[100% Success!Braindump2go 1867Q&As SY0-401 Exam PDF Dumps(August-2016)Free Download[NQ41-NQ50

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 41 - NEW QUESTION 50: 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 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 services C. 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. /27 C. /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: EF Explanation: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. !!!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