Vendor: CWNP

Exam Code: CWSP-208

Exam Name: Certified Wireless Security Professional (CWSP)

Version: DEMO

QUESTION 1
As part of your penetration testing procedure, you want to discover extensive details about all wireless access points within radio range of your testing device. What is the best way to view this information?

A. Portable wireless scanner
B. Access to the hardware abstraction layer
C. A wireless spectrum analyzer
D. Built-in wireless adapter drivers

Answer: A
Explanation:
A portable wireless scanner (device + scanning software) captures management frames and displays comprehensive details for every AP in range - SSID, BSSID, channel, RSSI, security/capability fields, and beacon/probe information - which is exactly what's needed for extensive discovery.

QUESTION 2
What security mechanism correctly describes a password-authenticated key exchange based on a zero-knowledge proof?

A. Simultaneous authentication of equals (SAE)
B. Pre-robust security network association (pre-RSNA)
C. EAPOL-Key encryption key (KEK)
D. Preshared key (PSK) authentication

Answer: A
Explanation:
Simultaneous Authentication of Equals (SAE) is a password-authenticated key exchange protocol that uses zero-knowledge proofs to securely establish cryptographic keys without revealing the password during the authentication process.

QUESTION 3
Wireless security policy enforcement can be provided by what method that is available for use with any Wi-Fi networking solution?

A. Network access control (NAC)
B. Opportunistic key caching (OKC)
C. Cyclic redundancy check (CRC)
D. Lightweight directory access protocol (LDAP)

Answer: A
Explanation:
Network Access Control (NAC) enforces wireless security policies by evaluating devices before granting network access. It can be applied across any Wi-Fi solution to ensure compliance with organizational security requirements.

QUESTION 4
When a user, trusted or otherwise, leaves the organization, what minimum task should be performed on your PSK network?

A. Revoke and re-issue all certificates
B. Upgrade to an 802.1X solution
C. Change the passphrase on all devices
D. Change the SSIDs

Answer: C
Explanation:
In a PSK (preshared key) network, when a user leaves, the shared passphrase must be changed on all devices to prevent the former user from accessing the network, maintaining security.

QUESTION 5
What is provided to stations connecting to APs when both support 802.11k?

A. A TCP-GRE tunnel for the data plane
B. An encrypted authentication tunnel
C. A neighboring AP list
D. An exchange of TxOP requirements

Answer: C
Explanation:
802.11k enables access points to provide a list of neighboring APs to client devices. This helps clients make informed roaming decisions, improving handoff efficiency and overall network performance.

QUESTION 6
What policy would help to mitigate the impact of peer-to-peer attacks against wireless-enabled corporate laptop computers when the laptops are also used on public access networks such as wireless hotspots?

A. Require VPN software for connectivity on public access networks
B. Require Port Address Translation (PAT) for all laptops connecting to public access networks
C. Require the use of HTTP for all communications so that they are encrypted
D. Require that public access networks implement WPA3 in the standard

Answer: A
Explanation:
Requiring VPN software for connectivity on public networks ensures that all data transmitted from corporate laptops is encrypted and protected, mitigating the risk of peer-to-peer attacks and eavesdropping on untrusted networks.

QUESTION 7
What administration component connected with wireless networks can be used in all systems supporting it to provide access and authorization based on individual groups, departments, users and possibly other parameters?

A. Discretionary access control (DAC)
B. Access control list (ACL)
C. Role based access control (RBAC)
D. Mandatory access control (MAC)

Answer: C
Explanation:
Role-Based Access Control (RBAC) assigns permissions and access rights based on user roles, groups, or departments. In wireless networks, RBAC allows centralized administration of access and authorization across multiple systems consistently.

QUESTION 8
You were hired as a contractor to assist with installation and support of a new enterprise wireless deployment. You have been assigned the task of ensuring the organization has up-to-date information about potential threats to the network infrastructure and all client device types. Which one of the following is the best way to ensure that you have the most up-to-date information?

A. Search the CVE database and run reports
B. Search and subscribe to various security blogs
C. Contact the WLAN manufacturers support team
D. Subscribe to the local regulatory agency's daily newsletter

Answer: A
Explanation:
The Common Vulnerabilities and Exposures (CVE) database provides authoritative, up-to-date information on known vulnerabilities affecting hardware and software. Searching and running reports from CVE ensures timely awareness of threats to both network infrastructure and client devices.

QUESTION 9
After a successful open authentication and association, to which device is a wireless client allowed to communicate prior to full 802.1X/EAP authentication?

A. The RADIUS server
B. The user database
C. The authentication server
D. The authenticator

Answer: D
Explanation:
Before full 802.1X/EAP authentication, a wireless client can only communicate with the authenticator (typically the access point). The authenticator controls access to the network and mediates the authentication process with the authentication server.

QUESTION 10
What term best describes a type of information technology threat that is usually in the form of an executable program that masquerades as a real program and is designed to perform malicious tasks when executed on the wireless client device as the result of a wireless social engineering attack?

A. Jailbreaking
B. Trojan
C. Worm
D. Rooting

Answer: B

Explanation:
A Trojan is a malicious program disguised as legitimate software. When executed, it performs unauthorized actions on the client device, often introduced through social engineering attacks over wireless networks.

QUESTION 11
What standard WLAN client device behavior can be exploited by an attacker during a hijacking attack?

A. 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.
B. When the RF signal between a client and an access point is disrupted, the client device will attempt to associate to an access point with better signal quality.
C. Client drivers scan for and connect to access points in the 2.4 GHz band before scanning the 5 GHz band.
D. As specified by the Wi-Fi Alliance, clients using Open System authentication must allow direct client-to-client connections, even in an infrastructure BSS.

Answer: B
Explanation:
In a hijacking attack, an attacker exploits the client's behavior of roaming to access points with stronger signals when connectivity drops. This allows the attacker to lure the client to a malicious AP, potentially intercepting or manipulating traffic.

QUESTION 12
When an attacker uses an AP with the same SSID or BSSID as your production network, what type of attack are they conducting?

A. Brute force
B. Evil Twin
C. Eavesdropping
D. ARP poisoning

Answer: B
Explanation:
An attacker using an AP with the same SSID or BSSID as a legitimate network is conducting an Evil Twin attack. This tricks clients into connecting to the malicious AP, allowing the attacker to intercept or manipulate network traffic.

QUESTION 13
How does Opportunistic Wireless Encryption (OWE) improve open or public network security?

A. It uses a cryptographic algorithm to encrypt user credentials when connecting to WPA3 supported hotspots.
B. It listens to see which encryption methods are being used on your network and predictively configures it on the clients.
C. It allows the client to negotiate which encryption method it will use when connecting, allowing multiple encryption types to be used in the same service set, including WPA, WPA2, and WPA3.
D. It uses a cryptographic handshake to encrypt traffic of devices connecting to open network access points.

Answer: D
Explanation:
Opportunistic Wireless Encryption (OWE) enhances security on open/public networks by performing a cryptographic handshake between the client and AP, establishing unique encryption keys for each session. This protects user traffic even without authentication.

QUESTION 14
What is a false statement regarding a robust security network association (RSNA)?

A. Disallows the use of WEP
B. Support for CCMP
C. Disallows the use of RC4
D. Allows for PSK implementation

Answer: C
Explanation:
RSNA does not explicitly disallow RC4; rather, it disallows weak ciphers such as WEP and promotes the use of strong encryption like CCMP (AES). RC4 may still be used in legacy WPA, but RSNA focuses on robust security implementations.

QUESTION 15
What metric defines the aggregate expected loss from a risk occurrence in a year?

A. SLE
B. DDE
C. ALE
D. ARO

Answer: C
Explanation:
The Annualized Loss Expectancy (ALE) estimates the total expected financial loss from a specific risk over a year, calculated by multiplying the Single Loss Expectancy (SLE) by the Annualized Rate of Occurrence (ARO).

QUESTION 16
You use a web-based administration interface to administer the WLAN controllers on your network. What should always be disabled in this implementation to ensure secure management practices?

A. HTTP
B. HTTPS
C. SSH
D. TLS

Answer: A
Explanation:
HTTP transmits data, including credentials, in clear text. Disabling HTTP and using HTTPS ensures that management traffic is encrypted, protecting the confidentiality and integrity of administrative sessions.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**