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

Which of the following is true about asymmetric encryption?

A. A message encrypted with the private key can be decrypted by the same key

B. A message encrypted with the public key can be decrypted with a shared key.

C. A message encrypted with a shared key, can be decrypted by the same key.

D. A message encrypted with the public key can be decrypted with the private key.

Correct Answer: D

Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes.

Incorrect Answers:

A: The message is encrypted with a public key, not with a private key.

B: The message is decrypted with a private key, not with a shared key.

C: The message is encrypted with a public key, not with a shared key.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 251-254

QUESTION 2

Matt, a developer, recently attended a workshop on a new application. The developer installs the new application on a production system to test the functionality. Which of the following is MOST likely affected?

A. Application design

B. Application security

C. Initial baseline configuration

D. Management of interfaces

Correct Answer: C

The initial baseline configuration of a computer system is an agreed configuration for the computer. For example, the initial baseline configuration will list what operating system he computer will run, what software applications and patches will be installed and what configuration settings should be applied to the system. In this question, we are installing a new software application on a server. After the installation of the software, the "configuration" of the server (installed software, settings etc) is now different from the initial baseline configuration.

Incorrect Answers:

A: Installing a new application on a production system will not affect the application design. We are not changing the design of the application by installing it on the server. This answer is therefore incorrect.

B: Installing a new application on a production system will not affect the application security. We are not changing the security configuration of the application by installing it on the server. This answer is therefore incorrect.

D: Installing a new application on a production system will not affect the management of the interfaces. The interfaces will continue to be managed as they were before. This answer is therefore incorrect.

QUESTION 3

Which of the following is a security benefit of providing additional HVAC capacity or increased tonnage in a datacenter?

A. Increased availability of network services due to higher throughput

B. Longer MTBF of hardware due to lower operating temperatures

C. Higher data integrity due to more efficient SSD cooling

D. Longer UPS run time due to increased airflow

Correct Answer: B

The mean time between failures (MTBF) is the measure of the anticipated incidence of failure for a system or component. This measurement determines the component\\'s anticipated lifetime. If the MTBF of a cooling system is one year, you can anticipate that the system will last for a one-year period; this means that you should be prepared to replace or rebuild the system once a year. If the system lasts longer than the MTBF, your organization receives a bonus. MTBF is helpful in evaluating a system\\'s reliability and life expectancy. Thus longer MTBF due to lower operating temperatures is a definite advantage

Incorrect Answers:

A: Availability means simply to make sure that the data and systems are available for authorized users. Data backups, redundant systems, and disaster recovery plans all support availability.

C: Data integrity refers to keeping data unaltered.

D: Longer UPS will allow you to continue to function in the absence of power and provide time to shut down gracefully in the event of power failures. It is thus a business continuity benefit.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 378, 456

QUESTION 4

A security administrator would like to ensure that system administrators are not using the same password for both their privileged and non-privileged accounts. Which of the following security controls BEST accomplishes this goal?

A. Require different account passwords through a policy

B. Require shorter password expiration for non-privileged accounts

C. Require shorter password expiration for privileged accounts

D. Require a greater password length for privileged accounts

Correct Answer: A

QUESTION 5

An administrator finds that non-production servers are being frequently compromised, production servers are rebooting at unplanned times and kernel versions are several releases behind the version with all current security fixes.

Which of the following should the administrator implement?

A. Snapshots

B. Sandboxing

C. Patch management

D. Intrusion detection system

Correct Answer: C

Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from newly discovered attacks and vulnerabilities.

Incorrect Answers:

A: Snapshots are backups of virtual machines that can be used to quickly recover from errors or poor updates. It does not ensure that the latest kernel version with all current security fixes is installed on the system.

B: Sandboxing is the process of isolating a system before installing new applications on it so as to restrict any potential malware that may be embedded in the new application from being able to cause harm to production systems. It does not ensure that the latest kernel version with all current security fixes is installed on the system.

D: An intrusion detection system (IDS) is an automated system that detects intrusions or security policy violations on networks or host systems. It does not ensure that the latest kernel version with all current security fixes is installed on the system.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 204-205, 220 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 21, 231-232, 249,

Latest JK0-022 Dumps JK0-022 PDF Dumps JK0-022 Study Guide