

➤ **Vendor: CompTIA**

➤ **Exam Code: CS0-002**

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

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

[Visit Braindump2go and Download Full Version CS0-002 Exam Dumps](#)

QUESTION 555

Which of the following attacks can be prevented by using output encoding?

- A. Server-side request forgery
- B. Cross-site scripting
- C. SQL injection
- D. Command injection
- E. Cross-site request forgery
- F. Directory traversal

Answer: B

QUESTION 556

The help desk provided a security analyst with a screenshot of a user's desktop:

```
$ aircrack-ng -e AHT4 -w dictionary.txt wpa2.pcapdump
Opening wpa2.pcapdump
Read 6396 packets.
Opening wpa2.pcapdump
Reading packets, please wait...
```

For which of the following is aircrack-ng being used?

- A. Wireless access point discovery
- B. Rainbow attack
- C. Brute-force attack
- D. PCAP data collection

Answer: B

QUESTION 557

A security manager has asked an analyst to provide feedback on the results of a penetration test. After reviewing the results, the manager requests information regarding the possible exploitation of vulnerabilities. Which of the following information data points would be MOST useful for the analyst to provide to the security manager, who would then communicate the risk factors to senior management? (Choose two.)

- A. Probability
- B. Adversary capability
- C. Attack vector

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

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

- D. Impact
- E. Classification
- F. Indicators of compromise

Answer: AD

QUESTION 558

A security analyst has been alerted to several emails that show evidence an employee is planning malicious activities that involve employee PII on the network before leaving the organization. The security analyst's BEST response would be to coordinate with the legal department and:

- A. the public relations department
- B. senior leadership
- C. law enforcement
- D. the human resources department

Answer: D

QUESTION 559

While preparing for an audit of information security controls in the environment, an analyst outlines a framework control that has the following requirements:

- All sensitive data must be classified.
- All sensitive data must be purged on a quarterly basis.
- Certificates of disposal must remain on file for at least three years.

This framework control is MOST likely classified as:

- A. prescriptive
- B. risk-based
- C. preventive
- D. corrective

Answer: A

QUESTION 560

An analyst performs a routine scan of a host using Nmap and receives the following output:

```
$ nmap -sS 10.0.3.1
Starting Nmap 8.9 (http://nmap.org) at 2019-01-19 12:03 PST
Nmap scan report for 10.0.3.1
Host is up (0.00098s latency).
Not shown: 979 closed ports
```

PORT	STATE	SERVICE
20/tcp	filtered	ftp-data
21/tcp	filtered	ftp
22/tcp	open	ssh
23/tcp	open	telnet
80/tcp	open	http

```
Nmap done: 1 IP address (1 host up) scanned in 0.840 seconds
```

Which of the following should the analyst investigate FIRST?

- A. Port 21
- B. Port 22

- C. Port 23
- D. Port 80

Answer: C

QUESTION 561

A security analyst at a technology solutions firm has uncovered the same vulnerabilities on a vulnerability scan for a long period of time. The vulnerabilities are on systems that are dedicated to the firm's largest client. Which of the following is MOST likely inhibiting the remediation efforts?

- A. The parties have an MOU between them that could prevent shutting down the systems
- B. There is a potential disruption of the vendor-client relationship
- C. Patches for the vulnerabilities have not been fully tested by the software vendor
- D. There is an SLA with the client that allows very little downtime

Answer: D

QUESTION 562

A security analyst gathered forensics from a recent intrusion in preparation for legal proceedings. The analyst used EnCase to gather the digital forensics, cloned the hard drive, and took the hard drive home for further analysis. Which of the following did the security analyst violate?

- A. Cloning procedures
- B. Chain of custody
- C. Hashing procedures
- D. Virtualization

Answer: B

QUESTION 563

A threat feed notes malicious actors have been infiltrating companies and exfiltrating data to a specific set of domains. Management at an organization wants to know if it is a victim. Which of the following should the security analyst recommend to identify this behavior without alerting any potential malicious actors?

- A. Create an IPS rule to block these domains and trigger an alert within the SIEM tool when these domains are requested.
- B. Add the domains to a DNS sinkhole and create an alert in the SIEM tool when the domains are queried
- C. Look up the IP addresses for these domains and search firewall logs for any traffic being sent to those IPs over port 443
- D. Query DNS logs with a SIEM tool for any hosts requesting the malicious domains and create alerts based on this information

Answer: B

QUESTION 564

A security analyst discovered a specific series of IP addresses that are targeting an organization. None of the attacks have been successful. Which of the following should the security analyst perform NEXT?

- A. Begin blocking all IP addresses within that subnet
- B. Determine the attack vector and total attack surface
- C. Begin a kill chain analysis to determine the impact
- D. Conduct threat research on the IP addresses

Answer: D

QUESTION 565

Which of the following is the MOST important objective of a post-incident review?

- A. Capture lessons learned and improve incident response processes
- B. Develop a process for containment and continue improvement efforts
- C. Identify new technologies and strategies to remediate
- D. Identify a new management strategy

Answer: A

QUESTION 566

An organization was alerted to a possible compromise after its proprietary data was found for sale on the Internet. An analyst is reviewing the logs from the next-generation UTM in an attempt to find evidence of this breach. Given the following output:

Src IP	Src DNS	Dst IP	Dst DNS	Port	Application
10.50.50.121	83hht23.org-int.org	8.8.8.8	google...dns-a.google.com	53	DNS
10.50.50.121	83hht23.org-int.org	77.88.55.66	yandex.ru	443	HTTPS
172.16.52.20	webserver.org-dmz.org	131.52.88.45	--	53	DNS
10.100.10.45	appserver.org-int.org	69.134.21.90	repo.its.utk.edu	21	FTP
172.16.52.20	webserver.org-dmz.org	131.52.88.45	--	10999	HTTPS
172.16.52.100	sftp.org-dmz.org	62.30.221.56	ftps.bluedmed.net	42991	SSH
172.16.52.20	webserver.org-dmz.org	131.52.88.45	--	10999	HTTPS

Which of the following should be the focus of the investigation?

- A. webserver.org-dmz.org
- B. sftp.org-dmz.org
- C. 83hht23.org-int.org
- D. ftps.bluedmed.net

Answer: A

QUESTION 567

A company wants to establish a threat-hunting team. Which of the following BEST describes the rationale for integrating intelligence into hunt operations?

- A. It enables the team to prioritize the focus areas and tactics within the company's environment
- B. It provides criticality analyses for key enterprise servers and services
- C. It allows analysts to receive routine updates on newly discovered software vulnerabilities
- D. It supports rapid response and recovery during and following an incident

Answer: A

QUESTION 568

A security analyst is investigating a compromised Linux server. The analyst issues the ps command and receives the following output:

```
1286 ? Ss 0:00 /usr/sbin/cupsd -f
1287 ? Ss 0:00 /usr/sbin/httpd
1297 ? Ssl 0:00 /usr/bin/libvirtd
1301 ? Ss 0:00 ./usr/sbin/sshd -D
1308 ? Ss 0:00 /usr/sbin/atd -f
```

Which of the following commands should the administrator run NEXT to further analyze the compromised system?

- A. strace /proc/1301
- B. rpm -V openssh-server

- C. /bin/ls -l /proc/1301/exe
- D. kill -9 1301

Answer: A

QUESTION 569

A security analyst is reviewing the following log entries to identify anomalous activity:

```
GET https://comptia.org/admin/login.html&user&password\ HTTP/1.1
GET http://comptia.org/index.php\ HTTP/1.1
GET http://comptia.org/scripts/../../../../Windows/System32/cmd.exe?/C+dir+c:\ HTTP/1.1
GET http://comptia.org/media/contactus.html\ HTTP/1.1
```

Which of the following attack types is occurring?

- A. Directory traversal
- B. SQL injection
- C. Buffer overflow
- D. Cross-site scripting

Answer: A

QUESTION 570

A web-based front end for a business intelligence application uses pass-through authentication to authenticate users. The application then uses a service account to perform queries and look up data in a database. A security analyst discovers employees are accessing data sets they have not been authorized to use. Which of the following will fix the cause of the issue?

- A. Change the security model to force the users to access the database as themselves
- B. Parameterize queries to prevent unauthorized SQL queries against the database
- C. Configure database security logging using syslog or a SIEM
- D. Enforce unique session IDs so users do not get a reused session ID

Answer: A

QUESTION 571

A company's Chief Information Security Officer (CISO) is concerned about the integrity of some highly confidential files. Any changes to these files must be tied back to a specific authorized user's activity session. Which of the following is the BEST technique to address the CISO's concerns?

- A. Configure DLP to reject all changes to the files without pre-authorization.
Monitor the files for unauthorized changes.
- B. Regularly use SHA-256 to hash the directory containing the sensitive information.
Monitor the files for unauthorized changes.
- C. Place a legal hold on the files.
Require authorized users to abide by a strict time context access policy.
Monitor the files for unauthorized changes.
- D. Use Wireshark to scan all traffic to and from the directory.
Monitor the files for unauthorized changes.

Answer: A