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.pass2lead.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

An administrator was asked to review user accounts. Which of the following has the potential to cause the MOST amount of damage if the account was compromised?

A. A password that has not changed in 180 days

B. A single account shared by multiple users

C. A user account with administrative rights

D. An account that has not been logged into since creation

Correct Answer: C

QUESTION 2

A small business needs to incorporate fault tolerance into their infrastructure to increase data availability. Which of the following options would be the BEST solution at a minimal cost?

A. Clustering

B. Mirrored server

C. RAID

D. Tape backup

Correct Answer: C

RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning. RAID can achieve fault tolerance using software which can be done using the existing hardware and software.

Incorrect Answers:

A: Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. Clustered systems utilize parallel processing (improving performance and availability) and add redundancy (but also add costs).

B: Mirrored server implies that you have a mirror / duplicate of the server which will provide you with 100 % redundancy, but it does not represent the least cost option.

D: Tape Backup will also incur costs and is means for backing up data to mitigate a loss.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 34, 234, 235

QUESTION 3

Which of the following allows a company to maintain access to encrypted resources when employee turnover is high?

A. Recovery agent

B. Certificate authority

C. Trust model

D. Key escrow

Correct Answer: A

If an employee leaves and we need access to data he has encrypted, we can use the key recovery agent to retrieve his decryption key. We can use this recovered key to access the data. A key recovery agent is an entity that has the ability to

recover a key, key components, or plaintext messages as needed. As opposed to escrow, recovery agents are typically used to access information that is encrypted with older keys.

Incorrect Answers:

B: A certificate authority (CA) is an organization. A CA is responsible for issuing, revoking, and distributing certificates. A CA cannot recovery keys.

C: A trust Model is collection of rules that informs application on how to decide the legitimacy of a Digital Certificate. A trust model cannot recover keys.

D: Key escrow is not used to recover old keys.

Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account (think of the term as it relates to home mortgages)

and made available if that third party requests them. The third party in question is generally the government, but it could also be an employer if an employee\\'s private messages have been called into question.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-280, 285-289

QUESTION 4

Ann, a sales manager, successfully connected her company-issued smartphone to the wireless network in her office without supplying a username/password combination. Upon disconnecting from the wireless network, she attempted to

connect her personal tablet computer to the same wireless network and could not connect.

Which of the following is MOST likely the reason?

A. The company wireless is using a MAC filter.

B. The company wireless has SSID broadcast disabled.

C. The company wireless is using WEP.

D. The company wireless is using WPA2.

Correct Answer: A

MAC filtering allows you to include or exclude computers and devices based on their MAC address.

Incorrect Answers:

B: because she could connect to the wireless with the first device, the SSID must be broadcasting. C, D: Both WEP and WPA2 require a password or phrase.

References:

https://technet.microsoft.com/en-us/magazine/ff521761.aspx Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 61.

QUESTION 5

Joe, a newly hired employee, has a corporate workstation that has been compromised due to several visits to P2P sites. Joe insisted that he was not aware of any company policy that prohibits the use of such web sites. Which of the following is the BEST method to deter employees from the improper use of the company\\'s information systems?

A. Acceptable Use Policy

B. Privacy Policy

C. Security Policy

D. Human Resource Policy

Correct Answer: A

Acceptable use policies (AUPs) describe how the employees in an organization can use company systems and resources, both software and hardware.

Incorrect Answers:

B: Privacy policies define what controls are required to implement and maintain the sanctity of data privacy in the work environment.

C: Security policies define what controls are required to implement and maintain the security of systems, users, and networks.

D: Human resources policy does not address issues regarding which website are prohibited.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 24 http://en.wikipedia.org/wiki/Acceptable_use_policy