



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.pass4lead.com/CAS-001.html>

100% Passing Guarantee
100% Money Back Assurance

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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

A forensic analyst receives a hard drive containing malware quarantined by the antivirus application.

After creating an image and determining the directory location of the malware file, which of the following helps to determine when the system became infected?

- A. The malware file's modify, access, change time properties.
- B. The timeline analysis of the file system.
- C. The time stamp of the malware in the swap file.
- D. The date/time stamp of the malware detection in the antivirus logs.

Correct Answer: B

QUESTION 2

A small bank is introducing online banking to its customers through its new secured website. The firewall has three interfaces: one for the Internet connection, another for the DMZ, and the other for the internal network. Which of the following will provide the MOST protection from all likely attacks on the bank?

- A. Implement NIPS inline between the web server and the firewall.
- B. Implement a web application firewall inline between the web server and the firewall.
- C. Implement host intrusion prevention on all machines at the bank.
- D. Configure the firewall policy to only allow communication with the web server using SSL.

Correct Answer: C

QUESTION 3

A startup company offering software on demand has hired a security consultant to provide expertise on data security. The company's clients are concerned about data confidentiality. The security consultant must design an environment with data confidentiality as the top priority, over availability and integrity.

Which of the following designs is BEST suited for this purpose?

- A. All of the company servers are virtualized in a highly available environment sharing common hardware and redundant virtual storage. Clients use terminal service access to the shared environment to access the virtualized applications. A secret key kept by the startup encrypts the application virtual memory and data store.
- B. All of the company servers are virtualized in a highly available environment sharing common hardware and redundant virtual storage. Clients use terminal service access to the shared environment and to access the virtualized applications.



Each client has a common shared key, which encrypts the application virtual memory and data store.

C. Each client is assigned a set of virtual hosts running shared hardware. Physical storage is partitioned into LUNS and assigned to each client. MPLS technology is used to segment and encrypt each of the client's networks. PKI based remote desktop with hardware tokens is used by the client to connect to the application.

D. Each client is assigned a set of virtual hosts running shared hardware. Virtual storage is partitioned and assigned to each client. VLAN technology is used to segment each of the client's networks. PKI based remote desktop access is used by the client to connect to the application.

Correct Answer: C

QUESTION 4

The Chief Information Officer (CIO) of Company XYZ has returned from a large IT conference where one of the topics was defending against zero day attacks - specifically deploying third party patches to vulnerable software. Two months prior, the majority of the company systems were compromised because of a zero day exploit. Due to budget constraints the company only has operational systems. The CIO wants the Security Manager to research the use of these patches.

Which of the following is the GREATEST concern with the use of a third party patch to mitigate another un-patched vulnerability?

A. The company does not have an adequate test environment to validate the impact of the third party patch, introducing unknown risks.

B. The third party patch may introduce additional unforeseen risks and void the software licenses for the patched applications.

C. The company's patch management solution only supports patches and updates released directly by the vendor.

D. Another period of vulnerability will be introduced because of the need to remove the third party patch prior to installing any vendor patch.

Correct Answer: A

QUESTION 5

A company has decided to move to an agile software development methodology. The company gives all of its developers security training. After a year of agile, a management review finds that the number of items on a vulnerability scan has actually increased since the methodology change.

Which of the following best practices has MOST likely been overlooked in the agile implementation?

A. Penetration tests should be performed after each sprint.

B. A security engineer should be paired with a developer during each cycle.

C. The security requirements should be introduced during the implementation phase.



D. The security requirements definition phase should be added to each sprint.

Correct Answer: D

[CAS-001 VCE Dumps](#)

[CAS-001 Practice Test](#)

[CAS-001 Braindumps](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.pass4lead.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



| | | |
|---|---|--|
|  <p>One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p> |  <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p> |  <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p> |
|---|---|--|

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © pass4lead, All Rights Reserved.