

Exam Questions CWSP-206

CWSP Certified Wireless Security Professional

<https://www.2passeasy.com/dumps/CWSP-206/>



NEW QUESTION 1

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

NEW QUESTION 2

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

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

In XYZ's small business, two autonomous 802.11ac APs and 12 client devices are in use with WPA2-Personal. What statement about the WLAN security of this company is true?

- A. Intruders may obtain the passphrase with an offline dictionary attack and gain network access, but will be unable to decrypt the data traffic of other users.
- B. Because WPA2-Personal uses Open System authentication followed by a 4-Way Handshake, hijacking attacks are easily performed.
- C. A successful attack against all unicast traffic on the network would require a weak passphrase dictionary attack and the capture of the latest 4-Way Handshake for each client.
- D. An unauthorized wireless client device cannot associate, but can eavesdrop on some data because WPA2-Personal does not encrypt multicast or broadcast traffic.
- E. An unauthorized WLAN user with a protocol analyzer can decode data frames of authorized users if he captures the BSSID, client MAC address, and a user's 4-Way Handshake.

Answer: C

NEW QUESTION 5

The Aircrack-ng WLAN software tool can capture and transmit modified 802.11 frames over the wireless network. It comes pre-installed on Kali Linux and some other Linux distributions. Which one of the following would not be a suitable penetration testing action taken with this tool?

- A. Auditing the configuration and functionality of a WIPS by simulating common attack sequences.
- B. Transmitting a deauthentication frame to disconnect a user from the AP.
- C. Cracking the authentication or encryption processes implemented poorly in some WLANs.
- D. Probing the RADIUS server and authenticator to expose the RADIUS shared secret.

Answer: D

NEW QUESTION 6

You perform a protocol capture using Wireshark and a compatible 802.11 adapter in Linux. When viewing the capture, you see an auth req frame and an auth rsp frame. Then you see an assoc req frame and an assoc rsp frame. Shortly after, you see DHCP communications and then ISAKMP protocol packets. What security solution is represented?

- A. 802.1X/EAP-TTLS
- B. WPA2-Personal with AES-CCMP
- C. 802.1X/PEAPv0/MS-CHAPv2
- D. EAP-MD5
- E. Open 802.11 authentication with IPSec

Answer: E

NEW QUESTION 7

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

NEW QUESTION 8

Fred works primarily from home and public wireless hotspots rather than commuting to office. He frequently accesses the office network remotely from his Mac laptop using the local 802.11 WLAN. In this remote scenario, what single wireless security practice will provide the greatest security for Fred?

- A. Use enterprise WIPS on the corporate office network.
- B. Use 802.1X/PEAPv0 to connect to the corporate office network from public hotspots.
- C. Use secure protocols, such as FTP, for remote file transfers.
- D. Use an IPSec VPN for connectivity to the office network.
- E. Use only HTTPS when agreeing to acceptable use terms on public networks.
- F. Use WIPS sensor software on the laptop to monitor for risks and attacks.

Answer: D

NEW QUESTION 9

What TKIP feature was introduced to counter the weak integrity check algorithm used in WEP?

- A. RC5 stream cipher
- B. Block cipher support
- C. Sequence counters
- D. 32-bit ICV (CRC-32)
- E. Michael

Answer: E

NEW QUESTION 10

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

NEW QUESTION 10

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

NEW QUESTION 12

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 13

XYZ Company has recently installed a controller-based WLAN and is using a RADIUS server to query authentication requests to an LDAP server. XYZ maintains user-based access policies and would like to use the RADIUS server to facilitate network authorization. What RADIUS feature could be used by XYZ to assign the proper network permissions to users during authentications?

- A. RADIUS can reassign a client's 802.11 association to a new SSID by referencing a username-to-SSID mapping table in the LDAP user database.
- B. The RADIUS server can support vendor-specific attributes in the ACCESS-ACCEPT response, which can be used for user policy assignment.
- C. The RADIUS server can communicate with the DHCP server to issue the appropriate IP address and VLAN assignment to users.
- D. RADIUS can send a DO-NOT-AUTHORIZE demand to the authenticator to prevent the STA from gaining access to specific files, but may only employ this in relation to Linux servers.

Answer: B

NEW QUESTION 15

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 19

ABC Company has recently installed a WLAN controller and configured it to support WPA2-Enterprise 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.
- D. 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

NEW QUESTION 22

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 25

The IEEE 802.11 Pairwise Transient Key (PTK) is derived from what cryptographic element?

- A. PeerKey (PK)
- B. Group Master Key (GMK)
- C. Key Confirmation Key (KCK)
- D. Pairwise Master Key (PMK)
- E. Phase Shift Key (PSK)
- F. Group Temporal Key (GTK)

Answer: D

NEW QUESTION 30

In the basic 4-way handshake used in secure 802.11 networks, what is the purpose of the ANonce and SNonce?

- A. They are added together and used as the GMK, from which the GTK is derived.
- B. They are used to pad Message 1 and Message 2 so each frame contains the same number of bytes.
- C. The IEEE 802.11 standard requires that all encrypted frames contain a nonce to serve as a Message Integrity Check (MIC).
- D. They are input values used in the derivation of the Pairwise Transient Key.

Answer: D

NEW QUESTION 34

ABC Company has a WLAN controller using WPA2-Enterprise with PEAPv0/MS-CHAPv2 and AES-CCMP to secure their corporate wireless data. They wish to implement a guest WLAN for guest users to have Internet access, but want to implement some security controls. The security requirements for the hotspot include:

- * Cannot access corporate network resources
- * Network permissions are limited to Internet access
- * All stations must be authenticated

What security controls would you suggest? (Choose the single best answer.)

- A. Configure access control lists (ACLs) on the guest WLAN to control data types and destinations.
- B. Require guest users to authenticate via a captive portal HTTPS login page and place the guest WLAN and the corporate WLAN on different VLANs.
- C. Implement separate controllers for the corporate and guest WLANs.
- D. Use a WIPS to deauthenticate guest users when their station tries to associate with the corporate WLAN.
- E. Force all guest users to use a common VPN protocol to connect.

Answer: B

NEW QUESTION 35

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 LDAP-compliant 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 38

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 12 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.
- D. A deauthentication flood from a WIPS blocking an AP.
- E. An HT-OFDM access point.
- F. A frequency hopping wireless device in discovery mode.

Answer: C

NEW QUESTION 41

XYZ Hospital plans to improve the security and performance of their Voice over Wi-Fi implementation and will be upgrading to 802.11n phones with 802.1X/EAP authentication. XYZ would like to support fast secure roaming for the phones and will require the ability to troubleshoot reassociations that are delayed or dropped during inter-channel roaming. What portable solution would be recommended for XYZ to troubleshoot roaming problems?

- A. Spectrum analyzer software installed on a laptop computer.
- B. An autonomous AP mounted on a mobile cart and configured to operate in monitor mode.
- C. Laptop-based protocol analyzer with multiple 802.11n adapters.
- D. WIPS sensor software installed on a laptop computer.

Answer: C

NEW QUESTION 42

For which one of the following purposes would a WIPS not be a good solution?

- A. Enforcing wireless network security policy.
- B. Detecting and defending against eavesdropping attacks.
- C. Performance monitoring and troubleshooting.
- D. Security monitoring and notification.

Answer: B

NEW QUESTION 46

A network security auditor is preparing to perform a comprehensive assessment of an 802.11ac network's security. What task should be performed at the beginning of the audit to maximize the auditor's ability to expose network vulnerabilities?

- A. Identify the IP subnet information for each network segment.
- B. Identify the manufacturer of the wireless infrastructure hardware.
- C. Identify the skill level of the wireless network security administrator(s).
- D. Identify the manufacturer of the wireless intrusion prevention system.
- E. Identify the wireless security solution(s) currently in use.

Answer: E

NEW QUESTION 48

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 associate.
- 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 49

The following numbered items show some of the contents of each of the four frames exchanged during the 4-way handshake.

- * 1. Encrypted GTK sent
- * 2. Confirmation of temporal key installation
- * 3. ANonce sent from authenticator to supplicant
- * 4. SNonce sent from supplicant to authenticator, MIC included

Arrange the frames in the correct sequence beginning with the start of the 4-way handshake.

- A. 1, 2, 3, 4
- B. 3, 4, 1, 2
- C. 4, 3, 1, 2
- D. 2, 3, 4, 1

Answer: B

NEW QUESTION 52

What security vulnerability may result from a lack of staging, change management, and installation procedures for WLAN infrastructure equipment?

- A. The WLAN system may be open to RF Denial-of-Service attacks.
- B. Authentication cracking of 64-bit Hex WPA-Personal PSK.
- C. AES-CCMP encryption keys may be decrypted.
- D. WIPS may not classify authorized, rogue, and neighbor APs accurately.

Answer: D

NEW QUESTION 53

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 56

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CWSP-206 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CWSP-206 Product From:

<https://www.2passeasy.com/dumps/CWSP-206/>

Money Back Guarantee

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 FirstTry
- * CWSP-206 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year