[2017 New 2017 New SY0-401 Exam PDF Ensure SY0-401 Certification Exam Pass 100% (26-50)

2017 July CompTIA Official New Released SY0-401 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! We offer the most current and best training materials of the SY0-401 certification Q&A , Practice Software, Study Packs, Preparation Labs and Audio Training you are looking for. Our online certification training offers you quick and cost-efficient way to train and become a certified professional in IT industry. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 26On Monday, all company employees report being unable to connect to the corporate wireless network, which uses 802.1x with PEAP. A technician verifies that no configuration changes were made to the wireless network and its supporting infrastructure, and that there are no outages.Which of the following is the MOST likely cause for this issue? A. Too many incorrect authentication attempts have caused users to be temporarily disabled.B. The DNS server is overwhelmed with connections and is unable to respond to queries.C. The company IDS detected a wireless attack and disabled the wireless network.D. The Remote Authentication Dial-In User Service server certificate has expired.Answer: DExplanation:The question states that the network uses 802.1x with PEAP. The 802.1x authentication server is typically an EAP-compliant Remote Access Dial-In User Service (RADIUS). A RADIUS server will be configured with a digital certificate. When a digital certificate is created, an expiration period is configured by the Certificate Authority (CA). The expiration period is commonly one or two years. The question states that no configuration changes have been made so it's likely that the certificate has expired. QUESTION 27A company determines a need for additional protection from rogue devices plugging into physical ports around the building.Which of the following provides the highest degree of protection from unauthorized wired network access? A. Intrusion Prevention SystemsB. MAC filteringC. Flood guardsD. 802.1x Answer: DExplanation:IEEE 802.1x is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols and provides an authentication mechanism to wireless devices connecting to a LAN or WLAN. QUESTION 28While configuring a new access layer switch, the administrator, Joe, was advised that he needed to make sure that only devices authorized to access the network would be permitted to login and utilize resources. Which of the following should the administrator implement to ensure this happens? A. Log AnalysisB. VLAN ManagementC. Network separationD. 802.1x Answer: DExplanation:802.1x is a port-based authentication mechanism. It's based on Extensible Authentication Protocol (EAP) and is commonly used in closed-environment wireless networks. 802.1x was initially used to compensate for the weaknesses of Wired Equivalent Privacy (WEP), but today it's often used as a component in more complex authentication and connection-management systems, including Remote Authentication Dial-In User Service (RADIUS), Diameter, Cisco System's Terminal Access Controller Access-Control System Plus (TACACS+), and Network Access Control (NAC). QUESTION 29A network administrator wants to block both DNS requests and zone transfers coming from outside IP addresses. The company uses a firewall which implements an implicit allow and is currently configured with the following ACL applied to its external interface. PERMIT TCP ANY ANY 80PERMIT TCP ANY ANY 443 Which of the following rules would accomplish this task? (Select TWO). A. Change the firewall default settings so that it implements an implicit denyB. Apply the current ACL to all interfaces of the firewallC. Remove the current ACLD. Add the following ACL at the top of the current ACL DENY TCP ANY ANY 53E. Add the following ACL at the bottom of the current ACL DENY ICMP ANY ANY 53F. Add the following ACL at the bottom of the current ACL DENY IP ANY ANY 53 Answer: AFExplanation: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. Implicit deny is the default response when an explicit allow or deny isn't present.DNS operates over TCP and UDP port 53. TCP port 53 is used for zone transfers. These are zone file exchanges between DNS servers, special manual queries, or used when a response exceeds 512 bytes. UDP port 53 is used for most typical DNS queries. QUESTION 30Users are unable to connect to the web server at IP 192.168.0.20. Which of the following can be inferred of a firewall that is configured ONLY with the following ACL? PERMIT TCP ANY HOST 192.168.0.10 EQ 80PERMIT TCP ANY HOST 192.168.0.10 EQ 443 A. It implements stateful packet filtering.B. It implements bottom-up processing.C. It failed closed.D. It implements an implicit deny. Answer: DExplanation: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. Implicit deny is the default response when an explicit allow or deny isn't present. QUESTION 31The Human Resources department has a parent shared folder setup on the server. There are two groups that have access, one called managers and one called staff. There are many sub folders under the parent shared folder, one is called payroll. The parent folder access control list propagates all subfolders and all subfolders inherit the parent permission. Which of the following is the quickest way to prevent the staff group from gaining access to the payroll folder? A. Remove the staff group from the payroll folderB. Implicit deny on the payroll folder for the staff groupC. Implicit deny on the

payroll folder for the managers groupD. Remove inheritance from the payroll folder Answer: BExplanation: 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. QUESTION 32A company has several conference rooms with wired network jacks that are used by both employees and guests. Employees need access to internal resources and guests only need access to the Internet. Which of the following combinations is BEST to meet the requirements? A. NAT and DMZB. VPN and IPSecC. Switches and a firewallD. 802.1x and VLANs Answer: DExplanation:802.1x is a port-based authentication mechanism. It's based on Extensible Authentication Protocol (EAP) and is commonly used in closed-environment wireless networks. 802.1x was initially used to compensate for the weaknesses of Wired Equivalent Privacy (WEP), but today it's often used as a component in more complex authentication and connection-management systems, including Remote Authentication Dial-In User Service (RADIUS), Diameter, Cisco System's Terminal Access Controller Access-Control System Plus (TACACS+), and Network Access Control (NAC).A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. By default, all ports on a switch are part of VLAN 1. But as the switch administrator changes the VLAN assignment on a port-by-port basis, various ports can be grouped together and be distinct from other VLAN port designations. 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 33Matt, the IT Manager, wants to create a new network available to virtual servers on the same hypervisor, and does not want this network to be routable to the firewall. How could this BEST be accomplished? A. Create a VLAN without a default gateway.B. Remove the network from the routing table.C. Create a virtual switch.D. Commission a stand-alone switch. Answer: CExplanation:A Hyper-V Virtual Switch implements policy enforcement for security, isolation, and service levels. QUESTION 34A Chief Information Security Officer (CISO) is tasked with outsourcing the analysis of security logs. These will need to still be reviewed on a regular basis to ensure the security of the company has not been breached. Which of the following cloud service options would support this requirement? A. SaaSB. MaaSC. IaaSD. PaaS Answer: BExplanation:Monitoring-as-a-service (MaaS) is a cloud delivery model that falls under anything as a service (XaaS). MaaS allows for the deployment of monitoring functionalities for several other services and applications within the cloud. QUESTION 35Joe, a security administrator, believes that a network breach has occurred in the datacenter as a result of a misconfigured router access list, allowing outside access to an SSH server. Which of the following should Joe search for in the log files? A. Failed authentication attemptsB. Network ping sweepsC. Host port scansD. Connections to port 22 Answer: DExplanation:Log analysis is the art and science of reviewing audit trails, log files, or other forms of computer- generated records for evidence of policy violations, malicious events, downtimes, bottlenecks, or other issues of concern.SSH uses TCP port 22. All protocols encrypted by SSH also use TCP port 22, such as SFTP, SHTTP, SCP, SExec, and slogin. QUESTION 36An organization does not have adequate resources to administer its large infrastructure. A security administrator wishes to combine the security controls of some of the network devices in the organization. Which of the following methods would BEST accomplish this goal? A. Unified Threat ManagementB. Virtual Private NetworkC. Single sign onD. Role-based management Answer: AExplanation:When you combine a firewall with other abilities (intrusion prevention, antivirus, content filtering, etc.), what used to be called an all-in-one appliance is now known as a unified threat management (UTM) system. The advantages of combining everything into one include a reduced learning curve (you only have one product to learn), a single vendor to deal with, and--typically--reduced complexity. QUESTION 37An organization does not have adequate resources to administer its large infrastructure. A security administrator wishes to integrate the security controls of some of the network devices in the organization. Which of the following methods would BEST accomplish this goal? A. Unified Threat ManagementB. Virtual Private NetworkC. Single sign onD. Role-based management Answer: AExplanation:Unified Threat Management (UTM) is, basically, the combination of a firewall with other abilities. These abilities include intrusion prevention, antivirus, content filtering, etc. Advantages of combining everything into one: You only have one product to learn.You only have to deal with a single vendor.IT provides reduced complexity. QUESTION 38A security administrator is segregating all web-facing server traffic from the internal network and restricting it to a single interface on a firewall. Which of the following BEST describes this new network? A. VLANB. SubnetC. VPND. DMZ Answer: DExplanation:A DMZ or demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node only has direct access to equipment in the DMZ, rather than any other part of the network. The name is derived from the term "demilitarized zone", an area between nation states in which military operation is not permitted. QUESTION 39Which of the following devices would MOST likely have a DMZ interface? A. FirewallB. SwitchC. Load balancerD. Proxy Answer: AExplanation: The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall. QUESTION 40A security analyst needs to ensure

all external traffic is able to access the company's front-end servers but protect all access to internal resources. Which of the following network design elements would MOST likely be recommended? A. DMZB. Cloud computingC. VLAND. Virtualization Answer: AExplanation:A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall. QUESTION 41Which of the following network architecture concepts is used to securely isolate at the boundary between networks? A. VLANB. SubnettingC. DMZD. NAT Answer: CExplanation:A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall. QUESTION 42When designing a new network infrastructure, a security administrator requests that the intranet web server be placed in an isolated area of the network for security purposes. Which of the following design elements would be implemented to comply with the security administrator's request? A. DMZB. Cloud servicesC. VirtualizationD. Sandboxing Answer: AExplanation:A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall. QUESTION 43Which of the following BEST describes a demilitarized zone? A. A buffer zone between protected and unprotected networks.B. A network where all servers exist and are monitored.C. A sterile, isolated network segment with access lists.D. A private network that is protected by a firewall and a VLAN. Answer: AExplanation:A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall. QUESTION 44Which of the following would allow the organization to divide a Class C IP address range into several ranges? A. DMZB. Virtual LANsC. NATD. Subnetting Answer: DExplanation:Subnetting is a dividing process used on networks to divide larger groups of hosts into smaller collections. QUESTION 45Which of the following IP addresses would be hosts on the same subnet given the subnet mask 255.255.255.224? (Select TWO). A. 10.4.4.125B. 10.4.4.158C. 10.4.4.165D. 10.4.4.189E. 10.4.4.199 Answer: CDExplanation:With the given subnet mask, a maximum number of 30 hosts between IP addresses 10.4.4.161 and 10.4.4.190 are allowed. Therefore, option C and D would be hosts on the same subnet, and the other options would not.http://www.subnetonline.com/pages/subnet-calculators/ip-subnet-calculator.php QUESTION 46Which of the following would the security engineer set as the subnet mask for the servers below to utilize host addresses on separate broadcast domains? Server 1: 192.168.100.6Server 2: 192.168.100.9Server 3: 192.169.100.20 A. /24B. /27C. /28D. /29E. /30 Answer: DExplanation:Using this option will result in all three servers using host addresses on different broadcast domains. QUESTION 47Which of the following is BEST used to break a group of IP addresses into smaller network segments or blocks? A. NATB. VirtualizationC. NACD. Subnetting Answer: DExplanation:Subnetting is a dividing process used on networks to divide larger groups of hosts into smaller collections. QUESTION 48A small company can only afford to buy an all-in-one wireless router/switch. The company has 3 wireless BYOD users and 2 web servers without wireless access. Which of the following should the company configure to protect the servers from the user devices? (Select TWO). A. Deny incoming connections to the outside router interface.B. Change the default HTTP portC. Implement EAP-TLS to establish mutual authenticationD. Disable the physical switch portsE. Create a server VLANF. Create an ACL to access the server Answer: EFExplanation:We can protect the servers from the user devices by separating them into separate VLANs (virtual local area networks).The network device in the question is a router/switch. We can use the router to allow access from devices in one VLAN to the servers in the other VLAN. We can configure an ACL (Access Control List) on the router to determine who is able to access the server.In computer networking, a single layer-2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain is referred to as a virtual local area network, virtual LAN or VLAN.This is usually achieved on switch or router devices. Simpler devices only support partitioning on a port level (if at all), so sharing VLANs across devices requires running dedicated cabling for each VLAN. More sophisticated devices can mark packets through tagging, so that a single interconnect (trunk) may be used to transport data for multiple VLANs. Grouping hosts with a common set of requirements regardless of their physical location by VLAN can greatly simplify network design. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together more easily even if they are not on the same network switch. The network described in this question is a DMZ, not a VLAN. QUESTION 49A network engineer is setting up a network for a company. There is a BYOD policy for the employees so that they can connect their laptops and mobile devices.Which of the following technologies should be employed to separate the administrative network from the network in which all of the employees' devices are connected? A. VPNB. VLANC. WPA2D. MAC filtering 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 50Pete, a network administrator, is capturing packets on the network and notices that a large amount of the traffic on the LAN is SIP and RTP protocols. Which of the following should he do to segment that traffic from the other traffic? A. Connect the WAP to a different switch.B. Create a voice VLAN.C. Create a DMZ.D. Set the switch ports to 802.1q mode. Answer: BExplanation:It is a common and recommended practice to separate voice and data traffic by using VLANs. Separating voice and data traffic using VLANs provides a solid security boundary, preventing data applications from reaching the voice traffic. It also gives you a simpler method to deploy QoS, prioritizing the voice traffic over the data. The strength of our SY0-401 dumps is the constant update that we perform to keep abreast with the market trends and changes. Our SY0-401 exam question is not only the best option for certification but also enhances your skill to an advance level. 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]