DUMPSBOSS.

Certified Wireless Security Professional (CWSP)

CWNP CWSP-207

Version Demo

Total Demo Questions: 13

Total Premium Questions: 131

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, WLAN Discovery Techniques	11
Topic 2, WLAN Intrusion and Attack Techniques	19
Topic 3, Wireless Security Solutions	65
Topic 4, Wireless Security Monitoring	22
Topic 5, WLAN Security Design	14
Total	131

QUESTION NO: 1

Your organization required compliance reporting and forensics features in relation to the 802.11ac WLAN they have recently installed. These features are not built into the management system provided by the WLAN vendor. The existing WLAN is managed through a centralized management console provided by the AP vendor with distributed APs and multiple WLAN controllers configured through this console.

What kind of system should be installed to provide the required compliance reporting and forensics features?

A. WNMS

B. WIPS overlay

C. WIPS integrated

D. Cloud management platform

ANSWER: B

Explanation:

WIPS overlay is correct because it is a separate wireless intrusion prevention system deployed alongside an existing WLAN infrastructure. Its dedicated sensors and management platform can collect wireless RF and 802.11 activity independently of the AP vendor's controller and management console. This makes it appropriate when the installed WLAN management system does not provide the organization's required reporting, event retention, alerting, investigation, and forensic-analysis capabilities. An overlay architecture can monitor the wireless environment across the organization, correlate observed activity, retain evidence for later review, and generate reports needed to demonstrate compliance without requiring replacement of the deployed APs or controllers. NIST describes wireless IDS capabilities as including monitoring wireless traffic, identifying suspicious activity, logging events, and supporting analysis and response; these are foundational functions for a dedicated monitoring and forensics platform. See NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems. This approach also aligns with CWNP's security focus on detecting and mitigating threats in operational enterprise WLANs, as reflected in the CWSP certification overview.

QUESTION NO: 2

Given: During 802.1X/LEAP authentication, the username is passed across the wireless medium in clear text.

From a security perspective, why is this significant?

A. The username is needed for Personal Access Credential (PAC) and X.509 certificate validation.

B. The username is an input to the LEAP challenge/response hash that is exploited, so the username must be known to conduct authentication cracking.

C. 4-Way Handshake nonces are based on the username in WPA and WPA2 authentication.

D. The username can be looked up in a dictionary file that lists common username/password combinations.

ANSWER: B

Explanation:

The username is an input to the LEAP challenge/response hash that is exploited, so the username must be known to conduct authentication cracking. LEAP uses a challenge-response design derived from Microsoft challenge-handshake methods and is susceptible to offline password-guessing attacks when an attacker captures the relevant authentication exchange. In this type of exchange, knowing the identity is important because the username participates in the challenge-response calculation and identifies the credentials against which guesses are being tested. An attacker who passively captures wireless traffic can therefore obtain the clear-text username along with the challenge and response values needed to mount a targeted cracking attempt, rather than first having to discover the account name. This makes credential attacks more practical and enables an attacker to focus dictionaries and password guesses on a known user identity. RFC 2759 documents the username's inclusion in the challenge-hash calculation used by the related MS-CHAPv2 mechanism: RFC 2759. The broader EAP framework also notes that clear-text identity exchange can create privacy and security concerns, particularly when identity protection is not provided: RFC 3748.

QUESTION NO: 3

Given: During an authorized assessment of a WPA2-Personal WLAN, a tester captures an RSN Association Request containing a PMKID for the target SSID. The tester does not capture a 4-Way Handshake for any client.

What attack capability may still be possible if the WLAN uses a weak passphrase?

A. Offline passphrase guessing using the captured PMKID as a validation value.

B. Direct recovery of the AP's current GTK without any passphrase guessing.

C. Decryption of all protected data frames without deriving a PMK.

D. Forging a valid RADIUS Access-Accept for the WLAN controller.

ANSWER: A

Explanation:

A captured PMKID can be used to validate passphrase guesses offline when the PMKID was derived from the PMK associated with the target PSK network. The tester can derive a candidate PMK from each passphrase guess and compare the resulting PMKID with the captured value. This can allow offline dictionary testing without capturing a client 4-Way Handshake.

The PMKID does not reveal the passphrase directly. A strong, randomly generated WPA2-Personal passphrase remains resistant to practical dictionary guessing, whereas a short or predictable passphrase may be recovered.

QUESTION NO: 4

In the IEEE 802.11-2012 standard, what is the purpose of the 802.1X Uncontrolled Port?

A. To allow only authentication frames to flow between the Supplicant and Authentication Server

B. To block authentication traffic until the 4-Way Handshake completes

C. To pass general data traffic after the completion of 802.11 authentication and key management

D. To block unencrypted user traffic after a 4-Way Handshake completes

ANSWER: A

Explanation:

To allow only authentication frames to flow between the Supplicant and Authentication Server is correct. IEEE 802.1X separates access through an authenticator into controlled and uncontrolled logical ports. Before network access is authorized, the controlled port remains closed to ordinary user data. The uncontrolled port remains available so that the authentication exchange required to determine authorization can occur. In an enterprise WLAN, this normally means carrying Extensible Authentication Protocol over LAN authentication traffic between the wireless client (the supplicant) and the access point (the authenticator); the access point relays the relevant authentication messages to the authentication server, commonly using a backend authentication protocol such as RADIUS.

This separation is fundamental to port-based network access control: a client must be able to perform authentication before it is permitted to use the protected network for general traffic. Following successful authentication and the applicable WLAN key-management process, the controlled port can be authorized for normal data communication. The uncontrolled port therefore supplies the narrowly scoped path needed for authentication while access authorization is being established. IEEE describes this controlled/uncontrolled port model in its 802.1X standard; its application to WLAN authentication is part of the IEEE 802.11 security architecture. See IEEE 802.1X Port-Based Network Access Control and IEEE 802.11 Wireless LAN Standard.

QUESTION NO: 5

What statements are true about IEEE 802.11 Shared Key authentication used with WEP? (Choose 2)

A. The plaintext challenge and encrypted response can provide an attacker with known plaintext for WEP analysis.

B. The authentication exchange does not provide strong mutual authentication of the AP to the client.

C. The authentication exchange derives a unique PTK for every client association.

D. The authentication exchange protects the challenge with AES-CCMP.

E. The authentication exchange prevents IV reuse by requiring a 48-bit packet number.

ANSWER: A B

Explanation:

Shared Key authentication uses a challenge-response exchange. The AP sends a challenge in plaintext, and the client returns the same challenge encrypted with the WEP key. An attacker who captures both values gains known plaintext and its corresponding RC4-encrypted form, which can reveal keystream information useful for attacking WEP.

Shared Key authentication authenticates the station to the AP, but it does not provide strong mutual authentication of the AP to the station. It is therefore vulnerable to impersonation and does not provide the protections expected from modern WPA2/WPA3 enterprise authentication methods.

QUESTION NO: 6

Given: WLAN attacks are typically conducted by hackers to exploit a specific vulnerability within a network.

What statement correctly pairs the type of WLAN attack with the exploited vulnerability? (Choose 3)

A. Management interface exploit attacks are attacks that use social engineering to gain credentials from managers.

B. Zero-day attacks are always authentication or encryption cracking attacks.

C. RF DoS attacks prevent successful wireless communication on a specific frequency or frequency range.

D. Hijacking attacks interrupt a user's legitimate connection and introduce a new connection with an evil twin AP.

E. Social engineering attacks are performed to collect sensitive information from unsuspecting users

F. Association flood attacks are Layer 3 DoS attacks performed against authenticated client stations

ANSWER: C D E

Explanation:

RF DoS attacks prevent successful wireless communication on a specific frequency or frequency range because they target the radio-frequency medium itself. Intentional interference or jamming raises the noise floor or occupies airtime, preventing stations from reliably transmitting and receiving frames in the affected channel or band. This is a wireless availability attack, and it can affect communications regardless of the higher-layer application in use. Hijacking attacks interrupt a user's legitimate connection and introduce a new connection with an evil twin AP because an attacker can use a convincingly named or configured rogue access point to lure a client away from its intended WLAN. Once the victim is connected through the attacker-controlled infrastructure, the attacker may observe, manipulate, or relay traffic. Social engineering attacks are performed to collect sensitive information from unsuspecting users because they exploit human trust and decision-making rather than a radio or protocol flaw. In WLAN environments, this can include convincing a user to reveal credentials, connect to an attacker-controlled network, or disclose information that enables later unauthorized access. These attack categories align with the availability, session/control, and human-security risks addressed in wireless-security guidance. See NIST SP 800-153: Guidelines for Securing WLANs and CISA guidance on social engineering and phishing.

QUESTION NO: 7

Given: A WLAN uses WPA2-Enterprise with 802.1X. A protocol capture shows EAP-MD5 authentication completing successfully and the RADIUS server returning an Access-Accept. However, the AP and client do not begin the 4-Way Handshake.

What is the most likely reason for this behavior?

A. EAP-MD5 does not generate the keying material required for the 4-Way Handshake.

B. EAP-MD5 requires TKIP rather than AES-CCMP as the data cipher.

C. The 4-Way Handshake is used only with WPA2-Personal authentication.

D. The RADIUS server must use LDAP rather than EAP-MD5 for the client identity store.

E. The client must receive a DHCP address before beginning the 4-Way Handshake.

ANSWER: A

Explanation:

EAP-MD5 does not generate the keying material required for IEEE 802.11 RSN key management. In an enterprise WLAN, successful EAP authentication must provide an MSK from which the PMK can be obtained. The PMK is then used by the AP and supplicant during the 4-Way Handshake to derive the PTK.

An Access-Accept alone does not guarantee that an EAP method is suitable for WPA2-Enterprise. EAP-MD5 is unsuitable because it lacks key derivation capability and does not provide mutual authentication.

QUESTION NO: 8

What protocols allow a network administrator to securely manage the configuration of WLAN controllers and access points? (Choose 2)

A. SNMPv1

B. HTTPS

C. Telnet

D. TFTP

E. FTP

F. SSHv2

ANSWER: B F

Explanation:

HTTPS and **SSHv2** provide secure administrative-management channels for WLAN controllers and access points because each protects management traffic in transit with authenticated encryption. HTTPS secures a controller or access point's web-based administrative interface by using HTTP over TLS. TLS provides confidentiality and integrity for the administrator's credentials, configuration changes, session cookies, and other web-management data, while also allowing the administrator to validate the device certificate. This makes HTTPS appropriate for securely managing devices through a browser-based GUI or a controller's web API.

SSHv2 is the current secure-shell protocol used for encrypted command-line administration. It supports server authentication and can use password authentication or public-key authentication for administrators. Its encrypted session protects CLI commands and returned configuration or status information from interception or modification on the management network. SSH is therefore a standard secure replacement for legacy plaintext remote terminal access when managing WLAN infrastructure through a CLI. For protocol details, see the IETF specifications for HTTP semantics and the SSH Transport Layer Protocol. In a CWSP-aligned design, administrators should use these encrypted management protocols together with strong authentication, trusted device certificates, role-based administrative access, and a properly segmented management network.

QUESTION NO: 9

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 individualshave 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. MS-CHAPv2 is subject to offline dictionary attacks.

C. LEAP's use of MS-CHAPv2 is only secure when combined with WEP.

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. When implemented with AES-CCMP encryption, MS-CHAPv2 is very secure.

ANSWER: B D

Explanation:

MS-CHAPv2 is subject to offline dictionary attacks because the protocol's challenge-response exchange can be captured by an attacker and used to make password guesses without interacting further with the authentication server. The practical security of the authentication therefore depends heavily on the entropy of the user password; weak or reused passwords can be recovered efficiently after capture. The protocol specification describes its challenge-response and password-hash-based operation in RFC 2759.

MS-CHAPv2 is only appropriate for WLAN security when used inside a TLS-encrypted tunnel. A TLS-protected EAP method, such as PEAP with EAP-MSCHAPv2 or EAP-TTLS with an appropriate inner method, protects the inner MS-CHAPv2 conversation from passive wireless capture and provides server authentication when clients correctly validate the server certificate. This substantially reduces exposure to credential-harvesting and rogue-authenticator attacks. Microsoft likewise notes that PEAP creates a protected TLS channel before carrying EAP authentication data; see Microsoft's PEAP and server-certificate guidance. Organizations should also enforce strong, unique passwords and certificate validation, since TLS tunneling complements rather than replaces sound credential policy.

QUESTION NO: 10

Given: AAA is an architectural framework used to provide three separate security components in a network. Listed below are three phrases that each describe one aspect of the AAA framework.

Option-1 — This AAA function is performed first and validates user identify prior to determining the network resources to which they will be granted access.

Option-2 — This function is used for monitoring and auditing purposes and includes the collection of data that identifies what a user has done while connected.

Option-3 — This function is used to designate permissions to a particular user.

What answer correctly pairs the AAA component with the descriptions provided above?

A. Option-1 – Access ControlOption-2 – AuthorizationOption-3 – Accounting

B. Option-1 – AuthenticationOption-2 – AccountingOption-3 – Association

C. Option-1 – AuthorizationOption-2 – Access ControlOption-3 – Association

D. Option-1 – AuthenticationOption-2 – AccountingOption-3 – Authorization

ANSWER: D

Explanation:

The correct pairing is “Option-1 – Authentication; Option-2 – Accounting; Option-3 – Authorization.” AAA is a security framework whose components are commonly applied in that sequence when a user attempts to obtain network access. Authentication occurs first: the network validates the identity claimed by the user or device, such as through credentials, a certificate, or an EAP-based authentication exchange. Establishing identity is essential before the network can make a policy decision about access.

After identity has been authenticated, authorization determines the permissions and network resources available to that authenticated identity. In enterprise Wi-Fi, an authorization decision can assign a VLAN, apply an access control list, set a role, or impose other policy attributes returned by an AAA server. Accounting records session-related activity for operational visibility, auditing, and reporting. Typical accounting information includes session start and stop times, session duration, bytes sent and received, and other usage details. This produces an auditable record of activity after access is granted. Cisco’s overview of AAA describes authentication, authorization, and accounting as the core functions of the AAA model: Cisco AAA Overview. RFC 2866 also specifies the RADIUS accounting model and accounting-record functions: RFC 2866.

QUESTION NO: 11

What are the three roles of the 802.1X framework, as defined by the 802.1X standard, that are performed by the client STA, the AP (or WLAN controller), and the RADIUS server? (Choose 3)

A. Enrollee

B. Registrar

C. AAA Server

D. Authentication Server

E. Supplicant

F. Authenticator

G. Control Point

ANSWER: D E F

Explanation:

The three 802.1X roles are **Supplicant**, **Authenticator**, and **Authentication Server**. The client station performs the supplicant role. It runs the 802.1X/EAP client functionality, responds to EAP requests, and supplies authentication credentials or proof of identity using the selected EAP method. The AP or WLAN controller performs the authenticator role. It controls access to the protected network, exchanges EAP over LAN traffic with the client, and encapsulates or relays EAP messages to the authentication server, commonly through RADIUS. Until authentication succeeds, the authenticator restricts the client to the uncontrolled port and prevents normal access to the protected network. The RADIUS server performs the authentication-server role. It validates the supplicant’s credentials according to the EAP method and identity store, then returns an accept or reject result and may provide authorization attributes and keying material. This separation is fundamental to enterprise WLAN access control: the wireless infrastructure enforces the access decision, while the centralized authentication service evaluates identity and credentials. The IEEE overview of 802.1X describes port-based network access control and the involved entities; CWNP’s CWSP certification materials also identify these core enterprise WLAN security concepts. See IEEE 802.1X standard information and CWNP CWSP certification.

QUESTION NO: 12

What information can RADIUS accounting provide to support WLAN security investigations and usage auditing? (Choose 2)

A. Session start and stop times for an authenticated connection

B. Usage information such as bytes sent and received during a session

C. The Pairwise Transient Key used to encrypt a client's unicast frames

D. The client private key used for EAP-TLS authentication

E. The GTK used to protect broadcast and multicast traffic

ANSWER: A B

Explanation:

RADIUS accounting records can identify when a wireless session started and stopped, which supports investigation of the period during which an authenticated identity was connected. Accounting records can also report session usage information, such as bytes sent and received, allowing administrators to review activity volume and correlate it with other network logs.

RADIUS accounting does not itself authenticate the user or derive the pairwise encryption keys used by the WLAN. Those functions are performed through authentication and RSN key-management processes.

QUESTION NO: 13

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. RF DoS and/or physical theft

C. MAC denial of service and/or physical theft

D. Authentication cracking and/or RF DoS

E. Code injection and/or XSS

ANSWER: A

Explanation:

Social engineering and/or eavesdropping is correct because both techniques can directly lead to the disclosure or capture of a legitimate hotspot user's credentials. Social engineering targets the human user rather than wireless cryptography; for example, an attacker can impersonate hotspot support staff, present a deceptive captive portal, or persuade a user to reveal a password or enter it into an attacker-controlled site. This is especially relevant in public-access environments, where users may have limited ability to verify the network operator or portal's identity.

Eavesdropping involves passively observing traffic or related user activity. If credentials are transmitted without effective transport-layer protection, or if a user is induced to use an unprotected or malicious service, captured communications may expose reusable credentials or authentication material. Public Wi-Fi security guidance emphasizes that open networks present interception risks and that users should protect sensitive communications with properly authenticated encryption. In CWSP security analysis, these are recognized credential-acquisition threats because they focus on obtaining valid user authentication information without requiring direct authorization.

See CWNP's CWSP certification overview and NIST's Guidelines for Securing Wireless Local Area Networks for wireless threat and protection context.