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

Sara, a security analyst, is trying to prove to management what costs they could incur if their customer database was breached. This database contains 250 records with PII. Studies show that the cost per record for a breach is $300. The likelihood that their database would be breached in the next year is only 5%. Which of the following is the ALE that Sara should report to management for a security breach?

A. $1,500

B. $3,750

C. $15,000

D. $75,000

Correct Answer: B

SLE ARO = ALE, where SLE is equal to asset value (AV) times exposure factor (EF); and ARO is the annualized rate of occurrence.

SLE = 250 x $300; ARO = 5%

$75000 x 0.05 = $3750

Incorrect Answers:

A: A $1500 amount assumes a breach likelihood of 2%.

C: A $15000 amount assumes that the likelihood of a breach is 20%.

D: $75000 would be the single loss expectancy.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 5-6

QUESTION 2

Highly sensitive data is stored in a database and is accessed by an application on a DMZ server. The disk drives on all servers are fully encrypted. Communication between the application server and end-users is also encrypted. Network ACLs prevent any connections to the database server except from the application server. Which of the following can still result in exposure of the sensitive data in the database server?

A. SQL Injection

B. Theft of the physical database server

C. Cookies

D. Cross-site scripting

Correct Answer: A

The question discusses a very secure environment with disk and transport level encryption and access control lists restricting access. SQL data in a database is accessed by SQL queries from an application on the application server. The data can still be compromised by a SQL injection attack. SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application\\'s software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

Incorrect Answers:

B: Theft of the physical database server would not expose the sensitive data in the database server because the disks are encrypted. You would need the certificate used to encrypt the data in order to decrypt the data on the disks. Therefore, this answer is incorrect.

C: Cookies are text files stored on a user\\'s computer to store website information. This is to provide the user with a consistent website browsing experience. Cookies do not pose a risk to the sensitive data on the database server. Therefore, this answer is incorrect.

D: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug- in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user. The sensitive data is stored in databases on the database server. It is therefore not vulnerable to an XSS attack. Therefore, this answer is incorrect.

References: http://en.wikipedia.org/wiki/SQL_injection http://en.wikipedia.org/wiki/Cross-site_scripting

QUESTION 3

A software development company wants to implement a digital rights management solution to protect its intellectual property. Which of the following should the company implement to enforce software digital rights?

A. Transport encryption

B. IPsec

C. Non-repudiation

D. Public key infrastructure

Correct Answer: D

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. A PKI can be used to protect software.

Incorrect Answers:

A: Transport encryption would protect data that is sent between two entities. It would not be able to protect use of software.

B: IPSec protect data that is sent between two entities through encryption. It would not be able to protect use of software.

C: Nonrepudiation is a means of ensuring that transferred data is valid. Nonrepudiation is not a way to protect software. Nonrepudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 249, 262, 274-275, 279-285

QUESTION 4

Which of the following is an attack vector that can cause extensive physical damage to a datacenter without physical access?

A. CCTV system access

B. Dial-up access

C. Changing environmental controls

D. Ping of death

Correct Answer: C

Environmental systems include heating, air conditioning, humidity control, fire suppression, and power systems. All of these functions are critical to a well-designed physical plant. A computer room will typically require full-time environmental control. Changing any of these controls (when it was set to its optimum values) will result in damage.

Incorrect Answers:

A: Closed Circuit TV (CCTV) surveillance can help lessen the success of unauthorized access attempts. This is an access control which prevents physical access to a data center. In this case the attack vendor should be one that can do damage without physical access.

B: Dial-up access when unauthorized may result in technical damage and not physical damage.

D: Ping of Death is a Denial of Service attack and involves technical controls and not an attack that results in physical damages.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 378

QUESTION 5

Which of the following is the LEAST volatile when performing incident response procedures?

A. Registers

B. RAID cache

C. RAM

D. Hard drive

Correct Answer: D

An example of OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and printouts. Of the options stated in the question the hard drive would be the least volatile.

Incorrect Answers:

A: The registers are part of the CPU cache and ranks quite high in OOV incident response procedure.

B: The RAID cache is more volatile than the RAM in an OOV incident response procedure.

C: A hard drive ranks lower than RAM in an OOV incident response procedure.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 453