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.geekcert.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

The security analyst received the monthly vulnerability report. The following findings were included in the report:

1.

Five of the systems only required a reboot to finalize the patch application

2.

Two of the servers are running outdated operating systems and cannot be patched

The analyst determines that the only way to ensure these servers cannot be compromised is to isolate them. Which of the following approaches will best minimize the risk of the outdated servers being compromised?

A. Compensating controls

B. Due diligence

C. Maintenance windows

D. Passive discovery

Correct Answer: A

Compensating controls are the best approach to minimize the risk of the outdated servers being compromised, as they can provide an alternative or additional layer of security when the primary control is not feasible or effective. Compensating controls are security measures that are implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. For example, if the servers are running outdated operating systems and cannot be patched, a compensating control could be to isolate them from the rest of the network, or to implement a firewall or an intrusion prevention system to monitor and block any malicious traffic to or from the servers. Compensating controls can help reduce the likelihood or impact of an exploit, but they do not eliminate the risk completely. Therefore, the security analyst should also consider upgrading or replacing the outdated servers as soon as possible.

QUESTION 2

An organization recently changed its BC and DR plans. Which of the following would best allow for the incident response team to test the changes without any impact to the business?

A. Perform a tabletop drill based on previously identified incident scenarios.

B. Simulate an incident by shutting down power to the primary data center.

C. Migrate active workloads from the primary data center to the secondary location.

D. Compare the current plan to lessons learned from previous incidents.

Correct Answer: A

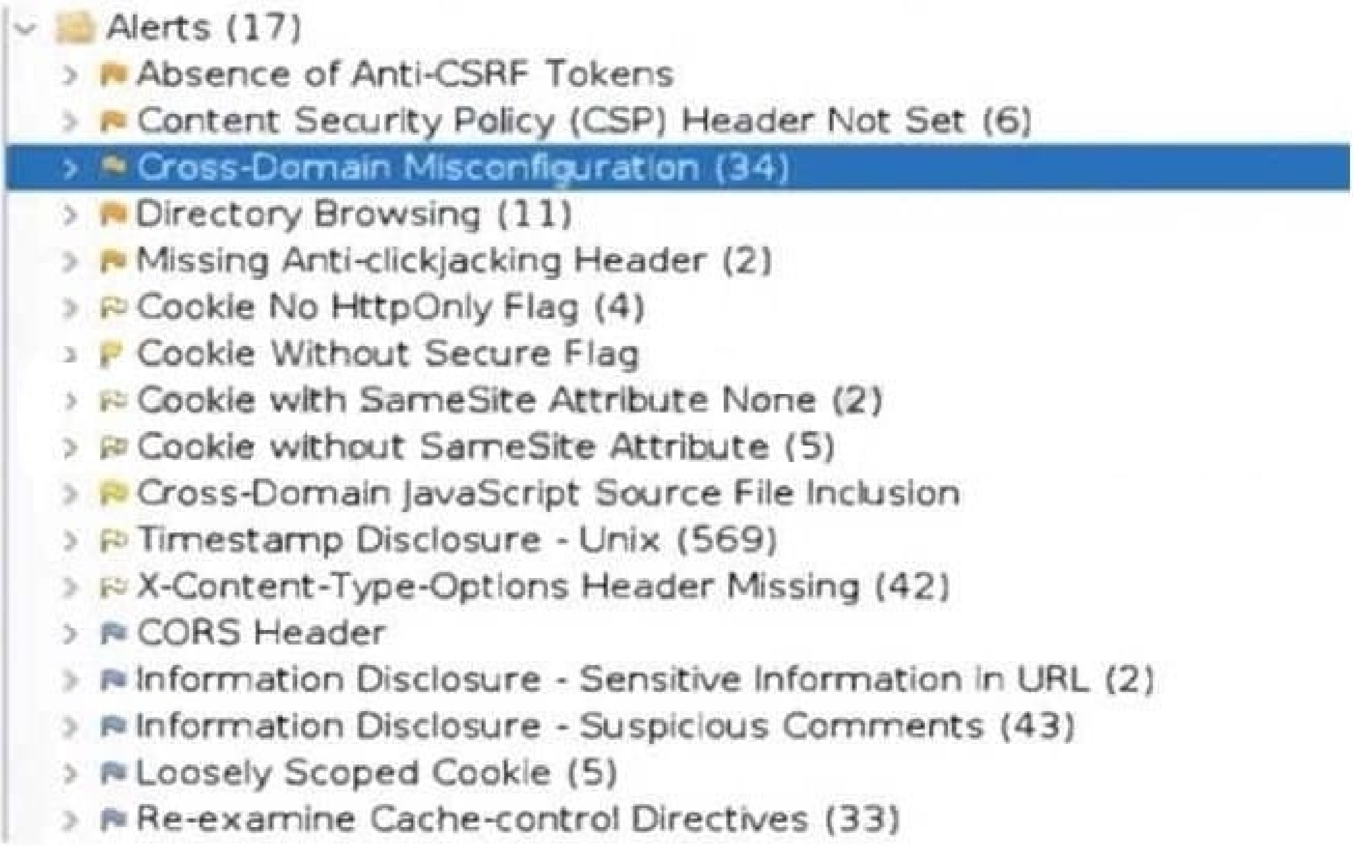
performing a tabletop drill based on previously identified incident scenarios, is the best choice to test the changes in the BC (Business Continuity) and DR (Disaster Recovery) plans without impacting the business.

A tabletop drill involves gathering key stakeholders and walking through various hypothetical scenarios and how they would be handled based on the updated plans.This approach ensures that the organization can test its preparedness without causing any actual disruption or risk to business operations.

Reference: https://www.alertmedia.com/blog/tabletop-exercises/

QUESTION 3

An organization conducted a web application vulnerability assessment against the corporate website, and the following output was observed:



Alerts (17)
- Absence of Anti-CSRF Tokens
- Content Security Policy (CSP) Header Not Set (6)
- Cross-Domain Misconfiguration (34)
- Directory Browsing (11)
- Missing Anti-clickjacking Header (2)
- Cookie No HttpOnly Flag (4)
- Cookie Without Secure Flag
- Cookie with SameSite Attribute None (2)
- Cookie without SameSite Attribute (5)
- Cross-Domain JavaScript Source File Inclusion
- Timestamp Disclosure - Unix (569)
- X-Content-Type-Options Header Missing (42)
- CORS Header
- Information Disclosure - Sensitive Information in URL (2)
- Information Disclosure - Suspicious Comments (43)
- Loosely Scoped Cookie (5)
- Re-examine Cache-control Directives (33)

Which of the following tuning recommendations should the security analyst share?

A. Set an HttpOnlvflaq to force communication by HTTPS

B. Block requests without an X-Frame-Options header

C. Configure an Access-Control-Allow-Origin header to authorized domains

D. Disable the cross-origin resource sharing header

Correct Answer: B

The output shows that the web application is vulnerable to clickjacking attacks, which allow an attacker to overlay a hidden frame on top of a legitimate page and trick users into clicking on malicious links. Blocking requests without an XFrame-Options header can prevent this attack by instructing the browser to not display the page within a frame.

QUESTION 4

A security analyst is revising a company\\'s MFA policy to prohibit the use of short message service (SMS) tokens. The Chief Information Officer has questioned this decision and asked for justification. Which of the following should the analyst provide as justification for the new policy?

A. SMS relies on untrusted, third-party carrier networks.

B. SMS tokens are limited to eight numerical characters.

C. SMS is not supported on all handheld devices in use.

D. SMS is a cleartext protocol and does not support encryption.

Correct Answer: D

QUESTION 5

Security awareness and compliance programs are most effective at reducing the likelihood and impact of attacks from:

A. advanced persistent threats.

B. corporate spies.

C. hacktivists.

D. insider threats.

Correct Answer: D