[2025-July-NewBraindump2go CWSP-208 VCE Free Download[Q1-Q50

July/2025 Latest Braindump2go CWSP-208 Exam Dumps with PDF and VCE Free Updated Today! Following are some new Braindump2go CWSP-208 Real Exam Questions!Question: 1 Given: John Smith uses a coffee shop's Internet hot-spot (no authentication or encryption) to transfer funds between his checking and savings accounts at his bank's website. The bank's website uses the HTTPS protocol to protect sensitive account information. While John was using the hot-spot, a hacker was able to obtain John's bank account user ID and password and exploit this information.What likely scenario could have allowed the hacker to obtain John's bank account user ID and password?A. John's bank is using an expired X.509 certificate on their web server. The certificate is on John's Certificate Revocation List (CRL), causing the user ID and password to be sent unencrypted.B. John uses the same username and password for banking that he does for email. John used a POP3 email client at the wireless hot-spot to check his email, and the user ID and password were not encrypted.C. John accessed his corporate network with his IPSec VPN software at the wireless hot-spot. An IPSec VPN only encrypts data, so the user ID and password were sent in clear text. John uses the same username and password for banking that he does for his IPSec VPN software.D. The bank's web server is using an X.509 certificate that is not signed by a root CA, causing the user ID and password to be sent unencrypted.E. Before connecting to the bank's website, John's association to the AP was hijacked. The attacker intercepted the HTTPS public encryption key from the bank's web server and has decrypted John's login credentials in near real-time.Answer: B Question: 2 What type of WLAN attack is prevented with the use of a per-MPDU TKIP sequence counter (TSC)?A. Weak-IVB. ForgeryC. ReplayD. Bit-flippingE. Session hijackingAnswer: C Question: 3 What 802.11 WLAN security problem is directly addressed by mutual authentication?A. Wireless hijacking attacksB. Weak password policiesC. MAC spoofingD. Disassociation attacksE. Offline dictionary attacksF. Weak Initialization VectorsAnswer: A Question: 4 ABC Company uses the wireless network for highly sensitive network traffic. For that reason, they intend to protect their network in all possible ways. They are continually researching new network threats and new preventative measures. They are interested in the security benefits of 802.11w, but would like to know its limitations.What types of wireless attacks are protected by 802.11w? (Choose 2)A. RF DoS attacksB. Layer 2 Disassociation attacksC. Robust management frame replay attacksD. Social engineering attacksAnswer: B, C Question: 5 You are configuring seven APs to prevent common security attacks. The APs are to be installed in a small business and to reduce costs, the company decided to install all consumer-grade wireless routers. The wireless routers will connect to a switch, which connects directly to the Internet connection providing 50 Mbps of Internet bandwidth that will be shared among 53 wireless clients and 17 wired clients.To ensure the wireless network is as secure as possible from common attacks, what security measure can you implement given only the hardware referenced?A. WPA-EnterpriseB. 802.1X/EAP-PEAPC. WPA2-EnterpriseD. WPA2-PersonalAnswer: D Question: 6 A WLAN is implemented using WPA-Personal and MAC filtering.To what common wireless network attacks is this network potentially vulnerable? (Choose 3)A. Offline dictionary attacksB. MAC SpoofingC. ASLEAPD. DoSAnswer: A, B, D Question: 7 An attack is under way on the network. The attack is preventing users from accessing resources required for business operations, but the attacker has not gained access to any files or data. What kind of attack is described?A. Man-in-the-middleB. HijackingC. ASLEAPD. DoSAnswer: D Question: 8 Given: WLAN attacks are typically conducted by hackers to exploit a specific vulnerability within a network.What statement correctly pairs the type of WLAN attack with the exploited vulnerability? (Choose 3)A. Management interface exploit attacks are attacks that use social engineering to gain credentials from managers.B. Zero-day attacks are always authentication or encryption cracking attacks.C. RF DoS attacks prevent successful wireless communication on a specific frequency or frequency range.D. Hijacking attacks interrupt a user's legitimate connection and introduce a new connection with an evil twin AP.E. Social engineering attacks are performed to collect sensitive information from unsuspecting usersF. Association flood attacks are Layer 3 DoS attacks performed against authenticated client stationsAnswer: C, D, E Question: 9 Given: One of the security risks introduced by WPA2-Personal is an attack conducted by an authorized network user who knows the passphrase. In order to decrypt other users' traffic, the attacker must obtain certain information from the 4-way handshake of the other users.In addition to knowing the Pairwise Master Key (PMK) and the supplicant's address (SA), what other three inputs must be collected with a protocol analyzer to recreate encryption keys? (Choose 3)A. Authenticator nonceB. Supplicant nonceC. Authenticator address (BSSID)D. GTKSAE. Authentication Server nonceAnswer: A, B, C Question: 10 What is a primary criteria for a network to qualify as a Robust Security Network (RSN)? A. Token cards must be used for authentication.B. Dynamic WEP-104 encryption must be enabled.C. WEP may not be used for encryption.D. WPA-Personal must be supported for authentication and encryption.E. WLAN controllers and APs must not support SSHv1.Answer: C Question: 11 Given: You are using a Wireless Aggregator utility to combine multiple packet captures. One capture exists for each of channels 1, 6 and 11. What kind of troubleshooting are you likely performing with such a tool?A. Wireless adapter failure analysis.B. Interference source location.C. Fast secure roaming problems.D. Narrowband DoS attack detection.Answer: C Question: 12 Which of the following security attacks cannot be detected by a WIPS solution of any kind? (Choose 2)A. Rogue APsB. DoSC. EavesdroppingD. Social engineeringAnswer: C, D Question: 13 Given: 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. All integrated 802.11ac adapters will work with most protocol analyzers for frame capture, including the Radio Tap Header.B. 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.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. The only method available to capture 802.11ac frames is to perform a remote capture with a compatible access point.Answer: B Question: 14 In order to acquire credentials of a valid user on a public hot-spot network, what attacks may be conducted? Choose the single completely correct answer.A. Social engineering and/or eavesdroppingB. RF DoS and/or physical theftC. MAC denial of service and/or physical theftD. Authentication cracking and/or RF DoSE. Code injection and/or XSSAnswer: A Question: 15 What WLAN client device behavior is exploited by an attacker during a hijacking attack?A. 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.B. 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.C. 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.D. As specified by the Wi-Fi Alliance, clients using Open System authentication must allow direct client-to-client connections, even in an infrastructure BSS.E. Client drivers scan for and connect to access points in the 2.4 GHz band before scanning the 5 GHz band.Answer: A Question: 16 What software and hardware tools are used together to hijack a wireless station from the authorized wireless network onto an unauthorized wireless network? (Choose 2)A. RF jamming device and a wireless radio cardB. A low-gain patch antenna and terminal emulation softwareC. A wireless workgroup bridge and a protocol analyzerD. DHCP server software and access point softwareE. MAC spoofing software and MAC DoS softwareAnswer: A, D Question: 17 Given: 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 hot-spot with this security solution, to what type of wireless attack is a user susceptible? (Choose 2)A. Man-in-the-MiddleB. Wi-Fi phishingC. Management interface exploitsD. UDP port redirectionE. IGMP snoopingAnswer: A, B Question: 18 Given: 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 is needed for Personal Access Credential (PAC) and X.509 certificate validation.B. The username is an input to the LEAP challenge/response hash that is exploited, so the username must be known to conduct authentication cracking.C. 4-Way Handshake nonces are based on the username in WPA and WPA2 authentication.D. The username can be looked up in a dictionary file that lists common username/password combinations.Answer: B Question: 19 Given: 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. 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.C. An unauthorized wireless client device cannot associate, but can eavesdrop on some data because WPA2-Personal does not encrypt multicast or broadcast traffic.D. 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.E. Because WPA2-Personal uses Open System authentication followed by a 4-Way Handshake, hijacking attacks are easily performed.Answer: B Question: 20 Given: 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. What are three uses for such a tool? (Choose 3)A. Transmitting a deauthentication frame to disconnect a user from the AP.B. Auditing the configuration and functionality of a WIPS by simulating common attack sequencesC. Probing the RADIUS server and authenticator to expose the RADIUS shared secretD. Cracking the authentication or encryption processes implemented poorly in some WLANsAnswer: A, B, D Question: 21 Given: You manage a wireless network that services 200 wireless users. Your facility requires 20 access points, and you have installed an IEEE 802.11-compliant implementation of 802.1X/LEAP with AES-CCMP as an authentication and encryption solution.In this configuration, the wireless network is initially susceptible to what type of attacks? (Choose 2)A. Encryption crackingB. Offline dictionary attacksC. Layer 3 peer-to-peerD. Application eavesdroppingE. Session hijackingF. Layer 1 DoSAnswer: B, F Question: 22 Given: 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? (Choose 2)A. MS-CHAPv2 is compliant with WPA-Personal, but not WPA2-Enterprise.B. MS-CHAPv2 is subject to offline dictionary attacks. C. LEAP's use of MS-CHAPv2 is only secure when combined with WEP.D. MS-CHAPv2 is only appropriate for WLAN security when used inside a TLS-encrypted tunnel.E. MS-CHAPv2 uses AES authentication, and is therefore secure.F. When implemented with AES-CCMP encryption, MS-CHAPv2 is very secure.Answer: B, D Question: 23 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-TTLSB. Open 802.11 authentication with IPSecC. 802.1X/PEAPv0/MS-CHAPv2D. WPA2-Personal with AES-CCMPE. EAP-MD5Answer: B Question: 24 Given: 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. 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.B. 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.C. 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.D. 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.Answer: C Topic 2, Security PolicyQuestion: 25 What elements should be addressed by a WLAN security policy? (Choose 2)A. Enabling encryption to prevent MAC addresses from being sent in clear textB. How to prevent non-IT employees from learning about and reading the user security policyC. End-user training for password selection and acceptable network useD. The exact passwords to be used for administration interfaces on infrastructure devicesE. Social engineering recognition and mitigation techniquesAnswer: C, E Question: 26 As a part of a large organization's security policy, how should a wireless security professional address the problem of rogue access points?A. Use a WPA2-Enterprise compliant security solution with strong mutual authentication and encryption for network access of corporate devices.B. Hide the SSID of all legitimate APs on the network so that intruders cannot copy this parameter on rogue APs.C. Conduct thorough manual facility scans with spectrum analyzers to detect rogue AP RF signatures.D. A trained employee should install and configure a WIPS for rogue detection and response measures.E. Enable port security on Ethernet switch ports with a maximum of only 3 MAC addresses on each port.Answer: D Question: 27 In what deployment scenarios would it be desirable to enable peer-to-peer traffic blocking? A. In home networks in which file and printer sharing is enabledB. At public hot-spots in which many clients use diverse applicationsC. In corporate Voice over Wi-Fi networks with push-to-talk multicast capabilitiesD. In university environments using multicast video training sourced from professor's laptopsAnswer: B Question: 28 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. MSCHAPv2 passwords used with EAP/PEAPv0 should be stronger than typical WPA2-PSK passphrases.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. Certificates should always be recommended instead of passwords for 802.11 client authentication.E. EAP-TLS must be implemented in such scenarios.Answer: C Question: 29 Given: 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. Awareness of the exact vendor devices being installedB. Management support for the processC. End-user training manuals for the policies to be createdD. Security policy generation softwareAnswer: B Question: 30 What policy would help mitigate the impact of peer-to-peer attacks against wireless-enabled corporate laptop computers when the laptops are also used on public access networks such as wireless hot-spots?A. Require Port Address Translation (PAT) on each laptop.B.

Require secure applications such as POP, HTTP, and SSH.C. Require VPN software for connectivity to the corporate network.D. Require WPA2-Enterprise as the minimal WLAN security solution.Answer: C Topic 3, WLAN Security Design and Architecture Question: 31 What is one advantage of using EAP-TTLS instead of EAP-TLS as an authentication mechanism in an802.11 WLAN?A. EAP-TTLS sends encrypted supplicant credentials to the authentication server, but EAP-TLS uses unencrypted user credentials.B. EAP-TTLS supports client certificates, but EAP-TLS does not.C. EAP-TTLS does not require an authentication server, but EAP-TLS does.D. EAP-TTLS does not require the use of a certificate for each STA as authentication credentials, but EAP-TLS does.Answer: D Question: 32 What wireless authentication technologies may build a TLS tunnel between the supplicant and the authentication server before passing client authentication credentials to the authentication server? (Choose 3)A. EAP-MD5B. EAP-TLSC. LEAPD. PEAPv0/MSCHAPv2E. EAP-TTLSAnswer: B, D, E Question: 33 While performing a manual scan of your environment using a spectrum analyzer on a laptop computer, you notice a signal in the real time FFT view. The signal is characterized by having peak power centered on channel 11 with an approximate width of 20 MHz at its peak. The signal widens to approximately 40 MHz after it has weakened by about 30 dB.What kind of signal is displayed in the spectrum analyzer?A. A frequency hopping device is being used as a signal jammer in 5 GHzB. A low-power wideband RF attack is in progress in 2.4 GHz, causing significant 802.11 interferenceC. An 802.11g AP operating normally in 2.4 GHzD. An 802.11a AP operating normally in 5 GHzAnswer: C Question: 34 You are using a protocol analyzer for random checks of activity on the WLAN. In the process, you notice two different EAP authentication processes. One process (STA1) used seven EAP frames (excluding ACK frames) before the 4-way handshake and the other (STA2) used 11 EAP frames (excluding ACK frames) before the 4-way handshake.Which statement explains why the frame exchange from one STA required more frames than the frame exchange from another STA when both authentications were successful? (Choose the single most probable answer given a stable WLAN.)A. STA1 and STA2 are using different cipher suites.B. STA2 has retransmissions of EAP frames.C. STA1 is a reassociation and STA2 is an initial association.D. STA1 is a TSN, and STA2 is an RSN.E. STA1 and STA2 are using different EAP types.Answer: E Question: 35 Given: ABC Corporation's 802.11 WLAN is comprised of a redundant WLAN controller pair (N+1) and 30 access points implemented in 2004. ABC implemented WEP encryption with IPSec VPN technology to secure their wireless communication because it was the strongest security solution available at the time it was implemented. IT management has decided to upgrade the WLAN infrastructure and implement Voice over Wi-Fi and is concerned with security because most Voice over Wi-Fi phones do not support IPSec.As the wireless network administrator, what new security solution would be best for protecting ABC's data?A. Migrate corporate data clients to WPA-Enterprise and segment Voice over Wi-Fi phones by assigning them to a different frequency band.B. Migrate corporate data and Voice over Wi-Fi devices to WPA2-Enterprise with fast secure roaming support, and segment Voice over Wi-Fi data on a separate VLAN.C. Migrate to a multi-factor security solution to replace IPSec; use WEP with MAC filtering, SSID hiding, stateful packet inspection, and VLAN segmentation.D. Migrate all 802.11 data devices to WPA-Personal, and implement a secure DHCP server to allocate addresses from a segmented subnet for the Voice over Wi-Fi phones.Answer: B Question: 36 Given: The ABC Corporation currently utilizes an enterprise Public Key Infrastructure (PKI) to allow employees to securely access network resources with smart cards. The new wireless network will use WPA2-Enterprise as its primary authentication solution. You have been asked to recommend a Wi-Fi Alliance-tested EAP method. What solutions will require the least change in how users are currently authenticated and still integrate with their existing PKI?A. EAP-FASTB. EAP-TLSC. PEAPv0/EAP-MSCHAPv2D. LEAPE. PEAPv0/EAP-TLSF. EAP-TTLS/MSCHAPv2Answer: B Question: 37 What statement accurately describes the functionality of the IEEE 802.1X standard?A. Port-based access control with EAP encapsulation over the LAN (EAPoL)B. Port-based access control with dynamic encryption key management and distributionC. Port-based access control with support for authenticated-user VLANs onlyD. Port-based access control with mandatory support of AES-CCMP encryptionE. Port-based access control, which allows three frame types to traverse the uncontrolled port: EAP, DHCP, and DNS.Answer: A Question: 38 In the IEEE 802.11-2012 standard, what is the purpose of the 802.1X Uncontrolled Port?A. To allow only authentication frames to flow between the Supplicant and Authentication ServerB. To block authentication traffic until the 4-Way Handshake completesC. To pass general data traffic after the completion of 802.11 authentication and key managementD. To block unencrypted user traffic after a 4-Way Handshake completesAnswer: A Question: 39 Given: An 802.1X/EAP implementation includes an Active Directory domain controller running Windows Server 2012 and an AP from a major vendor. A Linux server is running RADIUS and it queries the domain controller for user credentials. A Windows client is accessing the network.What device functions as the EAP Supplicant?A. Linux serverB. Windows clientC. Access pointD. Windows serverE. An unlisted switchF. An unlisted WLAN controller Answer: B Question: 40 What wireless security protocol provides mutual authentication without using an X.509 certificate?A. EAP-FASTB. EAP-MD5C. EAP-TLSD. PEAPv0/EAP-MSCHAPv2E. EAP-TTLSF. PEAPv1/EAP-GTCAnswer: A Question: 41 Given: ABC

Company has 20 employees and only needs one access point to cover their entire facility. Ten of ABC Company's employees have laptops with radio cards capable of only WPA security. The other ten employees have laptops with radio cards capable of WPA2 security. The network administrator wishes to secure all wireless communications (broadcast and unicast) for each laptop with its strongest supported security mechanism, but does not wish to implement a RADIUS/AAA server due to complexity.What security implementation will allow the network administrator to achieve this goal?A. Implement an SSID with WPA2-Personal that allows both AES-CCMP and TKIP clients to connect.B. Implement an SSID with WPA-Personal that allows both AES-CCMP and TKIP clients to connect.C. Implement two separate SSIDs on the AP?one for WPA-Personal using TKIP and one for WPA2- Personal using AES-CCMP.D. Implement an SSID with WPA2-Personal that sends all broadcast traffic using AES-CCMP and unicast traffic using either TKIP or AES-CCMP.Answer: C Question: 42What disadvantage does EAP-TLS have when compared with PEAPv0 EAP/MSCHAPv2 as an 802.11 WLAN security solution?A. Fast/secure roaming in an 802.11 RSN is significantly longer when EAP-TLS is in use.B. EAP-TLS does not protect the client's username and password inside an encrypted tunnel.C. EAP-TLS cannot establish a secure tunnel for internal EAP authentication.D. EAP-TLS is supported only by Cisco wireless infrastructure and client devices.E. EAP-TLS requires extensive PKI use to create X.509 certificates for both the server and all clients, which increases administrative overhead.Answer: E Question: 43 Given: You are using WEP as an encryption solution. You are using VLANs for network segregation. Why can you not establish an RSNA?A. RSNA connections require TKIP or CCMP.B. RSNA connections require BIP and do not support TKIP, CCMP or WEP.C. RSNA connections require CCMP and do not support TKIP or WEP.D. RSNA connections do not work in conjunction with VLANs. Answer: A Question: 44 When used as part of a WLAN authentication solution, what is the role of LDAP?A. A data retrieval protocol used by an authentication service such as RADIUSB. An IEEE X.500 standard compliant database that participates in the 802.1X port-based access control processC. A SQL compliant authentication service capable of dynamic key generation and distributionD. A role-based access control protocol for filtering data to/from authenticated stations.E. An Authentication Server (AS) that communicates directly with, and provides authentication for, the Supplicant.Answer: A Question: 45 When implementing a WPA2-Enterprise security solution, what protocol must the selected RADIUS server support?A. LWAPP, GRE, or CAPWAPB. IPSec/ESPC. EAPD. CCMP and TKIPE. LDAPAnswer: C Question: 46 Given: XYZ Company has recently installed an 802.11ac WLAN. The company needs the ability to control access to network services, such as file shares, intranet web servers, and Internet access based on an employee's job responsibilities.What WLAN security solution meets this requirement?A. An autonomous AP system with MAC filtersB. WPA2-Personal with support for LDAP queriesC. A VPN server with multiple DHCP scopesD. A WLAN controller with RBAC featuresE. A WLAN router with wireless VLAN supportAnswer: D Question: 47 Given: Your network includes a controller-based WLAN architecture with centralized data forwarding. The AP builds an encrypted tunnel to the WLAN controller. The WLAN controller is uplinked to the network via a trunked 1 Gbps Ethernet port supporting all necessary VLANs for management, control, and client traffic.What processes can be used to force an authenticated WLAN client's data traffic into a specific VLAN as it exits the WLAN controller interface onto the wired uplink? (Choose 3) A. On the Ethernet switch that connects to the AP, configure the switch port as an access port (not trunking) in the VLAN of supported clients.B. During 802.1X authentication, RADIUS sends a return list attribute to the WLAN controller assigning the user and all traffic to a specific VLAN.C. In the WLAN controller's local user database, create a static username-to-VLAN mapping on the WLAN controller to direct data traffic from a specific user to a designated VLAN.D. Configure the WLAN controller with static SSID-to-VLAN mappings; the user will be assigned to a VLAN according to the SSID being used.Answer: B, C, D Question: 48 What is the purpose of the Pairwise Transient Key (PTK) in IEEE 802.11 Authentication and Key Management?A. The PTK is a type of master key used as an input to the GMK, which is used for encrypting multicast data frames.B. The PTK contains keys that are used to encrypt unicast data frames that traverse the wireless medium.C. The PTK is XOR'd with the PSK on the Authentication Server to create the AAA key.D. The PTK is used to encrypt the Pairwise Master Key (PMK) for distribution to the 802.1X Authenticator prior to the 4-Way Handshake.Answer: B Question: 49 Which one of the following describes the correct hierarchy of 802.1X authentication key derivation?A. The MSK is generated from the 802.1X/EAP authentication. The PMK is derived from the MSK. The PTK is derived from the PMK, and the keys used for actual data encryption are a part of the PTK.B. If passphrase-based client authentication is used by the EAP type, the PMK is mapped directly from the user's passphrase. The PMK is then used during the 4-way handshake to create data encryption keys.C. After successful EAP authentication, the RADIUS server generates a PMK. A separate key, the MSK, is derived from the AAA key and is hashed with the PMK to create the PTK and GTK.D. The PMK is generated from a successful mutual EAP authentication. When mutual authentication is not used, an MSK is created. Either of these two keys may be used to derive the temporal data encryption keys during the 4-way handshake. Answer: A Question: 50 What statement is true regarding the nonces (ANonce and SNonce) used in the IEEE 802.11 4 Way Handshake?A. Both nonces are used by the Supplicant and Authenticator in the derivation of a single PTK.B. The Supplicant uses the SNonce to derive its unique PTK and the Authenticator uses the ANonce to derive its unique PTK, but the nonces are not shared.C. Nonces are sent in EAPoL frames to indicate to the receiver that the sending station has installed and validated the encryption keys.D. The nonces are created by combining the MAC addresses of the Supplicant, Authenticator, and Authentication Server into a mixing algorithm.Answer: A Resources From:1.2024 Latest Braindump2go CWSP-208 Exam Dumps (PDF & VCE) Free Share: **https://www.braindump2go.com/cwsp-208.html**2.2024 Latest Braindump2go CWSP-208 PDF and CWSP-208 VCE Dumps Free Share:**https://drive.google.com/drive/folders/1Bvb61r1HCJtouuhDMQ5hzuZX6FDCrD7O?usp=sharing3.2023 Free Braindump2go CWSP-208 Exam Questions Download: https://www.braindump2go.com/free-online-pdf/CWSP-208-VCE-Dumps(1-50).pdfFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!**