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

QUESTION 1

A staff member reported that a laptop has degraded performance. The security analyst has investigated the issue and discovered that CPU utilization, memory utilization, and outbound network traffic are consuming the laptop\\'s resources. Which of the following is the BEST course of actions to resolve the problem?

A. Identify and remove malicious processes.

B. Disable scheduled tasks.

C. Suspend virus scan.

D. Increase laptop memory.

E. Ensure the laptop OS is properly patched.

Correct Answer: A

QUESTION 2

Which of the following could be directly impacted by an unpatched vulnerability in vSphere ESXi?

A. The organization\\'s physical routers

B. The organization\\'s mobile devices

C. The organization\\'s virtual infrastructure

D. The organization\\'s VPN

Correct Answer: C

QUESTION 3

A security analyst is making recommendations for securing access to the new forensic workstation and workspace. Which of the following security measures should the analyst recommend to protect access to forensic data?

A. Multifactor authentication Polarized lens protection Physical workspace isolation

B. Secure ID token Security reviews of the system at least yearly Polarized lens protection

C. Bright lightning in all access areas Security reviews of the system at least yearly Multifactor authentication

D. Two-factor authentication into the building Separation of duties Warning signs placed in clear view

Correct Answer: A

QUESTION 4

A system\\'s authority to operate (ATO) is set to expire in four days. Because of other activities and limited staffing, the organization has neglected to start reauthentication activities until now. The cybersecurity group just performed a vulnerability scan with the partial set of results shown below:

```
-----
Scan Host: 192.168.1.13
15-Jan-16 08:12:10.1 EDT

Vulnerability CVE-2015-1635
HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8,
Windows 8.1 and Windows Server 2012 allows remote attackers to execute
arbitrary code via crafted HTTP requests, aka "HTTP.sys remote code execution
vulnerability"

Severity: 10.0 (high)

Expected Result: enforceHTTPValidation='enabled';
Current Value: enforceHTTPValidation=enabled;

Evidence:
C:\%system%\Windows\config\web.config
-----
```


Based on the scenario and the output from the vulnerability scan, which of the following should the security team do with this finding?

A. Remediate by going to the web config file, searching for the enforce HTTP validation setting, and manually updating to the correct setting.

B. Accept this risk for now because this is a "high" severity, but testing will require more than the four days available, and the system ATO needs to be competed.

C. Ignore it. This is false positive, and the organization needs to focus its efforts on other findings.

D. Ensure HTTP validation is enabled by rebooting the server.

Correct Answer: A

QUESTION 5

Which of the following describes why it is important for an organization\\'s incident response team and legal department to meet and discuss communication processes during the incident response process?

A. To comply with existing organization policies and procedures on interacting with internal and external parties

B. To ensure all parties know their roles and effective lines of communication are established

C. To identify which group will communicate details to law enforcement in the event of a security incident

D. To predetermine what details should or should not be shared with internal or external parties in the event of an incident

Correct Answer: A