CWSP-205Q&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.certbus.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

Given: An 802.1X/EAP implementation includes an Active Directory domain controller running Windows Server 2012 and an AP from a major vendor. A Linux server is running RADIUS and it queries the domain controller for user credentials. A Windows client is accessing the network.

What device functions as the EAP Supplicant?

A. Linux server

B. Windows client

C. Access point

D. Windows server

E. An unlisted switch

F. An unlisted WLAN controller

Correct Answer: B

QUESTION 2

What statement is true regarding the nonces (ANonce and SNonce) used in the IEEE 802.11 4 Way Handshake?

A. Both nonces are used by the Supplicant and Authenticator in the derivation of a single PTK.

B. The Supplicant uses the SNonce to derive its unique PTK and the Authenticator uses the ANonce to derive its unique PTK, but the nonces are not shared.

C. Nonces are sent in EAPoL frames to indicate to the receiver that the sending station has installed and validated the encryption keys.

D. The nonces are created by combining the MAC addresses of the Supplicant, Authenticator, and Authentication Server into a mixing algorithm.

Correct Answer: A

QUESTION 3

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

A. Configuration distribution for autonomous APs

B. Wireless vulnerability assessment

C. Application-layer traffic inspection

D. Analysis and reporting of AP CPU utilization

E. Policy enforcement and compliance management

Correct Answer: BE

QUESTION 4

Given: ABC Company secures their network with WPA2-Personal authentication and AES- CCMP encryption.

What part of the 802.11 frame is always protected from eavesdroppers by this type of security?

A. All MSDU contents

B. All MPDU contents

C. All PPDU contents

D. All PSDU contents

Correct Answer: A

QUESTION 5

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. 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.

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. 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.

Correct Answer: B

QUESTION 6

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 7

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 8

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. Authorized PEAP usernames must be added to the WIPS server\\'s user database.

B. WLAN devices that are discovered must be classified (rogue, authorized, neighbor, etc.) and a WLAN policy must define how to classify new devices.

C. Separate security profiles must be defined for network operation in different regulatory domains

D. Upstream and downstream throughput thresholds must be specified to ensure that service- level agreements are being met.

Correct Answer: B

QUESTION 9

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. 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.

B. 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.

C. An unauthorized wireless client device cannot associate, but can eavesdrop on some data because WPA2-Personal does not encrypt multicast or broadcast traffic.

D. 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.

E. Because WPA2-Personal uses Open System authentication followed by a 4-Way Handshake, hijacking attacks are easily performed.

Correct Answer: B

QUESTION 10

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 11

Given: ABC Corporation\\'s 802.11 WLAN is comprised of a redundant WLAN controller pair (N+1) and 30 access points implemented in 2004. ABC implemented WEP encryption with IPSec VPN technology to secure their wireless communication because it was the strongest security solution available at the time it was implemented. IT management has decided to upgrade the WLAN infrastructure and implement Voice over Wi-Fi and is concerned with security because most Voice over Wi-Fi phones do not support IPSec.

As the wireless network administrator, what new security solution would be best for protecting ABC\\'s data?

A. Migrate corporate data clients to WPA-Enterprise and segment Voice over Wi-Fi phones by assigning them to a different frequency band.

B. Migrate corporate data and Voice over Wi-Fi devices to WPA2-Enterprise with fast secure roaming support, and segment Voice over Wi-Fi data on a separate VLAN.

C. Migrate to a multi-factor security solution to replace IPSec; use WEP with MAC filtering, SSID hiding, stateful packet inspection, and VLAN segmentation.

D. Migrate all 802.11 data devices to WPA-Personal, and implement a secure DHCP server to allocate addresses from a segmented subnet for the Voice over Wi-Fi phones.

Correct Answer: B

QUESTION 12

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 13

Given: The Marketing department\\'s WLAN users need to reach their file and email server as well as the Internet, but should not have access to any other network resources.

What single WLAN security feature should be implemented to comply with these requirements?

A. Mutual authentication

B. Captive portal

C. Role-based access control

D. Group authentication

E. RADIUS policy accounting

Correct Answer: C

QUESTION 14

Given: A WLAN consultant has just finished installing a WLAN controller with 15 controller- based APs.

Two SSIDs with separate VLANs are configured for this network, and both VLANs are configured to use

the same RADIUS server. The SSIDs are configured as follows:

SSID Blue - VLAN 10 - Lightweight EAP (LEAP) authentication - CCMP cipher suite SSID Red - VLAN 20 PEAPv0/EAP-TLS authentication - TKIP cipher suite The consultant\\'s computer can successfully

authenticate and browse the Internet when using the Blue SSID. The same computer cannot authenticate

when using the Red SSID.

What is a possible cause of the problem?

A. The Red VLAN does not use server certificate, but the client requires one.

B. The TKIP cipher suite is not a valid option for PEAPv0 authentication.

C. The client does not have a proper certificate installed for the tunneled authentication within the established TLS tunnel.

D. The consultant does not have a valid Kerberos ID on the Blue VLAN.

Correct Answer: C

QUESTION 15

Given: A large enterprise is designing a secure, scalable, and manageable 802.11n WLAN that will support thousands of users. The enterprise will support both 802.1X/EAP-TTLS and PEAPv0/MSCHAPv2. Currently, the company is upgrading network servers as well and will replace their existing Microsoft IAS implementation with Microsoft NPS, querying Active Directory for user authentication.

For this organization, as they update their WLAN infrastructure, what WLAN controller feature will likely be least valuable?

A. WPA2-Enterprise authentication/encryption

B. Internal RADIUS server

C. WIPS support and integration

D. 802.1Q VLAN trunking

E. SNMPv3 support

Correct Answer: B