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

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

QUESTION 1

A security analyst discovers the company\\'s website is vulnerable to cross-site scripting. Which of the following solutions will BEST remedy the vulnerability?

A. Prepared statements

B. Server-side input validation

C. Client-side input encoding

D. Disabled JavaScript filtering

Correct Answer: B

The BEST solution to remedy the cross-site scripting vulnerability on the company\\'s website is option B, server-side input validation.

Server-side input validation involves checking user input on the server side to ensure that it meets expected criteria before it is processed or stored. This can prevent malicious code from being injected into the website and reduce the risk of cross-site scripting attacks.

QUESTION 2

A security analyst is trying to identify anomalies on the network routing. Which of the following functions can the analyst use on a shell script to achieve the objective most accurately?

A. function x() { info=$(geoiplookup $1) andand echo "$1 | $info" }

B. function x() { info=$(ping -c 1 $""o "$1 | $info" }

C. function x() { info=$(dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-a" \\').origin.asn.cymru.com TXT +short) andand echo "$1 | $info" }

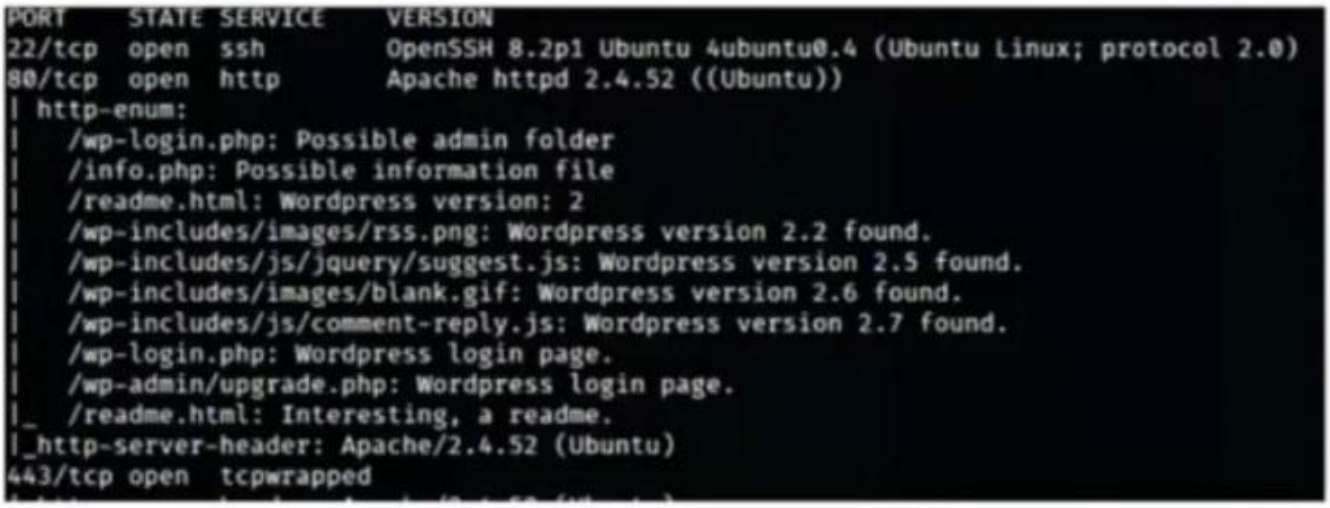
D. function x() { info=$(tracerou""$1 | $info" }

Correct Answer: C

The function that can be used on a shell script to identify anomalies on the network routing most accurately is: function x() { info=(dig(dig -x $1 | grep PTR | tail -n 1 | awk" " " } This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address. The function then prints the IP address and the ASN information, which can help identify any routing anomalies or inconsistencies

QUESTION 3

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.

QUESTION 4

An analyst is reviewing a vulnerability report and must make recommendations to the executive team. The analyst finds that most systems can be upgraded with a reboot resulting in a single downtime window. However, two of the critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. Which of the following inhibitors to remediation do these systems and associated vulnerabilities best represent?

A. Proprietary systems

B. Legacy systems

C. Unsupported operating systems

D. Lack of maintenance windows

Correct Answer: A

Proprietary systems are systems that are owned and controlled by a specific vendor or manufacturer, and that use proprietary standards or protocols that are not compatible with other systems. Proprietary systems can pose a challenge for vulnerability management, as they may not allow users to access or modify their configuration, update their software, or patch their vulnerabilities. In this case, two of the critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. This indicates that these systems and associated vulnerabilities are examples of proprietary systems as inhibitors to remediation

QUESTION 5

A SOC manager receives a phone call from an upset customer. The customer received a vulnerability report two hours ago: but the report did not have a follow-up remediation response from an analyst. Which of the following documents should the SOC manager review to ensure the team is meeting the appropriate contractual obligations for the customer?

A. SLA

B. MOU

C. NDA

D. Limitation of liability

Correct Answer: A

SLA stands for service level agreement, which is a contract or document that defines the expectations and obligations between a service provider and a customer regarding the quality, availability, performance, or scope of a service. An SLA may also specify the metrics, penalties, or remedies for measuring or ensuring compliance with the agreed service levels. An SLA can help the SOC manager review if the team is meeting the appropriate contractual obligations for the customer, such as response time, resolution time, reporting frequency, or communication channels.

CS0-003 VCE Dumps CS0-003 Study Guide CS0-003 Braindumps