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

An analyst connects to a company web conference hosted on www.webconference.com/meetingID#01234 and observes that numerous guests have been allowed to join, without providing identifying information. The topics covered during the web conference are considered proprietary to the company. Which of the following security concerns does the analyst present to management?

A. Guest users could present a risk to the integrity of the company\\'s information.

B. Authenticated users could sponsor guest access that was previously approved by management.

C. Unauthenticated users could present a risk to the confidentiality of the company\\'s information.

D. Meeting owners could sponsor guest access if they have passed a background check.

Correct Answer: C

The issue at stake in this question is confidentiality of information. Topics covered during the web conference are considered proprietary and should remain confidential, which means it should not be shared with unauthorized users.

QUESTION 2

An industry organization has implemented a system to allow trusted authentication between all of its partners. The system consists of a web of trusted RADIUS servers communicating over the Internet. An attacker was able to set up a malicious server and conduct a successful man-in-the-middle attack. Which of the following controls should be implemented to mitigate the attack in the future?

A. Use PAP for secondary authentication on each RADIUS server

B. Disable unused EAP methods on each RADIUS server

C. Enforce TLS connections between RADIUS servers

D. Use a shared secret for each pair of RADIUS servers

Correct Answer: C

A man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. One example is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. As an attack that aims at circumventing mutual authentication, or lack thereof, a man-in- the-middle attack can succeed only when the attacker can impersonate each endpoint to their satisfaction as expected from the legitimate other end. Most cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks. For example, TLS can authenticate one or both parties using a mutually trusted certification authority. Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

QUESTION 3

An extensible commercial software system was upgraded to the next minor release version to patch a security vulnerability. After the upgrade, an unauthorized intrusion into the system was detected. The software vendor is called in to troubleshoot the issue and reports that all core components were updated properly. Which of the following has been overlooked in securing the system? (Select TWO).

A. The company\\'s IDS signatures were not updated.

B. The company\\'s custom code was not patched.

C. The patch caused the system to revert to http.

D. The software patch was not cryptographically signed.

E. The wrong version of the patch was used.

F. Third-party plug-ins were not patched.

Correct Answer: BF

In this question, we have an extensible commercial software system. Extensibility is a software design principle defined as a system\\'s ability to have new functionality extended, in which the system\\'s internal structure and data flow are

minimally or not affected, particularly that recompiling or changing the original source code is unnecessary when changing a system\\'s behavior, either by the creator or other programmers.

Extensible systems are typically modified either by custom code or third party plugins. In this question, the core application was updated/patched. However, the custom code and third-party plugins were not patched. Therefore, a security

vulnerability remained with was exploited.

QUESTION 4

The network administrator at an enterprise reported a large data leak. One compromised server was used to aggregate data from several critical application servers and send it out to the Internet using HTTPS. Upon investigation, there have been no user logins over the previous week and the endpoint protection software is not reporting any issues. Which of the following BEST provides insight into where the compromised server collected the information?

A. Review the flow data against each server\\'s baseline communications profile.

B. Configure the server logs to collect unusual activity including failed logins and restarted services.

C. Correlate data loss prevention logs for anomalous communications from the server.

D. Setup a packet capture on the firewall to collect all of the server communications.

Correct Answer: A

Network logging tools such as Syslog, DNS, NetFlow, behavior analytics, IP reputation, honeypots, and DLP solutions provide visibility into the entire infrastructure. This visibility is important because signature-based systems are no longer sufficient for identifying the advanced attacker that relies heavily on custom malware and zero-day exploits. Having knowledge of each host\\'s communications, protocols, and traffic volumes as well as the content of the data in question is key to identifying zero-day and APT (advance persistent threat) malware and agents. Data intelligence allows forensic analysis to identify anomalous or suspicious communications by comparing suspected traffic patterns against normal data communication behavioral baselines. Automated network intelligence and next-generation live forensics provide

insight into network events and rely on analytical decisions based on known vs. unknown behavior taking place within a corporate network.

QUESTION 5

A large corporation which is heavily reliant on IT platforms and systems is in financial difficulty and needs to drastically reduce costs in the short term to survive. The Chief Financial Officer (CFO) has mandated that all IT and architectural functions will be outsourced and a mixture of providers will be selected. One provider will manage the desktops for five years, another provider will manage the network for ten years, another provider will be responsible for security for four years, and an offshore provider will perform day to day business processing functions for two years. At the end of each contract the incumbent may be renewed or a new provider may be selected. Which of the following are the MOST likely risk implications of the CFO\\'s business decision?

A. Strategic architecture will be adversely impacted through the segregation of duties between the providers. Vendor management costs will remain unchanged. The risk position of the organization will decline as specialists now maintain the environment. The implementation of security controls and security updates will improve. Internal knowledge of IT systems will improve as providers maintain system documentation.

B. Strategic architecture will improve as more time can be dedicated to strategy. System stability will improve as providers use specialists and tested processes to maintain systems. Vendor management costs will increase and the organization\\'s flexibility to react to new market conditions will be reduced slightly. Internal knowledge of IT systems will improve as providers maintain system documentation. The risk position of the organization will remain unchanged.

C. Strategic architecture will not be impacted in the short term, but will be adversely impacted in the long term through the segregation of duties between the providers. Vendor management costs will stay the same and the organization\\'s flexibility to react to new market conditions will be improved through best of breed technology implementations. Internal knowledge of IT systems will decline over time. The implementation of security controls and security updates will not change.

D. Strategic architecture will be adversely impacted through the segregation of duties between the providers. Vendor management costs will increase and the organization\\'s flexibility to react to new market conditions will be reduced. Internal knowledge of IT systems will decline and decrease future platform development. The implementation of security controls and security updates will take longer as responsibility crosses multiple boundaries.

Correct Answer: D