CWSP-206 Q&As

CWSP Certified Wireless Security Professional

Pass CWNP CWSP-206 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/cwsp-206.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CWNP Official Exam Center

QUESTION 1

What attack cannot be detected by a Wireless Intrusion Prevention System (WIPS)?

A. Deauthentication flood

B. Soft AP

C. EAP flood

D. Eavesdropping

E. MAC Spoofing

F. Hotspotter

Correct Answer: D

QUESTION 2

In order to acquire credentials of a valid user on a public hotspot network, what attacks may be conducted? Choose the single completely correct answer.

A. MAC denial of service and/or physical theft

B. Social engineering and/or eavesdropping

C. Authentication cracking and/or RF DoS

D. Code injection and/or XSS

E. RF DoS and/or physical theft

Correct Answer: B

QUESTION 3

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 4

You manage a wireless network that services 200 wireless users. Your facility requires 20 access points, and you have installed an IEEE 802.11-compliant implementation of 802.1X/LEAP with AES-CCMP as an authentication and encryption solution. In this configuration, the wireless network is initially susceptible to what type of attack?

A. Offline dictionary attacks

B. Application eavesdropping

C. Session hijacking

D. Layer 3 peer-to-peer

E. Encryption cracking

Correct Answer: A

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

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 7

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. WPA2-Personal with AES-CCMP

C. 802.1X/PEAPv0/MS-CHAPv2

D. EAP-MD5

E. Open 802.11 authentication with IPSec

Correct Answer: E

QUESTION 8

What field in the RSN information element (IE) will indicate whether PSK- or Enterprise-based WPA or WPA2 is in use?

A. Group Cipher Suite

B. Pairwise Cipher Suite List

C. AKM Suite List

D. RSN Capabilities

Correct Answer: C

QUESTION 9

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 10

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