[December-2020Braindump2go CS0-002 Free VCE Dumps Download[Q551-Q571

December/2020 Latest Braindump2go CS0-002 Exam Dumps with PDF and VCE Free Updated Today! Following are some new CS0-002 Real Exam Questions!QUESTION 551A cybersecurity analyst is reading a daily intelligence digest of new vulnerabilities. The type of vulnerability that should be disseminated FIRST is one that:A. enables remote code execution that is being exploited in the wildB. enables data leakage but is not known to be in the environmentC. enables lateral movement and was reported as a proof of conceptD. affected the organization in the past but was probably contained and eradicatedAnswer: AQUESTION 552A company's incident response team is handling a threat that was identified on the network. Security analysts have determined a web server is making multiple connections from TCP port 445 outbound to servers inside its subnet as well as at remote sites. Which of the following is the MOST appropriate next step in the incident response plan?A. Quarantine the web serverB. Deploy virtual firewallsC. Capture a forensic image of the memory and diskD. Enable web server containerizationAnswer: AQUESTION 553 During an incident, a cybersecurity analyst found several entries in the web server logs that are related to an IP with a bad reputation. Which of the following would cause the analyst to further review the incident?A. BadReputationIp - - [2019-04-12 10:43Z] "GET /etc/passwd" 403 1023B. BadReputationIp - - [2019-04-12 10:43Z] "GET /index.html?src=../.ssh/id_rsa" 401 17044C. BadReputationIp - - [2019-04-12 10:43Z] "GET /a.php?src=/etc/passwd" 403 11056D. BadReputationIp - - [2019-04-12 10:43Z] "GET /a.php?src=../../.ssh/id_rsa" 200 15036E. BadReputationIp - - [2019-04-12 10:43Z] "GET /favicon.ico?src=../usr/share/ icons" 200 19064Answer: EQUESTION 554A developer wrote a script to make names and other PII data unidentifiable before loading a database export into the testing system. Which of the following describes the type of control that is being used?A. Data encodingB. Data maskingC. Data loss preventionD. Data classificationAnswer: BQUESTION 555 Which of the following attacks can be prevented by using output encoding?A. Server-side request forgeryB. Cross-site scripting C. SQL injectionD. Command injectionE. Cross-site request forgeryF. Directory traversalAnswer: BQUESTION 556The 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 [illegible] packets...
Opening wpa2.pcapdump
Reading packets, please wait...
```


For which of the following is aircrack-ng being used?A. Wireless access point discoveryB. Rainbow attackC. Brute-force attackD. PCAP data collectionAnswer: BQUESTION 557A 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. ProbabilityB. Adversary capabilityC. Attack vectorD. ImpactE. ClassificationF. Indicators of compromiseAnswer: ADQUESTION 558A 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 departmentB. senior leadershipC. law enforcementD. the human resources departmentAnswer: DQUESTION 559While 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. prescriptiveB. risk-basedC. preventiveD. correctiveAnswer: AQUESTION 560An 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   [illegible]
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 21B. Port 22C. Port 23D. Port 80Answer: CQUESTION 561A 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 systemsB. There is a potential disruption of the vendor-client relationshipC. Patches for the vulnerabilities have not been fully tested by the software vendorD. There is an SLA with the client that allows very little downtimeAnswer: DQUESTION 562A 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 proceduresB. Chain of custodyC. Hashing proceduresD. VirtualizationAnswer: BQUESTION 563A 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 queriedC. Look up the IP addresses for these domains and search firewall logs for any traffic being sent to those IPs over port 443D. Query DNS logs with a SIEM tool for any hosts requesting the malicious domains and create alerts based on this informationAnswer: BQUESTION 564A 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 subnetB. Determine the attack vector and total attack surfaceC. Begin a kill chain analysis to determine the impactD. Conduct threat research on the IP addressesAnswer: DQUESTION 565Which of the following is the MOST important objective of a post-incident review?A. Capture lessons learned and improve incident response processesB. Develop a process for containment and continue improvement effortsC. Identify new technologies and strategies to remediateD. Identify a new management strategyAnswer: AQUESTION 566An 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	0.0.0.0	google...dns-a.google.com	53	DNS
10.50.50.121	83hht23.org-int.org	72.88.55.66	yandex.ru	443	HTTPS
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.bluemed.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.orgB. sftp.org-dmz.orgC. 83hht23.org-int.orgD. ftps.bluemed.netAnswer: AQUESTION 567A 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 environmentB. It provides criticality analyses for key enterprise servers and services C. It allows analysts to receive routine updates on newly discovered software vulnerabilitiesD. It supports rapid response and recovery during and following an incidentAnswer: AQUESTION 568A 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   ?    Sl    0:00    /usr/sbin/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/1301B. rpm ?V openssh-serverC. /bin/ls ?l /proc/1301/exeD. kill -9 1301Answer: AQUESTION 569A 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 HTTP/1.1
GET http://comptia.org/media/contactus.html\ HTTP/1.1
```


Which of the following attack types is occurring?A. Directory traversalB. SQL injectionC. Buffer overflowD. Cross-site scriptingAnswer: AQUESTION 570A 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 themselvesB. Parameterize queries to

prevent unauthorized SQL queries against the databaseC. Configure database security logging using syslog or a SIEMD. Enforce unique session IDs so users do not get a reused session IDAnswer: AQUESTION 571A 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: AResources From:1.2020 Latest Braindump2go CS0-002 Exam Dumps (PDF & VCE) Free Share: https://www.braindump2go.com/cs0-002.html2.2020 Latest Braindump2go CS0-002 PDF and CS0-002 VCE Dumps Free Share: https://drive.google.com/drive/folders/1ijxiiJOyOJ7Z8VAogjAysf7iznDnjE46?usp=sharing3.2020 Free Braindump2go CS0-002 PDF Download:https://www.braindump2go.com/free-online-pdf/CS0-002-PDF(531-542).pdf https://www.braindump2go.com/free-online-pdf/CS0-002-PDF-Dumps(519-530).pdf https://www.braindump2go.com/free-online-pdf/CS0-002-VCE(543-554).pdf https://www.braindump2go.com/free-online-pdf/CS0-002-VCE-Dumps(555-571).pdfFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!