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

CompTIA Security+ Certification

Pass CompTIA JK0-022 Exam with 100% Guarantee

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

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

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Users can authenticate to a company\\'s web applications using their credentials from a popular social media site. Which of the following poses the greatest risk with this integration?

A. Malicious users can exploit local corporate credentials with their social media credentials

B. Changes to passwords on the social media site can be delayed from replicating to the company

C. Data loss from the corporate servers can create legal liabilities with the social media site

D. Password breaches to the social media site affect the company application as well

Correct Answer: D

Social networking and having you company\\'s application authentication `linked\\' to users\\' credential that they use on social media sites exposes your company\\'s application exponentially more than is necessary. You should strive to practice risk avoidance.

Incorrect Answers:

A: One would assume that only the company\\'s users would be able to authenticate to the company\\'s application and you would be able to audit log on attempts.

B: Delays in password when changes are made is not such a sever security risk as a breach in passwords.

C: Data loss on your company servers does not pose as great a security risk as breach of passwords.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 364, 406

QUESTION 2

An Information Systems Security Officer (ISSO) has been placed in charge of a classified peer- to-peer network that cannot connect to the Internet. The ISSO can update the antivirus definitions manually, but which of the following steps is MOST important?

A. A full scan must be run on the network after the DAT file is installed.

B. The signatures must have a hash value equal to what is displayed on the vendor site.

C. The definition file must be updated within seven days.

D. All users must be logged off of the network prior to the installation of the definition file.

Correct Answer: B

A hash value can be used to uniquely identify secret information. This requires that the hash function is collision resistant, which means that it is very hard to find data that generate the same hash value and thus it means that in hashing two different inputs will not yield the same output. Thus the hash value must be equal to that displayed on the vendor site.

Incorrect Answers:

A: To run a full scan is just important to check the status of your computer insofar as virus infections may be concerned, not the updating of the antivirus definitions when you cannot connect the P2P to the internet.

C: This not a time constraint issue.

D: Logging off of the network is not a requirement to install updates.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 255

QUESTION 3

A new intern was assigned to the system engineering department, which consists of the system architect and system software developer\\'s teams. These two teams have separate privileges. The intern requires privileges to view the system

architectural drawings and comment on some software development projects.

Which of the following methods should the system administrator implement?

A. Group based privileges

B. Generic account prohibition

C. User access review

D. Credential management

Correct Answer: A

You can assign permissions to access resources either to a user or a group. The most efficient way is to assign permissions to a group (group based privileges). By assigning the intern\\'s user account to both groups, the intern will inherit the permissions assigned to those groups.

Incorrect Answers:

B: Generic account prohibition is a rule that states no generic, shared, or anonymous accounts should be allowed in private networks or on any system where security is important. This will not allow the intern to view the system architectural drawings and comment on some software development projects.

C: User access reviews are performed to conclude whether users have been performing their work tasks correctly or if there have been failed and/or successful attempts at violating company policies or the law. This will not allow the intern to view the system architectural drawings and comment on some software development projects.

D: Credential management is a service or software product that is designed to store and manage user credentials. It allows users to specify longer and more random credentials for their different accounts without having to remember or writing them down. This will not allow the intern to view the system architectural drawings and comment on some software development projects.

References:

https://technet.microsoft.com/en-gb/library/cc786285%28v=ws.10%29.aspx Stewart, James Michael, CompTIA

Security+ Review Guide, Sybex, Indianapolis, 2014, pp 291- 294.

QUESTION 4

Which of the following is a hardware-based security technology included in a computer?

A. Symmetric key

B. Asymmetric key

C. Whole disk encryption

D. Trusted platform module

Correct Answer: D

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system\\'s motherboard and is enabled or disable in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or

certificates.

Incorrect Answers:

A, B: Symmetrical and Asymmetrical keys are used in hardware- or software-based cryptography.

C: Whole disk and 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. This encryption can be provided by a software or a hardware solution.

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 236,

QUESTION 5

Which of the following identifies certificates that have been compromised or suspected of being compromised?

A. Certificate revocation list

B. Access control list

C. Key escrow registry

D. Certificate authority

Correct Answer: A

Certificates that have been compromised or are suspected of being compromised are revoked. A CRL is a locally stored record containing revoked certificates and revoked keys.

Incorrect Answers:

B: Access control lists (ACLs) enable devices in your network to ignore requests from specified users or systems or to grant them access to certain network capabilities. ACLs cannot be used for certificates or keys.

C: Key escrow is not related to revoked certificates.

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.

D: In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates. You don\\'t use a CA to store revoked certificates.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 156-157, 262, 279-280, 285

Latest JK0-022 Dumps JK0-022 VCE Dumps JK0-022 Practice Test