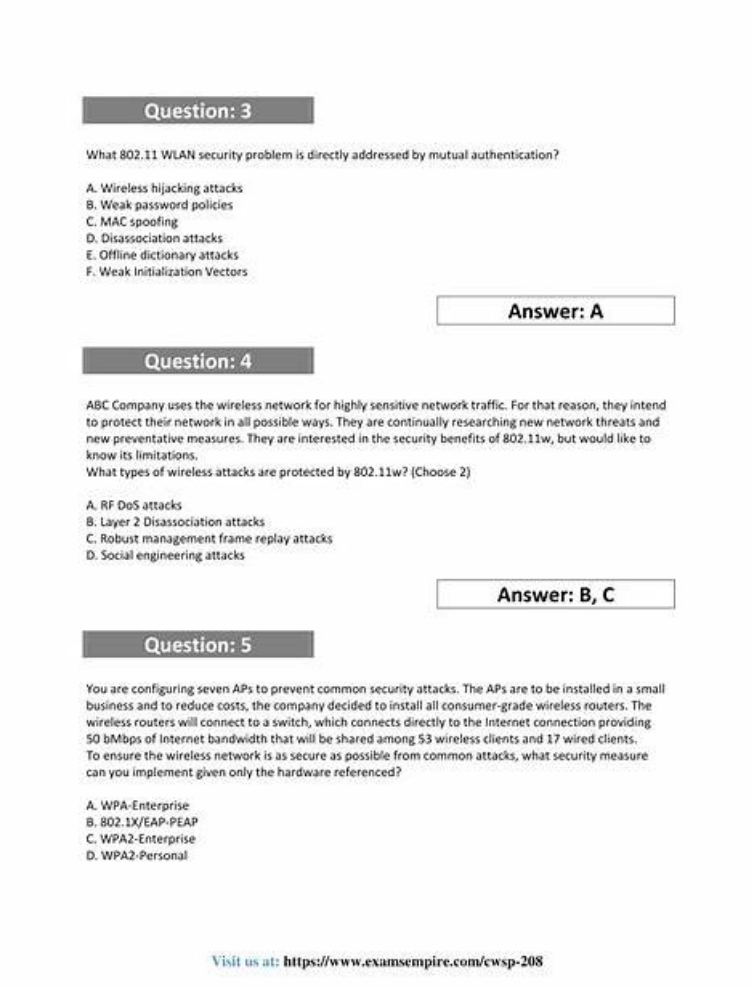
CWSP-208시험대비 & CWSP-208인기덤프



Question: 3

What 802.11 WLAN security problem is directly addressed by mutual authentication?

A. Wireless hijacking attacks
B. Weak password policies
C. MAC spoofing
D. Disassociation attacks
E. Offline dictionary attacks
F. Weak Initialization Vectors

Answer: A

Question: 4

ABC Company uses the wireless network for highly sensitive network traffic. For that reason, they intend to protect their network in all possible ways. They are continually researching new network threats and new preventative measures. They are interested in the security benefits of 802.11w, but would like to know its limitations.
What types of wireless attacks are protected by 802.11w? (Choose 2)

A. RF DoS attacks
B. Layer 2 Disassociation attacks
C. Robust management frame replay attacks
D. Social engineering attacks

Answer: B, C

Question: 5

You are configuring seven APs to prevent common security attacks. The APs are to be installed in a small business and to reduce costs, the company decided to install all consumer-grade wireless routers. The wireless routers will connect to a switch, which connects directly to the Internet connection providing 50 bMbps of Internet bandwidth that will be shared among 53 wireless clients and 17 wired clients.
To ensure the wireless network is as secure as possible from common attacks, what security measure can you implement given only the hardware referenced?

A. WPA-Enterprise
B. 802.1X/EAP-PEAP
C. WPA2-Enterprise
D. WPA2-Personal

Visit us at: https://www.examsempire.com/cwsp-208

2025 KoreaDumps 최신 CWSP-208 PDF 버전 시험 문제집과 CWSP-208 시험 문제 및 답변 무료 공유: https://drive.google.com/open?id=1q09WtAXTywfzpaS_uwEs76jMSKRLNm8_

CWNP 인증 CWSP-208시험대비덤프를 찾고 계시다면KoreaDumps가 제일 좋은 선택입니다.저희KoreaDumps에서는 여라가지 IT자격증시험에 대비하여 모든 과목의 시험대비 자료를 발췌하였습니다. KoreaDumps에서 시험대비 덤프자료를 구입하시면 시험불합격시 덤프비용환불신청이 가능하고 덤프 1년 무료 업데이트서비스도 가능합니다. KoreaDumps를 선택하시면 후회하지 않을것입니다.

CWNP CWSP-208 시험요강:

주제	소개
주제 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.

주제 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.
주제 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.
주제 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.

시험패스 가능한 CWSP-208시험대비 최신버전 덤프자료

여러분은CWNP CWSP-208인증시험을 패스함으로 IT업계관련 직업을 찾고자하는 분들에게는 아주 큰 가산점이 될수 있으며, 성덩한 IT업계사업자와 한걸음 가까와 집니다.

최신 CWNP CWSP CWSP-208 무료샘플문제 (Q79-Q84):

질문 # 79
Wireless Intrusion Prevention Systems (WIPS) provide what network security services? (Choose 2)

- A. Wireless vulnerability assessment
- B. Policy enforcement and compliance management
- C. Configuration distribution for autonomous APs
- D. Application-layer traffic inspection
- E. Analysis and reporting of AP CPU utilization

정답： A,B

설명:
WIPS systems provide proactive security by continuously scanning for threats and ensuring WLAN policy compliance. Their capabilities include:
B). Wireless vulnerability assessment: Scanning for misconfigured APs, weak encryption, and unauthorized devices.
E). Policy enforcement and compliance: Ensuring security settings adhere to enterprise or regulatory requirements and alerting on deviations.
Other options like application-layer inspection and AP CPU monitoring are outside the WIPS function scope.
References:
CWSP-208 Study Guide, Chapter 7 - WIPS Services and Capabilities

CWNP CWSP-208 Objectives: "WIPS Threat Mitigation and Enforcement"

질문 # 80
In order to acquire credentials of a valid user on a public hot-spot network, what attacks may be conducted?
Choose the single completely correct answer.

- A. Social engineering and/or eavesdropping
- B. Authentication cracking and/or RF DoS
- C. Code injection and/or XSS
- D. RF DoS and/or physical theft
- E. MAC denial of service and/or physical theft

정답： A

설명:
Comprehensive Detailed Explanation:
On public Wi-Fi hotspots (typically unsecured), attackers often perform:
Eavesdropping: By passively listening to unencrypted traffic, an attacker can capture credentials or sensitive data.
Social engineering: Users may be tricked into entering their credentials on a spoofed login page or disclosing them directly through phishing or manipulation.
These are the most effective and common methods for credential theft in open network environments.
Incorrect:
B & C. Physical theft is not network-based and not relevant to hotspot-based credential acquisition.
D). Authentication cracking is not applicable to open networks with captive portals.
E). Code injection/XSS may happen in web apps but are not directly methods for acquiring hotspot credentials.
References:
CWSP-208 Study Guide, Chapter 5 (Threats and Attacks)
CWNP Security Essentials: Eavesdropping and Social Engineering in WLANs

질문 # 81
Given: In XYZ's small business, two autonomous 802.11ac APs and 12 client devices are in use with WPA2- Personal.
What statement about the WLAN security of this company is true?

- A. An unauthorized WLAN user with a protocol analyzer can decode data frames of authorized users if he captures the BSSID, client MAC address, and a user's 4-Way Handshake.
- B. An unauthorized wireless client device cannot associate, but can eavesdrop on some data because WPA2-Personal does not encrypt multicast or broadcast traffic.
- C. Because WPA2-Personal uses Open System authentication followed by a 4-Way Handshake, hijacking attacks are easily performed.
- D. Intruders may obtain the passphrase with an offline dictionary attack and gain network access, but will be unable to decrypt the data traffic of other users.
- E. A successful attack against all unicast traffic on the network would require a weak passphrase dictionary attack and the capture of the latest 4-Way Handshake for each client.

정답： E

설명:
In WPA2-Personal, each client derives its Pairwise Transient Key (PTK) based on a shared Pairwise Master Key (PMK) and values exchanged during the 4-Way Handshake. Therefore, even if the passphrase is cracked, an attacker must still capture the 4-Way Handshake for each target client in order to decrypt their unicast traffic.
Incorrect:
A). Incorrect because cracking the passphrase allows decrypting data traffic after capturing the 4-Way Handshake.
C). WPA2 encrypts multicast and broadcast traffic using the GTK, which unauthorized clients cannot derive.
D). Capturing BSSID and MAC isn't enough without knowing the passphrase and the full 4-Way Handshake.
E). Hijacking is harder in WPA2-Personal due to the dynamic PTK derived per session.
References:
CWSP-208 Study Guide, Chapter 3 (WPA2-PSK Key Management)
CWNP Learning: WLAN Encryption and PTK Derivation

질문 # 82
Which one of the following describes the correct hierarchy of 802.1X authentication key derivation?

- A. If passphrase-based client authentication is used by the EAP type, the PMK is mapped directly from the user's passphrase. The PMK is then used during the 4-way handshake to create data encryption keys.
- B. The PMK is generated from a successful mutual EAP authentication. When mutual authentication is not used, an MSK is created. Either of these two keys may be used to derive the temporal data encryption keys during the 4-way handshake.
- C. After successful EAP authentication, the RADIUS server generates a PMK. A separate key, the MSK, is derived from the AAA key and is hashed with the PMK to create the PTK and GTK.
- D. The MSK is generated from the 802.1X/EAP authentication. The PMK is derived from the MSK. The PTK is derived from the PMK, and the keys used for actual data encryption are a part of the PTK.

정답：D

설명：
In 802.1X/EAP authentication:
The EAP method (e.g., EAP-TLS, PEAP) results in the generation of a Master Session Key (MSK).
The Pairwise Master Key (PMK) is derived from the MSK.
The Pairwise Transient Key (PTK) is derived from the PMK using nonces and MAC addresses during the 4- Way Handshake.
The PTK includes the actual keys used for data encryption.
Incorrect:
B). This applies to WPA/WPA2-Personal, not 802.1X/EAP.
C). The RADIUS server sends the MSK, not the PMK directly.
D). The MSK is always derived during EAP authentication, mutual or not.
References:
CWSP-208 Study Guide, Chapter 3 (Key Hierarchy)
IEEE 802.11i Specification

질문 # 83
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. 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.
- C. 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.
- 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 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.

정답：B

설명：
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

질문 # 84
.....