[2016 August-NewCompTIA SY0-401 Exam Questions PDF 1867Q&As [NQ21-NQ30Download

2016/08 SY0-401: CompTIA Security+ Certification Exam Questions New Updated Today! Free Instant Download SY0-401 Exam Dumps(PDF & VCE) 1867Q&As from Braindump2go.com!100% Real Exam Questions! 100% Exam Pass Guaranteed! NEW QUESTION 21 - NEW QUESTION 30: 1.|2016/08 SY0-401 Exam Dumps(PDF & VCE) 1867Q&As Download:http://www.braindump2go.com/sy0-401.html 2.|2016/08 SY0-401 Exam Questions & Answers:https://drive.google.com/folderview?id=0B75b5xYLjSSNTldvc1ZkQlNUc0k&usp=sharing 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-list E. 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. 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 443Which 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. !!!RECOMMEND!!! 1.|2016/08 SY0-401 PDF Dumps & VCE Dumps 1867Q&As Download: http://www.braindump2go.com/sy0-401.html 2.|2016/08 SY0-401 Questions & Answers: https://drive.google.com/folderview?id=0B75b5xYLjSSNTldvc1ZkQlNUc0k&usp=sharing