Vendor:CWNP

Exam Code:CWSP-206

Exam Name:CWSP Certified Wireless Security Professional

Version: Demo

QUESTION 1

Your organization is using EAP as an authentication framework with a specific type that meets the requirements of your corporate policies. Which one of the following statements is true related to this implementation?

A. The client STAs may communicate over the controlled port in order to authenticate as soon as the Open System authentication completes.

B. The client STAs may communicate over the uncontrolled port in order to authenticate as soon as the Open System authentication completes.

C. The client STAs may use a different, but complementary, EAP type than the AP STAs.

D. The client will be the authenticator in this scenario.

Correct Answer: B

QUESTION 2

The following numbered items show some of the contents of each of the four frames exchanged during the 4-way handshake.

1.

Encrypted GTK sent

2.

Confirmation of temporal key installation

3.

ANonce sent from authenticator to supplicant

4.

SNonce sent from supplicant to authenticator, MIC included

Arrange the frames in the correct sequence beginning with the start of the 4-way handshake.

A. 1, 2, 3, 4

B. 3, 4, 1, 2

C. 4, 3, 1, 2

D. 2, 3, 4, 1

Correct Answer: B

QUESTION 3

You must implement 7 APs for a branch office location in your organizations. All APs will be autonomous and provide the same two SSIDs (CORP1879 and Guest).

Because each AP is managed directly through a web-based interface, what must be changed on every AP before enabling the WLANs to ensure proper staging procedures are followed?

A. Output power

B. Fragmentation threshold

C. Administrative password

D. Cell radius

Correct Answer: C

QUESTION 4

What WLAN client device behavior is exploited by an attacker during a hijacking attack?

A. 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.

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

C. 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.

D. 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.

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

Correct Answer: C

QUESTION 5

A WLAN protocol analyzer trace reveals the following sequence of frames (excluding the ACK frames):

1.

802.11 Probe Req and 802.11 Probe Rsp

2.

802.11 Auth and then another 802.11 Auth

3.

802.11 Assoc Req and 802.11 Assoc Rsp

4.

EAPOL-KEY

5.

EAPOL-KEY

6.

EAPOL-KEY

7.

EAPOL-KEY

What security mechanism is being used on the WLAN?

A. WPA2-Personal

B. 802.1X/LEAP

C. EAP-TLS

D. WPA-Enterprise

E. WEP-128

Correct Answer: A

QUESTION 6

What TKIP feature was introduced to counter the weak integrity check algorithm used in WEP?

A. RC5 stream cipher

B. Block cipher support

C. Sequence counters

D. 32-bit ICV (CRC-32)

E. Michael

Correct Answer: E

QUESTION 7

As the primary security engineer for a large corporate network, you have been asked to author a new security policy for the wireless network. While most client devices support 802.1X authentication, some legacy devices still only support passphrase/PSK-based security methods. When writing the 802.11 security policy, what password-related items should be addressed?

A. Certificates should always be recommended instead of passwords for 802.11 client authentication.

B. Password complexity should be maximized so that weak WEP IV attacks are prevented.

C. Static passwords should be changed on a regular basis to minimize the vulnerabilities of a PSK-based authentication.

D. EAP-TLS must be implemented in such scenarios.

E. MS-CHAPv2 passwords used with EAP/PEAPv0 should be stronger than typical WPA2-PSK passphrases.

Correct Answer: C

QUESTION 8

ABC Company is deploying an IEEE 802.11-compliant wireless security solution using 802.1X/EAP authentication. According to company policy, the security solution must prevent an eavesdropper from decrypting data frames traversing a wireless connection. What security characteristic and/or component plays a role in preventing data decryption?

A. 4-Way Handshake

B. PLCP Cyclic Redundancy Check (CRC)

C. Multi-factor authentication

D. Encrypted Passphrase Protocol (EPP)

E. Integrity Check Value (ICV)

Correct Answer: A

QUESTION 9

For which one of the following purposes would a WIPS not be a good solution?

A. Enforcing wireless network security policy.

B. Detecting and defending against eavesdropping attacks.

C. Performance monitoring and troubleshooting.

D. Security monitoring and notification.

Correct Answer: B

QUESTION 10

ABC Company has a WLAN controller using WPA2-Enterprise with PEAPv0/MS-CHAPv2 and AES-CCMP to secure their corporate wireless data. They wish to implement a guest WLAN for guest users to have Internet access, but want to implement some security controls. The security requirements for the hotspot include:

Cannot access corporate network resources Network permissions are limited to Internet access All stations must be

authenticated

What security controls would you suggest? (Choose the single best answer.)

A. Configure access control lists (ACLs) on the guest WLAN to control data types and destinations.

B. Require guest users to authenticate via a captive portal HTTPS login page and place the guest WLAN and the corporate WLAN on different VLANs.

C. Implement separate controllers for the corporate and guest WLANs.

D. Use a WIPS to deauthenticate guest users when their station tries to associate with the corporate WLAN.

E. Force all guest users to use a common VPN protocol to connect.

Correct Answer: B

QUESTION 11

Your company has just completed installation of an IEEE 802.11 WLAN controller with 20 controller-based APs. The CSO has specified PEAPv0/EAP-MSCHAPv2 as the only authorized WLAN authentication mechanism. Since an LDAP-compliant user database was already in use, a RADIUS server was installed and is querying authentication requests to the LDAP server. Where must the X.509 server certificate and private key be installed in this network?

A. Controller-based APs

B. WLAN controller

C. RADIUS server

D. Supplicant devices

E. LDAP server

Correct Answer: C

QUESTION 12

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. SNMPv3 support

B. 802.1Q VLAN trunking

C. Internal RADIUS server

D. WIPS support and integration

E. WPA2-Enterprise authentication/encryption

Correct Answer: C