JK0-022 Q&As

CompTIA Security+ Certification

Pass CompTIA JK0-022 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/jk0-022.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A 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. VLAN

B. Subnet

C. VPN

D. DMZ

Correct Answer: D

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.

Incorrect Answers:

A: 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.

B: A subnet is a logical IP network. A DMZ will contain a subnet but it could also contain multiple subnets. Computers on a subnet can communicate with computers on a different subnet through a router.

C: A VPN (Virtual Private Network) is a secure network connection over an insecure network such as the Internet. For example, two geographically separate sites could be connected by a VPN using the Internet for the physical network connection. The network described in this question is a DMZ, not a VPN.

References: http://en.wikipedia.org/wiki/DMZ_%28computing%29 http://en.wikipedia.org/wiki/Virtual_LAN

QUESTION 2

A datacenter requires that staff be able to identify whether or not items have been removed from the facility. Which of the following controls will allow the organization to provide automated notification of item removal?

A. CCTV

B. Environmental monitoring

C. RFID

D. EMI shielding

Correct Answer: C

RFID is radio frequency identification that works with readers that work with 13.56 MHz smart cards and 125 kHz proximity cards and can open turnstiles, gates, and any other physical security safeguards once the signal is read. Fitting out the equipment with RFID will allow you to provide automated notification of item removal in the event of any of the equipped items is taken off the premises.

Incorrect Answers:

A: CCTV will record events, but will not automatically notify you of item removal.

B: Environmental monitoring concerns events such as water, flood, humidity, fire, etc. types of threats and not theft as in the case of item removal.

D: EMI shielding refers to the process of preventing electronic emissions from your computer systems from being used to gather intelligence and preventing outside electronic emissions from disrupting you information-processing abilities. It is not designed to automatically notify you of events when items are removed.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 368
http://en.wikipedia.org/wiki/Radio-frequency_identification

QUESTION 3

Ann, the Chief Technology Officer (CTO), has agreed to allow users to bring their own device (BYOD) in order to leverage mobile technology without providing every user with a company owned device. She is concerned that users may not

understand the company\\'s rules, and she wants to limit potential legal concerns.

Which of the following is the CTO concerned with?

A. Data ownership

B. Device access control

C. Support ownership

D. Acceptable use

Correct Answer: A

QUESTION 4

A security administrator wishes to increase the security of the wireless network. Which of the following BEST addresses this concern?

A. Change the encryption from TKIP-based to CCMP-based.

B. Set all nearby access points to operate on the same channel.

C. Configure the access point to use WEP instead of WPA2.

D. Enable all access points to broadcast their SSIDs.

Correct Answer: A

CCMP makes use of 128-bit AES encryption with a 48-bit initialization vector. This initialization vector makes cracking a bit more difficult.

Incorrect Answers:

B: Wireless APs with overlapping signals should use unique channel frequencies to reduce interference between them.

C: WEP is not a secure encryption protocol.

D: This will make the network visible, and open for attacks.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 172, 178.

https://technet.microsoft.com/en-us/library/cc783011(v=ws.10).aspx

QUESTION 5

Which of the following is an authentication and accounting service that uses TCP for connecting to routers and switches?

A. DIAMETER

B. RADIUS

C. TACACS+

D. Kerberos

Correct Answer: C

TACACS+ is an authentication, authorization, and accounting (AAA) service that makes us of TCP only. Incorrect Answers:

A: DIAMETER makes use of TCP, as well as SCTP.

B: RADIUS makes use of UDP.

D: Kerberos is not an authentication and accounting service, but an authentication protocol.

References: http://en.wikipedia.org/wiki/TACACS http://en.wikipedia.org/wiki/Diameter_(protocol) http://en.wikipedia.org/wiki/RADIUS http://en.wikipedia.org/wiki/Kerberos_(protocol)