- **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 23
A security analyst is assisting in the redesign of a network to make it more secure. The solution should be low cost, and access to the secure segments should be easily monitored, secured, and controlled. Which of the following should be implemented?

A. System isolation
B. Honeyport
C. Jump box
D. Mandatory access control

Answer: C

QUESTION 24
A Chief Information Security Officer (CISO) needs to ensure that a laptop image remains unchanged and can be verified before authorizing the deployment of the image to 4000 laptops. Which of the following tools would be appropriate to use in this case?

A. MSBA
B. SHA1sum
C. FIM
D. DLP

Answer: B

QUESTION 25
Which of the following systems or services is MOST likely to exhibit issues stemming from the Heartbleed vulnerability (Choose two.)

A. SSH daemons
B. Web servers
C. Modbus devices
D. TLS VPN services
E. IPSec VPN concentrators
F. SMB service

Answer: DE

QUESTION 26
An analyst was investigating the attack that took place on the network. A user was able to access the system without

proper authentication. Which of the following will the analyst recommend, related to management approaches, in order to control access? (Choose three.)

A. RBAC
B. LEAP
C. DAC
D. PEAP
E. MAC
F. SCAP
G. BCP

Answer: ACE

QUESTION 27
In reviewing service desk requests, management has requested that the security analyst investigate the requests submitted by the new human resources manager. The requests consist of "unlocking" files that belonged to the previous human manager. The security analyst has uncovered a tool that is used to display five-level passwords. This tool is being used by several members of the service desk to unlock files. The content of these particular files is highly sensitive information pertaining to personnel.
Which of the following BEST describes this scenario? (Choose two.)

A. Unauthorized data exfiltration
B. Unauthorized data masking
C. Unauthorized access
D. Unauthorized software
E. Unauthorized controls

Answer: CE

QUESTION 28
A security analyst receives a mobile device with symptoms of a virus infection. The virus is morphing whenever it is from sandbox to sandbox to analyze. Which of the following will help to identify the number of variations through the analysis life cycle?

A. Journaling
B. Hashing utilities
C. Log viewers
D. OS and process analysis

Answer: D

QUESTION 29
A security engineer has been asked to reduce the attack surface on an organization's production environment. To limit access, direct VPN access to all systems must be terminated, and users must utilize multifactor authentication to access a constrained VPN connection and then pivot to other production systems form a bastion host. The MOST appropriate way to implement the stated requirement is through the use of a:

A. sinkhole.
B. multitenant platform.
C. single-tenant platform.
D. jump box

Answer: D

QUESTION 30
An analyst is performing penetration testing and vulnerability assessment activities against a new vehicle automation

platform.
Which of the following is MOST likely an attack vector that is being utilized as part of the testing and assessment?

A. FaaS
B. RTOS
C. SoC
D. GPS
E. CAN bus

Answer: B

QUESTION 31
An information security analyst observes anomalous behavior on the SCADA devices in a power plant. This behavior results in the industrial generators overheating and destabilizing the power supply.
Which of the following would BEST identify potential indicators of compromise?

A. Use Burp Suite to capture packets to the SCADA device's IP.
B. Use tcpdump to capture packets from the SCADA device IP.
C. Use Wireshark to capture packets between SCADA devices and the management system.
D. Use Nmap to capture packets from the management system to the SCADA devices.

Answer: C

QUESTION 32
Which of the following would MOST likely be included in the incident response procedure after a security breach of customer PII?

A. Human resources
B. Public relations
C. Marketing
D. Internal network operations center

Answer: B

QUESTION 33
An analyst is working with a network engineer to resolve a vulnerability that was found in a piece of legacy hardware, which is critical to the operation of the organization's production line. The legacy hardware does not have third-party support, and the OEM manufacturer of the controller is no longer in operation. The analyst documents the activities and verifies these actions prevent remote exploitation of the vulnerability.
Which of the following would be the MOST appropriate to remediate the controller?

A. Segment the network to constrain access to administrative interfaces.
B. Replace the equipment that has third-party support.
C. Remove the legacy hardware from the network.
D. Install an IDS on the network between the switch and the legacy equipment.

Answer: D