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 BEST describes part of the PKI process?

A. User1 decrypts data with User2\\'s private key

B. User1 hashes data with User2\\'s public key

C. User1 hashes data with User2\\'s private key

D. User1 encrypts data with User2\\'s public key

Correct Answer: D

In a PKI the sender encrypts the data using the receiver\\'s public key. The receiver decrypts the data using his own private key. PKI is a two-key, asymmetric system with four main components: certificate authority (CA), registration authority

(RA), RSA (the encryption algorithm), and digital certificates. Messages are encrypted with a public key and decrypted with a private key.

A PKI example:

1.

You want to send an encrypted message to Jordan, so you request his public key.

2.

Jordan responds by sending you that key.

3.

You use the public key he sends you to encrypt the message.

4.

You send the message to him.

5.

Jordan uses his private key to decrypt the message.

Incorrect Answers:

A: You must use your own private key to decrypt data.

B: In a PKI data is encrypted and decrypted. Data is not hashed.

C: In a PKI data is encrypted and decrypted. Data is not hashed.

References:

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

QUESTION 2

Users require access to a certain server depending on their job function. Which of the following would be the MOST appropriate strategy for securing the server?

A. Common access card

B. Role based access control

C. Discretionary access control

D. Mandatory access control

Correct Answer: B

Role-based Access Control is basically based on a user\\'s job description. When a user is assigned a specific role in an environment, that user\\'s access to objects is granted based on the required tasks of that role. Incorrect Answers:

A: Smart cards are credit-card-sized IDs, badges, or security passes with an embedded integrated circuit chip. Common Access Cards (CACs) are the U.S. government and military version of a smart card.

C: Discretionary access control (DAC) allows access to be granted or restricted by an object\\'s owner based on user identity and on the discretion of the object owner. It does not rely on job function.

D: Mandatory Access Control allows access to be granted or restricted based on the rules of classification. It does not rely on job function.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 278- 284.

QUESTION 3

A system administrator has concerns regarding their users accessing systems and secured areas using others\\' credentials. Which of the following can BEST address this concern?

A. Create conduct policies prohibiting sharing credentials.

B. Enforce a policy shortening the credential expiration timeframe.

C. Implement biometric readers on laptops and restricted areas.

D. Install security cameras in areas containing sensitive systems.

Correct Answer: C

Biometrics is an authentication process that makes use of physical characteristics to establish identification. This will prevent users making use of others credentials.

Incorrect Answers:

A: Policies need to be implemented and making use of biometrics would be to a way to prohibit sharing credentials.

B: This is still granting the same type of access that is already being abused with a time limit the only difference.

D: Security cameras are used to surveil and record; not to prevent access.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 375

QUESTION 4

Which of the following can a security administrator implement on mobile devices that will help prevent unwanted people from viewing the data if the device is left unattended?

A. Screen lock

B. Voice encryption

C. GPS tracking

D. Device encryption

Correct Answer: A

Screen-lock is a security feature that requires the user to enter a PIN or a password after a short period of inactivity before they can access the system again. This feature ensures that if your device is left unattended or is lost or stolen, it will be difficult for anyone else to access your data or applications.

Incorrect Answers:

B: Voice encryption is used to protect audio (voice) transmission. It cannot secure data stored on a mobile device.

C: Global Positioning System (GPS) tracking can be used to identify its location of a stolen device and can allow authorities to recover the device. However, for GPS tracking to work, the device must have an Internet connection or a wireless phone service over which to send its location information.

D: Device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 418-419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 237 https://

www.ukash.com/en-SI/mobile-device-security/

QUESTION 5

A new MPLS network link has been established between a company and its business partner.

The link provides logical isolation in order to prevent access from other business partners. Which of the following should be applied in order to achieve confidentiality and integrity of all data across the link?

A. MPLS should be run in IPVPN mode.

B. SSL/TLS for all application flows.

C. IPSec VPN tunnels on top of the MPLS link.

D. HTTPS and SSH for all application flows.

Correct Answer: C

IPSec can very well be used with MPLS. IPSec could provide VPN tunnels on top if the MPLS link. Internet Protocol Security (IPSec) isn\\'t a tunneling protocol, but it\\'s used in conjunction with tunneling protocols. IPSec is oriented primarily toward LAN-to-LAN connections, but it can also be used with dial-up connections. IPSec provides secure authentication and encryption of data and headers; this makes it a good choice for security.

Incorrect Answers:

A: MPLS tunnelling would not hide the logical MPLS link.

B: SSL/TLS could provide encryption, but not the tunnelling required for the logical isolation.

D: To provide the required logical isolation tunnelling should be used. HTTPS and SSH cannot provide tunnelling.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 91, 103-105, 268, 271, 274, 274-275 http:// www.networkworld.com/article/2297191/lan-wan/chapter-6--how-ipseccomplements- mpls.html