

Free Download Pass4sure and Lead2pass CWNP PW0-204 Exam Question with PDF & VCE (1-10)

QUESTION 1 Given: ABC company is developing an IEEE 802.11 compliant wireless security solution using 802.1X/EAP authentication. According to company policy the security should prevent an eavesdropper from decrypting data frames traversing a wireless connection. What security solution features play a role in adhering to this policy requirement? (Choose 2) A. Group temporal key B. Message integrity check (MIC) C. Multi-factor authentication D. Encrypted passphrase E. Integrity check value F. 4-Way handshake Answer: AF

QUESTION 2 Given: John smith uses a coffee shop's internet hot spot to transfer funds between his checking and saving accounts at his bank's website. The bank's website uses HTTPS protocol to protect sensitive account information. A hacker was able to obtain john's bank account user ID and password and transfers john's money to another account. How did the hacker obtain john's bank Account user ID and password? A. John uses same username and password for banking that he does for email. John used a pop3 email client at the wireless hotspot to check the email and the user ID and password were not encrypted. B. The bank's web server is using an X509 certificate that is not signed by a root CA, causing the user ID and password to be sent unencrypted. C. John's bank is using an expired X509 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. D. Before connecting to the bank's website, john's association to the AP was hijacked. The Attacker interrupted the HTTPS public encryption key from the bank's web server and has decrypted john's login credentials in real time. E. John accessed his corporate network with the IPsec VPN software at the wireless hotspot. 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. Answer: D

QUESTION 3 What statement accurately describes the functions of the IEEE 802.1X standard? A. Port-based access control with support for EAP authentication and AES-CCMP encryption only B. Port-based access control with encryption key management and distribution C. Port-based access control with support for authenticated-user VLANs only D. Port-based access control with 802.3 and 802.11 LANs E. Port-based access control with permission for three frame types: EAP, DHCP, DNS. Answer: A

QUESTION 4 Company's 500 employees use ABC's dual band HT 802.11 WLAN extensively general data traffic, VoWiFi, and guest access internet-only data. Size and network applications, what solution effects common and recommended security practices for this type of network? A. His high security requirements, support EAP-TLS for corporate data and VoWiFi, require WPA or WPA2-personal as well as MAC address filtering for all guest solutions. Segment each data type using a separate data type SSID, frequently band, and VLAN. B. WPA2-Personal for corporate data and VoWiFi application with a long passphrase. For guest access, implement open authentication. Configure two VLANs - one for corporate access and one for guest access - and support WMM on the corporate network. For ease-of-use and network discovery hide the corporate broadcast to the guest SSID. C. PEAPv0/EAP-MSCHAPv2 for corporate data and VoWiFi, use open authentication with captive portal on the guest network. If the VoWiFi phones can not support, use WPA2-personal with a strong passphrase. Segment the three types of traffic by using separate SSIDs and VLANs. D. WPA2 enterprise for all types of network access. For added configuration simplicity, authenticate all users from a single VLAN but apply filtering with IP ACLs by giving each user to group using RADIUS group attributes. Configure the IP ACLs so that each group can only access the necessary resources. Answer: B

QUESTION 5 Given: A VLAN consultant has just finished installing a WLAN controller with 15 controller based APs. Two SSIDs with separate VLANs are configured for this network and LANs are configured to use the same RADIUS server. The SSIDs are configured as follows: SSID Blue-VLAN 10-lightweight EAP (LEAP) authentication-CCMP cipher suite SSID Red-VLAN 20-802.1X/PEAPv0 authentication-TKIP cipher suite The consultant's computer can successfully authenticate and browse the internet when using the Blue SSID. The same computer can authenticate when using the Red SSID. What is most likely cause of problem? A. The consultant does not have a valid Kerberos ID on the Blue VLAN. B. The TKIP cipher suite is not a valid option for 802.1X/PEAPv0 authentications. C. The clock on the consultant's computer post dates the RADIUS server's certificate expiration date/time. D. PEAPv0 authentication is not supported over controller based access points. E. The red VLAN does not support certificate based authentication traffic. Answer: E

QUESTION 6 After completing the installation of new overlay WIPS, what baseline function MUST be performed? A. Approved 802.1X/EAP methods need to be selected and confirmed. B. Configure specifications for upstream and downstream throughput thresholds. C. Classify the authorized, neighbor, and rogue WLAN devices. D. Configure profiles for operation among different regularity domains. Answer: C

QUESTION 7 What different security benefits are provided by endpoint security solution software? (Choose 3) A. Can collect statistics about a user's network use and monitor network threats while they are connected. B. Must be present for support of 802.11k neighbor reports, which improves fast BSS transitions. C. Can be used to monitor and prevent network activity from nearby rogue clients or APs. D. Can prevent connections to networks with security settings that do not confirm to company policy. E.

Can restrict client connections to network with specific SSIDs and encryption types. Answer: ADE QUESTION 8 What software and hardware tools are used together to hijack a wireless station from the authorized wireless network in to an unauthorized wireless networks? (Choose 2) A. A low-gain patch antenna and terminal emulation software B. Narrow band RF jamming devices and wireless radio card C. DHCP server software and access point software D. A wireless work group bridge and protocol analyzer E. MAC spoofing software and MAC DOS software Answer: BC QUESTION 9 Given: ABC company is implementing a secure 802.11 WLAN at their head quarters building in New York and at each of the 10 small, remote branch offices around the country 802.1X/EAP is ABC's preferred security solution. Where possible At all access points (at the headquarters building and all branch offices) connect to single WLAN controller located at the head quarters building, what additional security considerations should be made? (Choose 2) A. An encrypted connection between the WLAN controller and each controller-based AP should be used or all branch offices should be connected to the head quarters building a VPN. B. Remote WIPS sensors should be installed at the headquarters building and at all branch office to monitor and enforce wireless security. C. RADIUS service should always be provided at branch offices so that user authentication is kept on the local network. D. Remote management via telnet, SSH, HTTP, HTTPS should be permitted across the WLAN link. Answer: AB QUESTION 10 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. NAV-based DoS attacks B. RF DoS attacks C. Layer 2 Disassociation attacks D. Robust management frame replay attacks E. EAPoL flood attacks Answer: CD If you want to pass the CWNP PW0-204 exam successfully, recommend to read latest CWNP [PW0-204 Dumps](#) full version.

