CAS-001 Q&As

CompTIA Advanced Security Practitioner

Pass CompTIA CAS-001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/CAS-001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

An organization has had six security incidents over the past year against their main web application. Each time the organization was able to determine the cause of the incident and restore operations within a few hours to a few days. Which of the following provides the MOST comprehensive method for reducing the time to recover?

A. Create security metrics that provide information on response times and requirements to determine the best place to focus time and money.

B. Conduct a loss analysis to determine which systems to focus time and money towards increasing security.

C. Implement a knowledge management process accessible to the help desk and finance departments to estimate cost and prioritize remediation.

D. Develop an incident response team, require training for incident remediation, and provide incident reporting and tracking metrics.

Correct Answer: D

QUESTION 2

A security administrator is conducting network forensic analysis of a recent defacement of the company\\'s secure web payment server (HTTPS). The server was compromised around the New Year\\'s holiday when all the company employees were off. The company\\'s network diagram is summarized below:

Internet

Gateway Firewall

IDS

Web SSL Accelerator

Web Server Farm

Internal Firewall

Company Internal Network

The security administrator discovers that all the local web server logs have been deleted. Additionally, the Internal Firewall logs are intact but show no activity from the internal network to the web server farm during the holiday.

Which of the following is true?

A. The security administrator should review the IDS logs to determine the source of the attack and the attack vector used to compromise the web server.

B. The security administrator must correlate the external firewall logs with the intrusion detection system logs to determine what specific attack led to the web server compromise.

C. The security administrator must reconfigure the network and place the IDS between the SSL accelerator and the

server farm to be able to determine the cause of future attacks.

D. The security administrator must correlate logs from all the devices in the network diagram to determine what specific attack led to the web server compromise.

Correct Answer: C

QUESTION 3

The VoIP administrator starts receiving reports that users are having problems placing phone calls. The VoIP administrator cannot determine the issue, and asks the security administrator for help. The security administrator reviews the switch interfaces and does not see an excessive amount of network traffic on the voice network. Using a protocol analyzer, the security administrator does see an excessive number of SIP INVITE packets destined for the SIP proxy.

Based on the information given, which of the following types of attacks is underway and how can it be remediated?

A. Man in the middle attack; install an IPS in front of SIP proxy.

B. Man in the middle attack; use 802.1x to secure voice VLAN.

C. Denial of Service; switch to more secure H.323 protocol.

D. Denial of Service; use rate limiting to limit traffic.

Correct Answer: D

QUESTION 4

Which of the following implementations of a continuous monitoring risk mitigation strategy is correct?

A. Audit successful and failed events, transfer logs to a centralized server, institute computer assisted audit reduction, and email alerts to NOC staff hourly.

B. Audit successful and critical failed events, transfer logs to a centralized server once a month, tailor logged event thresholds to meet organization goals, and display alerts in real time when thresholds are approached.

C. Audit successful and failed events, transfer logs to a centralized server, institute computer assisted audit reduction, tailor logged event thresholds to meet organization goals, and display alerts in real time when thresholds are exceeded.

D. Audit failed events only, transfer logs to a centralized server, implement manual audit reduction, tailor logged event thresholds to meet organization goals, and display alerts in real time when thresholds are approached and exceeded.

Correct Answer: C

QUESTION 5

A company has purchased a new system, but security personnel are spending a great deal of time on system maintenance. A new third party vendor has been selected to maintain and manage the company\\'s system.

Which of the following document types would need to be created before any work is performed?

A. IOS

B. ISA

C. SLA

D. OLA

Correct Answer: C