[2017 New 2017 New SY0-401 Exam PDF Ensure SY0-401 Certification Exam Pass 100% (51-75)

2017 July CompTIA Official New Released SY0-401 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! Lead2pass is now offering Lead2pass SY0-401 dumps PDF and Test Engine with 100% passing guarantee. Buy Lead2pass SY0-401 PDF and pass your exam easily. If you want real exam simulation then buy test engine and install on your pc for preparation. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 51An administrator connects VoIP phones to the same switch as the network PCs and printers. Which of the following would provide the BEST logical separation of these three device types while still allowing traffic between them via ACL? A. Create three VLANs on the switch connected to a routerB. Define three subnets, configure each device to use their own dedicated IP address range, and then connect the network to a routerC. Install a firewall and connect it to the switchD. Install a firewall and connect it to a dedicated switch for each device typeAnswer: AExplanation:A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. Communications between ports within the same VLAN occur without hindrance, but communications between VLANs require a routing function. QUESTION 52An administrator needs to segment internal traffic between layer 2 devices within the LAN. Which of the following types of network design elements would MOST likely be used? A. RoutingB. DMZC. VLAND. NAT Answer: CExplanation:A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. Communications between ports within the same VLAN occur without hindrance, but communications between VLANs require a routing function. QUESTION 53Pete, a security administrator, is informed that people from the HR department should not have access to the accounting department's server, and the accounting department should not have access to the HR department's server. The network is separated by switches. Which of the following is designed to keep the HR department users from accessing the accounting department's server and vice-versa? A. ACLsB. VLANsC. DMZsD. NATS Answer: BExplanation:A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. Communications between ports within the same VLAN occur without hindrance, but communications between VLANs require a routing function. QUESTION 54According to company policy an administrator must logically keep the Human Resources department separated from the Accounting department. Which of the following would be the simplest way to accomplish this? A. NIDSB. DMZC. NATD. VLAN Answer: DExplanation: A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. QUESTION 55Review the following diagram depicting communication between PC1 and PC2 on each side of a router. Analyze the network traffic logs which show communication between the two computers as captured by the computer with IP 10.2.2.10. DIAGRAMPC1 PC2[192.168.1.30]--------[INSIDE 192.168.1.1 router OUTSIDE 10.2.2.1]---------[10.2.2.10] LOGS10:30:22, SRC 10.2.2.1:3030, DST 10.2.2.10:80, SYN10:30:23, SRC 10.2.2.10:80, DST 10.2.2.1:3030, SYN/ACK10:30:24, SRC 10.2.2.1:3030, DST 10.2.2.10:80, ACK Given the above information, which of the following can be inferred about the above environment? A. 192.168.1.30 is a web server.B. The web server listens on a non-standard port.C. The router filters port 80 traffic.D. The router implements NAT. Answer: DExplanation:Network address translation (NAT) allows you to share a connection to the public Internet via a single interface with a single public IP address. NAT maps the private addresses to the public address. In a typical configuration, a local network uses one of the designated "private" IP address subnets. A router on that network has a private address (192.168.1.1) in that address space, and is also connected to the Internet with a "public" address (10.2.2.1) assigned by an Internet service provider. QUESTION 56An administrator wishes to hide the network addresses of an internal network when connecting to the Internet. The MOST effective way to mask the network address of the users would be by passing the traffic through a: A. stateful firewallB. packet-filtering firewallC. NIPSD. NAT Answer: DExplanation:NAT serves as a basic firewall by only allowing incoming traffic that is in response to an internal system's request. QUESTION 57A company's business model was changed to provide more web presence and now its ERM software is no longer able to support the security needs of the company. The current data center will continue to provide network and security services. Which of the following network elements would be used to support the new business model? A. Software as a ServiceB. DMZC. Remote access supportD. Infrastructure as a Service Answer: AExplanation:Software as a Service (SaaS) allows for on-demand online access to specific software applications or suites without having to install it locally. This will allow the data center to continue providing network and security services. QUESTION 58The Chief Information Officer (CIO) has mandated web based Customer Relationship Management (CRM) business functions be moved offshore to reduce cost, reduce IT overheads, and improve availability. The Chief Risk Officer (CRO) has agreed with the CIO's direction but has mandated that key authentication systems be run within the organization's network. Which of the following would BEST meet the CIO and

CRO's requirements? A. Software as a ServiceB. Infrastructure as a ServiceC. Platform as a ServiceD. Hosted virtualization service Answer: AExplanation:Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. QUESTION 59An IT director is looking to reduce the footprint of their company's server environment. They have decided to move several internally developed software applications to an alternate environment, supported by an external company. Which of the following BEST describes this arrangement? A. Infrastructure as a ServiceB. Storage as a ServiceC. Platform as a ServiceD. Software as a Service Answer: AExplanation:Cloud users install operating-system images and their application software on the cloud infrastructure to deploy their applications. In this model, the cloud user patches and maintains the operating systems and the application software. QUESTION 60Which of the following offerings typically allows the customer to apply operating system patches? A. Software as a serviceB. Public CloudsC. Cloud Based StorageD. Infrastructure as a service Answer: DExplanation:Cloud users install operating-system images and their application software on the cloud infrastructure to deploy their applications. In this model, the cloud user patches and maintains the operating systems and the application software. QUESTION 61Which of the following technologies can store multi-tenant data with different security requirements? A. Data loss preventionB. Trusted platform moduleC. Hard drive encryptionD. Cloud computing Answer: DExplanation:One of the ways cloud computing is able to obtain cost efficiencies is by putting data from various clients on the same machines. This "multitenant" nature means that workloads from different clients can be on the same system, and a flaw in implementation could compromise security. QUESTION 62Multi-tenancy is a concept found in which of the following? A. Full disk encryptionB. Removable mediaC. Cloud computingD. Data loss prevention Answer: CExplanation:One of the ways cloud computing is able to obtain cost efficiencies is by putting data from various clients on the same machines. This "multitenant" nature means that workloads from different clients can be on the same system, and a flaw in implementation could compromise security. QUESTION 63Which of the following devices is BEST suited to protect an HTTP-based application that is susceptible to injection attacks? A. Protocol filterB. Load balancerC. NIDSD. Layer 7 firewall Answer: DExplanation:An application-level gateway firewall filters traffic based on user access, group membership, the application or service used, or even the type of resources being transmitted. This type of firewall operates at the Application layer (Layer 7) of the OSI model. QUESTION 64Concurrent use of a firewall, content filtering, antivirus software and an IDS system would be considered components of: A. Redundant systems.B. Separation of duties.C. Layered security.D. Application control. Answer: CExplanation:Layered security is the practice of combining multiple mitigating security controls to protect resources and data. QUESTION 65A network engineer is designing a secure tunneled VPN. Which of the following protocols would be the MOST secure? A. IPsecB. SFTPC. BGPD. PPTP Answer: AExplanation:Layer 2 Tunneling Protocol (L2TP) came about through a partnership between Cisco and Microsoft with the intention of providing a more secure VPN protocol. L2TP is considered to be a more secure option than PPTP, as the IPSec protocol which holds more secure encryption algorithms, is utilized in conjunction with it. It also requires a pre-shared certificate or key. L2TP's strongest level of encryption makes use of 168 bit keys, 3 DES encryption algorithm and requires two levels of authentication.L2TP has a number of advantages in comparison to PPTP in terms of providing data integrity and authentication of origin verification designed to keep hackers from compromising the system. However, the increased overhead required to manage this elevated security means that it performs at a slower pace than PPTP. QUESTION 66Pete, a network administrator, is implementing IPv6 in the DMZ. Which of the following protocols must he allow through the firewall to ensure the web servers can be reached via IPv6 from an IPv6 enabled Internet host? A. TCP port 443 and IP protocol 46B. TCP port 80 and TCP port 443C. TCP port 80 and ICMPD. TCP port 443 and SNMP Answer: BExplanation:HTTP and HTTPS, which uses TCP port 80 and TCP port 443 respectively, is necessary for Communicating with Web servers. It should therefore be allowed through the firewall. QUESTION 67Which of the following ports and protocol types must be opened on a host with a host-based firewall to allow incoming SFTP connections? A. 21/UDPB. 21/TCPC. 22/UDPD. 22/TCP Answer: DExplanation:SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. QUESTION 68A network administrator is asked to send a large file containing PII to a business associate.Which of the following protocols is the BEST choice to use? A. SSHB. SFTPC. SMTPD. FTP Answer: BExplanation:SFTP encrypts authentication and data traffic between the client and server by making use of SSH to provide secure FTP communications. As a result, SFTP offers protection for both the authentication traffic and the data transfer taking place between a client and server. QUESTION 69Which of the following is a difference between TFTP and FTP? A. TFTP is slower than FTP.B. TFTP is more secure than FTP.C. TFTP utilizes TCP and FTP uses UDP.D. TFTP utilizes UDP and FTP uses TCP. Answer: DExplanation:FTP employs TCP ports 20 and 21 to establish and maintain client-to-server communications, whereas TFTP makes use of UDP port 69. QUESTION 70Which of the following is the default port for TFTP? A. 20B. 69C. 21D. 68 Answer: BExplanation:TFTP makes use of UDP port 69. QUESTION 71A network consists of various remote sites that connect

back to two main locations. Pete, the security administrator, needs to block TELNET access into the network. Which of the following, by default, would be the BEST choice to accomplish this goal? A. Block port 23 on the L2 switch at each remote siteB. Block port 23 on the network firewallC. Block port 25 on the L2 switch at each remote siteD. Block port 25 on the network firewall Answer: BExplanation:Telnet is a terminal-emulation network application that supports remote connectivity for executing commands and running applications but doesn't support transfer of fi les. Telnet uses TCP port 23. Because it's a clear text protocol and service, it should be avoided and replaced with SSH. QUESTION 72A security analyst noticed a colleague typing the following command: `Telnet some-host 443' Which of the following was the colleague performing? A. A hacking attempt to the some-host web server with the purpose of achieving a distributed denial of service attack.B. A quick test to see if there is a service running on some-host TCP/443, which is being routed correctly and not blocked by a firewall.C. Trying to establish an insecure remote management session. The colleague should be using SSH or terminal services instead.D. A mistaken port being entered because telnet servers typically do not listen on port 443. Answer: BExplanation:B: The Telnet program parameters are: telnet <hostname> <port> <hostname> is the name or IP address of the remote server to connect to. <port> is the port number of the service to use for the connection. TCP port 443 provides the HTTPS (used for secure web connections) service; it is the default SSL port. By running the Telnet some-host 443 command, the security analyst is checking that routing is done properly and not blocked by a firewall. QUESTION 73Which of the following secure file transfer methods uses port 22 by default? A. FTPSB. SFTPC. SSLD. S/MIME Answer: BExplanation:SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. QUESTION 74Which of the following BEST describes the weakness in WEP encryption? A. The initialization vector of WEP uses a crack-able RC4 encryption algorithm.Once enough packets are captured an XOR operation can be performed and the asymmetric keys can be derived.B. The WEP key is stored in plain text and split in portions across 224 packets of random data.Once enough packets are sniffed the IV portion of the packets can be removed leaving the plain text key.C. The WEP key has a weak MD4 hashing algorithm used.A simple rainbow table can be used to generate key possibilities due to MD4 collisions.D. The WEP key is stored with a very small pool of random numbers to make the cipher text.As the random numbers are often reused it becomes easy to derive the remaining WEP key. Answer: DExplanation:WEP is based on RC4, but due to errors in design and implementation, WEP is weak in a number of areas, two of which are the use of a static common key and poor implementation of initiation vectors (IVs). When the WEP key is discovered, the attacker can join the network and then listen in on all other wireless client communications. QUESTION 75Which of the following would satisfy wireless network implementation requirements to use mutual authentication and usernames and passwords? A. EAP-MD5B. WEPC. PEAP-MSCHAPv2D. EAP-TLS Answer: CExplanation: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. Now we are one step ahead in providing updated real exam dumps for SY0-401. We provide 100% SY0-401 exam passing guarantee as we will provide you same questions of SY0-401 exam with their answers. Our CompTIA SY0-401 new questions are verified by experts. 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]