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.geekcert.com/cs0-001.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An investigation showed a worm was introduced from an engineer\\'s laptop. It was determined the company does not provide engineers with company-owned laptops, which would be subject to company policy and technical controls.

Which of the following would be the MOST secure control implement?

A. Deploy HIDS on all engineer-provided laptops, and put a new router in the management network.

B. Implement role-based group policies on the management network for client access.

C. Utilize a jump box that is only allowed to connect to clients from the management network.

D. Deploy a company-wide approved engineering workstation for management access.

Correct Answer: D

QUESTION 2

An organization has had problems with security teams remediating vulnerabilities that are either false positives or are not applicable to the organization\\'s servers. Management has put emphasis on security teams conducting detailed analysis and investigation before conducting any remediation.

The output from a recent Apache web server scan is shown below:

```
- - -
Scan Host: 192.168.1.18
15-Jan-16 10:12:10.1 PDT

Vulnerability CVE-2006-5752
Cross-site scripting (XSS) vulnerability in the mod_status
module of Apache server (httpd), when ExtendedStatus is enabled
and a public-server-status page is used, allows remote attackers
to inject arbitrary web script or HTML.

Severity: 4.3 (medium)
- - -
```


The team performs some investigation and finds this statement from Apache on 07/02/2008:

"Fixed in Apache HTTP server 2.2.6, 2.0.61, and 1.3.39"

Which of the following conditions would require the team to perform remediation on this finding?

A. The organization is running version 2.2.6 and has ExtendedStatus enabled

B. The organization is running version 2.0.59 is not using a public-server-status page

C. The organization is running version 1.3.39 and is using a public-server-status page

D. The organization is running version 2.0.5 and has ExtendedStatus enabled

Correct Answer: D

QUESTION 3

Which of the following is a feature of virtualization that can potentially create a single point of failure?

A. Server consolidation

B. Load balancing hypervisors

C. Faster server provisioning

D. Running multiple OS instances

Correct Answer: A

QUESTION 4

A security analyst has been asked to remediate a server vulnerability. Once the analyst has located a patch for the vulnerability, which of the following should happen NEXT?

A. Start the change control process.

B. Rescan to ensure the vulnerability still exists.

C. Implement continuous monitoring.

D. Begin the incident response process.

Correct Answer: A

QUESTION 5

A security analyst wants to confirm a finding from a penetration test report on the internal web server. To do so, the analyst logs into the web server using SSH to send the request locally. The report provides a link to https://hrserver.internal/../

../etc/passwd, and the server IP address is 10.10.10.15.

However, after several attempts, the analyst cannot get the file, despite attempting to get it using different ways, as shown below.

Request	Response
https://hrserver.internal/../../etc/passwd	Host not found
https://localhost/../../etc/passwd	File not found
https://10.10.10.15/../../etc/passwd	File not found

Which of the following would explain this problem? (Choose two.)

A. The web server uses SNI to check for a domain name

B. Requests can only be sent remotely to the web server

C. The password file is write protected

D. The web service has not started

Correct Answer: A