



CS0-001^{Q&As}

CompTIA Cybersecurity Analyst

Pass CompTIA CS0-001 Exam with 100% Guarantee

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

<https://www.pass4itsure.com/cs0-001.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**

An organization is attempting to harden its web servers and reduce the information that might be disclosed by potential attackers. A security analyst is reviewing vulnerability scan results from a recent web server scan.

Portions of the scan results are shown below:

Finding#5144322

First Time Detected 10 Nov 2015 09:00 GMT-0600

Last Time Detected 10 Nov 2015 09:00 GMT-0600

CVSS Base: 5

Access Path: <https://myOrg.com/maillingList.htm>

Request: <https://myOrg.com/maillingList.aspx?content=volunteer>

Reponse: C:\Documents\MarySmith\maillingList.pdf

Which of the following lines indicates information disclosure about the host that needs to be remediated?

- A. Response: :Documents\MarySmith\maillingList.pdf
- B. Finding#5144322
- C. First Time Detected 10 Nov 2015 09:00 GMT-0600
- D. Access Path: <http://myOrg.com/maillingList.htm>
- E. Request: GET <http://myOrg.com/maillingList.aspx?content=volunteer>

Correct Answer: A

QUESTION 2

A security analyst is reviewing output from a CVE-based vulnerability scanner. Before conducting the scan, the analyst was careful to select only Windows-based servers in a specific datacenter. The scan revealed that the datacenter includes 27 machines running Windows 2003 Server Edition (Win2003SE). In 2015, there were 36 new vulnerabilities discovered in the Win2003SE environment. Which of the following statements are MOST likely applicable? (Choose two.)

- A. Remediation is likely to require some form of compensating control.
- B. Microsoft's published schedule for updates and patches for Win2003SE have continued uninterrupted.
- C. Third-party vendors have addressed all of the necessary updates and patches required by Win2003SE.
- D. The resulting report on the vulnerability scan should include some reference that the scan of the datacenter included 27 Win2003SE machines that should be scheduled for replacement and deactivation.
- E. Remediation of all Win2003SE machines requires changes to configuration settings and compensating controls to be



made through Microsoft Security Center\\s Win2003SE Advanced Configuration Toolkit.

Correct Answer: DE

QUESTION 3

A security analyst has created an image of a drive from an incident. Which of the following describes what the analyst should do NEXT?

- A. The analyst should create a backup of the drive and then hash the drive.
- B. The analyst should begin analyzing the image and begin to report findings.
- C. The analyst should create a hash of the image and compare it to the original drive\\s hash.
- D. The analyst should create a chain of custody document and notify stakeholders.

Correct Answer: C

QUESTION 4

A security analyst notices PII has been copied from the customer database to an anonymous FTP server in the DMZ. Firewall logs indicate the customer database has not been accessed from anonymous FTP server. Which of the following departments should make a decision about pursuing further investigation? (Choose two.)

- A. Human resources
- B. Public relations
- C. Legal
- D. Executive management
- E. IT management

Correct Answer: D

QUESTION 5

During a quarterly review of user accounts and activity, a security analyst noticed that after a password reset the head of human resources has been logging in from multiple external locations, including several overseas. Further review of the account showed access rights to a number of corporate applications, including a sensitive accounting application used for employee bonuses. Which of the following security methods could be used to mitigate this risk?

- A. RADIUS identity management
- B. Context-based authentication
- C. Privilege escalation restrictions



D. Elimination of self-service password resets

Correct Answer: B

[Latest CS0-001 Dumps](#)

[CS0-001 PDF Dumps](#)

[CS0-001 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

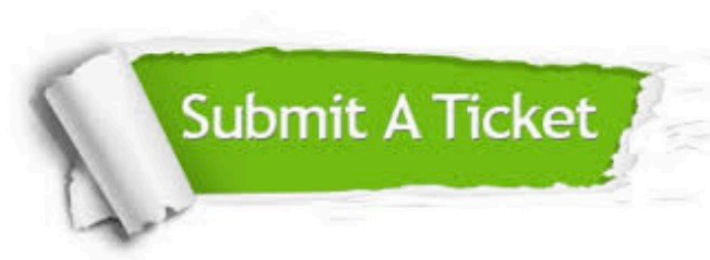
We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.pass4itsure.com/allproducts>

Need Help

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

To update a previously submitted ticket:



| | | |
|---|---|--|
|  One Year Free Update <p>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> |  Money Back Guarantee <p>To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p> |  Security & Privacy <p>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 © pass4itsure, All Rights Reserved.