Vendor:CWNP

Exam Code:CWSP-205

Exam Name: Certified Wireless Security Professional

Version: Demo

QUESTION 1

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

QUESTION 2

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

QUESTION 3

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 4

Given: During 802.1X/LEAP authentication, the username is passed across the wireless medium in clear text.

From a security perspective, why is this significant?

A. The username is needed for Personal Access Credential (PAC) and X.509 certificate validation.

B. The username is an input to the LEAP challenge/response hash that is exploited, so the username must be known to conduct authentication cracking.

C. 4-Way Handshake nonces are based on the username in WPA and WPA2 authentication.

D. The username can be looked up in a dictionary file that lists common username/password combinations.

Correct Answer: B

QUESTION 5

In the IEEE 802.11-2012 standard, what is the purpose of the 802.1X Uncontrolled Port?

A. To allow only authentication frames to flow between the Supplicant and Authentication Server

B. To block authentication traffic until the 4-Way Handshake completes

C. To pass general data traffic after the completion of 802.11 authentication and key management

D. To block unencrypted user traffic after a 4-Way Handshake completes

Correct Answer: A

QUESTION 6

Given: ABC Company is implementing a secure 802.11 WLAN at their headquarters (HQ) building in New York and at each of the 10 small, remote branch offices around the United States. 802.1X/EAP is ABC\\'s preferred security solution, where possible. All access points (at the HQ building and all branch offices) connect to a single WLAN controller located at HQ. Each branch office has only a single AP and minimal IT resources.

What security best practices should be followed in this deployment scenario?

A. An encrypted VPN should connect the WLAN controller and each remote controller-based AP, or each remote site should provide an encrypted VPN tunnel to HQ.

B. APs at HQ and at each branch office should not broadcast the same SSID; instead each branch should have a unique ID for user accounting purposes.

C. RADIUS services should be provided at branch offices so that authentication server and supplicant credentials are not sent over the Internet.

D. Remote management of the WLAN controller via Telnet, SSH, HTTP, and HTTPS should be prohibited across the WAN link.

Correct Answer: A

QUESTION 7

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 8

Given: The ABC Corporation currently utilizes an enterprise Public Key Infrastructure (PKI) to allow employees to securely access network resources with smart cards. The new wireless network will use WPA2-Enterprise as its primary authentication solution. You have been asked to recommend a Wi-Fi Alliance-tested EAP method.

What solutions will require the least change in how users are currently authenticated and still integrate with their existing PKI?

A. EAP-FAST

B. EAP-TLS

C. PEAPv0/EAP-MSCHAPv2

D. LEAP

E. PEAPv0/EAP-TLS

F. EAP-TTLS/MSCHAPv2

Correct Answer: B

QUESTION 9

An attack is under way on the network. The attack is preventing users from accessing resources required for business operations, but the attacker has not gained access to any files or data. What kind of attack is described?

A. Man-in-the-middle

B. Hijacking

C. ASLEAP

D. DoS

Correct Answer: D

QUESTION 10

Your organization required compliance reporting and forensics features in relation to the 802.11ac WLAN they have recently installed. These features are not built into the management system provided by the WLAN vendor. The existing WLAN is managed through a centralized management console provided by the AP vendor with distributed APs and multiple WLAN controllers configured through this console.

What kind of system should be installed to provide the required compliance reporting and forensics features?

A. WNMS

B. WIPS overlay

C. WIPS integrated

D. Cloud management platform

Correct Answer: B

QUESTION 11

Wireless Intrusion Prevention Systems (WIPS) are used for what purposes? (Choose 3)

A. Performance monitoring and troubleshooting

B. Enforcing wireless network security policy

C. Detecting and defending against eavesdropping attacks

D. Security monitoring and notification

E. Preventing physical carrier sense attacks

F. Classifying wired client devices

Correct Answer: ABD

QUESTION 12

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