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.pass4itsure.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 is the best reason why organizations need operational security controls?

A. To supplement areas that other controls cannot address

B. To limit physical access to areas that contain sensitive data

C. To assess compliance automatically against a secure baseline

D. To prevent disclosure by potential insider threats

Correct Answer: A

Operational security controls are security measures that are implemented and executed by people rather than by systems. Operational security controls are needed to supplement areas that other controls, such as technical or physical controls, cannot address. For example, operational security controls can include policies, procedures, training, awareness, audits, reviews, testing, etc. These controls can help ensure that employees follow best practices, comply with regulations, detect and report incidents, and respond to emergencies. The other options are not specific to operational security controls or are too narrow in scope. CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0002), page 14; https://www.isaca.org/resources/isacajournal/issues6/volume-3/operational-security-controls

QUESTION 2

Which of the following is the most important reason for an incident response team to develop a formal incident declaration?

A. To require that an incident be reported through the proper channels

B. To identify and document staff who have the authority to declare an incident

C. To allow for public disclosure of a security event impacting the organization

D. To establish the department that is responsible for responding to an incident

Correct Answer: B

Explanation: The formal incident declaration is crucial to identify and document the staff who have the authority to declare an incident, ensuring that incidents are handled by authorized personnel. References: CompTIA CySA+ Study Guide: S0-003, 3rd Edition, Chapter 5: Incident Response, page 197.

QUESTION 3

A risk assessment concludes that the perimeter network has the highest potential for compromise by an attacker, and it is labeled as a critical risk environment. Which of the following is a valid compensating control to reduce the volume of valuable information in the perimeter network that an attacker could gain using active reconnaissance techniques?

A. A control that demonstrates that all systems authenticate using the approved authentication method

B. A control that demonstrates that access to a system is only allowed by using SSH

C. A control that demonstrates that firewall rules are peer reviewed for accuracy and approved before deployment

D. A control that demonstrates that the network security policy is reviewed and updated yearly

Correct Answer: C

A valid compensating control to reduce the volume of valuable information in the perimeter network that an attacker could gain using active reconnaissance techniques is a control that demonstrates that firewall rules are peer reviewed for accuracy and approved before deployment. This control can help ensure that the firewall rules are configured correctly and securely, and that they do not allow unnecessary or unauthorized access to the perimeter network. The other options are not compensating controls or do not address the risk of active reconnaissance. CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 14; https://www.isaca.org/resources/isaca-journal/issues6/volume-3/ compensating-controls

QUESTION 4

An older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. Which of the following factors would an analyst most likely communicate as the reason for this escalation?

A. Scope

B. Weaponization

C. CVSS

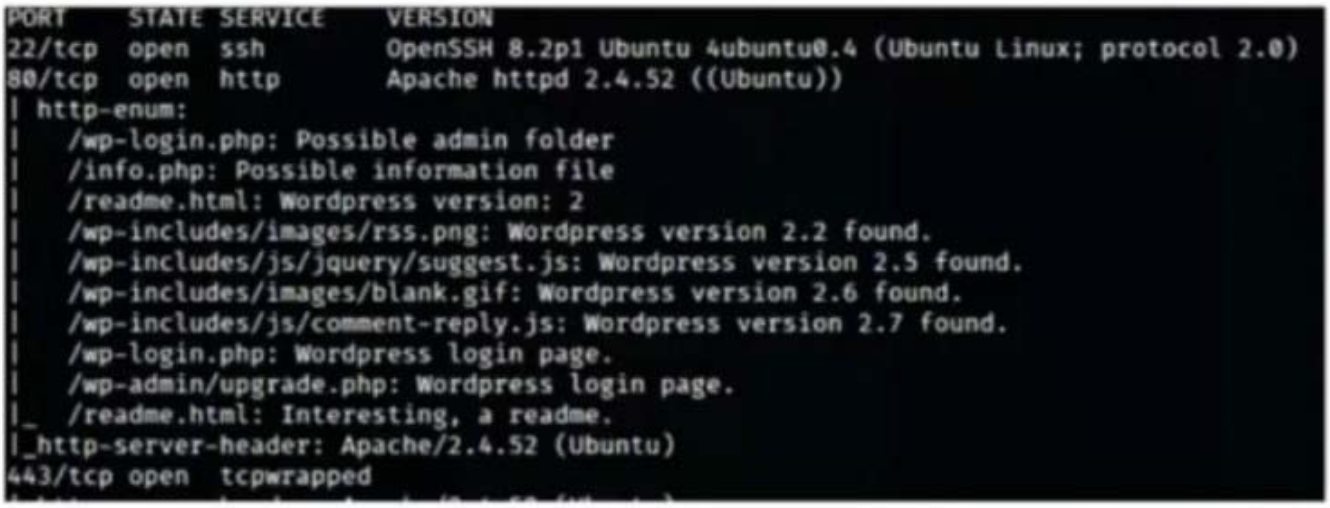
D. Asset value

Correct Answer: B

Weaponization is a factor that describes how an adversary develops or acquires an exploit or payload that can take advantage of a vulnerability and deliver a malicious effect. Weaponization can increase the severity or impact of a vulnerability, as it makes it easier or more likely for an attacker to exploit it successfully and cause damage or harm. Weaponization can also indicate the level of sophistication or motivation of an attacker, as well as the availability or popularity of an exploit or payload in the cyber threat landscape. In this case, an older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. This indicates that weaponization was the reason for this escalation.

QUESTION 5

A security analyst reviews the following extract of a vulnerability scan that was performed against the web server:



Which of the following recommendations should the security analyst provide to harden the web server?

A. Remove the version information on http-server-header.

B. Disable tcp_wrappers.

C. Delete the /wp-login.php folder.

D. Close port 22.

Correct Answer: A

Explanation: The vulnerability scan shows that the version information is visible in the http-server-header, which can be exploited by attackers to identify vulnerabilities specific to that version. Removing or obfuscating this information can enhance security. References: CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 4: Vulnerability Management, page 172; CompTIA CySA+ Study Guide: S0-003, 3rd Edition, Chapter 5: Vulnerability Management, page

223.