

➤ **Vendor: CompTIA**

➤ **Exam Code: CS0-002**

➤ **Exam Name: CompTIA CSA+ Certification Exam**

➤ **New Updated Questions from [Braindump2go](#) (Updated in [July/2020](#))**

### **Visit Braindump2go and Download Full Version CS0-002 Exam Dumps**

#### **QUESTION 1**

An incident responder successfully acquired application binaries off a mobile device for later forensic analysis. Which of the following should the analyst do NEXT?

- A. Decompile each binary to derive the source code.
- B. Perform a factory reset on the affected mobile device.
- C. Compute SHA-256 hashes for each binary.
- D. Encrypt the binaries using an authenticated AES-256 mode of operation.
- E. Inspect the permissions manifests within each application.

**Answer: D**

#### **QUESTION 2**

A security analyst needs to reduce the overall attack surface. Which of the following infrastructure changes should the analyst recommend?

- A. Implement a honeypot.
- B. Air gap sensitive systems.
- C. Increase the network segmentation.
- D. Implement a cloud-based architecture.

**Answer: C**

#### **QUESTION 3**

A security analyst is reviewing the following log from an email security service.

```
Rejection type:      Drop
Rejection description: IP found in RBL
Event time:         Today at 16:06
Rejection information: mail.comptia.org
                    https://www.spamfilter.org/query?P=192.167.28.243
From address:       user@comptex.org
To address:         tests@comptia.org
IP address:         192.167.28.243
Remote server name: 192.167.28.243
```

Which of the following BEST describes the reason why the email was blocked?

- A. The To address is invalid.
- B. The email originated from the www.spamfilter.org URL.
- C. The IP address and the remote server name are the same.
- D. The IP address was blacklisted.

**[CS0-002 Exam Dumps](#) [CS0-002 Exam Questions](#) [CS0-002 PDF Dumps](#) [CS0-002 VCE Dumps](#)**

**<https://www.braindump2go.com/cs0-002.html>**

E. The From address is invalid.

**Answer: D**

#### QUESTION 4

A user's computer has been running slowly when the user tries to access web pages. A security analyst runs the command `netstat -aon` from the command line and receives the following output:

LINE	PROTOCOL	LOCAL ADDRESS	FOREIGN ADDRESS	STATE
1	TCP	127.0.0.1:15453	127.0.0.1:16374	ESTABLISHED
2	TCP	127.0.0.1:8193	127.0.0.1:8192	ESTABLISHED
3	TCP	192.168.0.23:443	185.23.17.119:17207	ESTABLISHED
4	TCP	192.168.0.23:13985	172.217.0.14:443	ESTABLISHED
5	TCP	192.168.0.23:6023	185.23.17.120:443	ESTABLISHED
6	TCP	192.168.0.23:7264	10.23.63.217:445	ESTABLISHED

Which of the following lines indicates the computer may be compromised?

- A. Line 1
- B. Line 2
- C. Line 3
- D. Line 4
- E. Line 5
- F. Line 6

**Answer: D**

#### QUESTION 5

As part of an exercise set up by the information security officer, the IT staff must move some of the network systems to an off-site facility and redeploy them for testing. All staff members must ensure their respective systems can power back up and match their gold image. If they find any inconsistencies, they must formally document the information. Which of the following BEST describes this test?

- A. Walk through
- B. Full interruption
- C. Simulation
- D. Parallel

**Answer: C**

#### QUESTION 6

A security analyst is reviewing a web application. If an unauthenticated user tries to access a page in the application, the user is redirected to the login page. After successful authentication, the user is then redirected back to the original page. Some users have reported receiving phishing emails with a link that takes them to the application login page but then redirects to a fake login page after successful authentication. Which of the following will remediate this software vulnerability?

- A. Enforce unique session IDs for the application.
- B. Deploy a WAF in front of the web application.
- C. Check for and enforce the proper domain for the redirect.
- D. Use a parameterized query to check the credentials.
- E. Implement email filtering with anti-phishing protection.

**Answer: A**

#### QUESTION 7

A Chief Information Security Officer (CISO) is concerned the development team, which consists of contractors, has too

[CS0-002 Exam Dumps](#) [CS0-002 Exam Questions](#) [CS0-002 PDF Dumps](#) [CS0-002 VCE Dumps](#)

<https://www.braindump2go.com/cs0-002.html>

much access to customer data. Developers use personal workstations, giving the company little to no visibility into the development activities.

Which of the following would be BEST to implement to alleviate the CISO's concern?

- A. DLP
- B. Encryption
- C. Test data
- D. NDA

**Answer: A**

#### **QUESTION 8**

A company was recently awarded several large government contracts and wants to determine its current risk from one specific APT.

Which of the following threat modeling methodologies would be the MOST appropriate to use during this analysis?

- A. Attack vectors
- B. Adversary capability
- C. Diamond Model of Intrusion Analysis
- D. Kill chain
- E. Total attack surface

**Answer: B**

#### **QUESTION 9**

A security analyst is reviewing vulnerability scan results and notices new workstations are being flagged as having outdated antivirus signatures. The analyst observes the following plugin output:

Antivirus is installed on the remote host:

Installation path: C:\Program Files\AVProduct\Win32\

Product Engine: 14.12.101

Engine Version: 3.5.71

Scanner does not currently have information about AVProduct version 3.5.71. It may no longer be supported.

The engine version is out of date. The oldest supported version from the vendor is 4.2.11.

The analyst uses the vendor's website to confirm the oldest supported version is correct.

Which of the following BEST describes the situation?

- A. This is a false positive, and the scanning plugin needs to be updated by the vendor.
- B. This is a true negative, and the new computers have the correct version of the software.
- C. This is a true positive, and the new computers were imaged with an old version of the software.
- D. This is a false negative, and the new computers need to be updated by the desktop team.

**Answer: D**

#### **QUESTION 10**

A SIEM solution alerts a security analyst of a high number of login attempts against the company's webmail portal. The analyst determines the login attempts used credentials from a past data breach.

Which of the following is the BEST mitigation to prevent unauthorized access?

- A. Single sign-on
- B. Mandatory access control
- C. Multifactor authentication
- D. Federation
- E. Privileged access management

**Answer: C**

**QUESTION 11**

A product manager is working with an analyst to design a new application that will perform as a data analytics platform and will be accessible via a web browser. The product manager suggests using a PaaS provider to host the application. Which of the following is a security concern when using a PaaS solution?

- A. The use of infrastructure-as-code capabilities leads to an increased attack surface.
- B. Patching the underlying application server becomes the responsibility of the client.
- C. The application is unable to use encryption at the database level.
- D. Insecure application programming interfaces can lead to data compromise.

**Answer: B**