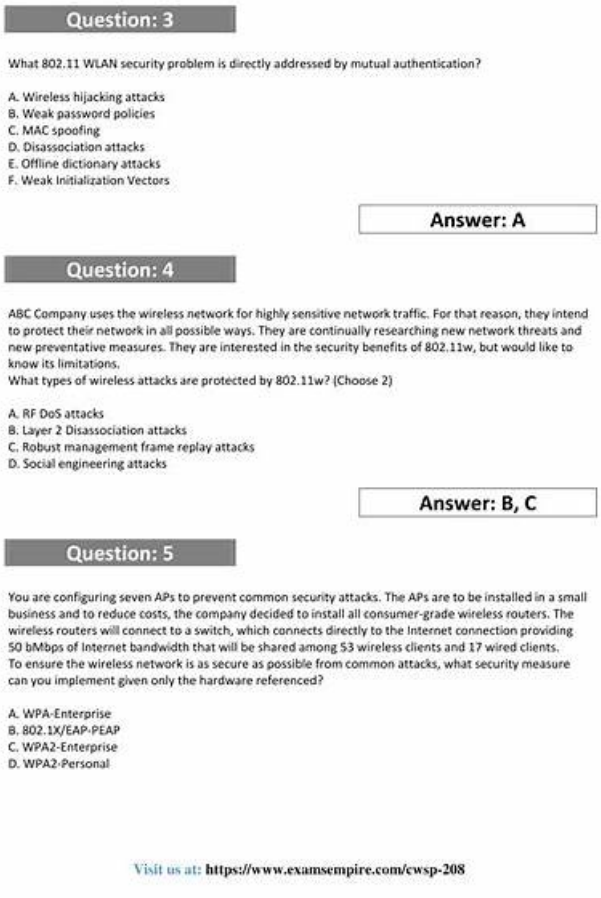
CWSP-208 Musterprüfungsfragen & CWSP-208 Prüfungs-Guide



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

Der Traum von IT ist immer gering in Wirklichkeit. Aber der Traum, die CWNP CWSP-208 Zertifizierungsprüfung zu bestehen, ist absolut in reichweite, wenn Sie ZertSoft benutzen. Wir ZertSoft bietet Ihnen hochwertigen Sevice, und die Genauigkeit der Fragenkataloge zur CWNP CWSP-208 Zertifizierungsprüfung ist so hoch, dass die Bestehensrate der CWNP CWSP-208 Zertifizierungsprüfung 100% beträgt. Solange Sie ZertSoft wählen, können wir Ihhen versprechen, dass Sie die CWNP CWSP-208 Zertifizierungsprüfung bestimmt bestehen!

CWNP CWSP-208 Prüfungsplan:

Thema	Einzelheiten
Thema 1	• 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.

Thema 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.
Thema 3	• 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.
Thema 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 Prüfungs-Guide, CWSP-208 Trainingsunterlagen

ZertSoft hat einen guten Online-Service. Wenn Sie die Produkte von ZertSoft kaufen, wird ZertSoft Ihnen einen einjährigen kostenlos Update-Service rund um die Uhr bieten. Wir benachritigen Ihnen rechtzeitig die neuesten Prüfungsinformationen zur CWNP CWSP-208 Zertifizierung, so dass Sie sich gut auf die CWNP CWSP-208 Zertifizierungsprüfung vorbereiten können. Mit wenig Zeit und Geld können Sie die IT-Prüfung bestehen. Es ist sehr preisgünstig, ZertSoft zu wählen und somit die CWNP CWSP-208 Zertifizierungsprüfung nur einmal zu bestehen.

CWNP Certified Wireless Security Professional (CWSP) CWSP-208 Prüfungsfragen mit Lösungen (Q51-Q56):

51. Frage
As the primary security engineer for a large corporate network, you have been asked to author a new security policy for the wireless network. While most client devices support 802.1X authentication, some legacy devices still only support passphrase/PSK-based security methods.
When writing the 802.11 security policy, what password-related items should be addressed?

- A. Certificates should always be recommended instead of passwords for 802.11 client authentication.
- B. EAP-TLS must be implemented in such scenarios.
- C. Static passwords should be changed on a regular basis to minimize the vulnerabilities of a PSK-based authentication.
- D. Password complexity should be maximized so that weak WEP IV attacks are prevented.
- E. MSCHAPv2 passwords used with EAP/PEAPv0 should be stronger than typical WPA2-PSK passphrases.

Antwort: C

Begründung:
In environments where PSK-based authentication (like WPA2-Personal) is still in use due to legacy device constraints:
C). Regularly changing static passwords helps limit exposure from credential leaks or previous employees retaining access.

Incorrect:
A). MSCHAPv2 is vulnerable to offline attacks; recommending strong passwords is good, but that alone isn't sufficient.
B). WEP is insecure regardless of password strength due to IV reuse.
D). Certificates are stronger, but not always feasible for legacy systems.
E). EAP-TLS is ideal but not always compatible with all devices; policies should be flexible to device capabilities.
References:
CWSP-208 Study Guide, Chapters 3 and 4 (WPA2-PSK and 802.1X Considerations) CWNP WLAN Security Lifecycle and Policy Development

52. Frage
What WLAN client device behavior is exploited by an attacker during a hijacking attack?

- A. When the RF signal between a client and an access point is disrupted for more than a few seconds, the client device will attempt to associate to an access point with better signal quality.
- B. Client drivers scan for and connect to access points in the 2.4 GHz band before scanning the 5 GHz band.
- C. As specified by the Wi-Fi Alliance, clients using Open System authentication must allow direct client- to-client connections, even in an infrastructure BSS.
- D. After the initial association and 4-way handshake, client stations and access points do not need to perform another 4-way handshake, even if connectivity is lost.
- E. When the RF signal between a client and an access point is lost, the client will not seek to reassociate with another access point until the 120 second hold down timer has expired.

Antwort: A

Begründung:
Hijacking attacks often rely on exploiting client behavior during signal disruption. Clients will seek better connections when RF is weak or interrupted. An attacker may:
Disrupt the signal (e.g., with a deauth attack)
Present a rogue access point (evil twin) with stronger signal
Trick the client into associating with the rogue AP, hijacking the session Incorrect:
B). There is no standard 120-second timer behavior.
C). Loss of connectivity typically triggers reassociation and reauthentication.
D). Direct client-to-client connections are not required in infrastructure mode.
E). Band selection logic varies and is unrelated to hijacking attacks.
References:
CWSP-208 Study Guide, Chapter 5 (Hijacking and Client Behavior)
CWNP Wi-Fi Threat Analysis

53. Frage
Given: ABC Company is deploying an IEEE 802.11-compliant wireless security solution using 802.1X/EAP authentication.
According to company policy, the security solution must prevent an eavesdropper from decrypting data frames traversing a wireless connection.
What security characteristics and/or components play a role in preventing data decryption? (Choose 2)

- A. PLCP Cyclic Redundancy Check (CRC)
- B. Integrity Check Value (ICV)
- C. Group Temporal Keys
- D. Encrypted Passphrase Protocol (EPP)
- E. Multi-factor authentication
- F. 4-Way Handshake

Antwort: C,F

Begründung:
To prevent data decryption:
B). The 4-Way Handshake derives and installs unique unicast keys (PTKs) on both client and AP.
F). The GTK is used to encrypt broadcast and multicast frames, ensuring group traffic is protected.
Incorrect:
A). Multi-factor authentication enhances identity assurance but not encryption.

C). PLCP CRC checks for transmission errors but does not secure data.
D). EPP is not a valid or recognized encryption protocol.
E). ICV was used in WEP and is cryptographically weak.
References:
CWSP-208 Study Guide, Chapter 3 (Key Hierarchy and 4-Way Handshake)
IEEE 802.11i Standard

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

Antwort: A

Begründung:
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"

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

Antwort: C

Begründung:
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

56. Frage
......

ZertSoft hat sich stetig entwickelt . Unsere Antriebe werden von unseren Kunden, die mit Hilfe unserer Produtkte die IT-Zertifizierung erwerbt haben, gegeben. Heute wird die CWNP CWSP-208 Prüfungssoftware von zahlosen Kunden geprüft und anerkannt. Die Software hilft ihnen, die Zertifizierung der CWNP CWSP-208 zu erwerben. Auf unserer offiziellen Webseite können Sie die Demo kostenfrei downloaden und probieren. Wir erwarten Ihre Anerkennung. Innerhalb einem Jahr nach Ihrem Kauf werden wir Ihnen Informationen über den Aktualisierungsstand der CWNP CWSP-208 rechtzeitig geben. Ihre Vorbereitungsprozess der Prüfung wird deshalb bestimmt leichter!

CWSP-208 Prüfungs-Guide: https://www.zertsoft.com/CWSP-208-pruefungsfragen.html