[2017 New 2017 New SY0-401 Exam PDF Ensure SY0-401 Certification Exam Pass 100% (1-25)

2017 July CompTIA Official New Released SY0-401 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! As a professional IT exam study material provider, Lead2pass gives you more than just SY0-401 exam questions and answers. We provide our customers with the most accurate study material about the SY0-401 exam and the guarantee of pass. We assist you to prepare for SY0-401 certification which is regarded valuable the IT sector. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 1Which of the following should be deployed to prevent the transmission of malicious traffic between virtual machines hosted on a singular physical device on a network? A. HIPS on each virtual machineB. NIPS on the networkC. NIDS on the networkD. HIDS on each virtual machineAnswer: AExplanation:Host-based intrusion prevention system (HIPS) is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host. QUESTION 2Which of the following components of an all-in-one security appliance would MOST likely be configured in order to restrict access to peer-to-peer file sharing websites? A. Spam filterB. URL filterC. Content inspectionD. Malware inspection Answer: BExplanation:The question asks how to prevent access to peer-to-peer file sharing websites. You access a website by browsing to a URL using a Web browser or peer-to-peer file sharing client software. A URL filter is used to block URLs (websites) to prevent users accessing the website.Incorrect Answer:A: A spam filter is used for email. All inbound (and sometimes outbound) email is passed through the spam filter to detect spam emails. The spam emails are then discarded or tagged as potential spam according to the spam filter configuration. Spam filters do not prevent users accessing peer- to-peer file sharing websites.C: Content inspection is the process of inspecting the content of a web page as it is downloaded. The content can then be blocked if it doesn't comply with the company's web policy. Content- control software determines what content will be available or perhaps more often what content will be blocked. Content inspection does not prevent users accessing peer-to-peer file sharing websites (although it could block the content of the sites as it is downloaded).D: Malware inspection is the process of scanning a computer system for malware. Malware inspection does not prevent users accessing peer-to-peer file sharing websites. QUESTION 3Pete, the system administrator, wants to restrict access to advertisements, games, and gambling web sites. Which of the following devices would BEST achieve this goal? A. FirewallB. SwitchC. URL content filterD. Spam filter Answer: CExplanation:URL filtering, also known as web filtering, is the act of blocking access to a site based on all or part of the URL used to request access. URL filtering can focus on all or part of a fully qualified domain name (FQDN), specific path names, specific filenames, specific fi le extensions, or entire specific URLs. Many URL-filtering tools can obtain updated master URL block lists from vendors as well as allow administrators to add or remove URLs from a custom list. QUESTION 4The administrator receives a call from an employee named Joe. Joe says the Internet is down and he is receiving a blank page when typing to connect to a popular sports website. The administrator asks Joe to try visiting a popular search engine site, which Joe reports as successful. Joe then says that he can get to the sports site on this phone. Which of the following might the administrator need to configure? A. The access rules on the IDSB. The pop up blocker in the employee's browserC. The sensitivity level of the spam filterD. The default block page on the URL filter Answer: DExplanation:A URL filter is used to block access to a site based on all or part of a URL. There are a number of URL-filtering tools that can acquire updated master URL block lists from vendors, as well as allow administrators to add or remove URLs from a custom list. QUESTION 5Layer 7 devices used to prevent specific types of html tags are called: A. FirewallsB. Content filtersC. RoutersD. NIDS Answer: BExplanation:A content filter is a is a type of software designed to restrict or control the content a reader is authorised to access, particularly when used to limit material delivered over the Internet via the Web, e-mail, or other means. Because the user and the OSI layer interact directly with the content filter, it operates at Layer 7 of the OSI model. QUESTION 6Pete, an employee, attempts to visit a popular social networking site but is blocked. Instead, a page is displayed notifying him that this site cannot be visited. Which of the following is MOST likely blocking Pete's access to this site? A. Internet content filterB. FirewallC. Proxy serverD. Protocol analyzer Answer: AExplanation:Web filtering software is designed to restrict or control the content a reader is authorised to access, especially when utilised to restrict material delivered over the Internet via the Web, e-mail, or other means. QUESTION 7A review of the company's network traffic shows that most of the malware infections are caused by users visiting gambling and gaming websites. The security manager wants to implement a solution that will block these websites, scan all web traffic for signs of malware, and block the malware before it enters the company network. Which of the following is suited for this purpose? A. ACLB. IDSC. UTMD. Firewall Answer: CExplanation:An all-in-one appliance, also known as Unified Threat Management (UTM) and Next Generation Firewall (NGFW), is one that provides a good foundation for security. A variety is available; those that you should be familiar with for the exam fall under the categories of providing URL filtering, content

inspection, or malware inspection.Malware inspection is the use of a malware scanner to detect unwanted software content in network traffic. If malware is detected, it can be blocked or logged and/or trigger an alert. QUESTION 8Which of the following is BEST at blocking attacks and providing security at layer 7 of the OSI model? A. WAFB. NIDSC. RoutersD. Switches Answer: AExplanation:A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked. The effort to perform this customization can be significant and needs to be maintained as the application is modified.As the protocols used to access a web server (typically HTTP and HTTPS) run in layer 7 of the OSI model, then web application firewall (WAF) is the correct answer. QUESTION 9Which of the following should the security administrator implement to limit web traffic based on country of origin? (Select THREE). A. Spam filterB. Load balancerC. AntivirusD. ProxiesE. FirewallF. NIDSG. URL filtering Answer: DEGExplanation:A proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers.Firewalls manage traffic using a rule or a set of rules. A URL is a reference to a resource that specifies the location of the resource. A URL filter is used to block access to a site based on all or part of a URL. QUESTION 10A security engineer is reviewing log data and sees the output below: POST: /payload.php HTTP/1.1HOST: localhostAccept: */*Referrer: http://localhost/ *******HTTP/1.1 403 ForbiddenConnection: closeLog: Access denied with 403. Pattern matches form bypass Which of the following technologies was MOST likely being used to generate this log? A. Host-based Intrusion Detection SystemB. Web application firewallC. Network-based Intrusion Detection SystemD. Stateful Inspection FirewallE. URL Content Filter Answer: BExplanation:A web application firewall is a device, server add-on, virtual service, or system filter that defines a strict set of communication rules for a website and all visitors. It's intended to be an application- specific firewall to prevent cross-site scripting, SQL injection, and other web application attacks. QUESTION 11An administrator would like to review the effectiveness of existing security in the enterprise. Which of the following would be the BEST place to start? A. Review past security incidents and their resolutionB. Rewrite the existing security policyC. Implement an intrusion prevention systemD. Install honey pot systems Answer: CExplanation:The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it QUESTION 12A company has proprietary mission critical devices connected to their network which are configured remotely by both employees and approved customers. The administrator wants to monitor device security without changing their baseline configuration. Which of the following should be implemented to secure the devices without risking availability? A. Host-based firewallB. IDSC. IPSD. Honeypot Answer: BExplanation:An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.IDPSes typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content. QUESTION 13Lab Sim - Configure the FirewallTask: Configure the firewall (fill out the table) to allow these four rules: - Only allow the Accounting computer to have HTTPS access to the Administrative server.- Only allow the HR computer to be able to communicate with the Server 2 System over SCP.- Allow the IT computer to have access to both the Administrative Server 1 and Administrative Server 2 Answer: Use the following answer for this simulation task. Below table has all the answers required for this question. Explanation:Firewall rules act like ACLs, and they are used to dictate what traffic can pass between the firewall and the internal network. Three possible actions can be taken based on the rule's criteria: Block the connectionAllow the connectionAllow the connection only if it is secured TCP is responsible for providing a reliable, one-to-one, connection-oriented session. TCP establishes a connection and ensures that the other end receives any packets sent. Two hosts communicate packet results with each other. TCP also ensures that packets are decoded and sequenced properly. This connection is persistent during the session. When the session ends, the connection is torn down.UDP provides an unreliable connectionless communication method between hosts. UDP is considered a best-effort protocol, but it's considerably faster than TCP. The sessions don't establish a synchronized session like the kind used in TCP, and UDP doesn't guarantee error-free communications. The primary purpose of UDP is to send small packets of

information. The application is responsible for acknowledging the correct reception of the data.Port 22 is used by both SSH and SCP with UDP.Port 443 is used for secure web connections ?HTTPS and is a TCP port. Thus to make sure only the Accounting computer has HTTPS access to the Administrative server you should use TCP port 443 and set the rule to allow communication between 10.4.255.10/24 (Accounting) and 10.4.255.101 (Administrative server1) Thus to make sure that only the HR computer has access to Server2 over SCP you need use of TCP port 22 and set the rule to allow communication between 10.4.255.10/23 (HR) and 10.4.255.2 (server2)Thus to make sure that the IT computer can access both the Administrative servers you need to use a port and accompanying port number and set the rule to allow communication between:10.4.255.10.25 (IT computer) and 10.4.255.101 (Administrative server1)10.4.255.10.25 (IT computer) and 10.4.255.102 (Administrative server2) QUESTION 14Hotspot QuestionThe security administrator has installed a new firewall which implements an implicit DENY policy by default Click on the firewall and configure it to allow ONLY the following communication. 1. The Accounting workstation can ONLY access the web server on the public network over the default HTTPS port. The accounting workstation should not access other networks.2. The HR workstation should be restricted to communicate with the Financial server ONLY, over the default SCP port3. The Admin workstation should ONLY be able to access the servers on the secure network over the default TFTP port. Instructions: The firewall will process the rules in a top-down manner in order as a first match The port number must be typed in and only one port number can be entered per rule Type ANY for all ports. The original firewall configuration can be reset at any time by pressing the reset button. Once you have met the simulation requirements, click save and then Done to submit. Answer: Explanation:Implicit deny is the default security stance that says if you aren't specifically granted access or privileges for a resource, you're denied access by default.Rule #1 allows the Accounting workstation to ONLY access the web server on the public network over the default HTTPS port, which is TCP port 443.Rule #2 allows the HR workstation to ONLY communicate with the Financial server over the default SCP port, which is TCP Port 22Rule #3 & Rule #4 allow the Admin workstation to ONLY access the Financial and Purchasing servers located on the secure network over the default TFTP port, which is Port 69. QUESTION 15Which of the following firewall rules only denies DNS zone transfers? A. deny udp any any port 53B. deny ip any anyC. deny tcp any any port 53D. deny all dns packets Answer: CExplanation:DNS operates over TCP and UDP port 53. TCP port 53 is used for zone transfers. QUESTION 16A security administrator suspects that an increase in the amount of TFTP traffic on the network is due to unauthorized file transfers, and wants to configure a firewall to block all TFTP traffic.Which of the following would accomplish this task? A. Deny TCP port 68B. Deny TCP port 69C. Deny UDP port 68D. Deny UDP port 69 Answer: DExplanation:Trivial File Transfer Protocol (TFTP) is a simple file-exchange protocol that doesn't require authentication. It operates on UDP port 69. QUESTION 17Sara, a security technician, has received notice that a vendor coming in for a presentation will require access to a server outside of the network. Currently, users are only able to access remote sites through a VPN connection. How could Sara BEST accommodate the vendor? A. Allow incoming IPSec traffic into the vendor's IP address.B. Set up a VPN account for the vendor, allowing access to the remote site.C. Turn off the firewall while the vendor is in the office, allowing access to the remote site.D. Write a firewall rule to allow the vendor to have access to the remote site. Answer: DExplanation:Firewall rules are used to define what traffic is able pass between the firewall and the internal network. Firewall rules block the connection, allow the connection, or allow the connection only if it is secured. Firewall rules can be applied to inbound traffic or outbound traffic and any type of network. QUESTION 18A technician is deploying virtual machines for multiple customers on a single physical host to reduce power consumption in a data center. Which of the following should be recommended to isolate the VMs from one another? A. Implement a virtual firewallB. Install HIPS on each VMC. Virtual switches with VLANsD. Develop a patch management guide Answer: CExplanation:A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. VLANs can be used to isolate traffic between network segments. QUESTION 19A router has a single Ethernet connection to a switch. In the router configuration, the Ethernet interface has three sub-interfaces, each configured with ACLs applied to them and 802.1q trunks.Which of the following is MOST likely the reason for the sub-interfaces? A. The network uses the subnet of 255.255.255.128.B. The switch has several VLANs configured on it.C. The sub-interfaces are configured for VoIP traffic.D. The sub-interfaces each implement quality of service. Answer: BExplanation:A subinterface is a division of one physical interface into multiple logical interfaces. Routers commonly employ subinterfaces for a variety of purposes, most common of these are for routing traffic between VLANs. Also, IEEE 802.1Q is the networking standard that supports virtual LANs (VLANs) on an Ethernet network. QUESTION 20Joe, a technician at the local power plant, notices that several turbines had ramp up in cycles during the week. Further investigation by the system engineering team determined that a timed .exe file had been uploaded to the system control console during a visit by international contractors. Which of the following actions should Joe recommend? A. Create a VLAN for the SCADAB. Enable PKI for the MainFrameC. Implement patch managementD. Implement stronger WPA2 Wireless Answer: AExplanation:VLANs are used for traffic management. VLANs can

be used to isolate traffic between network segments. This can be accomplished by not defining a route between different VLANs or by specifying a deny filter between certain VLANs (or certain members of a VLAN). Any network segment that doesn't need to communicate with another in order to accomplish a work task/function shouldn't be able to do so. QUESTION 21The security administrator needs to manage traffic on a layer 3 device to support FTP from a new remote site. Which of the following would need to be implemented? A. Implicit denyB. VLAN managementC. Port securityD. Access control lists Answer: DExplanation:In the OSI model, IP addressing and IP routing are performed at layer 3 (the network layer). In this question we need to configure routing. When configuring routing, you specify which IP range (in this case, the IP subnet of the remote site) is allowed to route traffic through the router to the FTP server.Traffic that comes into the router is compared to ACL entries based on the order that the entries occur in the router. New statements are added to the end of the list. The router continues to look until it has a match. If no matches are found when the router reaches the end of the list, the traffic is denied. For this reason, you should have the frequently hit entries at the top of the list. There is an implied deny for traffic that is not permitted. QUESTION 22Matt, the network engineer, has been tasked with separating network traffic between virtual machines on a single hypervisor. Which of the following would he implement to BEST address this requirement? (Select TWO). A. Virtual switchB. NATC. System partitioningD. Access-listE. Disable spanning treeF. VLAN Answer: AFExplanation:A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. A virtual switch is a software application that allows communication between virtual machines. A combination of the two would best satisfy the question. QUESTION 23A database administrator contacts a security administrator to request firewall changes for a connection to a new internal application. The security administrator notices that the new application uses a port typically monopolized by a virus. The security administrator denies the request and suggests a new port or service be used to complete the application's task. Which of the following is the security administrator practicing in this example? A. Explicit denyB. Port securityC. Access control listsD. Implicit deny Answer: CExplanation:Traffic that comes into the router is compared to ACL entries based on the order that the entries occur in the router. New statements are added to the end of the list. The router continues to look until it has a match. If no matches are found when the router reaches the end of the list, the traffic is denied. For this reason, you should have the frequently hit entries at the top of the list. There is an implied deny for traffic that is not permitted. QUESTION 24An administrator needs to connect a router in one building to a router in another using Ethernet. Each router is connected to a managed switch and the switches are connected to each other via a fiber line. Which of the following should be configured to prevent unauthorized devices from connecting to the network? A. Configure each port on the switches to use the same VLAN other than the default oneB. Enable VTP on both switches and set to the same domainC. Configure only one of the routers to run DHCP servicesD. Implement port security on the switches Answer: DExplanation:Port security in IT can mean several things:The physical control of all connection points, such as RJ-45 wall jacks or device ports, so that no unauthorized users or unauthorized devices can attempt to connect into an open port. The management of TCP and User Datagram Protocol (UDP) ports. If a service is active and assigned to a port, then that port is open. All the other 65,535 ports (of TCP or UDP) are closed if a service isn't actively using them.Port knocking is a security system in which all ports on a system appear closed. However, if the client sends packets to a specific set of ports in a certain order, a bit like a secret knock, then the desired service port becomes open and allows the client software to connect to the service. QUESTION 25At an organization, unauthorized users have been accessing network resources via unused network wall jacks. Which of the following would be used to stop unauthorized access? A. Configure an access list.B. Configure spanning tree protocol.C. Configure port security.D. Configure loop protection. Answer: CExplanation:Port security in IT can mean several things. It can mean the physical control of all connection points, such as RJ-45 wall jacks or device ports, so that no unauthorized users or unauthorized devices can attempt to connect into an open port. This can be accomplished by locking down the wiring closet and server vaults and then disconnecting the workstation run from the patch panel (or punch-down block) that leads to a room's wall jack. Any unneeded or unused wall jacks can (and should) be physically disabled in this manner. Another option is to use a smart patch panel that can monitor the MAC address of any device connected to each and every wall port across a building and detect not just when a new device is connected to an empty port, but also when a valid device is disconnected or replaced by an invalid device. Lead2pass.com has been the world leader in providing online training solutions for SY0-401 Certification. You use our training materials that have been rigorously tested by international 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]