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.pass4lead.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

During a physical penetration test at a client site, a local law enforcement officer stumbled upon the test questioned the legitimacy of the team. Which of the following information should be shown to the officer?

A. Letter of engagement

B. Scope of work

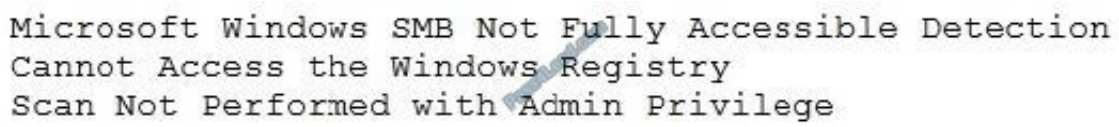
C. Timing information

D. Team reporting

Correct Answer: A

QUESTION 2

In an effort to be proactive, an analyst has run an assessment against a sample workstation before auditors visit next month. The scan results are as follows:



Based on the output of the scan, which of the following is the BEST answer?

A. Failed credentialed scan

B. Failed compliance check

C. Successful sensitivity level check

D. Failed asset inventory

Correct Answer: A

QUESTION 3

A recent audit included a vulnerability scan that found critical patches released 60 days prior were not applied to servers in the environment. The infrastructure team was able to isolate the issue and determined it was due to a service being disabled on the server running the automated patch management application. Which of the following would be the MOST efficient way to avoid similar audit findings in the future?

A. Implement a manual patch management application package to regain greater control over the process.

B. Create a patch management policy that requires all servers to be patched within 30 days of patch release.

C. Implement service monitoring to validate that tools are functioning properly.

D. Set services on the patch management server to automatically run on start-up.

Correct Answer: D

QUESTION 4

After implementing and running an automated patching tool, a security administrator ran a vulnerability scan that reported no missing patches found. Which of the following BEST describes why this tool was used?

A. To create a chain of evidence to demonstrate when the servers were patched.

B. To harden the servers against new attacks.

C. To provide validation that the remediation was active.

D. To generate log data for unreleased patches.

Correct Answer: B

QUESTION 5

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