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

CompTIA Security+ Certification

Pass CompTIA JK0-022 Exam with 100% Guarantee

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

QUESTION 1

An organization is implementing a password management application which requires that all local administrator passwords be stored and automatically managed. Auditors will be responsible for monitoring activities in the application by reviewing the logs. Which of the following security controls is the BEST option to prevent auditors from accessing or modifying passwords in the application?

A. Time of day restrictions

B. Create user accounts for the auditors and assign read-only access

C. Mandatory access control

D. Role-based access with read-only

Correct Answer: D

QUESTION 2

An administrator discovers that many users have used their same passwords for years even though the network requires that the passwords be changed every six weeks. Which of the following, when used together, would BEST prevent users from reusing their existing password? (Select TWO).

A. Length of password

B. Password history

C. Minimum password age

D. Password expiration

E. Password complexity

F. Non-dictionary words

Correct Answer: BC

In this question, users are forced to change their passwords every six weeks. However, they are able to change their password and enter the same password as the new password. Password history determines the number of previous passwords that cannot be used when a user changes his password. For example, a password history value of 5 would disallow a user from changing his password to any of his previous 5 passwords.

When a user is forced to change his password due to a maximum password age period expiring, (the question states that the network requires that the passwords be changed every six weeks) he could change his password to a previously used password. Or if a password history value of 5 is configured, the user could change his password six times to cycle back round to his original password. This is where the minimum password age comes in. This is the period that a password must be used for. For example, a minimum password age of 30 would determine that when a user changes his password, he must continue to use the same password for at least 30 days.

Incorrect Answers:

A: The length of password determines how many characters a password must contain. It will not prevent users from changing their passwords multiple times to cycle back to their original passwords.

D: Password expiration determines how long a password can be used for before it must be changed. In this question, the password expiration is 6 weeks. Password expiration will force users to change their passwords but it will not prevent users from changing their passwords multiple times to cycle back to their original passwords.

E: Password complexity determines what a password should include. For example, you could require a password to contain uppercase and lowercase letters and numbers. . It will not prevent users from changing their passwords multiple times to cycle back to their original passwords.

F: Non-dictionary words is a setting that determines that a password should not be a word that can be found in a dictionary. This is to prevent a "dictionary attack" where software can be used to attempt to access a system by using the words of a dictionary as the password.

References:
https://technet.microsoft.com/enus/library/cc757692%28v=ws.10%29.aspx#w2k3tr_sepol_accou_set_kuwh

QUESTION 3

A large multinational corporation with networks in 30 countries wants to establish an understanding of their overall public-facing network attack surface. Which of the following security techniques would be BEST suited for this?

A. External penetration test

B. Internal vulnerability scan

C. External vulnerability scan

D. Internal penetration test

Correct Answer: C

QUESTION 4

Sara, the Chief Security Officer (CSO), has had four security breaches during the past two years. Each breach has cost the company $3,000. A third party vendor has offered to repair the security hole in the system for $25,000. The breached system is scheduled to be replaced in five years.

Which of the following should Sara do to address the risk?

A. Accept the risk saving $10,000.

B. Ignore the risk saving $5,000.

C. Mitigate the risk saving $10,000.

D. Transfer the risk saving $5,000.

Correct Answer: D

Risk transference involves sharing some of the risk burden with someone else, such as an insurance company. The cost of the security breach over a period of 5 years would amount to $30,000 and it is better to save $5,000.

Incorrect Answers:

A: Risk acceptance is often the choice you must make when the cost of implementing any of the other four choices exceeds the value of the harm that would occur if the risk came to fruition. In this case there is no saving and the risk already happened.

B: Ignoring the risk will not save you $5,000 since the system is due to be replaced within a 5 year period which will cost your company $30,000.

C: Risk mitigation is accomplished any time you take steps to reduce risk. This category includes installing antivirus software, educating users about possible threats, monitoring network traffic, adding a firewall, and so on. You should however address the security breach else there will be no saving.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 9

QUESTION 5

After Matt, a user enters his username and password at the login screen of a web enabled portal, the following appears on his screen:

`Please only use letters and numbers on these fields\\'

Which of the following is this an example of?

A. Proper error handling

B. Proper input validation

C. Improper input validation

D. Improper error handling

Correct Answer: B

Input validation is an aspect of secure coding and is intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that

input. The check could be a length, a character type, a language type, or a domain.

Incorrect Answers:

A, D: Error handling is an aspect of secure coding. When errors occur, the system should revert back to a secure state. This must be coded into the system, and should include error and exception handling.

C: Improper input validation would allow user input to be used as an attack vector. In such an event input would not be checked and the use would not receive a message from the system.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 257
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 319,

JK0-022 VCE Dumps JK0-022 Exam Questions JK0-022 Braindumps