CS0-003 Reliable Exam Braindumps - CS0-003 New Dumps Questions

P.S. Free 2026 CompTIA CS0-003 dumps are available on Google Drive shared by ExamcollectionPass: https://drive.google.com/open?id=1wcWtugPrT7h_8jq5U5ZIO6B88E03v-pL

To make sure your situation of passing the certificate efficiently, our CS0-003 practice materials are compiled by first-rank experts. So the proficiency of our team is unquestionable. They help you review and stay on track without wasting your precious time on useless things. They handpicked what the CS0-003 Study Guide usually tested in exam recent years and devoted their knowledge accumulated into these CS0-003 actual tests. We are on the same team, and it is our common wish to help your realize it. So good luck!

CompTIA CySA+ certification exam focuses on the development of technical skills required to prevent, detect, and respond to cybersecurity threats. CS0-003 Exam covers a wide range of topics, including threat and vulnerability management, incident response, security operations and monitoring, and compliance and governance. CS0-003 exam requires candidates to demonstrate their knowledge of these topics through multiple-choice questions and performance-based simulations.

CompTIA CySA+ certification is ideal for cybersecurity analysts who want to advance their careers in this field. CompTIA Cybersecurity Analyst (CySA+) Certification Exam certification is recognized by many employers as a valuable qualification and can lead to better job opportunities and higher salaries. Additionally, passing the CompTIA CySA+ certification exam can also help candidates to demonstrate their expertise in this field and increase their credibility among their peers and clients.

>> CS0-003 Reliable Exam Braindumps <<

CS0-003 New Dumps Questions | CS0-003 Sample Test Online

Our CompTIA dumps files contain the latest CS0-003 practice questions with detailed answers and explanations, which written by our professional trainers and experts. And we check the updating of CS0-003 exam pdf everyday to make sure the accuracy of our questions. There are demo of CS0-003 free vce for you download in our exam page. One week preparation prior to attend exam is highly recommended.

CompTIA Cybersecurity Analyst (CySA+) Certification Exam Sample

Questions (Q102-Q107):

NEW QUESTION # 102
A code review reveals a web application is using lime-based cookies for session management.
This is a security concern because lime-based cookies are easy to:

- A. decode.
- B. guess.
- C. decrypt.
- D. parameterize.

Answer: D

NEW QUESTION # 103
A security analyst performs a vulnerability scan. Based on the metrics from the scan results, the analyst must prioritize which hosts to patch. The analyst runs the tool and receives the following output:

```
Host    CVE: (Vulnerability Name)          Metrics
----    -------------------------          ---------------
host01  CVE-2003-99992: (TransAtl)         DDS:NOA:HVT
host02  CVE-2004-99993: (TjBeP)            DDS:AEX:NOA
host03  CVE-2007-99996:
        (NarrowStairs)                     RCE:AEX:HVT
host04  CVE-2009-99998:
        (Topendoor)                        UDD:NOA

--- metrics ---
DDS: Denial of service vulnerability
RCE: Remote code execution vulnerability
UDD: Unauthorized disclosure of data vulnerability
AEX: Vulnerability is being exploited actively exploited
NOA: No authentication required
HVT: Host is a high value target
HEX: Host is externally available to public Internet
```

Which of the following hosts should be patched first, based on the metrics?

- A. host04
- B. host03
- C. host02
- D. host01

Answer: B

Explanation:
Host03 should be patched first, based on the metrics, as it has the highest risk score and the highest number of critical vulnerabilities. The risk score is calculated by multiplying the CVSS score by the exposure factor, which is the percentage of systems that are vulnerable to the exploit. Host03 has a risk score of 10 x 0.9 = 9, which is higher than any other host. Host03 also has 5 critical vulnerabilities, which are the most severe and urgent to fix, as they can allow remote code execution, privilege escalation, or data loss. The other hosts have lower risk scores and lower numbers of critical vulnerabilities, so they can be patched later.

NEW QUESTION # 104
Which of the following would an organization use to develop a business continuity plan?

- A. A diagram of all systems and interdependent applications
- B. A configuration management database in print at an off-site location
- C. A prioritized list of critical systems defined by executive leadership
- D. A repository for all the software used by the organization

Answer: C

NEW QUESTION # 105
An analyst is reviewing an SSLscan from a web server in an environment:

```
Supported Server Cipher(s):
Preferred TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve P-384 DHE 384
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits DHE-RSA-AES256-GCM-SHA384 DHE 2048 bits
Accepted TLSv1.2 128 bits DHE-RSA-AES128-GCM-SHA256 DHE 2048 bits
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve P-384 DHE 384
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve P-384 DHE 384
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA Curve 25519 DHE 253
Accepted TLSv1.2 256 bits AES256-GCM-SHA384
Accepted TLSv1.2 128 bits AES128-GCM-SHA256
Accepted TLSv1.2 256 bits AES256-SHA256
Accepted TLSv1.2 128 bits AES128-SHA256
Accepted TLSv1.2 256 bits AES256-SHA
Accepted TLSv1.2 128 bits AES128-SHA
Accepted TLSv1.2 112 bits DES-CBC3-SHA
```


The analyst needs to immediately disable ciphers that do not comply with company security standards. Which of the following ciphers is the least secure and should be disabled?

- A. 128 bits DHE-RSA-AES128-GCM-SHA256 DHE 2048 bits
- B. DES-CBC3-SHA
- C. AES256-GCM-SHA384
- D. ECDHE-RSA-AES256-GCM-SHA384 Curve P-384 DHE 384
- E. AES128-SHA
- F. ECDHE-RSA-AES128-SHA Curve 25519 DHE 253

Answer: B

Explanation:
DES-CBC3-SHA (3DES) is the least secure cipher listed. It is considered deprecated due to known vulnerabilities, limited key size (112 bits in this context), and susceptibility to attacks like SWEET32. It should be disabled immediately to comply with modern security standards.

NEW QUESTION # 106
A security analyst recently used Arachni to perform a vulnerability assessment of a newly developed web application. The analyst is concerned about the following output:
[+] XSS: In form input 'txtSearch' with action https://localhost/search.aspx
[-] XSS: Analyzing response #1...
[-] XSS: Analyzing response #2...
[-] XSS: Analyzing response #3...
[+] XSS: Response is tainted. Looking for proof of the vulnerability.
Which of the following is the most likely reason for this vulnerability?

- A. The developer did not set proper cross-site request forgery protections.
- B. The developer did not implement default protections in the web application build.
- C. The developer did not set proper cross-site scripting protections in the header.
- D. The developer set input validation protection on the specific field of search.aspx.

Answer: C

Explanation:
The most likely reason for this vulnerability is B. The developer did not set proper cross-site scripting protections in the header. Cross-site scripting (XSS) is a type of web application vulnerability that allows an attacker to inject malicious code into a web page that is viewed by other users. XSS can be used to steal cookies, session tokens, credentials, or other sensitive information, or to perform actions on behalf of the victim1.
One of the common ways to prevent XSS attacks is to set proper HTTP response headers that instruct the browser how to handle the content of the web page. For example, the Content-Type header can specify the MIME type and character encoding of the web page, which can help the browser avoid interpreting data as code. The X-XSS-Protection header can enable or disable the browser's built-in XSS filter, which can block or sanitize suspicious scripts. The Content-Security-Policy header can define a whitelist of sources and directives that control what resources and scripts can be loaded or executed on the web page2.
According to the output of Arachni, a web application security scanner framework3, it detected an XSS vulnerability in the form input 'txtSearch' with action https://localhost/search.aspx. This means that Arachni was able to inject a malicious script into the input field and observe its execution in the response. This indicates that the developer did not set proper cross-site scripting protections in the header of search.aspx, which allowed Arachni to bypass the browser's default security mechanisms and execute arbitrary code on the web page.

NEW QUESTION # 107
.....