CWSP-205Q&As

Certified Wireless Security Professional

Pass CWNP CWSP-205 Exam with 100% Guarantee

QUESTION 1

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 2

You have an AP implemented that functions only using 802.11-2012 standard methods for the WLAN communications on the RF side and implementing multiple SSIDs and profiles on the management side configured as follows:

1.

SSID: Guest VLAN 90 Security: Open with captive portal authentication 2 current clients

2.

SSID: ABCData VLAN 10 Security: PEAPv0/EAP-MSCHAPv2 with AES-CCMP 5 current clients

3.

SSID: ABCVoice VLAN 60 Security: WPA2-Personal 2 current clients

Two client STAs are connected to ABCData and can access a media server that requires authentication at the Application Layer and is used to stream multicast video streams to the clients.

What client stations possess the keys that are necessary to decrypt the multicast data packets carrying these videos?

A. Only the members of the executive team that are part of the multicast group configured on the media server

B. All clients that are associated to the AP using the ABCData SSID

C. All clients that are associated to the AP using any SSID

D. All clients that are associated to the AP with a shared GTK, which includes ABCData and ABCVoice.

Correct Answer: B

QUESTION 3

What is the purpose of the Pairwise Transient Key (PTK) in IEEE 802.11 Authentication and Key Management?

A. The PTK is a type of master key used as an input to the GMK, which is used for encrypting multicast data frames.

B. The PTK contains keys that are used to encrypt unicast data frames that traverse the wireless medium.

C. The PTK is XOR\\'d with the PSK on the Authentication Server to create the AAA key.

D. The PTK is used to encrypt the Pairwise Master Key (PMK) for distribution to the 802.1X Authenticator prior to the 4-Way Handshake.

Correct Answer: B

QUESTION 4

Given: Many computer users connect to the Internet at airports, which often have 802.11n access points with a captive portal for authentication.

While using an airport hot-spot with this security solution, to what type of wireless attack is a user susceptible? (Choose 2)

A. Man-in-the-Middle

B. Wi-Fi phishing

C. Management interface exploits

D. UDP port redirection

E. IGMP snooping

Correct Answer: AB

QUESTION 5

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 6

You are implementing an 802.11ac WLAN and a WIPS at the same time. You must choose between integrated and overlay WIPS solutions. Which of the following statements is true regarding integrated WIPS solutions?

A. Integrated WIPS always perform better from a client throughput perspective because the same radio that performs the threat scanning also services the clients.

B. Integrated WIPS use special sensors installed alongside the APs to scan for threats.

C. Many integrated WIPS solutions that detect Voice over Wi-Fi traffic will cease scanning altogether to accommodate the latency sensitive client traffic.

D. Integrated WIPS is always more expensive than overlay WIPS.

Correct Answer: C

QUESTION 7

What security vulnerabilities may result from a lack of staging, change management, and installation procedures for WLAN infrastructure equipment? (Choose 2)

A. The WLAN system may be open to RF Denial-of-Service attacks

B. WIPS may not classify authorized, rogue, and neighbor APs accurately

C. Authentication cracking of 64-bit Hex WPA-Personal PSK

D. Management interface exploits due to the use of default usernames and passwords for AP management

E. AES-CCMP encryption keys may be decrypted

Correct Answer: BD

QUESTION 8

In the basic 4-way handshake used in secure 802.11 networks, what is the purpose of the ANonce and SNonce? (Choose 2)

A. They are used to pad Message 1 and Message 2 so each frame contains the same number of bytes.

B. The IEEE 802.11 standard requires that all encrypted frames contain a nonce to serve as a Message Integrity Check (MIC).

C. They are added together and used as the GMK, from which the GTK is derived.

D. They are input values used in the derivation of the Pairwise Transient Key.

E. They allow the participating STAs to create dynamic keys while avoiding sending unicast encryption keys across the wireless medium.

Correct Answer: DE

QUESTION 9

Given: XYZ Company has recently installed an 802.11ac WLAN. The company needs the ability to control access to network services, such as file shares, intranet web servers, and Internet access based on an employee\\'s job responsibilities.

What WLAN security solution meets this requirement?

A. An autonomous AP system with MAC filters

B. WPA2-Personal with support for LDAP queries

C. A VPN server with multiple DHCP scopes

D. A WLAN controller with RBAC features

E. A WLAN router with wireless VLAN support

Correct Answer: D

QUESTION 10

You must locate non-compliant 802.11 devices. Which one of the following tools will you use and why?

A. A spectrum analyzer, because it can show the energy footprint of a device using WPA differently from a device using WPA2.

B. A spectrum analyzer, because it can decode the PHY preamble of a non-compliant device.

C. A protocol analyzer, because it can be used to view the spectrum energy of non-compliant 802.11 devices, which is always different from compliant devices.

D. A protocol analyzer, because it can be used to report on security settings and regulatory or rule compliance

Correct Answer: D

QUESTION 11

Role-Based Access Control (RBAC) allows a WLAN administrator to perform what network function?

A. Minimize traffic load on an AP by requiring mandatory admission control for use of the Voice access category.

B. Allow access to specific files and applications based on the user\\'s WMM access category.

C. Provide two or more user groups connected to the same SSID with different levels of network privileges.

D. Allow simultaneous support for multiple EAP types on a single access point.

Correct Answer: C

QUESTION 12

Given: You are installing 6 APs on the outside of your facility. They will be mounted at a height of 6 feet. What must you do to implement these APs in a secure manner beyond the normal indoor AP implementations? (Choose the single best answer.)

A. User external antennas.

B. Use internal antennas.

C. Power the APs using PoE.

D. Ensure proper physical and environmental security using outdoor ruggedized APs or enclosures.

Correct Answer: D

QUESTION 13

A WLAN is implemented using WPA-Personal and MAC filtering.

To what common wireless network attacks is this network potentially vulnerable? (Choose 3)

A. Offline dictionary attacks

B. MAC Spoofing

C. ASLEAP

D. DoS

Correct Answer: ABD

QUESTION 14

Given: Fred works primarily from home and public wireless hot-spots rather than commuting to the office. He frequently accesses the office network remotely from his Mac laptop using the local 802.11 WLAN.

In this remote scenario, what single wireless security practice will provide the greatest security for Fred?

A. Use an IPSec VPN for connectivity to the office network

B. Use only HTTPS when agreeing to acceptable use terms on public networks

C. Use enterprise WIPS on the corporate office network

D. Use WIPS sensor software on the laptop to monitor for risks and attacks

E. Use 802.1X/PEAPv0 to connect to the corporate office network from public hot-spots

F. Use secure protocols, such as FTP, for remote file transfers.

Correct Answer: A

QUESTION 15

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

CWSP-205 PDF Dumps CWSP-205 Exam Questions CWSP-205 Braindumps