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

QUESTION 1

A new piece of ransomware got installed on a company\\'s backup server which encrypted the hard drives containing the OS and backup application configuration but did not affect the deduplication data hard drives. During the incident response, the company finds that all backup tapes for this server are also corrupt. Which of the following is the PRIMARY concern?

A. Determining how to install HIPS across all server platforms to prevent future incidents

B. Preventing the ransomware from re-infecting the server upon restore

C. Validating the integrity of the deduplicated data

D. Restoring the data will be difficult without the application configuration

Correct Answer: D

Ransomware is a type of malware that restricts access to a computer system that it infects in some way, and demands that the user pay a ransom to the operators of the malware to remove the restriction.

Since the backup application configuration is not accessible, it will require more effort to recover the data.

Eradication and Recovery is the fourth step of the incident response. It occurs before preventing future problems.

QUESTION 2

A network engineer wants to deploy user-based authentication across the company\\'s wired and wireless infrastructure at layer 2 of the OSI model. Company policies require that users be centrally managed and authenticated and that each user\\'s network access be controlled based on the user\\'s role within the company. Additionally, the central authentication system must support hierarchical trust and the ability to natively authenticate mobile devices and workstations. Which of the following are needed to implement these requirements? (Select TWO).

A. SAML

B. WAYF

C. LDAP

D. RADIUS

E. Shibboleth

F. PKI

Correct Answer: CD

RADIUS is commonly used for the authentication of WiFi connections. We can use LDAP and RADIUS for the authentication of users and devices. LDAP and RADIUS have something in common. They`re both mainly protocols (more than a database) which uses attributes to carry information back and forth. They`re clearly defined in RFC documents so you can expect products from different vendors to be able to function properly together. RADIUS is NOT a database. It\\'s a protocol for asking intelligent questions to a user database. LDAP is just a database. In recent offerings it contains a bit of intelligence (like Roles, Class of Service and so on) but it still is mainly just a rather stupid database. RADIUS (actually RADIUS servers like FreeRADIUS) provide the administrator the tools to not only perform

user authentication but also to authorize users based on extremely complex checks and logic. For instance you can allow access on a specific NAS only if the user belongs to a certain category, is a member of a specific group and an outside script allows access. There\\'s no way to perform any type of such complex decisions in a user database.

QUESTION 3

An assessor identifies automated methods for identifying security control compliance through validating sensors at the endpoint and at Tier 2. Which of the following practices satisfy continuous monitoring of authorized information systems?

A. Independent verification and validation

B. Security test and evaluation

C. Risk assessment

D. Ongoing authorization

Correct Answer: D

Ongoing assessment and authorization is often referred to as continuous monitoring. It is a process that determines whether the set of deployed security controls in an information system continue to be effective with regards to planned and

unplanned changes that occur in the system and its environment over time.

Continuous monitoring allows organizations to evaluate the operating effectiveness of controls on or near a real-time basis. Continuous monitoring enables the enterprise to detect control failures quickly because it transpires immediately or

closely after events in which the key controls are utilized.

QUESTION 4

The Chief Executive Officer (CEO) of a company that allows telecommuting has challenged the Chief Security Officer\\'s (CSO) request to harden the corporate network\\'s perimeter. The CEO argues that the company cannot protect its employees at home, so the risk at work is no different. Which of the following BEST explains why this company should proceed with protecting its corporate network boundary?

A. The corporate network is the only network that is audited by regulators and customers.

B. The aggregation of employees on a corporate network makes it a more valuable target for attackers.

C. Home networks are unknown to attackers and less likely to be targeted directly.

D. Employees are more likely to be using personal computers for general web browsing when they are at home.

Correct Answer: B

Data aggregation is any process in which information is gathered and expressed in a summary form, for purposes such as statistical analysis. Data aggregation increases the impact and scale of a security breach. The amount of data aggregation on the corporate network is much more that on an employee\\'s home network, and is therefore more valuable.

QUESTION 5

An application present on the majority of an organization\\'s 1,000 systems is vulnerable to a buffer overflow attack. Which of the following is the MOST comprehensive way to resolve the issue?

A. Deploy custom HIPS signatures to detect and block the attacks.

B. Validate and deploy the appropriate patch.

C. Run the application in terminal services to reduce the threat landscape.

D. Deploy custom NIPS signatures to detect and block the attacks.

Correct Answer: B

If an application has a known issue (such as susceptibility to buffer overflow attacks) and a patch is released to resolve the specific issue, then the best solution is always to deploy the patch.

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user\\'s files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

QUESTION 6

The internal audit department is investigating a possible breach of security. One of the auditors is sent to interview the following employees:

Employee A: Works in the accounts receivable office and is in charge of entering data into the finance system.

Employee B: Works in the accounts payable office and is in charge of approving purchase orders.

Employee C: Is the manager of the finance department, supervises Employee A and Employee B, and can perform the functions of both Employee A and Employee B.

Which of the following should the auditor suggest be done to avoid future security breaches?

A. All employees should have the same access level to be able to check on each others.

B. The manager should only be able to review the data and approve purchase orders.

C. Employee A and Employee B should rotate jobs at a set interval and cross-train.

D. The manager should be able to both enter and approve information.

Correct Answer: B

QUESTION 7

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 8

A company has implemented data retention policies and storage quotas in response to their legal department\\'s requests and the SAN administrator\\'s recommendation. The retention policy states all email data older than 90 days should be eliminated. As there are no technical controls in place, users have been instructed to stick to a storage quota of 500Mb of network storage and 200Mb of email storage. After being presented with an e- discovery request from an opposing legal council, the security administrator discovers that the user in the suit has 1Tb of files and 300Mb of email spanning over two years. Which of the following should the security administrator provide to opposing council?

A. Delete files and email exceeding policy thresholds and turn over the remaining files and email.

B. Delete email over the policy threshold and hand over the remaining emails and all of the files.

C. Provide the 1Tb of files on the network and the 300Mb of email files regardless of age.

D. Provide the first 200Mb of e-mail and the first 500Mb of files as per policy.

Correct Answer: C

QUESTION 9

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 10

A security analyst, Ann, states that she believes Internet facing file transfer servers are being attacked. Which of the following is evidence that would aid Ann in making a case to management that action needs to be taken to safeguard these servers?

A. Provide a report of all the IP addresses that are connecting to the systems and their locations

B. Establish alerts at a certain threshold to notify the analyst of high activity

C. Provide a report showing the file transfer logs of the servers

D. Compare the current activity to the baseline of normal activity

Correct Answer: D

In risk assessment a baseline forms the foundation for how an organization needs to increase or enhance its current level of security. This type of assessment will provide Ann with the necessary information to take to management.

QUESTION 11

There have been some failures of the company\\'s internal facing website. A security engineer has found the WAF to be the root cause of the failures. System logs show that the WAF has been unavailable for 14 hours over the past month, in four separate situations. One of these situations was a two hour scheduled maintenance time, aimed at improving the stability of the WAF. Using the MTTR based on the last month\\'s performance figures, which of the following calculations is the percentage of uptime assuming there were 722 hours in the month?

A. 92.24 percent

B. 98.06 percent

C. 98.34 percent

D. 99.72 percent

Correct Answer: B

A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing

the rules to your application, many attacks can be identified and blocked.

14h of down time in a period of 772 supposed uptime = 14/772 x 100 = 1.939 % Thus the % of uptime = 100% - 1.939% = 98.06%

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley and Sons, Indianapolis, 2012, pp. 43, 116

QUESTION 12

A security administrator was doing a packet capture and noticed a system communicating with an unauthorized address within the 2001::/32 prefix. The network administrator confirms there is no IPv6 routing into or out of the network.

Which of the following is the BEST course of action?

A. Investigate the network traffic and block UDP port 3544 at the firewall

B. Remove the system from the network and disable IPv6 at the router

C. Locate and remove the unauthorized 6to4 relay from the network

D. Disable the switch port and block the 2001::/32 traffic at the firewall

Correct Answer: A

The 2001::/32 prefix is used for Teredo tunneling. Teredo is a transition technology that gives full IPv6 connectivity for IPv6-capable hosts that are on the IPv4 Internet but have no native connection to an IPv6 network. Unlike similar protocols,

it can perform its function even from behind network address translation (NAT) devices such as home routers.

Teredo provides IPv6 (Internet Protocol version 6) connectivity by encapsulating IPv6 datagram packets within IPv4 User Datagram Protocol (UDP) packets. Teredo routes these datagrams on the IPv4 Internet and through NAT devices.

Teredo nodes elsewhere on the IPv6 network (called Teredo relays) receive the packets, decapsulate them, and pass them on. The Teredo server listens on UDP port 3544.

Teredo clients are assigned an IPv6 address that starts with the Teredo prefix (2001::/32). In this question, the BEST course of action would be to block UDP port 3544 at the firewall. This will block the unauthorized communication. You can

then investigate the traffic within the network.

QUESTION 13

A company that must comply with regulations is searching for a laptop encryption product to use for its 40,000 end points. The product must meet regulations but also be flexible enough to minimize overhead and support in regards to password resets and lockouts. Which of the following implementations would BEST meet the needs?

A. A partition-based software encryption product with a low-level boot protection and authentication

B. A container-based encryption product that allows the end users to select which files to encrypt

C. A full-disk hardware-based encryption product with a low-level boot protection and authentication

D. A file-based encryption product using profiles to target areas on the file system to encrypt

Correct Answer: D

The question is asking for a solution that will minimize overhead and support in regards to password resets and lockouts.

File based encryption products operate under the context of the computer user\\'s user account. This means that the user does not need to remember a separate password for the encryption software. If the user forgets his user account

password or is locked out due to failed login attempts, the support department can reset his password from a central database of user accounts (such as Active Directory) without the need to visit the user\\'s computer.

Profiles can be used to determine areas on the file system to encrypt such as Document folders.

QUESTION 14

A risk manager has decided to use likelihood and consequence to determine the risk of an event occurring to a company asset. Which of the following is a limitation of this approach to risk management?

A. Subjective and based on an individual\\'s experience.

B. Requires a high degree of upfront work to gather environment details.

C. Difficult to differentiate between high, medium, and low risks.

D. Allows for cost and benefit analysis.

E. Calculations can be extremely complex to manage.

Correct Answer: A

Using likelihood and consequence to determine risk is known as qualitative risk analysis. With qualitative risk analysis, the risk would be evaluated for its probability and impact using a numbered ranking system such as low, medium, and high

or perhaps using a 1 to 10 scoring system.

After qualitative analysis has been performed, you can then perform quantitative risk analysis. A Quantitative risk analysis is a further analysis of the highest priority risks during which a numerical or quantitative rating is assigned to the risk.

Qualitative risk analysis is usually quick to perform and no special tools or software is required. However, qualitative risk analysis is subjective and based on the user\\'s experience.

QUESTION 15

Which of the following represents important technical controls for securing a SAN storage infrastructure? (Select TWO).

A. Synchronous copy of data

B. RAID configuration

C. Data de-duplication

D. Storage pool space allocation

E. Port scanning

F. LUN masking/mapping

G. Port mapping

Correct Answer: FG

A logical unit number (LUN) is a unique identifier that designates individual hard disk devices or grouped devices for address by a protocol associated with a SCSI, iSCSI, Fibre Channel (FC) or similar interface. LUNs are central to the

management of block storage arrays shared over a storage area network (SAN).

LUN masking subdivides access to a given port. Then, even if several LUNs are accessed through the same port, the server masks can be set to limit each server\\'s access to the appropriate LUNs. LUN masking is typically conducted at the

host bus adapter (HBA) or switch level.

Port mapping is used in `Zoning\\'. In storage networking, Fibre Channel zoning is the partitioning of a Fibre Channel fabric into smaller subsets to restrict interference, add security, and to simplify management. While a SAN makes available

several devices and/or ports to a single device, each system connected to the SAN should only be allowed access to a controlled subset of these devices/ports. Zoning can be applied to either the switch port a device is connected to OR the

WWN World Wide Name on the host being connected. As port based zoning restricts traffic flow based on the specific switch port a device is connected to, if the device is moved, it will lose access. Furthermore, if a different device is

connected to the port in question, it will gain access to any resources the previous host had access to.