# [Free OfferSY0-401 Dumps PDF VCE for CompTIA SY0-401 Exam 1867Q&As(2016-August)from Braindump2go[NQ81-NQ90

2016/08 SY0-401: CompTIA Security+ Certification Exam Questions New Updated Today! Free Instant Download SY0-401 Exam Dumps(PDF & VCE) 1867Q&As from Braindump2go.com!100% Real Exam Questions! 100% Exam Pass Guaranteed! NEW QUESTION 81 - NEW QUESTION 90: 1.|2016/08 SY0-401 Exam Dumps(PDF & VCE) 1867Q&As Download:http://www.braindump2go.com/sy0-401.html 2.|2016/08 SY0-401 Exam Questions & Answers:https://drive.google.com/folderview?id=0B75b5xYLjSSNTldvc1ZkQlNUc0k&usp=sharing QUESTION 81If you don't know the MAC address of a Linux-based machine, what command-line utility can you use to ascertain it? A. macconfigB. ifconfigC. ipconfigD. config Answer: BExplanation:To find MAC address of a Unix/Linux workstation, use ifconfig or ip a. QUESTION 82An organization does not want the wireless network name to be easily discovered. Which of the following software features should be configured on the access points? A. SSID broadcastB. MAC filterC. WPA2D. Antenna placement Answer: AExplanation:Numerous networks broadcast their name (known as an SSID broadcast) to reveal their presence. QUESTION 83A security architect wishes to implement a wireless network with connectivity to the company's internal network. Before they inform all employees that this network is being put in place, the architect wants to roll it out to a small test segment. Which of the following allows for greater secrecy about this network during this initial phase of implementation? A. Disabling SSID broadcastingB. Implementing WPA2 - TKIPC. Implementing WPA2 - CCMPD. Filtering test workstations by MAC address Answer: AExplanation:Network administrators may choose to disable SSID broadcast to hide their network from unauthorized personnel. However, the SSID is still needed to direct packets to and from the base station, so it's a discoverable value using a wireless packet sniffer. Thus, the SSID should be disabled if the network isn't for public use. QUESTION 84While previously recommended as a security measure, disabling SSID broadcast is not effective against most attackers because network SSIDs are: A. no longer used to authenticate to most wireless networks.B. contained in certain wireless packets in plaintext.C. contained in all wireless broadcast packets by default.D. no longer supported in 802.11 protocols. Answer: BExplanation:The SSID is still required for directing packets to and from the base station, so it can be discovered using a wireless packet sniffer. QUESTION 85A company provides secure wireless Internet access for visitors and vendors working onsite. Some of the vendors using older technology report that they are unable to access the wireless network after entering the correct network information. Which of the following is the MOST likely reason for this issue? A. The SSID broadcast is disabled.B. The company is using the wrong antenna type.C. The MAC filtering is disabled on the access point.D. The company is not using strong enough encryption. Answer: AExplanation:When the SSID is broadcast, any device with an automatic detect and connect feature is able to see the network and can initiate a connection with it. The fact that they cannot access the network means that they are unable to see it. QUESTION 86Which of the following best practices makes a wireless network more difficult to find? A. Implement MAC filteringB. UseWPA2-PSKC. Disable SSID broadcastD. Power down unused WAPs Answer: CExplanation:Network administrators may choose to disable SSID broadcast to hide their network from unauthorized personnel. However, the SSID is still needed to direct packets to and from the base station, so it's a discoverable value using a wireless packet sniffer. Thus, the SSID should be disabled if the network isn't for public use. QUESTION 87Jane, the security administrator, sets up a new AP but realizes too many outsiders are able to connect to that AP and gain unauthorized access.Which of the following would be the BEST way to mitigate this issue and still provide coverage where needed? (Select TWO). A. Disable the wired portsB. Use channels 1, 4 and 7 onlyC. Enable MAC filteringD. Disable SSID broadcastE. Switch from 802.11a to 802.11b Answer: CDExplanation: Network administrators may choose to disable SSID broadcast to hide their network from unauthorized personnel. However, the SSID is still needed to direct packets to and from the base station, so it's a discoverable value using a wireless packet sniffer. Thus, the SSID should be disabled if the network isn't for public use.A MAC filter is a list of authorized wireless client interface MAC addresses that is used by a WAP to block access to all unauthorized devices. QUESTION 88Which of the following wireless security technologies continuously supplies new keys for WEP? A. TKIPB. Mac filteringC. WPA2D. WPA Answer: AExplanation: TKIP is a suite of algorithms that works as a "wrapper" to WEP, which allows users of legacy WLAN equipment to upgrade to TKIP without replacing hardware. TKIP uses the original WEP programming but "wraps" additional code at the beginning and end to encapsulate and modify it. QUESTION 89A network administrator has been tasked with securing the WLAN. Which of the following cryptographic products would be used to provide the MOST secure environment for the WLAN? A. WPA2 CCMPB. WPAC. WPA with MAC filteringD. WPA2 TKIP Answer: AExplanation:CCMP is the standard encryption protocol for use with the WPA2 standard and is much more secure than the WEP protocol and TKIP protocol of WPA. CCMP provides the following security services:Data confidentiality; ensures only authorized parties can access the information Authentication; provides proof of

genuineness of the user Access control in conjunction with layer managementBecause CCMP is a block cipher mode using a 128-bit key, it is secure against attacks to the 264 steps of operation. QUESTION 90An access point has been configured for AES encryption but a client is unable to connect to it. Which of the following should be configured on the client to fix this issue? A. WEPB. CCMPC. TKIPD. RC4 Answer: BExplanation:CCMP is an encryption protocol designed for Wireless LAN products that implement the standards of the IEEE 802.11i amendment to the original IEEE 802.11 standard. CCMP is an enhanced data cryptographic encapsulation mechanism designed for data confidentiality and based upon the Counter Mode with CBC-MAC (CCM) of the AES standard. !!!RECOMMEND!!! 1.|2016/08 SY0-401 PDF Dumps & VCE Dumps 1867Q&As Download: http://www.braindump2go.com/sy0-401.html 2.|2016/08 SY0-401 Questions & Answers: https://drive.google.com/folderview?id=0B75b5xYLjSSNTldvc1ZkQlNUc0k&usp=sharing