# [2017 New Free Downloading SY0-401 Exam Dumps PDF From Lead2pass (76-100)

2017 July CompTIA Official New Released SY0-401 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! After purchasing the dumps for the SY0-401 Exam from Lead2pass, I had no doubt that I'd easily pass the exam. Bundle of thanks to Lead2pass for helping me pass the exam without any troubles. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 76Matt, a systems security engineer, is determining which credential-type authentication to use within a planned 802.1x deployment. He is looking for a method that does not require a client certificate, has a server side certificate, and uses TLS tunnels for encryption. Which credential type authentication method BEST fits these requirements? A. EAP-TLSB. EAP-FASTC. PEAP-CHAPD. PEAP-MSCHAPv2Answer: DExplanation: PEAP-MS-CHAP v2 is easier to deploy than EAP-TLS or PEAP-TLS because user authentication is accomplished via password-base credentials (user name and password) rather than digital certificates or smart cards. Only servers running Network Policy Server (NPS) or PEAP-MS-CHAP v2 are required to have a certificate. QUESTION 77Which of the following means of wireless authentication is easily vulnerable to spoofing? A. MAC FilteringB. WPA - LEAPC. WPA - PEAPD. Enabled SSID Answer: AExplanation:Each network interface on your computer or any other networked device has a unique MAC address. These MAC addresses are assigned in the factory, but you can easily change, or "spoof," MAC addresses in software.Networks can use MAC address filtering, only allowing devices with specific MAC addresses to connect to a network. This isn't a great security tool because people can spoof their MAC addresses. QUESTION 78Ann, a sales manager, successfully connected her company-issued smartphone to the wireless network in her office without supplying a username/password combination. Upon disconnecting from the wireless network, she attempted to connect her personal tablet computer to the same wireless network and could not connect. Which of the following is MOST likely the reason? A. The company wireless is using a MAC filter.B. The company wireless has SSID broadcast disabled.C. The company wireless is using WEP.D. The company wireless is using WPA2. Answer: AExplanation: MAC filtering allows you to include or exclude computers and devices based on their MAC address. QUESTION 79After entering the following information into a SOHO wireless router, a mobile device's user reports being unable to connect to the network: PERMIT 0A: D1: FA. B1: 03: 37DENY 01: 33: 7F: AB: 10: AB Which of the following is preventing the device from connecting? A. WPA2-PSK requires a supplicant on the mobile device.B. Hardware address filtering is blocking the device.C. TCP/IP Port filtering has been implemented on the SOHO router.D. IP address filtering has disabled the device from connecting. Answer: B Explanation:MAC filtering allows you to include or exclude computers and devices based on their MAC address. QUESTION 80A security analyst has been tasked with securing a guest wireless network. They recommend the company use an authentication server but are told the funds are not available to set this up.Which of the following BEST allows the analyst to restrict user access to approved devices? A. Antenna placementB. Power level adjustmentC. Disable SSID broadcastingD. MAC filtering Answer: DExplanation: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 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: A Explanation: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. QUESTION 91A security administrator wishes to increase the security of the wireless network. Which of the following BEST addresses this concern? A. Change the encryption from TKIP-based to CCMP-based.B. Set all nearby access points to operate on the same channel.C. Configure the access point to use WEP instead of WPA2.D. Enable all access points to broadcast their SSIDs. Answer: AExplanation:CCMP makes use of 128-bit AES encryption with a 48-bit initialization vector. This initialization vector makes cracking a bit more difficult. QUESTION 92The security administrator has been tasked to update all the access points to provide a more secure connection. All access points currently use WPA TKIP for encryption. Which of the following would be configured to provide more secure connections? A. WEPB. WPA2 CCMPC. Disable SSID broadcast and increase power levelsD. MAC filtering Answer: BExplanation:CCMP makes use of 128-bit AES encryption with a 48-bit initialization vector. This initialization vector makes cracking a bit more difficult. QUESTION 93A system administrator wants to enable WPA2 CCMP. Which of the following is the only encryption used? A. RC4B. DESC. 3DESD. AES Answer: DExplanation:Cipher Block Chaining Message Authentication Code Protocol (CCMP) makes use of 128-bit AES encryption with a 48-bit initialization vector. QUESTION 94Jane, an administrator, needs to make sure the wireless network is not accessible from the parking area of their office. Which of the following would BEST help Jane when deploying a new access point? A. Placement of antennaB. Disabling the SSIDC. Implementing WPA2D. Enabling the MAC filtering Answer: A Explanation:You should try to avoid placing access points near metal (which includes appliances) or near the ground. Placing them in the center of the area to be served and high enough to get around most obstacles is recommended. On the chance that the signal is actually traveling too far, some access points include power level controls, which allow you to reduce the amount of output provided. QUESTION 95A security team has identified that the wireless signal is broadcasting into the parking lot. To reduce the risk of an attack against the wireless network from the parking lot, which of the following controls should be used? (Select TWO). A. Antenna placementB. InterferenceC. Use WEPD. Single Sign onE. Disable the SSIDF. Power levels Answer: AF

Explanation:Placing the antenna in the correct position is crucial. You can then adjust the power levels to exclude the parking lot. QUESTION 96Which of the following would Pete, a security administrator, do to limit a wireless signal from penetrating the exterior walls? A. Implement TKIP encryptionB. Consider antenna placementC. Disable the SSID broadcastD. Disable WPA Answer: BExplanation: Cinderblock walls, metal cabinets, and other barriers can reduce signal strength significantly. Therefore, antenna placement is critical. QUESTION 97Ann, a security administrator, has concerns regarding her company's wireless network. The network is open and available for visiting prospective clients in the conference room, but she notices that many more devices are connecting to the network than should be.Which of the following would BEST alleviate Ann's concerns with minimum disturbance of current functionality for clients? A. Enable MAC filtering on the wireless access point.B. Configure WPA2 encryption on the wireless access point.C. Lower the antenna's broadcasting power.D. Disable SSID broadcasting. Answer: C Explanation:Some access points include power level controls that allow you to reduce the amount of output provided if the signal is traveling too far. QUESTION 98After reviewing the firewall logs of her organization's wireless APs, Ann discovers an unusually high amount of failed authentication attempts in a particular segment of the building. She remembers that a new business moved into the office space across the street. Which of the following would be the BEST option to begin addressing the issue? A. Reduce the power level of the AP on the network segmentB. Implement MAC filtering on the AP of the affected segmentC. Perform a site survey to see what has changed on the segmentD. Change the WPA2 encryption key of the AP in the affected segment Answer: A Explanation:Some access points include power level controls that allow you to reduce the amount of output provided if the signal is traveling too far. QUESTION 99An administrator wants to establish a WiFi network using a high gain directional antenna with a narrow radiation pattern to connect two buildings separated by a very long distance. Which of the following antennas would be BEST for this situation? A. DipoleB. YagiC. SectorD. Omni Answer: BExplanation:A Yagi-Uda antenna, commonly known simply as a Yagi antenna, is a directional antenna consisting of multiple parallel dipole elements in a line, usually made of metal rods. It consists of a single driven element connected to the transmitter or receiver with a transmission line, and additional parasitic elements: a so-called reflector and one or more directors. The reflector element is slightly longer than the driven dipole, whereas the directors are a little shorter. This design achieves a very substantial increase in the antenna's directionality and gain compared to a simple dipole. QUESTION 100A company has recently implemented a high density wireless system by having a junior technician install two new access points for every access point already deployed. Users are now reporting random wireless disconnections and slow network connectivity. Which of the following is the MOST likely cause? A. The old APs use 802.11aB. Users did not enter the MAC of the new APsC. The new APs use MIMOD. A site survey was not conducted Answer: DExplanation:To test the wireless AP placement, a site survey should be performed. I understood all of the questions very easily. I scored 96% on my first try. I am definitely going to spread the word amongst friends and colleagues. Keep up the great work. SY0-401 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDVzFZWExUbFM0YU0 2017 CompTIA **SY0-401** exam dumps (All 1868 Q&As) from Lead2pass: https://www.lead2pass.com/sy0-401.html [100% Exam Pass Guaranteed]