RC0-C02$^{\text{Q\&As}}$

CompTIA Advanced Security Practitioner (CASP) Recertification Exam for Continuing Education

Pass CompTIA RC0-C02 Exam with 100% Guarantee

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

https://www.geekcert.com/rc0-c02.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A company decides to purchase commercially available software packages. This can introduce new security risks to the network. Which of the following is the BEST description of why this is true?

A. Commercially available software packages are typically well known and widely available. Information concerning vulnerabilities and viable attack patterns are never revealed by the developer to avoid lawsuits.

B. Commercially available software packages are often widely available. Information concerning vulnerabilities is often kept internal to the company that developed the software.

C. Commercially available software packages are not widespread and are only available in limited areas. Information concerning vulnerabilities is often ignored by business managers.

D. Commercially available software packages are well known and widely available. Information concerning vulnerabilities and viable attack patterns are always shared within the IT community.

Correct Answer: B

Commercially available software packages are often widely available. Huge companies like Microsoft develop software packages that are widely available and in use on most computers. Most companies that develop commercial software make their software available through many commercial outlets (computer stores, online stores etc). Information concerning vulnerabilities is often kept internal to the company that developed the software. The large companies that develop commercial software packages are accountable for the software. Information concerning vulnerabilities being made available could have a huge financial cost to the company in terms of loss of reputation and lost revenues. Information concerning vulnerabilities is often kept internal to the company at least until a patch is available to fix the vulnerability.

QUESTION 2

A critical system audit shows that the payroll system is not meeting security policy due to missing OS security patches. Upon further review, it appears that the system is not being patched at all. The vendor states that the system is only supported on the current OS patch level. Which of the following compensating controls should be used to mitigate the vulnerability of missing OS patches on this system?

A. Isolate the system on a secure network to limit its contact with other systems

B. Implement an application layer firewall to protect the payroll system interface

C. Monitor the system\\'s security log for unauthorized access to the payroll application

D. Perform reconciliation of all payroll transactions on a daily basis

Correct Answer: A

The payroll system is not meeting security policy due to missing OS security patches. We cannot apply the patches to the system because the vendor states that the system is only supported on the current OS patch level. Therefore, we need

another way of securing the system.

We can improve the security of the system and the other systems on the network by isolating the payroll system on a secure network to limit its contact with other systems. This will reduce the likelihood of a malicious user accessing the payroll system and limit any damage to other systems if the payroll system is attacked.

QUESTION 3

select id, firstname, lastname from authors User input= firstname= Hack;man lastname=Johnson Which of the following types of attacks is the user attempting?

A. XML injection

B. Command injection

C. Cross-site scripting

D. SQL injection

Correct Answer: D

The code in the question is SQL code. The attack is 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.

QUESTION 4

The risk committee has endorsed the adoption of a security system development life cycle (SSDLC) designed to ensure compliance with PCI-DSS, HIPAA, and meet the organization\\'s mission. Which of the following BEST describes the correct order of implementing a five phase SSDLC?

A. Initiation, assessment/acquisition, development/implementation, operations/maintenance and sunset.

B. Initiation, acquisition/development, implementation/assessment, operations/maintenance and sunset.

C. Assessment, initiation/development, implementation/assessment, operations/maintenance and disposal.

D. Acquisition, initiation/development, implementation/assessment, operations/maintenance and disposal.

Correct Answer: B

QUESTION 5

In order to reduce costs and improve employee satisfaction, a large corporation is creating a BYOD policy. It will allow access to email and remote connections to the corporate enterprise from personal devices; provided they are on an approved device list. Which of the following security measures would be MOST effective in securing the enterprise under the new policy? (Select TWO).

A. Provide free email software for personal devices.

B. Encrypt data in transit for remote access.

C. Require smart card authentication for all devices.

D. Implement NAC to limit insecure devices access.

E. Enable time of day restrictions for personal devices.

Correct Answer: BD

In this question, we are allowing access to email and remote connections to the corporate enterprise from personal devices. When providing remote access to corporate systems, you should always ensure that data travelling between the corporate network and the remote device is encrypted. We need to provide access to devices only if they are on an approved device list. Therefore, we need a way to check the device before granting the device access to the network if it is an approved device. For this we can use NAC (Network Access Control). When a computer connects to a computer network, it is not permitted to access anything unless it complies with a business defined policy; including anti-virus protection level, system update level and configuration. While the computer is being checked by a pre- installed software agent, it can only access resources that can remediate (resolve or update) any issues. Once the policy is met, the computer is able to access network resources and the Internet, within the policies defined within the NAC system. NAC solutions allow network operators to define policies, such as the types of computers or roles of users allowed to access areas of the network, and enforce them in switches, routers, and network middleboxes.