CWNP CWSP-208 Practice Questions

Shared by Mullen on 06-11-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Given: The Marketing department's WLAN users need to reach their file and email server as well as the Internet, but should not have access to any other network resources.

What single WLAN security feature should be implemented to comply with these requirements?

Options:

A- Mutual authentication
B- Captive portal
C- Role-based access control
D- Group authentication
E- RADIUS policy accounting

Answer:

C

Question 2

Question Type: MultipleChoice

Given: You have a Windows laptop computer with an integrated, dual-band, Wi-Fi compliant adapter. Your laptop computer has protocol analyzer software installed that is capable of capturing and decoding 802.11ac data.

What statement best describes the likely ability to capture 802.11ac frames for security testing purposes?

Options:

A- All integrated 802.11ac adapters will work with most protocol analyzers for frame capture, including the Radio Tap Header.
B- Integrated 802.11ac adapters are not typically compatible with protocol analyzers in Windows laptops. It is often best to use a USB adapter or carefully select a laptop with an integrated adapter that will work.
C- Laptops cannot be used to capture 802.11ac frames because they do not support MU-MIMO.
D- Only Wireshark can be used to capture 802.11ac frames as no other protocol analyzer has implemented the proper frame decodes.
E- The only method available to capture 802.11ac frames is to perform a remote capture with a

compatible access point.

Answer:

B

Question 3

Question Type: MultipleChoice

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

Options:

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 4

Question Type: MultipleChoice

While seeking the source of interference on channel 11 in your 802.11n WLAN running within 2.4 GHz, you notice a signal in the spectrum analyzer real time FFT display. The signal is characterized with the greatest strength utilizing only 1-2 megahertz of bandwidth and it does not use significantly more bandwidth until it has weakened by roughly 20 dB. At approximately -70 dB, it spreads across as much as 35 megahertz of bandwidth.

What kind of signal is described?

Options:

A- A high-power, narrowband signal
B- A 2.4 GHz WLAN transmission using transmit beam forming
C- An HT-OFDM access point
D- A frequency hopping wireless device in discovery mode
E- A deauthentication flood from a WIPS blocking an AP
F- A high-power ultra wideband (UWB) Bluetooth transmission

Answer:

A

Question 5

Question Type: MultipleChoice

Which of the following security attacks cannot be detected by a WIPS solution of any kind? (Choose 2)

Options:

A- Rogue APs
B- DoS
C- Eavesdropping
D- Social engineering

Answer:

C, D

Question 6

Question Type: MultipleChoice

Wireless Intrusion Prevention Systems (WIPS) provide what network security services? (Select 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 7

Question Type: MultipleChoice

What statement accurately describes the functionality of the IEEE 802.1X standard?

Options:

A- Port-based access control with EAP encapsulation over the LAN (EAPoL)
B- Port-based access control with dynamic encryption key management and distribution
C- Port-based access control with support for authenticated-user VLANs only
D- Port-based access control with mandatory support of AES-CCMP encryption
E- Port-based access control, which allows three frame types to traverse the uncontrolled port: EAP, DHCP, and DNS.

Answer:

A

To Get Premium Files for CWSP-208 Visit

https://www.p2pexams.com/products/cwsp-208

For More Free Questions Visit

https://www.p2pexams.com/cwnp/pdf/cwsp-208

