DUMPSQUEEN

CWSP Certified Wireless Security Professional

CWNP CWSP-206

Version Demo

Total Demo Questions: 10

Total Premium Questions: 60

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

QUESTION NO: 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.

ANSWER: B

QUESTION NO: 2

You support a coffee shop and have recently installed a free 802.11ac wireless hotspot for the benefit of your customers. You want to minimize legal risk in the event that the hotspot is used for illegal Internet activity. What option specifies the best approach to minimize legal risk at this public hotspot while maintaining an open venue for customer Internet access?

A. Require client STAs to have updated firewall and antivirus software.

B. Block TCP port 25 and 80 outbound on the Internet router.

C. Use a WIPS to monitor all traffic and deauthenticate malicious stations.

D. Implement a captive portal with an acceptable use disclaimer.

E. Allow only trusted patrons to use the WLAN.

F. Configure WPA2-Enterprise security on the access point.

ANSWER: D

QUESTION NO: 3

For a WIPS system to identify the location of a rogue WLAN device using location pattering (RF fingerprinting), what must be done as part of the WIPS installation?

A. A location chipset (GPS) must be installed with it.

B. At least six antennas must be installed in each sector.

C. The RF environment must be sampled during an RF calibration process.

D. All WIPS sensors must be installed as dual-purpose (AP/sensor) devices.

ANSWER: C

QUESTION NO: 4

ABC Hospital wishes to create a strong security policy as a first step in securing their 802.11 WLAN. Before creating the WLAN security policy, what should you ensure you possess?

A. Management support for the process.

B. Security policy generation software.

C. End-user training manuals for the policies to be created.

D. Awareness of the exact vendor devices being installed.

ANSWER: A

QUESTION NO: 5

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?

A. 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.

B. Laptops cannot be used to capture 802.11ac frames because they do not support MU-MIMO.

C. Only Wireshark can be used to capture 802.11ac frames as no other protocol analyzer has implemented the proper frame decodes.

D. All integrated 802.11ac adapters will work with most protocol analyzers for frame capture, including the Radio Tap Header.

E. The only method available to capture 802.11ac frames is to perform a remote capture with a compatible access point.

ANSWER: A

QUESTION NO: 6

What software and hardware tools are used in the process performed to hijack a wireless station from the authorized wireless network onto an unauthorized wireless network?

A. A low-gain patch antenna and terminal emulation software

B. MAC spoofing software and MAC DoS software

C. RF jamming device and a wireless radio card

D. A wireless workgroup bridge and a protocol analyzer

ANSWER: C

QUESTION NO: 7

What preventative measures are performed by a WIPS against intrusions?

A. Uses SNMP to disable the switch port to which rogue APs connect.

B. Evil twin attack against a rogue AP.

C. EAPoL Reject frame flood against a rogue AP.

D. Deauthentication attack against a classified neighbor AP.

E. ASLEAP attack against a rogue AP.

ANSWER: A

QUESTION NO: 8

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.

ANSWER: C

QUESTION NO: 9

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: 10

ABC Company has recently installed a WLAN controller and configured it to support WPA2Enterprise security. The administrator has configured a security profile on the WLAN controller for each group within the company (Marketing, Sales, and Engineering). How are authenticated users assigned to groups so that they receive the correct security profile within the WLAN controller?

A. The RADIUS server sends the list of authenticated users and groups to the WLAN controller as part of a 4-Way Handshake prior to user authentication.

B. The WLAN controller polls the RADIUS server for a complete list of authenticated users and groups after each user authentication.

C. The RADIUS server sends a group name return list attribute to the WLAN controller during every successful user authentication.
The RADIUS server forwards the request for a group attribute to an LDAP database service,
and LDAP sends the group attribute to the WLAN controller.

ANSWER: C