RC0-C02^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.leads4pass.com/rc0-c02.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

A mature organization with legacy information systems has incorporated numerous new processes and dependencies to manage security as its networks and infrastructure are modernized. The Chief Information Office has become increasingly frustrated with frequent releases, stating that the organization needs everything to work completely, and the vendor should already have those desires built into the software product. The vendor has been in constant communication with personnel and groups within the organization to understand its business process and capture new software requirements from users. Which of the following methods of software development is this organization\\'s configuration management process using?

A. Agile

B. SDL

C. Waterfall

D. Joint application development

Correct Answer: A

In agile software development, teams of programmers and business experts work closely together, using an iterative approach.

QUESTION 2

Executive management is asking for a new manufacturing control and workflow automation solution. This application will facilitate management of proprietary information and closely guarded corporate trade secrets.

The information security team has been a part of the department meetings and come away with the following notes:

Human resources would like complete access to employee data stored in the application. They would like automated data interchange with the employee management application, a cloud-based SaaS application.

Sales is asking for easy order tracking to facilitate feedback to customers.

Legal is asking for adequate safeguards to protect trade secrets. They are also concerned with data ownership questions and legal jurisdiction.

Manufacturing is asking for ease of use. Employees working the assembly line cannot be bothered with additional steps or overhead. System interaction needs to be quick and easy.

Quality assurance is concerned about managing the end product and tracking overall performance of the product being produced. They would like read-only access to the entire workflow process for monitoring and baselining.

The favored solution is a user friendly software application that would be hosted onsite. It has extensive ACL functionality, but also has readily available APIs for extensibility. It supports read-only access, kiosk automation, custom fields, and

data encryption.

Which of the following departments\\' request is in contrast to the favored solution?

A. Manufacturing

B. Legal

C. Sales

D. Quality assurance

E. Human resources

Correct Answer: E

The human resources department wanted complete access to employee data stored in the application, and an automated data interchange with their cloud-based SaaS employee management application. However, the favored solution provides read-only access and is hosted onsite.

QUESTION 3

A security engineer is a new member to a configuration board at the request of management. The company has two new major IT projects starting this year and wants to plan security into the application deployment. The board is primarily concerned with the applications\\' compliance with federal assessment and authorization standards. The security engineer asks for a timeline to determine when a security assessment of both applications should occur and does not attend subsequent configuration board meetings. If the security engineer is only going to perform a security assessment, which of the following steps in system authorization has the security engineer omitted?

A. Establish the security control baseline

B. Build the application according to software development security standards

C. Review the results of user acceptance testing

D. Consult with the stakeholders to determine which standards can be omitted

Correct Answer: A

A security baseline is the minimum level of security that a system, network, or device must adhere to. It is the initial point of reference for security and the document against which assessments would be done.

QUESTION 4

A security manager has received the following email from the Chief Financial Officer (CFO):

"While I am concerned about the security of the proprietary financial data in our ERP application, we have had a lot of turnover in the accounting group and I am having a difficult time meeting our monthly performance targets. As things

currently stand, we do not allow employees to work from home but this is something I am willing to allow so we can get back on track. What should we do first to securely enable this capability for my group?"

Based on the information provided, which of the following would be the MOST appropriate response to the CFO?

A. Remote access to the ERP tool introduces additional security vulnerabilities and should not be allowed.

B. Allow VNC access to corporate desktops from personal computers for the users working from home.

C. Allow terminal services access from personal computers after the CFO provides a list of the users working from

home.

D. Work with the executive management team to revise policies before allowing any remote access.

Correct Answer: D

The Chief Financial Officer (CFO) wants to change company policy to allow employees to work from home. Before the new policy is implemented, the relevant documented company policies should be updated to reflect the new policy. Company policies are rarely defined by a single person in a company; they are usually defined by executive management. Therefore, you should work with the executive management team to revise the policies.

QUESTION 5

A well-known retailer has experienced a massive credit card breach. The retailer had gone through an audit and had been presented with a potential problem on their network. Vendors were authenticating directly to the retailer\\'s AD servers, and an improper firewall rule allowed pivoting from the AD server to the DMZ where credit card servers were kept. The firewall rule was needed for an internal application that was developed, which presents risk. The retailer determined that because the vendors were required to have site to site VPN\\'s no other security action was taken.

To prove to the retailer the monetary value of this risk, which of the following type of calculations is needed?

A. Residual Risk calculation

B. A cost/benefit analysis

C. Quantitative Risk Analysis

D. Qualitative Risk Analysis

Correct Answer: C

Performing quantitative risk analysis focuses on assessing the probability of risk with a metric measurement which is usually a numerical value based on money or time.

QUESTION 6

The security administrator has just installed an active\passive cluster of two firewalls for enterprise perimeter defense of the corporate network. Stateful firewall inspection is being used in the firewall implementation. There have been numerous reports of dropped connections with external clients. Which of the following is MOST likely the cause of this problem?

A. TCP sessions are traversing one firewall and return traffic is being sent through the secondary firewall and sessions are being dropped.

B. TCP and UDP sessions are being balanced across both firewalls and connections are being dropped because the session IDs are not recognized by the secondary firewall.

C. Prioritize UDP traffic and associated stateful UDP session information is traversing the passive firewall causing the connections to be dropped.

D. The firewall administrator connected a dedicated communication cable between the firewalls in order to share a single state table across the cluster causing the sessions to be dropped.

Correct Answer: A

QUESTION 7

An architect has been engaged to write the security viewpoint of a new initiative. Which of the following BEST describes a repeatable process that can be used for establishing the security architecture?

A. Inspect a previous architectural document. Based on the historical decisions made, consult the architectural control and pattern library within the organization and select the controls that appear to best fit this new architectural need.

B. Implement controls based on the system needs. Perform a risk analysis of the system. For any remaining risks, perform continuous monitoring.

C. Classify information types used within the system into levels of confidentiality, integrity, and availability. Determine minimum required security controls. Conduct a risk analysis. Decide on which security controls to implement.

D. Perform a risk analysis of the system. Avoid extreme risks. Mitigate high risks. Transfer medium risks and accept low risks. Perform continuous monitoring to ensure that the system remains at an adequate security posture.

Correct Answer: C

QUESTION 8

Ann, a software developer, wants to publish her newly developed software to an online store. Ann wants to ensure that the software will not be modified by a third party or end users before being installed on mobile devices. Which of the following should Ann implement to stop modified copies of her software from running on mobile devices?

A. Single sign-on

B. Identity propagation

C. Remote attestation

D. Secure code review

Correct Answer: C

Trusted Computing (TC) is a technology developed and promoted by the Trusted Computing Group. With Trusted Computing, the computer will consistently behave in expected ways, and those behaviors will be enforced by computer

hardware and software. Enforcing this behavior is achieved by loading the hardware with a unique encryption key inaccessible to the rest of the system.

Remote attestation allows changes to the user\\'s computer to be detected by authorized parties. For example, software companies can identify unauthorized changes to software, including users tampering with their software to circumvent

technological protection measures. It works by having the hardware generate a certificate stating what software is currently running. The computer can then present this certificate to a remote party to show that unaltered software is currently

executing.

Remote attestation is usually combined with public-key encryption so that the information sent can only be read by the

programs that presented and requested the attestation, and not by an eavesdropper.

QUESTION 9

A security analyst at Company A has been trying to convince the Information Security Officer (ISO) to allocate budget towards the purchase of a new intrusion prevention system (IPS) capable of analyzing encrypted web transactions. Which of the following should the analyst provide to the ISO to support the request? (Select TWO).

A. Emerging threat reports

B. Company attack trends

C. Request for Quote (RFQ)

D. Best practices

E. New technologies report

Correct Answer: AB

QUESTION 10

A security administrator is tasked with increasing the availability of the storage networks while enhancing the performance of existing applications. Which of the following technologies should the administrator implement to meet these goals? (Select TWO).

A. LUN masking

B. Snapshots

C. vSAN

D. Dynamic disk pools

E. Multipath

F. Deduplication

Correct Answer: DE

We can use dynamic disk pools (DDP) to increase availability and improve performance compared to traditional RAID. Multipathing also improves availability by creating multiple paths to the storage (in case one path fails) and it improves the

performance by aggregating the performance of the multiple paths. DDP dynamically distributes all data, spare capacity, and protection information across a pool of drives. Effectively, DDP is a new type of RAID level, built on RAID 6. It uses

an intelligent algorithm to define where each chunk of data should reside. In traditional RAID, drives are organized into arrays, and logical drives are written across stripes on the physical drives in the array. Hot spares contain no data until a

drive fails, leaving that spare capacity stranded and without a purpose. In the event of a drive failure, the data is recreated on the hot spare, significantly impacting the performance of all drives in the array during the rebuild process.

With DDP, each logical drive\\'s data and spare capacity is distributed across all drives in the pool, so all drives contribute to the aggregate IO of the logical drive, and the spare capacity is available to all logical drives. In the event of a physical

drive failure, data is reconstructed throughout the disk pool. Basically, the data that had previously resided on the failed drive is redistributed across all drives in the pool. Recovery from a failed drive may be up to ten times faster than a rebuild

in a traditional RAID set, and the performance degradation is much less during the rebuild.

In computer storage, multipath I/O is a fault-tolerance and performance-enhancement technique that defines more than one physical path between the CPU in a computer system and its mass-storage devices through the buses, controllers,

switches, and bridge devices connecting them.

As an example, a SCSI hard disk drive may connect to two SCSI controllers on the same computer, or a disk may connect to two Fibre Channel ports. Should one controller, port or switch fail, the operating system can route the I/O through

the remaining controller, port or switch transparently and with no changes visible to the applications.

QUESTION 11

A security administrator has been asked to select a cryptographic algorithm to meet the criteria of a new application. The application utilizes streaming video that can be viewed both on computers and mobile devices. The application designers have asked that the algorithm support the transport encryption with the lowest possible performance overhead. Which of the following recommendations would BEST meet the needs of the application designers? (Select TWO).

A. Use AES in Electronic Codebook mode

B. Use RC4 in Cipher Block Chaining mode

C. Use RC4 with Fixed IV generation

D. Use AES with cipher text padding

E. Use RC4 with a nonce generated IV

F. Use AES in Counter mode

Correct Answer: EF

In cryptography, an initialization vector (IV) is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message. Some cryptographic primitives require the IV only to be non-repeating, and the required randomness is derived internally. In this case, the IV is commonly called a nonce (number used once), and the primitives are described as stateful as opposed to randomized. This is because the IV need not be explicitly forwarded to a recipient but may be derived from a common state updated at both sender and receiver side. An example of stateful encryption schemes is the counter mode of operation, which uses a sequence number as a nonce.

AES is a block cipher. Counter mode turns a block cipher into a stream cipher. It generates the next keystream block by encrypting successive values of a "counter". The counter can be any function which produces a sequence which is guaranteed not to repeat for a long time, although an actual increment-by-one counter is the simplest and most popular.

QUESTION 12

A member of the software development team has requested advice from the security team to implement a new secure lab for testing malware. Which of the following is the NEXT step that the security team should take?

A. Purchase new hardware to keep the malware isolated.

B. Develop a policy to outline what will be required in the secure lab.

C. Construct a series of VMs to host the malware environment.

D. Create a proposal and present it to management for approval.

Correct Answer: D

Before we can create a solution, we need to motivate why the solution needs to be created and plan the best implementation with in the company\\'s business operations. We therefore need to create a proposal that explains the intended implementation and allows for the company to budget for it.

QUESTION 13

An organization determined that each of its remote sales representatives must use a smartphone for email access. The organization provides the same centrally manageable model to each person. Which of the following mechanisms BEST protects the confidentiality of the resident data?

A. Require dual factor authentication when connecting to the organization\\'s email server.

B. Require each sales representative to establish a PIN to access the smartphone and limit email storage to two weeks.

C. Require encrypted communications when connecting to the organization\\'s email server.

D. Require a PIN and automatic wiping of the smartphone if someone enters a specific number of incorrect PINs.

Correct Answer: D

QUESTION 14

A bank has decided to outsource some existing IT functions and systems to a third party service provider. The third party service provider will manage the outsourced systems on their own premises and will continue to directly interface with the bank\\'s other systems through dedicated encrypted links. Which of the following is critical to ensure the successful management of system security concerns between the two organizations?

A.ISA

B. BIA

C. MOU

D. SOA

E. BPA

Correct Answer: A

An interconnection security agreement (ISA) is a security document that derails the requirements for establishing, maintaining, and operating an interconnection between systems or networks. It specifies the requirements for connecting the systems and networks and details what security controls are co be used to protect the systems and sensitive data.

QUESTION 15

A trust relationship has been established between two organizations with web based services. One organization is acting as the Requesting Authority (RA) and the other acts as the Provisioning Service Provider (PSP). Which of the following is correct about the trust relationship?

A. The trust relationship uses SAML in the SOAP header. The SOAP body transports the SPML requests / responses.

B. The trust relationship uses XACML in the SAML header. The SAML body transports the SOAP requests / responses.

C. The trust relationship uses SPML in the SOAP header. The SOAP body transports the SAML requests / responses.

D. The trust relationship uses SPML in the SAML header. The SAML body transports the SPML requests / responses.

Correct Answer: A

Latest RC0-C02 Dumps RC0-C02 PDF Dumps RC0-C02 Braindumps