



CWNP

Exam Questions CWSP-206

CWSP Certified Wireless Security Professional

NEW QUESTION 1

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 laptop
- B. 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. All integrated 802.11ac adapters will work with most protocol analyzers for frame capture, including the Radio Tap Header.
- F. The only method available to capture 802.11ac frames is to perform a remote capture with a compatible access point.

Answer: A

NEW QUESTION 2

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

NEW QUESTION 3

During 802.1X/LEAP authentication, the username is passed across the wireless medium in clear text. From a security perspective, why is this significant?

- A. The username can be looked up in a dictionary file that lists common username/password combinations.
- B. The username is needed for Personal Access Credential (PAC) and X.509 certificate validation.
- C. 4-Way Handshake nonces are based on the username in WPA and WPA2 authentication.
- D. The username is an input to the LEAP challenge/response hash that is exploited, so the username must be known to conduct authentication cracking.

Answer: D

NEW QUESTION 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

NEW QUESTION 5

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

NEW QUESTION 6

You are installing 6 APs on the outside of your facility. They will be mounted at a height of 6 feet. What must you do to implement these APs in a secure manner beyond the normal indoor AP implementations? (Choose the single best answer.)

- A. Ensure proper physical and environmental security using outdoor ruggedized APs or enclosures.
- B. Use internal antennas.
- C. Use external antennas.
- D. Power the APs using PoE.

Answer: A

NEW QUESTION 7

A WLAN consultant has just finished installing a WLAN controller with 15 controller-based APs. Two SSIDs with separate VLANs are configured for this network, and both VLANs are configured to use the same RADIUS server. The SSIDs are configured as follows:

- * 1. SSID Blue – VLAN 10 – Lightweight EAP (LEAP) authentication – CCMP cipher suite
- * 2. SSID Red – VLAN 20 – PEAPv0/EAP-TLS authentication – TKIP cipher suite

The consultant's computer can successfully authenticate and browse the Internet when using the Blue SSID. The same computer cannot authenticate when using the Red SSID. What is a possible cause of the problem?

- A. The consultant does not have a valid Kerberos ID on the Blue VLAN.
- B. The client does not have a proper certificate installed for the tunneled authentication within the established TLS tunnel.
- C. The TKIP cipher suite is not a valid option for PEAPv0 authentication.
- D. The Red VLAN does not use server certificate, but the client requires one.

Answer: B

NEW QUESTION 8

In an IEEE 802.11-compliant WLAN, when is the 802.1X Controlled Port placed into the unblocked state?

- A. After EAP authentication is successful
- B. After Open System authentication
- C. After the 4-Way Handshake
- D. After any Group Handshake

Answer: A

NEW QUESTION 9

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

NEW QUESTION 10

What protocol, listed here, allows a network manager to securely administer the network?

- A. TFTP
- B. Telnet
- C. HTTPS
- D. SNMPv2

Answer: C

NEW QUESTION 10

A large enterprise is designing a secure, scalable, and manageable 802.11n WLAN that will support thousands of users. The enterprise will support both 802.1X/EAP-TTLS and PEAPv0/MSCHAPv2. Currently, the company is upgrading network servers as well and will replace their existing Microsoft IAS implementation with Microsoft NPS, querying Active Directory for user authentication. For this organization, as they update their WLAN infrastructure, what WLAN controller feature will likely be least valuable?

- A. SNMPv3 support
- B. 802.1Q VLAN trunking
- C. Internal RADIUS server
- D. WIPS support and integration
- E. WPA2-Enterprise authentication/encryption

Answer: C

NEW QUESTION 13

ABC Company is an Internet Service Provider with thousands of customers. ABC's customers are given login credentials for network access when they become a customer. ABC uses an LDAP server as the central user credential database. ABC is extending their service to existing customers in some public access areas and would like to use their existing database for authentication. How can ABC Company use their existing user database for wireless user authentication as they implement a large-scale WPA2-Enterprise WLAN security solution?

- A. Implement a RADIUS server and query user authentication requests through the LDAP server.
- B. Mirror the LDAP server to a RADIUS database within a WLAN controller and perform daily backups to synchronize the user databases.
- C. Import all users from the LDAP server into a RADIUS server with an LDAP-to-RADIUS conversion tool.
- D. Implement an X.509 compliant Certificate Authority and enable SSL queries on the LDAP server.

Answer: A

NEW QUESTION 15

ABC Company is deploying an IEEE 802.11-compliant wireless security solution using 802.1X/EAP authentication. According to company policy, the security solution must prevent an eavesdropper from decrypting data frames traversing a wireless connection. What security characteristic and/or component plays a role in preventing data decryption?

- A. 4-Way Handshake
- B. PLCP Cyclic Redundancy Check (CRC)

- C. Multi-factor authentication
- D. Encrypted Passphrase Protocol (EPP)
- E. Integrity Check Value (ICV)

Answer: A

NEW QUESTION 20

The IEEE 802.11 standard defined Open System authentication as consisting of two auth frames and two assoc frames. In a WPA2-Enterprise network, what process immediately follows the 802.11 association procedure?

- A. 802.1X/ EAP authentication
- B. Group Key Handshake
- C. DHCP Discovery
- D. RADIUS shared secret lookup
- E. 4-Way Handshake
- F. Passphrase-to-PSK mapping

Answer: A

NEW QUESTION 22

Your company has just completed installation of an IEEE 802.11 WLAN controller with 20 controller-based APs. The CSO has specified PEAPv0/EAP-MSCHAPv2 as the only authorized WLAN authentication mechanism. Since an LDAPcompliant user database was already in use, a RADIUS server was installed and is querying authentication requests to the LDAP server. Where must the X.509 server certificate and private key be installed in this network?

- A. Controller-based APs
- B. WLAN controller
- C. RADIUS server
- D. Supplicant devices
- E. LDAP server

Answer: C

NEW QUESTION 24

Joe's new laptop is experiencing difficulty connecting to ABC Company's 802.11 WLAN using 802.1X/EAP PEAPv0. The company's wireless network administrator assured Joe that his laptop was authorized in the WIPS management console for connectivity to ABC's network before it was given to him. The WIPS termination policy includes alarms for rogue stations, rogue APs, DoS attacks and unauthorized roaming. What is a likely reason that Joe cannot connect to the network?

- A. An ASLEAP attack has been detected on APs to which Joe's laptop was trying to associat
- B. The WIPS responded by disabling the APs.
- C. Joe configured his 802.11 radio card to transmit at 100 mW to increase his SN
- D. The WIPS is detecting this much output power as a DoS attack.
- E. Joe's integrated 802.11 radio is sending multiple Probe Request frames on each channel.
- F. Joe disabled his laptop's integrated 802.11 radio and is using a personal PC card radio with a different chipset, drivers, and client utilities.

Answer: D

NEW QUESTION 25

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

NEW QUESTION 27

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

Answer: C

NEW QUESTION 31

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

Answer: A

NEW QUESTION 34

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

CWSP-206 Practice Exam Features:

- * CWSP-206 Questions and Answers Updated Frequently
- * CWSP-206 Practice Questions Verified by Expert Senior Certified Staff
- * CWSP-206 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * CWSP-206 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CWSP-206 Practice Test Here](#)