CS0-003 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

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

https://www.passapply.com/cs0-003.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

While observing several host machines, a security analyst notices a program is overwriting data to a buffer. Which of the following controls will best mitigate this issue?

A. Data execution prevention

B. Output encoding

C. Prepared statements

D. Parameterized queries

Correct Answer: A

Data execution prevention (DEP) is a security feature that prevents code from being executed in memory regions that are marked as data-only. This helps mitigate buffer overflow attacks, which are a type of attack where a program overwrites data to a buffer beyond its allocated size, potentially allowing malicious code to be executed. DEP can be implemented at the hardware or software level and can prevent unauthorized code execution in memory buffers. CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 10; https://docs.microsoft.com/enus/windows/win32/memory/data-execution-prevention

QUESTION 2

A security analyst must preserve a system hard drive that was involved in a litigation request

Which of the following is the best method to ensure the data on the device is not modified?

A. Generate a hash value and make a backup image.

B. Encrypt the device to ensure confidentiality of the data.

C. Protect the device with a complex password.

D. Perform a memory scan dump to collect residual data.

Correct Answer: A

Generating a hash value and making a backup image is the best method to ensure the data on the device is not modified, as it creates a verifiable copy of the original data that can be used for forensic analysis. Encrypting the device, protecting it with a password, or performing a memory scan dump do not prevent the data from being altered or deleted. Verified References: CompTIA CySA+ CS0-002 Certification Study Guide, page 3291

QUESTION 3

During the forensic analysis of a compromised machine, a security analyst discovers some binaries that are exhibiting abnormal behaviors. After extracting the strings, the analyst finds unexpected content. Which of the following is the next step the analyst should take?

A. Validate the binaries\\' hashes from a trusted source.

B. Use file integrity monitoring to validate the digital signature

C. Run an antivirus against the binaries to check for malware.

D. Only allow binaries on the approve list to execute.

Correct Answer: A

" from a trusted source is the next step the analyst should take after discovering some binaries that are exhibiting abnormal behaviors and finding unexpected content in their strings. A hash is a fixed-length value that uniquely represents the contents of a file or message. By comparing the hashes of the binaries on the compromised machine with the hashes of the original or legitimate binaries from a trusted source, such as the software vendor or repository, the analyst can determine whether the binaries have been modified or replaced by malicious code. If the hashes do not match, it indicates that the binaries have been tampered with and may contain malware.

QUESTION 4

A cybersecurity analyst is tasked with scanning a web application to understand where the scan will go and whether there are URIs that should be denied access prior to more in-depth scanning. Which of following best fits the type of scanning activity requested?

A. Uncredentialed scan

B. Discovery scan

C. Vulnerability scan

D. Credentialed scan

Correct Answer: B

A discovery scan is typically used to identify the scope of a web application and understand where the scan will go. This type of scan is often the first step in assessing a web application\\'s security and helps the analyst determine which areas

should be further examined or tested in-depth.

Reference: https://qualysguard.qg2.apps.qualys.com/portal-help/en/was/scans/scanning_basics.htm

QUESTION 5

The analyst reviews the following endpoint log entry: Which of the following has occurred?

```
invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator
-ScriptBlock {HOSTName} clientcomputer1

invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator
-ScriptBlock {net user /add invoke_u1}
The command completed successfully.
```

A. Registry change

B. Rename computer

C. New account introduced

D. Privilege escalation

Correct Answer: C

The endpoint log entry shows that a new account named “admin” has been created on a Windows system with a local group membership of “Administrators”.

This indicates that a new account has been introduced on the system with administrative privileges. This could be a sign of malicious activity, such as privilege escalation or backdoor creation, by an attacker who has compromised the system.