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.pass4itsure.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 corporation has expanded for the first time by integrating several newly acquired businesses. Which of the following are the FIRST tasks that the security team should undertake? (Select TWO).

A. Remove acquired companies Internet access.

B. Federate identity management systems.

C. Install firewalls between the businesses.

D. Re-image all end user computers to a standard image.

E. Develop interconnection policy.

F. Conduct a risk analysis of each acquired company\\'s networks.

Correct Answer: EF

QUESTION 2

An international shipping company discovered that deliveries left idle are being tampered with. The company wants to reduce the idle time associated with international deliveries by ensuring that personnel are automatically notified when an inbound delivery arrives at the transit dock. Which of the following should be implemented to help the company increase the security posture of its operations?

A. Back office database

B. Asset tracking

C. Geo-fencing

D. Barcode scanner

Correct Answer: C

Mobile device management (MDM) is a type of security software used by an IT department to monitor, manage and secure employees\\' mobile devices that are deployed across multiple mobile service providers and across multiple mobile

operating systems being used in the organization.

A secure container, in a mobile security context, is an authenticated and encrypted area of an employee\\'s device that separates sensitive corporate information from the owner\\'s personal data and apps.

The purpose of containerization is to prevent malware, intruders, system resources or other applications from interacting with the secured application and associated corporate data. Secure data containers are third-party mobile apps. The

container acts as a storage area that is authenticated and encrypted by software and governed by corporate IT security policies. Such apps let IT enforce security policies on the same sensitive business data across different devices, which is

especially useful because native device security capabilities vary.

As BYOD (bring your own device) and consumerization trends have grown, the challenges involved in protecting both corporate data and user privacy have also increased. Containerization is one means of providing administrators with full

control over corporate applications and data without affecting those of the user.

QUESTION 3

A forensic analyst receives a hard drive containing malware quarantined by the antivirus application. After creating an image and determining the directory location of the malware file, which of the following helps to determine when the system became infected?

A. The malware file\\'s modify, access, change time properties.

B. The timeline analysis of the file system.

C. The time stamp of the malware in the swap file.

D. The date/time stamp of the malware detection in the antivirus logs.

Correct Answer: B

Timelines can be used in digital forensics to identify when activity occurred on a computer. Timelines are mainly used for data reduction or identifying specific state changes that have occurred on a computer.

QUESTION 4

An administrator has four virtual guests on a host server. Two of the servers are corporate SQL servers, one is a corporate mail server, and one is a testing web server for a small group of developers. The administrator is experiencing difficulty connecting to the host server during peak network usage times. Which of the following would allow the administrator to securely connect to and manage the host server during peak usage times?

A. Increase the virtual RAM allocation to high I/O servers.

B. Install a management NIC and dedicated virtual switch.

C. Configure the high I/O virtual servers to use FCoE rather than iSCSI.

D. Move the guest web server to another dedicated host.

Correct Answer: B

QUESTION 5

Company A is merging with Company B. Company B uses mostly hosted services from an outside vendor, while Company A uses mostly in-house products. The project manager of the merger states the merged systems should meet these goals:

-Ability to customize systems per department

-Quick implementation along with an immediate ROI

-The internal IT team having administrative level control over all products

The project manager states the in-house services are the best solution. Because of staff shortages, the senior security administrator argues that security will be best maintained by continuing to use outsourced services. Which of the following solutions BEST solves the disagreement?

A. Raise the issue to the Chief Executive Officer (CEO) to escalate the decision to senior management with the recommendation to continue the outsourcing of all IT services.

B. Calculate the time to deploy and support the in-sourced systems accounting for the staff shortage and compare the costs to the ROI costs minus outsourcing costs. Present the document numbers to management for a final decision.

C. Perform a detailed cost benefit analysis of outsourcing vs. in-sourcing the IT systems and review the system documentation to assess the ROI of in-sourcing. Select COTS products to eliminate development time to meet the ROI goals.

D. Arrange a meeting between the project manager and the senior security administrator to review the requirements and determine how critical all the requirements are.

Correct Answer: B

QUESTION 6

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 7

A security manager looked at various logs while investigating a recent security breach in the data center from an external source. Each log below was collected from various security devices compiled from a report through the company\\'s

security information and event management server.

Logs:

Log 1:

Feb 5 23:55:37.743: %SEC-6-IPACCESSLOGS: list 10 denied 10.2.5.81 3 packets

Log 2:

HTTP://www.company.com/index.php?user=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

Log 3:

Security Error Alert

Event ID 50: The RDP protocol component X.224 detected an error in the protocol stream and has disconnected the client

Log 4:

Encoder oe = new OracleEncoder ();

String query = "Select user_id FROM user_data WHERE user_name = ` "

+ oe.encode (req.getParameter("userID")) + " ` and user_password = ` "

+ oe.encode (req.getParameter("pwd")) +" ` ";

Vulnerabilities

Buffer overflow

SQL injection

ACL

XSS

Which of the following logs and vulnerabilities would MOST likely be related to the security breach? (Select TWO).

A. Log 1

B. Log 2

C. Log 3

D. Log 4

E. Buffer overflow

F. ACL

G. XSS

H. SQL injection

Correct Answer: BE

Log 2 indicates that the security breach originated from an external source. And the vulnerability that can be associated with this security breach is a buffer overflow that happened when the amount of data written into the buffer exceeded the limit of that particular buffer.

QUESTION 8

A business wants to start using social media to promote the corporation and to ensure that customers have a good experience with their products. Which of the following security items should the company have in place before implementation? (Select TWO).

A. The company must dedicate specific staff to act as social media representatives of the company.

B. All staff needs to be instructed in the proper use of social media in the work environment.

C. Senior staff blogs should be ghost written by marketing professionals.

D. The finance department must provide a cost benefit analysis for social media.

E. The security policy needs to be reviewed to ensure that social media policy is properly implemented.

F. The company should ensure that the company has sufficient bandwidth to allow for social media traffic.

Correct Answer: AE

QUESTION 9

A security administrator is shown the following log excerpt from a Unix system:

2013 Oct 10 07:14:57 web14 sshd[1632]: Failed password for root from 198.51.100.23 port 37914 ssh2

2013 Oct 10 07:14:57 web14 sshd[1635]: Failed password for root from 198.51.100.23 port 37915 ssh2

2013 Oct 10 07:14:58 web14 sshd[1638]: Failed password for root from 198.51.100.23 port 37916 ssh2

2013 Oct 10 07:15:59 web14 sshd[1640]: Failed password for root from 198.51.100.23 port 37918 ssh2

2013 Oct 10 07:16:00 web14 sshd[1641]: Failed password for root from 198.51.100.23 port 37920 ssh2

2013 Oct 10 07:16:00 web14 sshd[1642]: Successful login for root from 198.51.100.23 port 37924 ssh2

Which of the following is the MOST likely explanation of what is occurring and the BEST immediate response? (Select TWO).

A. An authorized administrator has logged into the root account remotely.

B. The administrator should disable remote root logins.

C. Isolate the system immediately and begin forensic analysis on the host.

D. A remote attacker has compromised the root account using a buffer overflow in sshd.

E. A remote attacker has guessed the root password using a dictionary attack.

F. Use iptables to immediately DROP connections from the IP 198.51.100.23.

G. A remote attacker has compromised the private key of the root account.

H. Change the root password immediately to a password not found in a dictionary.

Correct Answer: CE

The log shows six attempts to log in to a system. The first five attempts failed due to `failed password\\'. The sixth attempt was a successful login. Therefore, the MOST likely explanation of what is occurring is that a remote attacker has

guessed the root password using a dictionary attack.

The BEST immediate response is to isolate the system immediately and begin forensic analysis on the host. You should isolate the system to prevent any further access to it and prevent it from doing any damage to other systems on the

network. You should perform a forensic analysis on the system to determine what the attacker did on the system after gaining access.

QUESTION 10

Statement: "The system shall implement measures to notify system administrators prior to a security incident occurring." Which of the following BEST restates the above statement to allow it to be implemented by a team of software developers?

A. The system shall cease processing data when certain configurable events occur.

B. The system shall continue processing in the event of an error and email the security administrator the error logs.

C. The system shall halt on error.

D. The system shall throw an error when specified incidents pass a configurable threshold.

Correct Answer: D

QUESTION 11

A penetration tester is assessing a mobile banking application. Man-in-the-middle attempts via an HTTP intercepting proxy are failing with SSL errors. Which of the following controls has likely been implemented by the developers?

A. SSL certificate revocation

B. SSL certificate pinning

C. Mobile device root-kit detection

D. Extended Validation certificates

Correct Answer: B

Users, developers, and applications expect end-to-end security on their secure channels, but some secure channels are not meeting the expectation. Specifically, channels built using well known protocols such as VPN, SSL, and TLS can be

vulnerable to a number of attacks.

Pinning is the process of associating a host with their expected X509 certificate or public key. Once a certificate or public key is known or seen for a host, the certificate or public key is associated or \\'pinned\\' to the host.

A host or service\\'s certificate or public key can be added to an application at development time, or it can be added upon first encountering the certificate or public key. The former - adding at development time - is preferred since preloading the

certificate or public key out of band usually means the attacker cannot taint the pin. If the certificate or public key is added upon first encounter, you will be using key continuity. Key continuity can fail if the attacker has a privileged position

during the first encounter.

QUESTION 12

A security solutions architect has argued consistently to implement the most secure method of encrypting corporate messages. The solution has been derided as not being cost effective by other members of the IT department. The proposed solution uses symmetric keys to encrypt all messages and is very resistant to unauthorized decryption. The method also requires special handling and security for all key material that goes above and beyond most encryption systems.

Which of the following is the solutions architect MOST likely trying to implement?

A. One time pads

B. PKI

C. Quantum cryptography

D. Digital rights management

Correct Answer: A

In cryptography, the one-time pad (OTP) is an encryption technique that cannot be cracked if used correctly. In this technique, a plaintext is paired with a random secret key (also referred to as a one-time pad). Then, each bit or character of

the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition. If the key is truly random, is at least as long as the plaintext, is never reused in whole or in part, and is kept completely

secret, then the resulting ciphertext will be impossible to decrypt or break. However, practical problems have prevented one-time pads from being widely used.

The "pad" part of the name comes from early implementations where the key material was distributed as a pad of paper, so that the top sheet could be easily torn off and destroyed after use.

The one-time pad has serious drawbacks in practice because it requires:

Truly random (as opposed to pseudorandom) one-time pad values, which is a non-trivial requirement.

Secure generation and exchange of the one-time pad values, which must be at least as long as the message. (The security of the one-time pad is only as secure as the security of the one-time pad exchange).

Careful treatment to make sure that it continues to remain secret, and is disposed of correctly preventing any reuse in whole or part--hence "one time".

Because the pad, like all shared secrets, must be passed and kept secure, and the pad has to be at least as long as the message, there is often no point in using one-time padding, as one can simply send the plain text instead of the pad (as

both can be the same size and have to be sent securely).

Distributing very long one-time pad keys is inconvenient and usually poses a significant security risk. The pad is essentially the encryption key, but unlike keys for modern ciphers, it must be extremely long and is much too difficult for humans

to remember. Storage media such as thumb drives, DVD-Rs or personal digital audio players can be used to carry a very large one-time-pad from place to place in a non-suspicious way, but even so the need to transport the pad physically is

a burden compared to the key negotiation protocols of a modern public-key cryptosystem, and such media cannot reliably be erased securely by any means short of physical destruction (e.g., incineration). The key material must be securely

disposed of after use, to ensure the key material is never reused and to protect the messages sent. Because the key material must be transported from one endpoint to another, and persist until the message is sent or received, it can be more

vulnerable to forensic recovery than the transient plaintext it protects.

QUESTION 13

A senior network security engineer has been tasked to decrease the attack surface of the corporate network. Which of the following actions would protect the external network interfaces from external attackers performing network scanning?

A. Remove contact details from the domain name registrar to prevent social engineering attacks.

B. Test external interfaces to see how they function when they process fragmented IP packets.

C. Enable a honeynet to capture and facilitate future analysis of malicious attack vectors.

D. Filter all internal ICMP message traffic, forcing attackers to use full-blown TCP port scans against external network interfaces.

Correct Answer: B

Fragmented IP packets are often used to evade firewalls or intrusion detection systems.

Port Scanning is one of the most popular reconnaissance techniques attackers use to discover services they can break into. All machines connected to a Local Area Network (LAN) or Internet run many services that listen at well-known and

not so well known ports. A port scan helps the attacker find which ports are available (i.e., what service might be listing to a port).

One problem, from the perspective of the attacker attempting to scan a port, is that services listening on these ports log scans. They see an incoming connection, but no data, so an error is logged. There exist a number of stealth scan

techniques to avoid this. One method is a fragmented port scan.

Fragmented packet Port Scan

The scanner splits the TCP header into several IP fragments. This bypasses some packet filter firewalls because they cannot see a complete TCP header that can match their filter rules. Some packet filters and firewalls do queue all IP

fragments, but many networks cannot afford the performance loss caused by the queuing.

QUESTION 14

A finance manager says that the company needs to ensure that the new system can "replay" data, up to the minute, for every exchange being tracked by the investment departments. The finance manager also states that the company\\'s transactions need to be tracked against this data for a period of five years for compliance. How would a security engineer BEST interpret the finance manager\\'s needs?

A. Compliance standards

B. User requirements

C. Data elements

D. Data storage

E. Acceptance testing

F. Information digest

G. System requirements

Correct Answer: B

User requirements are used to specify what the USER expects an application or system to do.

In this question, the finance manager has stated what he wants the system to do. Therefore, the answer to this question is `user requirements\\'.

QUESTION 15

A new IDS device is generating a very large number of irrelevant events. Which of the following would BEST remedy this problem?

A. Change the IDS to use a heuristic anomaly filter.

B. Adjust IDS filters to decrease the number of false positives.

C. Change the IDS filter to data mine the false positives for statistical trending data.

D. Adjust IDS filters to increase the number of false negatives.

Correct Answer: B

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