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

QUESTION 1

The organization has an IT driver on cloud computing to improve delivery times for IT solution provisioning. Separate to this initiative, a business case has been approved for replacing the existing banking platform for credit card processing with a newer offering. It is the security practitioner\\'s responsibility to evaluate whether the new credit card processing platform can be hosted within a cloud environment. Which of the following BEST balances the security risk and IT drivers for cloud computing?

A. A third-party cloud computing platform makes sense for new IT solutions. This should be endorsed going forward so as to align with the IT strategy. However, the security practitioner will need to ensure that the third-party cloud provider does regular penetration tests to ensure that all data is secure.

B. Using a third-party cloud computing environment should be endorsed going forward. This aligns with the organization\\'s strategic direction. It also helps to shift any risk and regulatory compliance concerns away from the company\\'s internal IT department. The next step will be to evaluate each of the cloud computing vendors, so that a vendor can then be selected for hosting the new credit card processing platform.

C. There may be regulatory restrictions with credit cards being processed out of country or processed by shared hosting providers. A private cloud within the company should be considered. An options paper should be created which outlines the risks, advantages, disadvantages of relevant choices and it should recommended a way forward.

D. Cloud computing should rarely be considered an option for any processes that need to be significantly secured. The security practitioner needs to convince the stakeholders that the new platform can only be delivered internally on physical infrastructure.

Correct Answer: C

QUESTION 2

A security administrator is performing VDI traffic data collection on a virtual server which migrates from one host to another. While reviewing the data collected by the protocol analyzer, the security administrator notices that sensitive data is present in the packet capture. Which of the following should the security administrator recommend to ensure the confidentiality of sensitive information during live VM migration, while minimizing latency issues?

A. A separate physical interface placed on a private VLAN should be configured for live host operations.

B. Database record encryption should be used when storing sensitive information on virtual servers.

C. Full disk encryption should be enabled across the enterprise to ensure the confidentiality of sensitive data.

D. Sensitive data should be stored on a backend SAN which uses an isolated fiber channel network.

Correct Answer: A

VDI virtual machines can be migrated across physical hosts while the virtual machines are still powered on. In VMware, this is called vMotion. In Microsoft Hyper-V, this is called Live Migration.

When a virtual machine is migrated between hosts, the data is unencrypted as it travels across the network. To prevent access to the data as it travels across the network, a dedicated network should be created for virtual machine migrations.

The dedicated migration network should only be accessible by the virtual machine hosts to maximize security.

QUESTION 3

Company A needs to export sensitive data from its financial system to company B\\'s database, using company B\\'s API in an automated manner. Company A\\'s policy prohibits the use of any intermediary external systems to transfer or store its sensitive data, therefore the transfer must occur directly between company A\\'s financial system and company B\\'s destination server using the supplied API. Additionally, company A\\'s legacy financial software does not support encryption, while company B\\'s API supports encryption. Which of the following will provide end-to-end encryption for the data transfer while adhering to these requirements?

A. Company A must install an SSL tunneling software on the financial system.

B. Company A\\'s security administrator should use an HTTPS capable browser to transfer the data.

C. Company A should use a dedicated MPLS circuit to transfer the sensitive data to company B.

D. Company A and B must create a site-to-site IPSec VPN on their respective firewalls.

Correct Answer: A

We need to transfer the data from company A\\'s financial system to company B\\'s destination server. Company B\\'s API does support encryption. Company A\\'s legacy financial software does not support encryption.

To provide end-to-end encryption for the data transfer, we need a way of enabling Company A\\'s financial system to support encryption. The easiest way to do this is to install an SSL tunneling software application on the financial system.

There are several SSL tunneling software applications out there; one example is STunnel.

QUESTION 4

A new IT company has hired a security consultant to implement a remote access system, which will enable employees to telecommute from home using both company issued as well as personal computing devices, including mobile devices. The company wants a flexible system to provide confidentiality and integrity for data in transit to the company\\'s internally developed application GUI. Company policy prohibits employees from having administrative rights to company issued devices. Which of the following remote access solutions has the lowest technical complexity?

A. RDP server

B. Client-based VPN

C. IPSec

D. Jump box

E. SSL VPN

Correct Answer: A

Connecting to a remote desktop server by using a remote desktop connection on a client device is has the lowest technical complexity.

Remote Desktop Services (or Remote Desktop Protocol server) is one of the components of Microsoft Windows that allows a user to take control of a remote computer or virtual machine over a network connection. RDS is Microsoft\\'s

implementation of thin client, where Windows software and the entire desktop of the computer running RDS, are made accessible to a remote client machine that supports Remote Desktop Protocol (RDP). With RDS, only software user

interfaces are transferred to the client system. All input from the client system is transmitted to the server, where software execution takes place.

QUESTION 5

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 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

Joe, the Chief Executive Officer (CEO), was an Information security professor and a Subject Matter Expert for over 20 years. He has designed a network defense method which he says is significantly better than prominent international standards. He has recommended that the company use his cryptographic method. Which of the following methodologies

should be adopted?

A. The company should develop an in-house solution and keep the algorithm a secret.

B. The company should use the CEO\\'s encryption scheme.

C. The company should use a mixture of both systems to meet minimum standards.

D. The company should use the method recommended by other respected information security organizations.

Correct Answer: D

In this question, we have one person\\'s opinion about the best way to secure the network. His method may be more secure than other systems. However, for consensus of opinion, it is better to use the method recommended by other respected information security organizations. If the CEO\\'s methods were the best methods, it is likely that the other respected information security organizations would have thought about them and would be using them. In other words, the methods recommended by other respected information security organizations are probably the best methods. Furthermore, if the company\\'s systems need to communicate with external systems, the systems will need to use a `standard\\' method otherwise the external system may not be able to decipher the communications from the company\\'s systems.

QUESTION 8

A small retail company recently deployed a new point of sale (POS) system to all 67 stores. The core of the POS is an extranet site, accessible only from retail stores and the corporate office over a split-tunnel VPN. An additional split-tunnel VPN provides bi-directional connectivity back to the main office, which provides voice connectivity for store VoIP phones. Each store offers guest wireless functionality, as well as employee wireless. Only the staff wireless network has access to the POS VPN. Recently, stores are reporting poor response times when accessing the POS application from store computers as well as degraded voice quality when making phone calls. Upon investigation, it is determined that three store PCs are hosting malware, which is generating excessive network traffic. After malware removal, the information security department is asked to review the configuration and suggest changes to prevent this from happening again. Which of the following denotes the BEST way to mitigate future malware risk?

A. Deploy new perimeter firewalls at all stores with UTM functionality.

B. Change antivirus vendors at the store and the corporate office.

C. Move to a VDI solution that runs offsite from the same data center that hosts the new POS solution.

D. Deploy a proxy server with content filtering at the corporate office and route all traffic through it.

Correct Answer: A

A perimeter firewall is located between the local network and the Internet where it can screen network traffic flowing in and out of the organization. A firewall with unified threat management (UTM) functionalities includes anti-malware capabilities.

QUESTION 9

A large company is preparing to merge with a smaller company. The smaller company has been very profitable, but the smaller company\\'s main applications were created in-house. Which of the following actions should the large company\\'s security administrator take in preparation for the merger?

A. A review of the mitigations implemented from the most recent audit findings of the smaller company should be performed.

B. An ROI calculation should be performed to determine which company\\'s application should be used.

C. A security assessment should be performed to establish the risks of integration or co- existence.

D. A regression test should be performed on the in-house software to determine security risks associated with the software.

Correct Answer: C

With any merger regardless of the monetary benefit there is always security risks and prior to the merger the security administrator should assess the security risks to as to mitigate these.

QUESTION 10

An accountant at a small business is trying to understand the value of a server to determine if the business can afford to buy another server for DR. The risk manager only provided the accountant with the SLE of $24,000, ARO of 20% and the exposure factor of 25%. Which of the following is the correct asset value calculated by the accountant?

A. $4,800

B. $24,000

C. $96,000

D. $120,000

Correct Answer: C

The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as: ALE = ARO x SLE

Single Loss Expectancy (SLE) is mathematically expressed as: Asset value (AV) x Exposure Factor (EF)

Thus if SLE = $ 24,000 and EF = 25% then the Asset value is SLE/EF = $ 96,000

References:

http://www.financeformulas.net/Return_on_Investment.html https://en.wikipedia.org/wiki/Risk_assessment

QUESTION 11

New zero-day attacks are announced on a regular basis against a broad range of technology systems. Which of the following best practices should a security manager do to manage the risks of these attack vectors? (Select TWO).

A. Establish an emergency response call tree.

B. Create an inventory of applications.

C. Backup the router and firewall configurations.

D. Maintain a list of critical systems.

E. Update all network diagrams.

Correct Answer: BD

QUESTION 12

A small company is developing a new Internet-facing web application. The security requirements are:

Users of the web application must be uniquely identified and authenticated.

Users of the web application will not be added to the company\\'s directory services.

Passwords must not be stored in the code.

Which of the following meets these requirements?

A. Use OpenID and allow a third party to authenticate users.

B. Use TLS with a shared client certificate for all users.

C. Use SAML with federated directory services.

D. Use Kerberos and browsers that support SAML.

Correct Answer: A

Users create accounts by selecting an OpenID identity provider, and then use those accounts to sign onto any website which accepts OpenID authentication. OpenID is an open standard and decentralized protocol by the non-profit OpenID Foundation that allows users to be authenticated by certain co-operating sites (known as Relying Parties or RP) using a third party service. This eliminates the need for webmasters to provide their own ad hoc systems and allowing users to consolidate their digital identities. In other words, users can log into multiple unrelated websites without having to register with their information over and over again. Several large organizations either issue or accept OpenIDs on their websites according to the OpenID Foundation: AOL, Blogger, Flickr, France Telecom, Google, Hyves, LiveJournal, Microsoft (provider name Microsoft account), Mixi, Myspace, Novell, Orange, Sears, Sun, Telecom Italia, Universal Music Group, VeriSign, WordPress, and Yahoo!. Other providers include BBC, IBM, PayPal, and Steam.

QUESTION 13

An insurance company is looking to purchase a smaller company in another country. Which of the following tasks would the security administrator perform as part of the security due diligence?

A. Review switch and router configurations

B. Review the security policies and standards

C. Perform a network penetration test

D. Review the firewall rule set and IPS logs

Correct Answer: B

IT security professionals should have a chance to review the security controls and practices of a company targeted for acquisition. Any irregularities that are found should be reported to management so that expenses and concerns are properly identified.

QUESTION 14

A Security Administrator has some concerns about the confidentiality of data when using SOAP. Which of the following BEST describes the Security Administrator\\'s concerns?

A. The SOAP header is not encrypted and allows intermediaries to view the header data. The body can be partially or completely encrypted.

B. The SOAP protocol supports weak hashing of header information. As a result the header and body can easily be deciphered by brute force tools.

C. The SOAP protocol can be easily tampered with, even though the header is encrypted.

D. The SOAP protocol does not support body or header encryption which allows assertions to be viewed in clear text by intermediaries.

Correct Answer: A

QUESTION 15

A business unit of a large enterprise has outsourced the hosting and development of a new external website which will be accessed by premium customers, in order to speed up the time to market timeline. Which of the following is the MOST appropriate?

A. The external party providing the hosting and website development should be obligated under contract to provide a secure service which is regularly tested (vulnerability and penetration). SLAs should be in place for the resolution of newly identified vulnerabilities and a guaranteed uptime.

B. The use of external organizations to provide hosting and web development services is not recommended as the costs are typically higher than what can be achieved internally. In addition, compliance with privacy regulations becomes more complex and guaranteed uptimes are difficult to track and measure.

C. Outsourcing transfers all the risk to the third party. An SLA should be in place for the resolution of newly identified vulnerabilities and penetration / vulnerability testing should be conducted regularly.

D. Outsourcing transfers the risk to the third party, thereby minimizing the cost and any legal obligations. An MOU should be in place for the resolution of newly identified vulnerabilities and penetration / vulnerability testing should be conducted regularly.

Correct Answer: A

A service level agreement (SLA) guarantees the level of service the partner is agreeing to provide. It specifies the uptime, response time, and maximum outage time that the partner is agreeing to.