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

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

QUESTION 1

A consumer credit card database was compromised, and multiple representatives are unable to review the appropriate customer information. Which of the following should the cybersecurity analyst do first?

A. Start the containment effort.

B. Confirm the incident.

C. Notify local law enforcement officials.

D. Inform the senior management team.

Correct Answer: B

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

As a proactive threat-hunting technique, hunters must develop situational cases based on likely attack scenarios derived from the available threat intelligence information. After forming the basis of the scenario, which of the following may the threat hunter construct to establish a framework for threat assessment?

A. Critical asset list

B. Threat vector

C. Attack profile

D. Hypothesis

Correct Answer: D

A hypothesis is a statement that can be tested by threat hunters to establish a framework for threat assessment. A hypothesis is based on situational awareness and threat intelligence information, and describes a possible attack scenario that may affect the organization. A hypothesis can help to guide threat hunters in their investigation by providing a clear and specific question to ans" there any evidence of lateral" https://www.crowdstrike.com/blog/tech-center/threat-huntinghypothesisdevelopment/

QUESTION 4

An organization is conducting a pilot deployment of an e-commerce application. The application\\'s source code is not available. Which of the following strategies should an analyst recommend to evaluate the security of the software?

A. Static testing

B. Vulnerability testing

C. Dynamic testing

D. Penetration testing

Correct Answer: D

Explanation: Penetration testing is the best strategy to evaluate the security of the software without the source code. Penetration testing is a type of security testing that simulates real-world attacks on the software to identify and exploit its vulnerabilities. Penetration testing can be performed on the software as a black box, meaning that the tester does not need to have access to the source code or the internal structure of the software. Penetration testing can help the analyst to assess the security posture of the software, the potential impact of the vulnerabilities, and the effectiveness of the existing security controls12. Static testing, vulnerability testing, and dynamic testing are other types of security testing, but they usually require access to the source code or the internal structure of the software. Static testing is the analysis of the software code or design without executing it. Vulnerability testing is the identification and evaluation of the software weaknesses or flaws. Dynamic testing is the analysis of the software code or design while executing it345. References: Penetration Testing - OWASP, What is a Penetration Test and How Does It Work?, Static Code Analysis | OWASP Foundation, Vulnerability Scanning Best Practices, Dynamic Testing - OWASP

QUESTION 5

An analyst reviews a recent government alert on new zero-day threats and finds the following CVE metrics for the most critical of the vulnerabilities:

CVSS: 3.1/AV:N/AC: L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:W/RC:R

Which of the following represents the exploit code maturity of this critical vulnerability?

A. E:U

B. S:C

C. RC:R

D. AV:N

E. AC:L

Correct Answer: A

The exploit code maturity of a vulnerability is indicated by the E metric in the CVSS temporal score. The value of U means that no exploit code is available or unknown1. The other options are not related to the exploit code maturity, but to other aspects of the vulnerability, such as attack vector, scope, availability, and complexity1.

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