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

Within an organization, there is a known lack of governance for solution designs. As a result there are inconsistencies and varying levels of quality for the artifacts that are produced. Which of the following will help BEST improve this situation?

A. Ensure that those producing solution artifacts are reminded at the next team meeting that quality is important.

B. Introduce a peer review process that is mandatory before a document can be officially made final.

C. Introduce a peer review and presentation process that includes a review board with representation from relevant disciplines.

D. Ensure that appropriate representation from each relevant discipline approves of the solution documents before official approval.

Correct Answer: C

QUESTION 2

An administrator believes that the web servers are being flooded with excessive traffic from time to time. The administrator suspects that these traffic floods correspond to when a competitor makes major announcements. Which of the following should the administrator do to prove this theory?

A. Implement data analytics to try and correlate the occurrence times.

B. Implement a honey pot to capture traffic during the next attack.

C. Configure the servers for high availability to handle the additional bandwidth.

D. Log all traffic coming from the competitor\\'s public IP addresses.

Correct Answer: A

There is a time aspect to the traffic flood and if you correlate the data analytics with the times that the incidents happened, you will be able to prove the theory.

QUESTION 3

An organization would like to allow employees to use their network username and password to access a third-party service. The company is using Active Directory Federated Services for their directory service. Which of the following should the company ensure is supported by the third-party? (Select TWO).

A. LDAP/S

B. SAML

C. NTLM

D. OAUTH

E. Kerberos

Correct Answer: BE

If we\\'re using Active Directory Federated Services, then we are using Active Directory Domain Services (AD DS). AD DS uses Kerberos for authentication. Active Directory Federated Services provides SAML services. AD FS is a standards-based service that allows the secure sharing of identity information between trusted business partners (known as a federation) across an extranet. When a user needs to access a Web application from one of its federation partners, the user\\'s own organization is responsible for authenticating the user and providing identity information in the form of "claims" to the partner that hosts the Web application. The hosting partner uses its trust policy to map the incoming claims to claims that are understood by its Web application, which uses the claims to make authorization decisions.

QUESTION 4

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 5

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.