[Lead2pass New Lead2pass Latest SY0-501 PDF Guarantee 100% Pass SY0-501 Exam (91-100)

Lead2pass 2017 November New CompTIA SY0-501 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! SY0-501 easy pass guide: Preparing for CompTIA SY0-501 exam is really a tough task to accomplish. However, Lead2pass delivers the most comprehensive braindumps, covering each and every aspect of SY0-501 exam curriculum. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-501.html QUESTION 91A company has three divisions, each with its own networks and services. The company decides to make its secure web portal accessible to all employees utilizing their existing usernames and passwords, The security administrator has elected to use SAML to support authentication. In this scenario, which of the following will occur when users try to authenticate to the portal? (Select TWO) A. The portal will function as an identity provider and issue an authentication assertionB. The portal will request an authentication ticket from each network that is transitively trustedC. The back-end networks will function as an identity provider and issue an authentication assertionD. The back-end networks will request authentication tickets from the portal, which will act as the third-party service provider authentication storeE. The back-end networks will verify the assertion token issued by the portal functioning as the identity providerAnswer: C QUESTION 92Which of the following would a security specialist be able to determine upon examination of a server's certificate? A. CA public keyB. Server private keyC. CSRD. OID Answer: B QUESTION 93A user suspects someone has been accessing a home network without permission by spoofing the MAC address of an authorized system While attempting to determine if an unauthorized user is togged into the home network, the user reviews the wireless router, which shows the following table for systems that are currently on the home network. Which of the following should be the NEXT step to determine if there is an unauthorized user on the network? A. Apply MAC filtering and see if the router drops any of the systems. B. Physically check each of the authorized systems to determine if they are togged onto the network.C. Deny the "unknown" host because the hostname is not known and MAC filtering is not applied to this host.D. Conduct a ping sweep of each of the authorized systems and see if an echo response is received. Answer: C QUESTION 94Drag and Drop QuestionA Security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center. Drag and Drop the applicable controls to each asset type.Instructions: Controls can be used multiple times and not all placeholders needs to be filled. When you have completed the simulation, Please select Done to submit. Answer: Explanation:Cable locks are used as a hardware lock mechanism ?thus best used on a Data Center Terminal Server.Network monitors are also known as sniffers ?thus best used on a Data Center Terminal Server.Install antivirus software. Antivirus software should be installed and definitions kept current on all hosts. Antivirus software should run on the server as well as on every workstation. In addition to active monitoring of incoming fi les, scans should be conducted regularly to catch any infections that have slipped through- thus best used on a Data Center Terminal Server.Proximity readers are used as part of physical barriers which makes it more appropriate to use on a center's entrance to protect the terminal server. Mentor app is an Apple application used for personal development and is best used on a mobile device such as a smart phone.Remote wipe is an application that can be used on devices that are stolen to keep data safe. It is basically a command to a phone that will remotely clear the data on that phone. This process is known as a remote wipe, and it is intended to be used if the phone is stolen or going to another user.Should a device be stolen, GPS (Global Positioning System) tracking can be used to identify its location and allow authorities to find it - thus best used on a smart phone. Screen Lock is where the display should be configured to time out after a short period of inactivity and the screen locked with a password. To be able to access the system again, the user must provide the password. After a certain number of attempts, the user should not be allowed to attempt any additional logons; this is called lockout ?thus best used on a smart phone.Strong Password since passwords are always important, but even more so when you consider that the device could be stolen and in the possession of someone who has unlimited access and time to try various values ?thus best use strong passwords on a smartphone as it can be stolen more easily than a terminal server in a data center. Device Encryption- Data should be encrypted on the device so that if it does fall into the wrong hands, it cannot be accessed in a usable form without the correct passwords. It is recommended to you use Trusted Platform Module (TPM) for all mobile devices where possible.Use pop-up blockers. Not only are pop-ups irritating, but they are also a security threat. Pop-ups (including pop-unders) represent unwanted programs running on the system, and they can jeopardize the system's well-being. This will be more effective on a mobile device rather than a terminal server.Use host-based firewalls. A firewall is the first line of defense against attackers and malware. Almost every current operating system includes a firewall, and most are turned on by Default- thus best used on a Data Center Terminal Server. QUESTION 95A security consultant discovers that an organization is using the PCL protocol to print documents, utilizing the default driver and print settings. Which of the following is the MOST likely risk in this situation? A. An attacker can access and change the printer configuration.B. SNMP data leaving the printer will

not be properly encrypted.C. An MITM attack can reveal sensitive information.D. An attacker can easily inject malicious code into the printer firmware.E. Attackers can use the PCL protocol to bypass the firewall of client computers. Answer: A QUESTION 96A security analyst is hardening a server with the directory services role installed. The analyst must ensure LDAP traffic cannot be monitored or sniffed and maintains compatibility with LDAP clients. Which of the following should the analyst implement to meet these requirements? (Select TWO). A. Generate an X 509-complaint certificate that is signed by a trusted CA.B. Install and configure an SSH tunnel on the LDAP server.C. Ensure port 389 is open between the clients and the servers using the communication.D. Ensure port 636 is open between the clients and the servers using the communication.E. Remove the LDAP directory service role from the server. Answer: AB QUESTION 97Drag and Drop QuestionDrag and drop the correct protocol to its default port. Answer: Explanation:FTP uses TCP port 21.Telnet uses port 23.SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP). Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP).SMTP uses TCP port 25.Port 69 is used by TFTP.SNMP makes use of UDP ports 161 and 162. http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers QUESTION 98A botnet has hit a popular website with a massive number of GRE-encapsulated packets to perform a DDoS attack News outlets discover a certain type of refrigerator was exploited and used to send outbound packets to the website that crashed. To which of the following categories does the refrigerator belong? A. SoCB. ICSC. IoTD. MFD Answer: D QUESTION 99The Chief Technology Officer (CTO) of a company, Ann, is putting together a hardware budget for the next 10 years. She is asking for the average lifespan of each hardware device so that she is able to calculate when she will have to replace each device. Which of the following categories BEST describes what she is looking for? A. ALEB. MTTRC. MTBFD. MTTF Answer: D QUESTION 100A software developer wants to ensure that the application is verifying that a key is valid before establishing SSL connections with random remote hosts on the Internet.Which of the following should be used in the code? (Select TWO.) A. Escrowed keysB. SSL symmetric encryption keyC. Software code private keyD. Remote server public keyE. OCSP Answer: CE More free Lead2pass SY0-501 exam new questions on Google Drive: https://drive.google.com/open?id=1Hm6GQHDVOsEnyhNf3EHqIGEtor5IUsfu Lead2pass provides guarantee of CompTIA SY0-501 exam because Lead2pass is an authenticated IT certifications site. The SY0-501 dump is updated with regular basis and the answers are rechecked of every exam. Good luck in your exam. 2017 CompTIA SY0-501 (All 166 Q&As) exam dumps (PDF&VCE) from Lead2pass: https://www.lead2pass.com/sy0-501.html [100% Exam Pass Guaranteed]