Free Questions for CWSP-207 by certsinside

Shared by Savage on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

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?

Options:

A- WNMS

B- WIPS overlay

C- WIPS integrated

D- Cloud management platform

Answer:

B

Question 2

In an effort to optimize WLAN performance, ABC Company has upgraded their WLAN infrastructure from 802.11a/g to 802.11n. 802.11a/g clients are still supported and are used throughout ABC's facility. ABC has always been highly security conscious, but due to budget limitations, they have not yet updated their overlay WIPS solution to 802.11n or 802.11ac.

Given ABC's deployment strategy, what security risks would not be detected by the 802.11a/g WIPS?

Options:

A- Hijacking attack performed by using a rogue 802.11n AP against an 802.11a client

B- Rogue AP operating in Greenfield 40 MHz-only mode

C- 802.11a STA performing a deauthentication attack against 802.11n APs

D- 802.11n client spoofing the MAC address of an authorized 802.11n client

Answer:

B

Question 3

ABC Company requires the ability to identify and quickly locate rogue devices. ABC has chosen an overlay WIPS solution with sensors that use dipole antennas to perform this task. Use your knowledge of location tracking techniques to answer the question.

In what ways can this 802.11-based WIPS platform determine the location of rogue laptops or APs? (Choose 3)

Options:

A- Time Difference of Arrival (TDoA)

B- Angle of Arrival (AoA)

C- Trilateration of RSSI measurements

D- GPS Positioning

E- RF Fingerprinting

Answer:

A, C, E

Question 4

Wireless Intrusion Prevention Systems (WIPS) provide what network security services? (Choose 2)
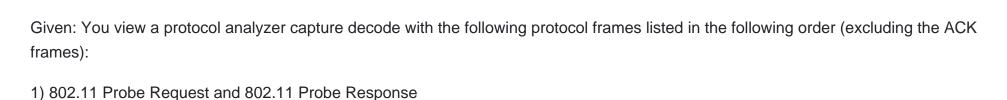
Options:

A- Configuration distribution for autonomous APs

B- Wireless vulnerability assessment

C- Application-layer traffic inspection

D- Analysis and reporting of AP CPU utilization

E- Policy enforcement and compliance management

Answer:

B, E

Question 5

Given: You view a protocol analyzer capture decode with the following protocol frames listed in the following order (excluding the ACK frames):

1) 802.11 Probe Request and 802.11 Probe Response

2) 802.11 Auth and another 802.11 Auth

2) 802.11 Assoc Req and 802.11 Assoc Rsp

4) EAPOL-Start

5) EAP Request and EAP Response

6) EAP Request and EAP Response

7) EAP Request and EAP Response

8) EAP Request and EAP Response

9) EAP Request and EAP Response

10) EAP Success

19) EAPOL-Key (4 frames in a row)

What are you seeing in the capture file? (Choose 4)

Options:

A- WPA2-Enterprise authentication

B- WPA2-Personal authentication

C- 802.11 Open System authentication

D- 802.1X with Dynamic WEP

E- Wi-Fi Protected Setup with PIN

F- Active Scanning

G- 4-Way Handshake

Answer:

A, C, F, G

Question 6

Question Type: **MultipleChoice**

You are implementing a wireless LAN that will be used by point-of-sale (PoS) systems in a retail environment. Thirteen PoS computers will be installed. To what industry requirement should you ensure you adhere?

Options:

A- ISA99

B- HIPAA

C- PCI-DSS

D- Directive 8500.01

Answer:

C

Question 7

Question Type: MultipleChoice

Given: Mary has just finished troubleshooting an 802.11g network performance problem using a laptop-based WLAN protocol analyzer. The wireless network implements 802.1X/PEAP and the client devices are authenticating properly. When Mary disables the WLAN protocol analyzer, configures her laptop for PEAP authentication, and then tries to connect to the wireless network, she is unsuccessful. Before using the WLAN protocol analyzer, Mary's laptop connected to the network without any problems.

What statement indicates why Mary cannot access the network from her laptop computer?

Options:

A- The nearby WIPS sensor categorized Mary's protocol analyzer adapter as a threat and is performing a deauthentication flood against her computer.

B- The PEAP client's certificate was voided when the protocol analysis software assumed control of the wireless adapter.

C- The protocol analyzer's network interface card (NIC) drivers are still loaded and do not support the version of PEAP being used.

D- Mary's supplicant software is using PEAPv0/EAP-MSCHAPv2, and the access point is using PEAPv1/EAP-GTC.

Answer:

C

Question 8

Question Type: **MultipleChoice**

You work as the security administrator for your organization. In relation to the WLAN, you are viewing a dashboard that shows security threat, policy compliance and rogue threat charts. What type of system is in view?

Options:

A- Wireshark Protocol Analyzer

B- Wireless VPN Management Systems

C- Wireless Intrusion Prevention System

D- Distributed RF Spectrum Analyzer
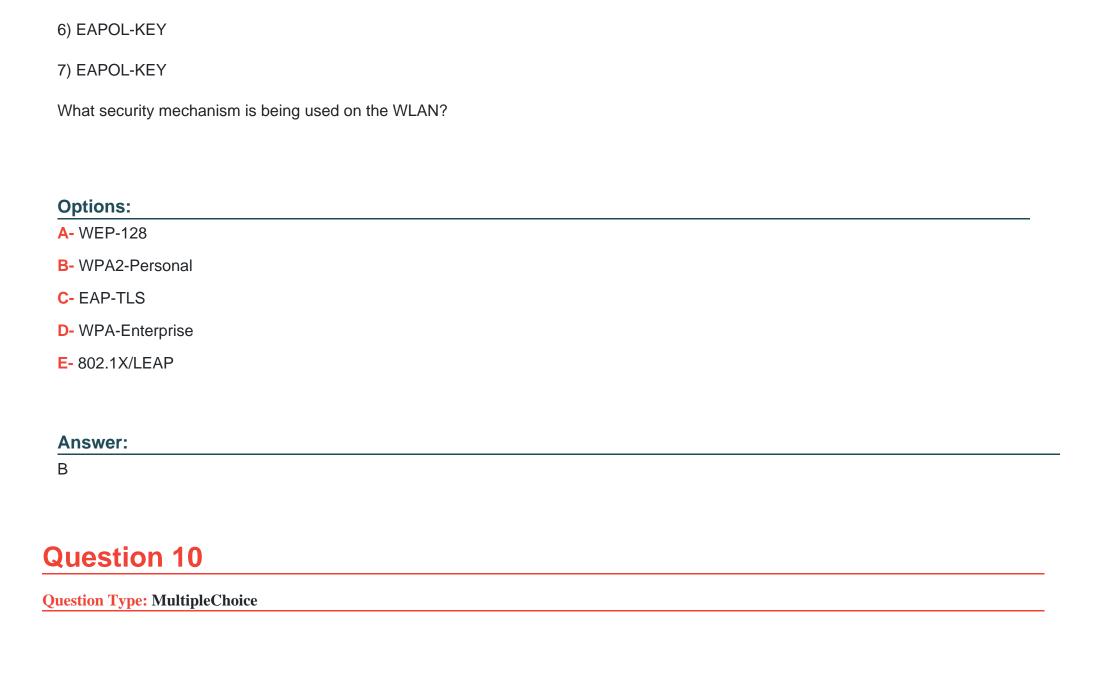
E- WLAN Emulation System

Answer:

C

Question 9

Given: 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?

Options:

A- WEP-128

B- WPA2-Personal

C- EAP-TLS

D- WPA-Enterprise

E- 802.1X/LEAP

Answer:

B

Question 10

Question Type: **MultipleChoice**

After completing the installation of a new overlay WIPS for the purpose of rogue detection and security monitoring at your corporate headquarters, what baseline function MUST be performed in order to identify security threats?

Options:

A- Authorized PEAP usernames must be added to the WIPS server's user database.

B- WLAN devices that are discovered must be classified (rogue, authorized, neighbor, etc.) and a WLAN policy must define how to classify new devices.

C- Separate security profiles must be defined for network operation in different regulatory domains

D- Upstream and downstream throughput thresholds must be specified to ensure that service-level agreements are being met.

Answer:

B

Question 11

Question Type: MultipleChoice

Given: WLAN protocol analyzers can read and record many wireless frame parameters.

What parameter is needed to physically locate rogue APs with a protocol analyzer?

Options:

A- SSID

B- IP Address

C- BSSID

D- Signal strength

E- RSN IE

F- Noise floor

Answer:

D

Question 12

Question Type: **MultipleChoice**

When monitoring APs within a LAN using a Wireless Network Management System (WNMS), what secure protocol may be used by the WNMS to issue configuration changes to APs?

Options:

A- IPSec/ESP

B- TFTP

C- 802.1X/EAP

D- SNMPv3

E- PPTP

Answer:

D