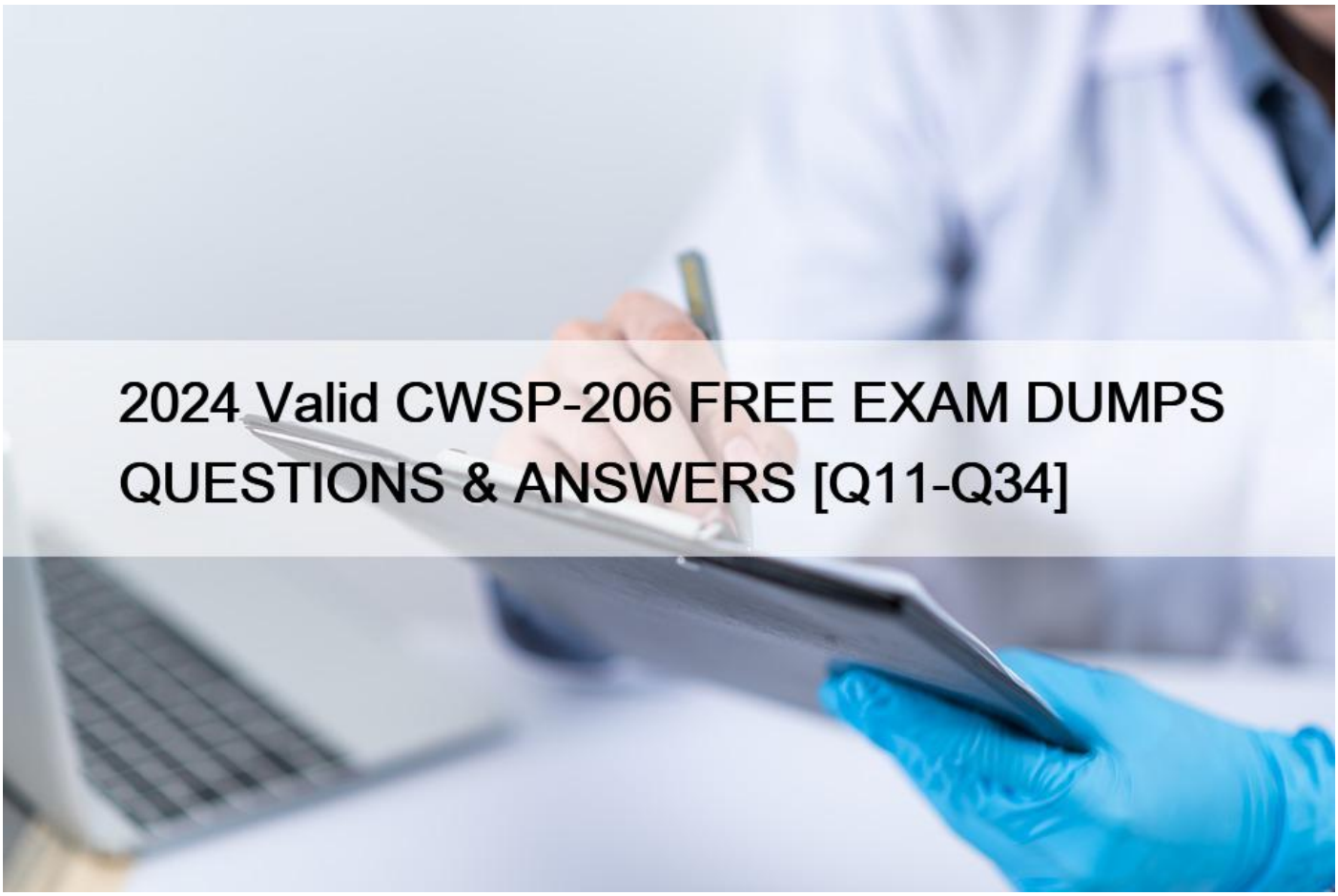
2024 Valid CWSP-206 FREE EXAM DUMPS QUESTIONS & ANSWERS [Q11-Q34



2024 Valid CWSP-206 FREE EXAM DUMPS QUESTIONS & ANSWERS
Free CWSP-206 Exam Braindumps CWNP Pratice Exam

The CWSP-206 certification exam is a challenging exam that requires a thorough understanding of wireless networking security. It is recommended that candidates have at least two years of experience in wireless networking security before attempting the exam. CWSP-206 exam consists of 60 multiple-choice questions and candidates have 90 minutes to complete the exam. Candidates who pass the exam will receive the CWSP-206 certification, which is valid for three years.

Q11. Which of the following does PEAP use to authenticate the user inside an encrypted tunnel? Each correct answer represents a complete solution. Choose two.
* RC4
* AES
* MS-CHAP v2
* GTC

Q12. You work as a Network Administrator for Tech Perfect Inc. The company has a secure wireless network. Since the company’s wireless network is so dynamic, it requires regular auditing to maintain proper security. For this reason, you are configuring NetStumbler as a wireless auditing tool. What services can NetStumbler provide? Each correct answer represents a complete solution. Choose all that apply.
* Detection of causes of wireless interference
* Verification of network configurations
* Detection of unauthorized (“rogue”) access points
* Capturing and decoding of packets

Q13. After completing the installation of a new overlay WIPS for the purpose of rogue detection and security monitoring at your corporate headquarters, what baseline function MUST be performed in order to identify the security threats?
* Separate security profiles must be defined for network operation in different regulatory domains.
* WLAN devices that are discovered must be classified (rogue, authorized, neighbor, etc.) and a WLAN policy must define how to classify new devices.
* Upstream and downstream throughput thresholds must be specified to ensure that service-level agreements are being met.
* Authorized PEAP usernames must be added to the WIPS server’s user database.
Explanation/Reference:

Q14. A networksecurity 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?
* Identify the IP subnet information for each network segment.
* Identify the manufacturer of the wireless infrastructure hardware.
* Identify the skill level of the wireless network security administrator(s).
* Identify the manufacturer of the wireless intrusion preventionsystem.
* Identify the wireless security solution(s) currently in use.

Q15. 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?
* 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.
* The WLAN controller polls the RADIUS server for a complete list of authenticated users and groups after each user authentication.
* 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.

Q16. You work as a network administrator for Web Perfect Inc. You configure both WPA and EAP authentications on a client computer in the company’s wireless network.

Where will the encryption key be located during the active user session? Each correct answer represents a part of the solution. Choose two.
* On the AP
* On the controller
* Shared with all clients in the network
* On the client

Q17. You work as a Network Administrator for Tech Perfect Inc. The company has a wireless LAN infrastructure. The management

wants to prevent unauthorized network access to local area networks and other information assets by the wireless devices. What will you do?
* Implement a dynamic NAT.
* Implement an ACL.
* Implement a WIPS.
* Implement a firewall.

Q18. Yousupport 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?
* Require client STAs to have updated firewall and antivirus software.
* Block TCP port 25 and 80 outbound on the Internet router.
* Use a WIPS to monitor all traffic and deauthenticate malicious stations.
* Implement a captive portal with an acceptable use disclaimer.
* Allow only trusted patrons to use the WLAN.
* Configure WPA2-Enterprise security on the access point.

Q19. 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 beimplemented to comply with these requirements?
* RADIUS policy accounting
* Captive portal
* Role-based access control
* Group authentication
* Mutual authentication

Q20. 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?
* An ASLEAP attack has been detected on APs to which Joe’s laptop was trying to associate. The WIPS responded by disabling the APs.
* Joe configured his 802.11 radio card to transmit at 100 mW to increase his SNR. The WIPS is detecting this much output power as a DoS attack.
* Joe’s integrated 802.11 radio is sending multiple Probe Request frames on each channel.
* 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.

Q21. For which one of the following purposes would aWIPS not be a good solution?
* Enforcing wireless network security policy.
* Detecting and defending against eavesdropping attacks.
* Performance monitoring and troubleshooting.
* Security monitoring and notification.

Q22. The following numbered items show some of the contents of each of the four frames exchanged during the

4-way handshake.

* Encrypted GTK sent

* Confirmation of temporal key installation

* ANonce sent from authenticator to supplicant

* SNonce sent from supplicant to authenticator, MIC included

Arrange the frames in the correct sequence beginning with the start of the 4-way handshake.
* 1, 2, 3, 4
* 3, 4, 1, 2
* 4, 3, 1, 2
* 2, 3, 4, 1

Q23. ABC Corporation is evaluating the security solution for their existing WLAN. Two of their supported solutions include a PPTP VPN and 802.1X/LEAP. They have used PPTP VPNs because of their wide support in server and desktop operating systems. While both PPTP and LEAP adhere to the minimum requirements of the corporate security policy, some individuals have raised concerns about MS-CHAPv2 (and similar) authentication and the known fact that MS-CHAPv2 has proven vulnerable in improper implementations. As a consultant, what do you tell ABC Corporation about implementing MS-CHAPv2 authentication?
* MS-CHAPv2 is only appropriate for WLAN security when used inside a TLS-encrypted tunnel.
* When implemented with AES-CCMP encryption, MS-CHAPv2 is very secure.
* MS-CHAPv2 uses AES authentication, and is therefore secure.
* MS-CHAPv2 is compliant with WPA-Personal, but not WPA2-Enterprise.
* LEAP’s use of MS-CHAPv2 is only secure when combined with WEP.
Explanation/Reference:

Q24. Which of the following security methods can be used to detect the DoS attack in order to enhance the security of the network?
* WLAN controller
* Spectrum analyzer
* Protocol analyzer
* WIPS

Q25. 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?
* Server credentials
* User credentials
* RADIUS shared secret
* X.509 certificates

Q26. 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?
* AAA Server
* Authentication Server
* Supplicant
* Authenticator

Q27. 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?
* WLAN Controller/AP
* MacBook Pro
* SRV21
* RADIUS server

Q28. You work as a Network Administrator for Blue Well Inc. The company has a Windows Server

2008 domain based network. All client computers on the network run Windows Vista Ultimate.

Andy, a Finance Manager, uses Windows Mail to download his e-mails to his inbox. He complains that every now and then he gets mails asking for revealing personal or financial information. He wants that such mails are not shown to him.

Which of the following steps will you take to accomplish the task?

* Configure phishing filter in Internet Explorer 7.0. Configure it to filter all phishing mails.
* Remove domain names of such emails from the Safe Sender’s list.
* Configure phishing filter in Windows Mail. Configure it to move such mails to the Junk Mail folder.
* Add domain names of such emails in the Block Sender’s list.

Q29. ABC Company is implementing a secure 802.11 WLAN at their headquarters (HQ) building in New York and at each of the 10 small, remote branch offices around the United States.

802.1X/EAP is ABC’s preferred security solution, where possible. All access points (at the HQ building and all branch offices) connect to a single WLAN controller located at HQ. Each branch office has only a single AP and minimal IT resources. What security best practices should be followed in this deployment scenario?
* Remote management of the WLAN controller via Telnet, SSH, HTTP, and HTTPS should be prohibited across the WAN link.
* RADIUS services should be provided at branch offices so that authentication server and suppliant credentials are not sent over the Internet.
* An encrypted VPN should connect the WLAN controller and each remote controller-based AP, or each remote site should provide an encrypted VPN tunnel to HQ.
* APs at HQ and at each branch office should not broadcast the same SSID; instead each branch should have a unique ID for user accounting purposes.

Q30. As the primary security engineer for a large corporate network, you have been asked to author a new securitypolicy 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?
* Certificates should always be recommended instead of passwords for 802.11 client authentication.
* Password complexity should be maximized so that weak WEP IV attacks are prevented.
* Static passwords should be changed on a regular basis to minimize the vulnerabilities of a PSK-based authentication.
* EAP-TLS must be implemented in such scenarios.
* MS-CHAPv2 passwords used with EAP/PEAPv0 should be stronger than typical WPA2-PSK passphrases.

Q31. 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?
* 802.1X/ EAPauthentication
* Group Key Handshake
* DHCP Discovery
* RADIUS shared secret lookup
* 4-Way Handshake
* Passphrase-to-PSK mapping

Q32. 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 high-power ultra wideband (UWB) Bluetooth transmission.
* A 2.4 GHz WLAN transmission using transmit beam forming.
* A high-power, narrowband signal.
* A deauthentication flood from a WIPS blocking an AP.
* An HT-OFDM access point.
* A frequency hopping wireless device in discovery mode.

Q33. Which of the following keys is derived from Group Master Key (GMK)?
* Private Key
* Group Temporal Key
* Public Key
* Pairwise Transient Key

Q34. Which of the following security protocols uses a single, manually configured, static key for data encryption that is shared by the client and the WAP?
* L2TP
* WEP
* IPSec
* WPA