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.lead4pass.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

The Chief Executive Officer (CEO) of a corporation purchased the latest mobile device and connected it to the internal network. The CEO proceeded to download sensitive financial documents through their email. The device was then lost in transit to a conference. The CEO notified the company helpdesk about the lost device and another one was shipped out, after which the helpdesk ticket was closed stating the issue was resolved.

This data breach was not properly reported due to insufficient training surrounding which of the following processes?

A. E-Discovery

B. Data handling

C. Incident response

D. Data recovery and storage

Correct Answer: C

QUESTION 2

An internal employee has sold a copy of the production customer database that was being used for upgrade testing to outside parties via HTTP file upload. The Chief Information Officer (CIO) has resigned and the Chief Executive Officer (CEO) has tasked the incoming CIO with putting effective controls in place to help prevent this from occurring again in the future.

Which of the following controls is the MOST effective in preventing this threat from re-occurring?

A. Network-based intrusion prevention system

B. Data loss prevention

C. Host-based intrusion detection system

D. Web application firewall

Correct Answer: B

QUESTION 3

A security analyst at Company A has been trying to convince the Information Security Officer (ISO) to allocate budget towards the purchase of a new intrusion prevention system (IPS) capable of analyzing encrypted web transactions.

Which of the following should the analyst provide to the ISO to support the request? (Select TWO).

A. Emerging threat reports

B. Company attack tends

C. Request for Quote (RFQ)

D. Best practices

E. New technologies report

Correct Answer: AB

QUESTION 4

A company has a single subnet in a small office. The administrator wants to limit non-web related traffic to the corporate intranet server as well as prevent abnormal HTTP requests and HTTP protocol anomalies from causing problems with the web server.

Which of the following is the MOST likely solution?

A. Application firewall and NIPS

B. Edge firewall and HIDS

C. ACLs and anti-virus

D. Host firewall and WAF

Correct Answer: D

QUESTION 5

A security administrator is shown the following log excerpt from a Unix system:

2013 Oct 10 07:14:57 web14 sshd[1632]: Failed password for root from 198.51.100.23 port 37914 ssh2 2013 Oct 10 07:14:57 web14 sshd[1635]: Failed password for root from 198.51.100.23 port 37915 ssh2 2013 Oct 10 07:14:58 web14 sshd[1638]: Failed password for root from 198.51.100.23 port 37916 ssh2 2013 Oct 10 07:15:59 web14 sshd[1640]: Failed password for root from 198.51.100.23 port 37918 ssh2 2013 Oct 10 07:16:00 web14 sshd[1641]: Failed password for root from 198.51.100.23 port 37920 ssh2 2013 Oct 10 07:16:00 web14 sshd[1642]: Successful login for root from 198.51.100.23 port 37924 ssh2

Which of the following is the MOST likely explanation of what is occurring and the BEST immediate response? (Select TWO).

A. An authorized administrator has logged into the root account remotely.

B. The administrator should disable remote root logins.

C. Isolate the system immediately and begin forensic analysis on the host.

D. A remote attacker has compromised the root account using a buffer overflow in sshd.

E. A remote attacker has guessed the root password using a dictionary attack.

F. Use iptables to immediately DROP connections from the IP 198.51.100.23.

G. A remote attacker has compromised the private key of the root account.

H. Change the root password immediately to a password not found in a dictionary.

Correct Answer: CE