CWSP-205 Q&As

Certified Wireless Security Professional

Pass CWNP CWSP-205 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/cwsp-205.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CWNP Official Exam Center

QUESTION 1

What wireless authentication technologies may build a TLS tunnel between the supplicant and the authentication server before passing client authentication credentials to the authentication server? (Choose 3)

A. EAP-MD5

B. EAP-TLS

C. LEAP

D. PEAPv0/MSCHAPv2

E. EAP-TTLS

Correct Answer: BDE

QUESTION 2

The IEEE 802.11 Pairwise Transient Key (PTK) is derived from what cryptographic element?

A. Phase Shift Key (PSK)

B. Group Master Key (GMK)

C. Pairwise Master Key (PMK)

D. Group Temporal Key (GTK)

E. PeerKey (PK)

F. Key Confirmation Key (KCK)

Correct Answer: C

QUESTION 3

What security benefits are provided by endpoint security solution software? (Choose 3)

A. Can prevent connections to networks with security settings that do not conform to company policy

B. Can collect statistics about a user\\'s network use and monitor network threats while they are connected

C. Can restrict client connections to networks with specific SSIDs and encryption types

D. Can be used to monitor for and prevent network attacks by nearby rogue clients or APs

Correct Answer: ABC

QUESTION 4

What drawbacks initially prevented the widespread acceptance and use of Opportunistic Key Caching (OKC)?

A. Sharing cached keys between controllers during inter-controller roaming created vulnerabilities that exposed the keys to attackers.

B. Because OKC is not defined by any standards or certification body, client support was delayed and sporadic early on.

C. Key exchanges during fast roams required processor-intensive cryptography, which was prohibitive for legacy devices supporting only TKIP.

D. The Wi-Fi Alliance continually delayed the creation of a client certification for OKC, even though it was defined by IEEE 802.11r.

Correct Answer: B

QUESTION 5

Given: Many corporations configure guest VLANs on their WLAN controllers that allow visitors to have Internet access only. The guest traffic is tunneled to the DMZ to prevent some security risks.

In this deployment, what risks are still associated with implementing the guest VLAN without any advanced traffic monitoring or filtering features enabled? (Choose 2)

A. Intruders can send spam to the Internet through the guest VLAN.

B. Peer-to-peer attacks can still be conducted between guest users unless application-layer monitoring and filtering are implemented.

C. Unauthorized users can perform Internet-based network attacks through the WLAN.

D. Guest users can reconfigure AP radios servicing the guest VLAN unless unsecure network management protocols (e.g. Telnet, HTTP) are blocked.

E. Once guest users are associated to the WLAN, they can capture 802.11 frames from the corporate VLANs.

Correct Answer: AC

QUESTION 6

Given: When the CCMP cipher suite is used for protection of data frames, 16 bytes of overhead are added to the Layer 2 frame. 8 of these bytes comprise the MIC.

What purpose does the encrypted MIC play in protecting the data frame?

A. The MIC is used as a first layer of validation to ensure that the wireless receiver does not incorrectly process corrupted signals.

B. The MIC provides for a cryptographic integrity check against the data payload to ensure that it matches the original transmitted data.

C. The MIC is a hash computation performed by the receiver against the MAC header to detect replay attacks prior to processing the encrypted payload.

D. The MIC is a random value generated during the 4-way handshake and is used for key mixing to enhance the strength of the derived PTK.

Correct Answer: B

QUESTION 7

A single AP is configured with three separate WLAN profiles, as follows:

1.

SSID: ABCData BSSID: 00:11:22:00:1F:C3 VLAN 10 Security: PEAPv0/EAP- MSCHAPv2 with AESCCMP 3 current clients

2.

SSID: ABCVoice BSSID: 00:11:22:00:1F:C4 VLAN 60 Security: WPA2-Personal with AES-CCMP 2 current clients

3.

SSID: Guest BSSID: 00:11:22:00:1F:C5 VLAN 90 Security: Open with captive portal authentication 3 current clients Three STAs are connected to ABCData. Three STAs are connected to Guest. Two STAs are connected to ABCVoice.

How many unique GTKs and PTKs are currently in place in this scenario?

A. 1 GTK 8 PTKs

B. 2 GTKs 5 PTKs

C. 2 GTKs 8 PTKs

D. 3 GTKs 8 PTKs

Correct Answer: B

QUESTION 8

What software and hardware tools are used together to hijack a wireless station from the authorized wireless network onto an unauthorized wireless network? (Choose 2)

A. RF jamming device and a wireless radio card

B. A low-gain patch antenna and terminal emulation software

C. A wireless workgroup bridge and a protocol analyzer

D. DHCP server software and access point software

E. MAC spoofing software and MAC DoS software

Correct Answer: AD

QUESTION 9

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. 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.

C. 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.

D. As specified by the Wi-Fi Alliance, clients using Open System authentication must allow direct client-toclient connections, even in an infrastructure BSS.

E. Client drivers scan for and connect to access points in the 2.4 GHz band before scanning the 5 GHz band.

Correct Answer: A

QUESTION 10

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

Correct Answer: CDE

QUESTION 11

Given: One of the security risks introduced by WPA2-Personal is an attack conducted by an authorized network user who knows the passphrase. In order to decrypt other users\\' traffic, the attacker must obtain certain information from the 4-way handshake of the other users.

In addition to knowing the Pairwise Master Key (PMK) and the supplicant\\'s address (SA), what other three inputs must be collected with a protocol analyzer to recreate encryption keys? (Choose 3)

A. Authenticator nonce

B. Supplicant nonce

C. Authenticator address (BSSID)

D. GTKSA

E. Authentication Server nonce

Correct Answer: ABC

QUESTION 12

You are using a protocol analyzer for random checks of activity on the WLAN. In the process, you notice two different EAP authentication processes. One process (STA1) used seven EAP frames (excluding ACK frames) before the 4-way handshake and the other (STA2) used 11 EAP frames (excluding ACK frames) before the 4-way handshake.

Which statement explains why the frame exchange from one STA required more frames than the frame exchange from another STA when both authentications were successful? (Choose the single most probable answer given a stable WLAN.)

A. STA1 and STA2 are using different cipher suites.

B. STA2 has retransmissions of EAP frames.

C. STA1 is a reassociation and STA2 is an initial association.

D. STA1 is a TSN, and STA2 is an RSN.

E. STA1 and STA2 are using different EAP types.

Correct Answer: E

QUESTION 13

While seeking the source of interference on channel 11 in your 802.11n WLAN running within 2.4 GHz, you notice a signal in the spectrum analyzer real time FFT display. The signal is characterized with the greatest strength utilizing only 1-2 megahertz of bandwidth and it does not use significantly more bandwidth until it has weakened by roughly 20 dB. At approximately -70 dB, it spreads across as much as 35 megahertz of bandwidth.

What kind of signal is described?

A. A high-power, narrowband signal

B. A 2.4 GHz WLAN transmission using transmit beam forming

C. An HT-OFDM access point

D. A frequency hopping wireless device in discovery mode

E. A deauthentication flood from a WIPS blocking an AP

F. A high-power ultra wideband (UWB) Bluetooth transmission

Correct Answer: A

QUESTION 14

Given: A network security auditor is preparing to perform a comprehensive assessment of an 802.11ac network\\'s security.

What task should be performed at the beginning of the audit to maximize the auditor\\'s ability to expose network vulnerabilities?

A. Identify the IP subnet information for each network segment.

B. Identify the manufacturer of the wireless intrusion prevention system.

C. Identify the skill level of the wireless network security administrator(s).

D. Identify the manufacturer of the wireless infrastructure hardware.

E. Identify the wireless security solution(s) currently in use.

Correct Answer: E

QUESTION 15

Given: ABC Company has 20 employees and only needs one access point to cover their entire facility. Ten of ABC Company\\'s employees have laptops with radio cards capable of only WPA security. The other ten employees have laptops with radio cards capable of WPA2 security. The network administrator wishes to secure all wireless communications (broadcast and unicast) for each laptop with its strongest supported security mechanism, but does not wish to implement a RADIUS/AAA server due to complexity.

What security implementation will allow the network administrator to achieve this goal?

A. Implement an SSID with WPA2-Personal that allows both AES-CCMP and TKIP clients to connect.

B. Implement an SSID with WPA-Personal that allows both AES-CCMP and TKIP clients to connect.

C. Implement two separate SSIDs on the AP--one for WPA-Personal using TKIP and one for WPA2Personal using AES-CCMP.

D. Implement an SSID with WPA2-Personal that sends all broadcast traffic using AES-CCMP and unicast traffic using either TKIP or AES-CCMP.

Correct Answer: C