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.leads4pass.com/cs0-003.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 analyst is conducting routine vulnerability assessments on the company infrastructure. When performing these scans, a business-critical server crashes, and the cause is traced back to the vulnerability scanner. Which of the following is the cause of this issue?

A. The scanner is running without an agent installed.

B. The scanner is running in active mode.

C. The scanner is segmented improperly

D. The scanner is configured with a scanning window

Correct Answer: B

These scans can sometimes overload or disrupt target systems, especially if they are not configured or managed properly. In some cases, active scans can trigger vulnerabilities or cause service disruptions, leading to unexpected issues like a server crash.

QUESTION 2

While reviewing a vulnerability assessment, an analyst notices the following issue is identified in the report:

```
The following certificates are part of the certificate chain but
using insecure signature algorithms:
Subject: CN=10.200.20.1,OU=HTTPS Management Certificate for SonicWALL (self-
-signed),O=HTTPS Management Certificate for SonicWALL (self-signed),
L=Sunnyvale,ST=Califor
nia,C=US
Signature Algorithm: sha1WithRSAEncryption
```

To address this finding, which of the following would be most appropriate for the analyst to recommend to the network engineer?

A. Reconfigure the device to support only connections leveraging TLSv1.2.

B. Obtain a new self-signed certificate and select AES as the hashing algorithm.

C. Replace the existing certificate with a certificate that uses only MDS for signing.

D. Use only signed certificates with cryptographically secure certificate sources.

Correct Answer: D

QUESTION 3

A security analyst needs to ensure that systems across the organization are protected based on the sensitivity of the content each system hosts. The analyst is working with the respective system owners to help determine the best methodology that seeks to promote confidentiality, availability, and integrity of the data being hosted. Which of the following should the security analyst perform first to categorize and prioritize the respective systems?

A. Interview the users who access these systems.

B. Scan the systems to see which vulnerabilities currently exist.

C. Configure alerts for vendor-specific zero-day exploits.

D. Determine the asset value of each system.

Correct Answer: D

Determining the asset value of each system is the best action to perform first, as it helps to categorize and prioritize the systems based on the sensitivity of the data they host. The asset value is a measure of how important a system is to the organization, in terms of its financial, operational, or reputational impact. The asset value can help the security analyst to assign a risk level and a protection level to each system, and to allocate resources accordingly. The other actions are not as effective as determining the asset value, as they do not directly address the goal of promoting confidentiality, availability, and integrity of the data. Interviewing the users who access these systems may provide some insight into how the systems are used and what data they contain, but it may not reflect the actual value or sensitivity of the data from an organizational perspective. Scanning the systems to see which vulnerabilities currently exist may help to identify and remediate some security issues, but it does not help to categorize or prioritize the systems based on their data sensitivity. Configuring alerts for vendor-specific zero-day exploits may help to detect and respond to some emerging threats, but it does not help to protect the systems based on their data sensitivity.

QUESTION 4

After completing a review of network activity, the threat hunting team discovers a device on the network that sends an outbound email via a mail client to a non-company email address daily at 10:00 p.m. Which of the following is potentially occurring?

A. Irregular peer-to-peer communication

B. Rogue device on the network

C. Abnormal OS process behavior

D. Data exfiltration

Correct Answer: D

Data exfiltration is the theft or unauthorized transfer or movement of data from a device or network. It can occur as part of an automated attack or manually, on-site or through an internet connection, and involve various methods. It can affect

personal or corporate data, such as sensitive or confidential information. Data exfiltration can be prevented or detected by using compression, encryption, authentication, authorization, and other controls

The network activity shows that a device on the network is sending an outbound email via a mail client to a non-company email address daily at 10:00 p.m. This could indicate that the device is compromised by malware or an insider threat,

and that the email is used to exfiltrate data from the network to an external party.

The email could contain attachments, links, or hidden data that contain the stolen information. The timing of the email could be designed to avoid detection by normal network monitoring or security systems.

QUESTION 5

A security analyst is trying to identify possible network addresses from different source networks belonging to the same company and region.

Which of the following shell script functions could help achieve the goal?

A. function x() { b=traceroute -m"" }

B. "u.com TXT +short }

C. function z() { c=$(geoip" }

Correct Answer: B

The shell script function that could help identify possible network addresses from different source networks belonging to the same company and region is:

"u.com TXT +short }

This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address, such as the country code, registry, or allocation date. The function then prints the IP address and the ASN information, which can help identify any network addresses that belong to the same ASN or region

CS0-003 VCE Dumps CS0-003 Exam Questions CS0-003 Braindumps