JK0-022$^{\text{Q\&As}}$

CompTIA Security+ Certification

QUESTION 1

Which of the following is the BEST method for ensuring all files and folders are encrypted on all corporate laptops where the file structures are unknown?

A. Folder encryption

B. File encryption

C. Whole disk encryption

D. Steganography

Correct Answer: C

Full-disk encryption encrypts the data on the hard drive of the device or on a removable drive. This feature ensures that the data on the device or removable drive cannot be accessed in a useable form should it be stolen. Furthermore, full-

disk encryption is not dependant on knowledge of the file structure.

Incorrect Answers:

A, B: File and Folder encryption encrypts the content of individual files and folders respectively. To implement file or folder encryption effectively, the file structure has to be known.

D: Steganography is a process of hiding one communication inside another communication. It can use passwords to prevent unauthorized extraction of the hidden communication and can also use encryption to mitigate against brute-force attempts at extraction. Steganography can also be used to detect theft, fraud, or modification when the hidden communication is a watermark.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 251- 252, 323

QUESTION 2

Which of the following allows an organization to store a sensitive PKI component with a trusted third party?

A. Trust model

B. Public Key Infrastructure

C. Private key

D. Key escrow

Correct Answer: D

Sensitive PKI data, such as private keys, can be put into key escrow data. The key escrow data can be kept at a trusted third party. Key escrow is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. These third parties may include businesses, who may want access to employees\\' private communications, or governments, who may wish to be able to view the contents of encrypted communications.

Incorrect Answers:

A: A trust Model is collection of rules that informs application on how to decide the legitimacy of a Digital Certificate. A trust model cannot store sensitive information.

B: A PKI cannot store sensitive information.

The Public-Key Infrastructure (PKI) is intended to offer a means of providing security to messages and transactions on a grand scale. The need for universal systems to support e- commerce, secure transactions, and information privacy is

one aspect of the issues being addressed with PKI.

C: A private key is a secret key. It is not used to stored sensitive information through a third party.

References:

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

QUESTION 3

Which of the following should Matt, a security administrator, include when encrypting smartphones? (Select TWO).

A. Steganography images

B. Internal memory

C. Master boot records

D. Removable memory cards

E. Public keys

Correct Answer: BD

All useable data on the device should be encrypted. This data can be located on the hard drive, or removable drives, such as USB devices and memory cards, and on internal memory. Incorrect Answers:

A: Steganography is a process of hiding one communication inside another communication. It can use passwords to prevent unauthorized extraction of the hidden communication and can also use encryption to mitigate against brute-force attempts at extraction. Steganography can also be used to detect theft, fraud, or modification when the hidden communication is a watermark.

C: The master boot record (MBR) stores information on how the logical partitions on a hard drive are organized and contains loaders for the operating system. This is not data at risk and does not need to be encrypted.

E: Public keys are used in asymmetrical cryptography. It is publicly available and is derived from the user\\'s private key. It does not hold any useable data as the private key cannot be used to reverse engineer the user\\'s private key.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 323,

QUESTION 4

A computer is suspected of being compromised by malware. The security analyst examines the computer and finds that a service called Telnet is running and connecting to an external website over port 443. This Telnet service was found by comparing the system\\'s services to the list of standard services on the company\\'s system image. This review process depends on:

A. MAC filtering.

B. System hardening.

C. Rogue machine detection.

D. Baselining.

Correct Answer: D

Application baseline defines the level or standard of security that will be implemented and maintained for the application. It may include requirements of hardware components, operating system versions, patch levels, installed applications and their configurations, and available ports and services. Systems can be compared to the baseline to ensure that the required level of security is being maintained.

Incorrect Answers:

A: MAC Filtering is used to secure access to wireless network access points. It is used to explicitly allow MAC addresses on a whitelist, blocking all other MAC addresses.

B: Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing or disabling unnecessary functions and features, removing or disabling unnecessary user accounts, disabling unnecessary protocols and ports, and disabling unnecessary services.

C: Rogue machine detection attempt to identify the presence of unauthorized systems on a network.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 178, 215-217, 219 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 206, 207, 208

QUESTION 5

Due to issues with building keys being duplicated and distributed, a security administrator wishes to change to a different security control regarding a restricted area. The goal is to provide access based upon facial recognition. Which of the following will address this requirement?

A. Set up mantraps to avoid tailgating of approved users.

B. Place a guard at the entrance to approve access.

C. Install a fingerprint scanner at the entrance.

D. Implement proximity readers to scan users\\' badges.

Correct Answer: B

A guard can be instructed to deny access until authentication has occurred will address the situation adequately.

Incorrect Answers:

A: Although mantraps require visual identification, as well as authentication, to gain access, setting up a mantrap will not keep those with keys out.

C: Fingerprint scanner is not facial recognition.

D: User badges and proximity readers will not necessarily make use of facial recognition.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 367, 374

Latest JK0-022 Dumps JK0-022 Practice Test JK0-022 Braindumps