CS0-002 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-002 Exam with 100% Guarantee

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

https://www.passapply.com/cs0-002.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A security analyst has received information from a third-party intelligence-sharing resource that indicates employee accounts were breached. Which of the following is the NEXT step the analyst should take to address the issue?

A. Audit access permissions for all employees to ensure least privilege.

B. Force a password reset for the impacted employees and revoke any tokens.

C. Configure SSO to prevent passwords from going outside the local network.

D. Set up privileged access management to ensure auditing is enabled.

Correct Answer: B

QUESTION 2

A security analyst is correlating, ranking, and enriching raw data into a report that will be interpreted by humans or machines to draw conclusions and create actionable recommendations.

Which of the following steps in the intelligence cycle is the security analyst performing?

A. Analysis and production

B. Processing and exploitation

C. Dissemination and evaluation

D. Data collection

E. Planning and direction

Correct Answer: A

Analysis is a human process that turns processed information into intelligence that can inform decisions. Depending on the circumstances, the decisions might involve whether to investigate a potential threat, what actions to take immediately to block an attack, how to strengthen security controls, or how much investment in additional security resources is justified. https://www.recordedfuture.com/threat-intelligence-lifecycle- phases

QUESTION 3

Various devices are connecting and authenticating to a single evil twin within the network. Which of the following are MOST likely being targeted?

A. Mobile devices

B. All endpoints

C. VPNs

D. Network infrastructure

E. Wired SCADA devices

Correct Answer: A

Reference: http://www.corecom.com/external/livesecurity/eviltwin1.htm

QUESTION 4

While investigating reports or issues with a web server, a security analyst attempts to log in remotely and recedes the following message:

```
[root@ localhost / root]# ssh user1@ 10.254.2.20
Connection timed out.
```

The analyst accesses the server console, and the following console messages are displayed:

```
Out of memory: Kill process 3448(httpd) score 41 or sacrifice child
Killed process 3448(httpd) totle-vm:74716KB, tile-ress:1683KB
Out of memory: Kill process 3449(httpd) score 41 or sacrifice child
Killed process 3449(httpd) totle-vm:74634KB, ancn-rss:28542KB, file-ress:1357KB
Out of memory: Kill process 3452(httpd) score 41 or sacrifice child
Killed process 3452(httpd) totle-vm: 73466KB, arcn-rss: 29753KB, file-ress:1925KB
```

The analyst is also unable to log in on the console. While reviewing network captures for the server, the analyst sees many packets with the following signature:

```
10.254.2.25.6781 > 128.50.100.23.80
10.254.2.25.6782 > 128.50.100.23.80
10.254.2.25.6783 > 128.50.100.23.80
10.254.2.25.6784 > 128.50.100.23.80
```

Which of the following is the BEST step for the analyst to lake next in this situation?

A. Load the network captures into a protocol analyzer to further investigate the communication with 128.30.100.23, as this may be a botnet command server

B. After ensuring network captures from the server are saved isolate the server from the network take a memory snapshot, reboot and log in to do further analysis.

C. Corporate data is being exfilltrated from the server Reboot the server and log in to see if it contains any sensitive data.

D. Cryptomining malware is running on the server and utilizing an CPU and memory. Reboot the server and disable any cron Jobs or startup scripts that start the mining software.

Correct Answer: B

QUESTION 5

An information security analyst on a threat-hunting team is working with administrators to create a hypothesis related to an internally developed web application. The working hypothesis is as follows:

1.

Due to the nature of the industry, the application hosts sensitive data associated with many clients and is a significant target.

2.

The platform is most likely vulnerable to poor patching and inadequate server hardening, which expose vulnerable services.

3.

The application is likely to be targeted with SQL injection attacks due to the large number of reporting capabilities within the application.

As a result, the systems administrator upgrades outdated service applications and validates the endpoint configuration against an industry benchmark. The analyst suggests developers receive additional training on implementing identity and access management, and also implements a WAF to protect against SQL injection attacks. Which of the following BEST represents the technique in use?

A. Improving detection capabilities

B. Bundling critical assets

C. Profiling threat actors and activities

D. Reducing the attack surface area

Correct Answer: D

QUESTION 6

A company stores all of its data in the cloud. All company-owned laptops are currently unmanaged, and all users have administrative rights. The security team is having difficulty identifying a way to secure the environment. Which of the following would be the BEST method to protect the company\\'s data?

A. Implement UEM on an systems and deploy security software.

B. Implement DLP on all workstations and block company data from being sent outside the company

C. Implement a CASB and prevent certain types of data from being downloaded to a workstation

D. Implement centralized monitoring and logging for an company systems.

Correct Answer: C

QUESTION 7

A security analyst has just completed a vulnerability scan of servers that support a business critical application that is managed by an outside vendor. The results of the scan indicate the devices are missing critical patches. Which of the following factors can inhibit remediation of these vulnerabilities? (Choose two.)

A. Inappropriate data classifications

B. SLAs with the supporting vendor

C. Business process interruption

D. Required sandbox testing

E. Incomplete asset inventory

Correct Answer: CD

QUESTION 8

Due to new regulations, a company has decided to institute an organizational vulnerability management program and assign the function to the security team. Which of the following frameworks would BEST support the program? (Select two.)

A. COBIT

B. NIST

C. ISO 27000 series

D. ITIL

E. OWASP

Correct Answer: BD

QUESTION 9

The software development team pushed a new web application into production for the accounting department. Shortly after the application was published, the head of the accounting department informed IT operations that the application was not performing as intended. Which of the following SDLC best practices was missed?

A. Peer code reviews

B. Regression testing

C. User acceptance testing

D. Fuzzing

E. Static code analysis

Correct Answer: C

QUESTION 10

A medical organization recently started accepting payments over the phone. The manager is concerned about the impact of the storage of different types of data. Which of the following types of data incurs the highest regulatory constraints?

A. PHI

B. PCI

C. PII

D. IP

Correct Answer: B

QUESTION 11

An analyst is responding to an incident within a cloud infrastructure Based on the logs and traffic analysis, the analyst thinks a container has been compromised.

Which of the following should Ihe analyst do FIRST?

A. Perform threat hunting in other areas of the cloud infrastructure

B. Contact law enforcement to report the incident

C. Perform a root cause analysis on the container and the service logs

D. Isolate the container from production using a predefined policy template

Correct Answer: D

QUESTION 12

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 13

A security analyst who works in the SOC receives a new requirement to monitor for indicators of compromise. Which of the following is the first action the analyst should take in this situation?

A. Develop a dashboard to track the indicators of compromise.

B. Develop a query to search for the indicators of compromise.

C. Develop a new signature to alert on the indicators of compromise.

D. Develop a new signature to block the indicators of compromise.

Correct Answer: B

QUESTION 14

A company has established an ongoing vulnerability management program and procured the latest technology to support it. However, the program is failing because several vulnerabilities have not been detected. Which of the following will reduce the number of false negatives?

A. Increase scan frequency.

B. Perform credentialed scans.

C. Update the security incident response plan.

D. Reconfigure scanner to brute force mechanisms.

Correct Answer: B

QUESTION 15

During a forensic investigation, a security analyst reviews some Session Initiation Protocol packets that came from a suspicious IP address. Law enforcement requires access to a VoIP call that originated from the suspicious IP address. Which of the following should the analyst use to accomplish this task?

A. Wireshark

B. iptables

C. Tcpdump

D. Netflow

Correct Answer: A