Vendor: CWNP

Exam Code: PW0-205

Exam Name: Certified Wireless Security Professional (CWSP)

Version: DEMO

QUESTION 1
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: CDE

QUESTION 2
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

Answer: ABC

QUESTION 3
You perform a protocol capture using Wireshark and a compatible 802.11 adapter in Linux. When viewing the capture, you see an auth req frame and an auth rsp frame. Then you see an assoc req frame and an assoc rsp frame. Shortly after, you see DHCP communications and then ISAKMP protocol packets. What security solution is represented?

A. 802.1X/EAP-TTLS
B. Open 802.11 authentication with IPSec
C. 802.1X/PEAPv0/MS-CHAPv2
D. WPA2-Personal with AES-CCMP
E. EAP-MD5

Answer: B

QUESTION 4
Given: In a security penetration exercise, a WLAN consultant obtains the WEP key of XYZ

Corporation's wireless network. Demonstrating the vulnerabilities of using WEP, the consultant uses a laptop running a software AP in an attempt to hijack the authorized user's connections.
XYZ's legacy network is using 802.11n APs with 802.11b, 11g, and 11n client devices.
With this setup, how can the consultant cause all of the authorized clients to establish Layer 2 connectivity with the software access point?

A. All WLAN clients will reassociate to the consultant's software AP if the consultant's software AP provides the same SSID on any channel with a 10 dB SNR improvement over the authorized AP.
B. A higher SSID priority value configured in the Beacon frames of the consultant's software AP will take priority over the SSID in the authorized AP, causing the clients to reassociate.
C. When the RF signal between the clients and the authorized AP is temporarily disrupted and the consultant's software AP is using the same SSID on a different channel than the authorized AP, the clients will reassociate to the software AP.
D. If the consultant's software AP broadcasts Beacon frames that advertise 802.11g data rates that are faster rates than XYZ's current 802.11b data rates, all WLAN clients will reassociate to the faster AP.

Answer: C

QUESTION 5
What elements should be addressed by a WLAN security policy? (Choose 2)

A. Enabling encryption to prevent MAC addresses from being sent in clear text
B. How to prevent non-IT employees from learning about and reading the user security policy
C. End-user training for password selection and acceptable network use
D. The exact passwords to be used for administration interfaces on infrastructure devices
E. Social engineering recognition and mitigation techniques

Answer: CE

QUESTION 6
As a part of a large organization's security policy, how should a wireless security professional address the problem of rogue access points?

A. Use a WPA2-Enterprise compliant security solution with strong mutual authentication and encryption for network access of corporate devices.
B. Hide the SSID of all legitimate APs on the network so that intruders cannot copy this parameter on rogue APs.
C. Conduct thorough manual facility scans with spectrum analyzers to detect rogue AP RF signatures.
D. A trained employee should install and configure a WIPS for rogue detection and response measures.
E. Enable port security on Ethernet switch ports with a maximum of only 3 MAC addresses on each port.

Answer: D

QUESTION 7
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

Answer: D

QUESTION 8
Given: Your network includes a controller-based WLAN architecture with centralized data forwarding. The AP builds an encrypted tunnel to the WLAN controller. The WLAN controller is uplinked to the network via a trunked 1 Gbps Ethernet port supporting all necessary VLANs for management, control, and client traffic.
What processes can be used to force an authenticated WLAN client's data traffic into a specific VLAN as it exits the WLAN controller interface onto the wired uplink? (Choose 3)

A. On the Ethernet switch that connects to the AP, configure the switch port as an access port (not trunking) in the VLAN of supported clients.
B. During 802.1X authentication, RADIUS sends a return list attribute to the WLAN controller assigning the user and all traffic to a specific VLAN.
C. In the WLAN controller's local user database, create a static username-to-VLAN mapping on the WLAN controller to direct data traffic from a specific user to a designated VLAN.
D. Configure the WLAN controller with static SSID-to-VLAN mappings; the user will be assigned to a VLAN according to the SSID being used.

Answer: BCD

QUESTION 9
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.

Answer: B

QUESTION 10
Which one of the following describes the correct hierarchy of 802.1X authentication key derivation?

A. The MSK is generated from the 802.1X/EAP authentication. The PMK is derived from the MSK. The PTK is derived from the PMK, and the keys used for actual data encryption are a part of the PTK.

B. If passphrase-based client authentication is used by the EAP type, the PMK is mapped directly from the user's passphrase. The PMK is then used during the 4-way handshake to create data encryption keys.
C. After successful EAP authentication, the RADIUS server generates a PMK. A separate key, the MSK, is derived from the AAA key and is hashed with the PMK to create the PTK and GTK.
D. The PMK is generated from a successful mutual EAP authentication. When mutual authentication is not used, an MSK is created. Either of these two keys may be used to derive the temporal data encryption keys during the 4-way handshake.

Answer: A

QUESTION 11
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.

Answer: A

QUESTION 12
When using the 802.1X/EAP framework for authentication in 802.11 WLANs, why is the 802.1X Controlled Port still blocked after the 802.1X/EAP framework has completed successfully?

A. The 802.1X Controlled Port is always blocked, but the Uncontrolled Port opens after the EAP authentication process completes.
B. The 802.1X Controlled Port remains blocked until an IP address is requested and accepted by the Supplicant.
C. The 4-Way Handshake must be performed before the 802.1X Controlled Port changes to the unblocked state.
D. The 802.1X Controlled Port is blocked until Vender Specific Attributes (VSAs) are exchanged inside a RADIUS packet between the Authenticator and Authentication Server.

Answer: C

QUESTION 13
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

Answer: A

QUESTION 14
When TKIP is selected as the pairwise cipher suite, what frame types may be protected with data confidentiality? (Choose 2)

A. Robust broadcast management
B. Robust unicast management
C. Control
D. Data
E. ACK
F. QoS Data

Answer: DF

QUESTION 15
What statements are true about 802.11-2012 Protected Management Frames? (Choose 2)

A. 802.11w frame protection protects against some Layer 2 denial-of-service (DoS) attacks, but it cannot prevent all types of Layer 2 DoS attacks.
B. When frame protection is in use, the PHY preamble and header as well as the MAC header are encrypted with 256- or 512-bit AES.
C. Authentication, association, and acknowledgment frames are protected if management frame protection is enabled, but deauthentication and disassociation frames are not.
D. Management frame protection protects disassociation and deauthentication frames.

Answer: AD

Thank You for Trying Our Product

Braindump2go 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.braindump2go.com/all-products.html

10% Discount Coupon Code: BDNT2014