CAS-003$^{Q\&As}$

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-003 Exam with 100% Guarantee

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

QUESTION 1

A security architect has been assigned to a new digital transformation program. The objectives are to provide better capabilities to customers and reduce costs. The program has highlighted the following requirements:

Long-lived sessions are required, as users do not log in very often.

The solution has multiple SPs, which include mobile and web applications.

A centralized IdP is utilized for all customer digital channels.

The applications provide different functionality types such as forums and customer portals.

The user experience needs to be the same across both mobile and web-based applications.

Which of the following would BEST improve security while meeting these requirements?

A. Social login to IdP, securely store the session cookies, and implement one-time passwords sent to the mobile device

B. Create-based authentication to IdP, securely store access tokens, and implement secure push notifications.

C. Username and password authentication to IdP, securely store refresh tokens, and implement context-aware authentication.

D. Username and password authentication to SP, securely store Java web tokens, and implement SMS OTPs.

Correct Answer: A

QUESTION 2

Following a recent network intrusion, a company wants to determine the current security awareness of all of its employees. Which of the following is the BEST way to test awareness?

A. Conduct a series of security training events with comprehensive tests at the end

B. Hire an external company to provide an independent audit of the network security posture

C. Review the social media of all employees to see how much proprietary information is shared

D. Send an email from a corporate account, requesting users to log onto a website with their enterprise account

Correct Answer: D

QUESTION 3

An organization is implementing a virtualized thin-client solution for normal user computing and access. During a review of the architecture, concerns were raised that an attacker could gain access to multiple user environments by simply gaining a foothold on a single one with malware. Which of the following reasons BEST explains this?

A. Malware on one virtual environment could enable pivoting to others by leveraging vulnerabilities in the hypervisor.

B. A worm on one virtual environment could spread to others by taking advantage of guest OS networking services vulnerabilities.

C. One virtual environment may have one or more application-layer vulnerabilities, which could allow an attacker to escape that environment.

D. Malware on one virtual user environment could be copied to all others by the attached network storage controller.

Correct Answer: A

QUESTION 4

A company has created a policy to allow employees to use their personally owned devices. The Chief Information Officer (CISO) is getting reports of company data appearing on unapproved forums and an increase in theft of personal electronic devices. Which of the following security controls would BEST reduce the risk of exposure?

A. Disk encryption on the local drive

B. Group policy to enforce failed login lockout

C. Multifactor authentication

D. Implementation of email digital signatures

Correct Answer: A

QUESTION 5

After the install process, a software application executed an online activation process. After a few months, the system experienced a hardware failure. A backup image of the system was restored on a newer revision of the same brand and model device. After the restore, the specialized application no longer works. Which of the following is the MOST likely cause of the problem?

A. The binary files used by the application have been modified by malware.

B. The application is unable to perform remote attestation due to blocked ports.

C. The restored image backup was encrypted with the wrong key.

D. The hash key summary of hardware and installed software no longer match.

Correct Answer: D

Different software vendors have different methods of identifying a computer used to activate software. However, a common component used in software activations is a hardware key (or hardware and software key). This key is a hash value generated based on the hardware (and possibly software) installed on the system.

For example, when Microsoft software is activated on a computer, the software generates an installation ID that consists of the software product key used during the installation and a hardware key (hash value generated from the computer\\'s hardware). The installation ID is submitted to Microsoft for software activation.

Changing the hardware on a system can change the hash key which makes the software think it is installed on another computer and is therefore not activated for use on that computer. This is most likely what has happened in this question.