RC0-C02$^{Q\&As}$

CompTIA Advanced Security Practitioner (CASP) Recertification Exam for Continuing Education

QUESTION 1

A small customer focused bank with implemented least privilege principles, is concerned about the possibility of branch staff unintentionally aiding fraud in their day to day interactions with customers. Bank staff has been encouraged to build friendships with customers to make the banking experience feel more personal. The security and risk team have decided that a policy needs to be implemented across all branches to address the risk. Which of the following BEST addresses the security and risk team\\'s concerns?

A. Information disclosure policy

B. Awareness training

C. Job rotation

D. Separation of duties

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 security policy states that all applications on the network must have a password length of eight characters. There are three legacy applications on the network that cannot meet this policy. One system will be upgraded in six months, and two are not expected to be upgraded or removed from the network. Which of the following processes should be followed?

A. Establish a risk matrix

B. Inherit the risk for six months

C. Provide a business justification to avoid the risk

D. Provide a business justification for a risk exception

Correct Answer: D

The Exception Request must include:

A description of the non-compliance.

The anticipated length of non-compliance (2-year maximum). The proposed assessment of risk associated with non-compliance. The proposed plan for managing the risk associated with non-compliance. The proposed metrics for evaluating

the success of risk management (if risk is significant). The proposed review date to evaluate progress toward compliance. An endorsement of the request by the appropriate Information Trustee (VP or Dean).

QUESTION 4

A company provides on-demand virtual computing for a sensitive project. The company implements a fully virtualized datacenter and terminal server access with two-factor authentication for access to sensitive data. The security administrator at the company has uncovered a breach in data confidentiality. Sensitive data was found on a hidden directory within the hypervisor. Which of the following has MOST likely occurred?

A. A stolen two factor token and a memory mapping RAM exploit were used to move data from one virtual guest to an unauthorized similar token.

B. An employee with administrative access to the virtual guests was able to dump the guest memory onto their mapped disk.

C. A host server was left un-patched and an attacker was able to use a VMEscape attack to gain unauthorized access.

D. A virtual guest was left un-patched and an attacker was able to use a privilege escalation attack to gain unauthorized access.

Correct Answer: C

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.