CS0-002Q&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.pass2lead.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 was asked to join an outage call for a critical web application. The web middleware support team determined the web server is running and having no trouble processing requests; however, some investigation has revealed firewall denies to the web server that began around 1.00 a.m. that morning. An emergency change was made to enable the access, but management has asked for a root cause determination. Which of the following would be the BEST next step?

A. Install a packet analyzer near the web server to capture sample traffic to find anomalies.

B. Block all traffic to the web server with an ACL.

C. Use a port scanner to determine all listening ports on the web server.

D. Search the logging servers for any rule changes.

Correct Answer: D

QUESTION 2

The security team has determined that the current incident response resources cannot meet management\\'s objective to secure a forensic image for all serious security incidents within 24 hours. Which of the following compensating controls can be used to help meet management\\'s expectations?

A. Separation of duties

B. Scheduled reviews

C. Dual control

D. Outsourcing

Correct Answer: D

QUESTION 3

An analyst is searching a log for potential credit card leaks. The log stores all data encoded in hexadecimal. Which of the following commands will allow the security analyst to confirm the incident?

A. cat log xxd -r -p | egrep \\' [0-9] {16}

B. egrep \\'(3(0-9)) (16) \\' log

C. cat log | xxd -r -p egrep \\'(0-9) (16)\\'

D. egrep \\' (0-9) (16) \\' log | xxdc

Correct Answer: C

QUESTION 4

A cybersecurity analyst was asked to review several results of web vulnerability scan logs. Given the following snippet of code:

```
Iframe src="http://65.240.22.1" width="0" height="0" frmeborder="0"
tabindex="-1" title="empty" style=visibility:hidden;display:none
/iframe
```

Which of the following BEST describes the situation and recommendations to be made?

A. The security analyst has discovered an embedded iframe pointing to source IP 65.240.22.1 network. The code should include the domain name. Recommend the entry be updated with the domain name.

B. The security analyst has discovered an embedded iframe that is hidden from users accessing the web page. This code is correct. This is a design preference, and no vulnerabilities are present.

C. The security analyst has discovered an embedded iframe pointing to source IP 65.240.22.1 network. The link is hidden and suspicious. Recommend the entry be removed from the web page.

D. The security analyst has discovered an embedded iframe pointing to source IP 65.240.22.1 network. Recommend making the iframe visible. Fixing the code will correct the issue.

Correct Answer: B

QUESTION 5

The security operations team is conducting a mock forensics investigation. Which of the following should be the FIRST action taken after seizing a compromised workstation?

A. Activate the escalation checklist

B. Implement the incident response plan

C. Analyze the forensic image

D. Perform evidence acquisition

Correct Answer: D

Reference: https://staff.washington.edu/dittrich/misc/forensics/

QUESTION 6

A development team recently released a new version of a public-facing website for testing prior to production. The development team is soliciting the help of various teams to validate the functionality of the website due to its high visibility. Which of the following activities best describes the process the development team is initiating?

A. Static analysis

B. Stress testing

C. Code review

D. User acceptance testing

Correct Answer: D

QUESTION 7

Law enforcement has contacted a corporation\\'s legal counsel because correlated data from a breach shows the organization as the common denominator from all indicators of compromise. An employee overhears the conversation between legal counsel and law enforcement, and then posts a comment about it on social media. The media then starts contacting other employees about the breach. Which of the following steps should be taken to prevent further disclosure of information about the breach?

A. Perform security awareness training about incident communication.

B. Request all employees verbally commit to an NDA about the breach.

C. Temporarily disable employee access to social media

D. Have law enforcement meet with employees.

Correct Answer: A

QUESTION 8

In reviewing firewall logs, a security analyst has discovered the following IP address, which several employees are using frequently:

The organization\\'s servers use IP addresses in the 192.168.0.1/24 CIDR. Additionally, the analyst has noticed that corporate data is being stored at this new location. A few of these employees are on the management and executive management teams. The analyst has also discovered that there is no record of this IP address or service in reviewing the known locations of managing system assets. Which of the following is occurring in this scenario?

A. Malicious process

B. Unauthorized change

C. Data exfiltration

D. Unauthorized access

Correct Answer: C

QUESTION 9

A security professional is analyzing the results of a network utilization report. The report includes the following information:

IP Address	Server Name	Server Uptine	Historical	Current
172.20.2.58	web.srvr.03	30D 12H 52M 09S	41.3GB	37.2GB
172.20.1.215	dev.web.srvr.01	30D 12H 52M 09S	1.81GB	2.2GB
172.20.1.22	hr.dbprod.01	30D 12H 17M 22S	2.24GB	29.97GB
172.20.1.26	mrktg.file.srvr.02	30D 12H 41M 09S	1.23GB	0.34GB
172.20.1.28	accnt.file.srvr.01	30D 12H 52M 09S	3.62GB	3.57GB
172.20.1.30	R&D.file.srvr.01	1D 4H 22M 01S	1.24GB	0.764GB

Which of the following servers needs further investigation?

A. hr.dbprod.01

B. RandD.file.srvr.01

C. mrktg.file.srvr.02

D. web.srvr.03

Correct Answer: A

QUESTION 10

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 11

Which of the following BEST describes how logging and monitonng work when entering into a public cloud relationship with a service provider?

A. Logging and monitonng are not needed in a public cloud environment

B. Logging and monitonng are done by the data owners

C. Logging and monitonng duties are specified in the SLA and contract

D. Logging and monitonng are done by the service provider

Correct Answer: C

QUESTION 12

In web application scanning, static analysis refers to scanning:

A. the system for vulnerabilities before installing the application.

B. the compiled code of the application to detect possible issues.

C. an application that is installed and active on a system.

D. an application that is installed on a system that is assigned a static IP.

Correct Answer: B

This type of analysis is performed before the application is installed and active on a system, and it involves examining the code without actually executing it in order to identify potential vulnerabilities or security risks.

As per CYSA+ 002 Study Guide: Static analysis is conducted by reviewing the code for an application. Static analysis does not run the program; instead, it focuses on understanding how the program is written and what the code is intended to do.

QUESTION 13

The Chief Information Officer (CIO) of a large healthcare institution is concerned about all machines having direct access to sensitive patient information. Which of the following should the security analyst implement to BEST mitigate the risk of sensitive data exposure?

A. A cloud access service broker system

B. NAC to ensure minimum standards are met

C. MFA on all workstations

D. Network segmentation

Correct Answer: D

QUESTION 14

Which of the following can detect vulnerable third-party libraries before code deployment?

A. Impact analysis

B. Dynamic analysis

C. Static analysis

D. Protocol analysis

Correct Answer: C

QUESTION 15

An analyst is reviewing the following output:

```
if (searchname != null)
 {
  %>
     employee <%searchname%> not found
  <%
 }
```

Vulnerability found: Improper neutralization of script-related HTML tag Which of the following was most likely used to discover this?

A. Reverse engineering using a debugger

B. A static analysis vulnerability scan

C. A passive vulnerability scan

D. A database vulnerability scan

Correct Answer: D