

DUMPS ARENA

CWSP Certified Wireless Security Professional

CWNP CWSP-206

Version Demo

Total Demo Questions: 10

Total Premium Questions: 60

Buy Premium PDF

<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 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

ANSWER: D**QUESTION NO: 2**

In a security penetration exercise, a WLAN consultant obtains the WEP key of XYZ Corporation's wireless network. Demonstrating the vulnerabilities of using WEP, the consultant uses a laptop running a software AP in an attempt to hijack the authorized user's connections. XYZ's legacy network is using 802.11n APs with 802.11b, 11g, and 11n client devices. With this setup, how can the consultant cause all of the authorized clients to establish Layer 2 connectivity with the software access point?

- A. When the RF signal between the clients and the authorized AP is temporarily disrupted and the consultant's software AP is using the same SSID on a different channel than the authorized AP, the clients will reassociate to the software AP.
- B. If the consultant's software AP broadcasts Beacon frames that advertise 802.11g data rates that are faster rates than XYZ's current 802.11b data rates, all WLAN clients will reassociate to the faster AP.
- C. A higher SSID priority value configured in the Beacon frames of the consultant's software AP will take priority over the SSID in the authorized AP, causing the clients to reassociate.
- D. All WLAN clients will reassociate to the consultant's software AP if the consultant's software AP provides the same SSID on any channel with a 10 dB SNR improvement over the authorized AP.

ANSWER: A**QUESTION NO: 3**

Which one of the following is not a role defined in the 802.1X authentication procedures used in 802.11 and 802.3 networks for port-based authentication?

- A. AAA Server

- B. Authentication Server
- C. Supplicant
- D. Authenticator

ANSWER: A

QUESTION NO: 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-to-client connections, even in an infrastructure BSS.

ANSWER: C

QUESTION NO: 5

Your network implements an 802.1X/EAP-based wireless security solution. A WLAN controller is installed and manages seven APs. FreeRADIUS is used for the RADIUS server and is installed on a dedicated server named SRV21. One example client is a MacBook Pro with 8 GB RAM. What device functions as the 802.1X/EAP Authenticator?

- A. WLAN Controller/AP
- B. MacBook Pro
- C. SRV21
- D. RADIUS server

ANSWER: A

QUESTION NO: 6

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?

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

ANSWER: C

QUESTION NO: 7

Many computer users connect to the Internet at airports, which often have 802.11n access points with a captive portal for authentication. While using an airport hotspot with this security solution, to what type of wireless attack is a user susceptible?

- A. Wi-Fi phishing
- B. Management interface exploits
- C. UDP port redirection
- D. IGMP snooping

ANSWER: A

QUESTION NO: 8

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

ANSWER: C

QUESTION NO: 9

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

ANSWER: B

QUESTION NO: 10

When using a tunneled EAP type, such as PEAP, what component is protected inside the TLS tunnel so that it is not sent in clear text across the wireless medium?

- A. Server credentials
- B. User credentials
- C. RADIUS shared secret
- D. X.509 certificates

ANSWER: B