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.pass2lead.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 Chief Executive Officer (CEO) has asked a security project manager to provide recommendations on the breakout of tasks for the development of a new product. The CEO thinks that by assigning areas of work appropriately the overall security of the product will be increased, because staff will focus on their areas of expertise. Given the below groups and tasks select the BEST list of assignments.

Groups: Networks, Development, Project Management, Security, Systems Engineering, Testing

Tasks: Decomposing requirements, Secure coding standards, Code stability, Functional validation, Stakeholder engagement, Secure transport

A. Systems Engineering: Decomposing requirements Development: Secure coding standards Testing: Code stability Project Management: Stakeholder engagement Security: Secure transport Networks: Functional validation

B. Systems Engineering: Decomposing requirements Development: Code stability Testing: Functional validation Project Management: Stakeholder engagement Security: Secure coding standards Networks: Secure transport

C. Systems Engineering: Functional validation Development: Stakeholder engagement Testing: Code stability Project Management: Decomposing requirements Security: Secure coding standards Networks: Secure transport

D. Systems Engineering: Decomposing requirements Development: Stakeholder engagement Testing: Code stability Project Management: Functional validation Security: Secure coding standards Networks: Secure transport

Correct Answer: B

QUESTION 2

Company XYZ has purchased and is now deploying a new HTML5 application. The company wants to hire a penetration tester to evaluate the security of the client and server components of the proprietary web application before launch. Which of the following is the penetration tester MOST likely to use while performing black box testing of the security of the company\\'s purchased application? (Select TWO).

A. Code review

B. Sandbox

C. Local proxy

D. Fuzzer

E. Port scanner

Correct Answer: CD

C: Local proxy will work by proxying traffic between the web client and the web server. This is a tool that can be put to good effect in this case.

D: Fuzzing is another form of blackbox testing and works by feeding a program multiple input iterations that are specially written to trigger an internal error that might indicate a bug and crash it.

QUESTION 3

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 4

A company has issued a new mobile device policy permitting BYOD and company-issued devices. The company-issued device has a managed middleware client that restricts the applications allowed on company devices and provides those that are approved. The middleware client provides configuration standardization for both company owned and BYOD to secure data and communication to the device according to industry best practices. The policy states that, "BYOD clients must meet the company\\'s infrastructure requirements to permit a connection." The company also issues a memorandum separate from the policy, which provides instructions for the purchase, installation, and use of the middleware client on BYOD. Which of the following is being described?

A. Asset management

B. IT governance

C. Change management

D. Transference of risk

Correct Answer: B

It governance is aimed at managing information security risks. It entails educating users about risk and implementing policies and procedures to reduce risk.

QUESTION 5

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.