

[July-2020-New100% Exam Pass-CS0-002 VCE and PDF Dumps Free from Braindump2go[21-34

2020/July New Braindump2go CS0-002 Exam Dumps with PDF and VCE Free Updated Today! Following are some new CS0-002 Real Exam Questions!

QUESTION 21A Chief Executive Officer (CEO) wants to implement BYOD in the environment. Which of the following options should the security analyst suggest to protect corporate data on these devices? (Choose two.)A. Disable VPN connectivity on the device.B. Disable Bluetooth on the device.C. Disable near-field communication on the device.D. Enable MDM/MAM capabilities.E. Enable email services on the device.F. Enable encryption on all devices.
Answer: DF

QUESTION 22A security analyst positively identified the threat, vulnerability, and remediation. The analyst is ready to implement the corrective control. Which of the following would be the MOST inhibiting to applying the fix?A. Requiring a firewall reboot.B. Resetting all administrator passwords.C. Business process interruption.D. Full desktop backups.
Answer: D

QUESTION 23A 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 isolationB. HoneypotC. Jump boxD. Mandatory access control
Answer: C

QUESTION 24A 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. MSBAB. SHA1sumC. FIMD. DLP
Answer: B

QUESTION 25Which of the following systems or services is MOST likely to exhibit issues stemming from the Heartbleed vulnerability (Choose two.)A. SSH daemonsB. Web serversC. Modbus devicesD. TLS VPN servicesE. IPSec VPN concentratorsF. SMB service
Answer: DE

QUESTION 26An 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. RBACB. LEAPC. DACD. PEAPE. MACF. SCAPG. BCP
Answer: ACE

QUESTION 27In 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 exfiltrationB. Unauthorized data maskingC. Unauthorized accessD. Unauthorized softwareE. Unauthorized controls
Answer: CE

QUESTION 28A 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. JournalingB. Hashing utilitiesC. Log viewersD. OS and process analysis
Answer: D

QUESTION 29A 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 from 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 30An 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. FaaSB. RTOSC. SoCD. GPSE. CAN bus
Answer: B

QUESTION 31An 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 32Which of the following would MOST likely be included in the incident response procedure after a security breach of customer PII?A. Human resourcesB. Public relationsC. MarketingD. Internal network operations center
Answer: B

QUESTION 33An 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

QUESTION 34A small electronics company decides to use a contractor to assist with the

development of a new FPGA- based device. Several of the development phases will occur off-site at the contractor's labs. Which of the following is the main concern a security analyst should have with this arrangement?A. Making multiple trips between development sites increases the chance of physical damage to the FPGAs.B. Moving the FPGAs between development sites will lessen the time that is available for security testing.C. Development phases occurring at multiple sites may produce change management issues.D. FPGA applications are easily cloned, increasing the possibility of intellectual property theft.

Answer: D
Resources From: 1.2020 Latest Braindump2go CS0-002 Exam Dumps (PDF & VCE) Free Share:

<https://www.braindump2go.com/cs0-002.html>2.2020 Latest Braindump2go CS0-002 PDF and CS0-002 VCE Dumps Free Share:

<https://drive.google.com/drive/folders/1ijxiiJOyOJ7Z8VAogjAysf7iznDnjE46?usp=sharing>3.2020 Free Braindump2go

CS0-002 PDF Download:[https://www.braindump2go.com/free-online-pdf/CS0-002-Dumps\(34-45\).pdf](https://www.braindump2go.com/free-online-pdf/CS0-002-Dumps(34-45).pdf)

[https://www.braindump2go.com/free-online-pdf/CS0-002-PDF\(1-11\).pdf](https://www.braindump2go.com/free-online-pdf/CS0-002-PDF(1-11).pdf)

[https://www.braindump2go.com/free-online-pdf/CS0-002-PDF-Dumps\(46-58\).pdf](https://www.braindump2go.com/free-online-pdf/CS0-002-PDF-Dumps(46-58).pdf)

[https://www.braindump2go.com/free-online-pdf/CS0-002-VCE\(23-33\).pdf](https://www.braindump2go.com/free-online-pdf/CS0-002-VCE(23-33).pdf)

[https://www.braindump2go.com/free-online-pdf/CS0-002-VCE-Dumps\(12-22\).pdf](https://www.braindump2go.com/free-online-pdf/CS0-002-VCE-Dumps(12-22).pdf)Free Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!