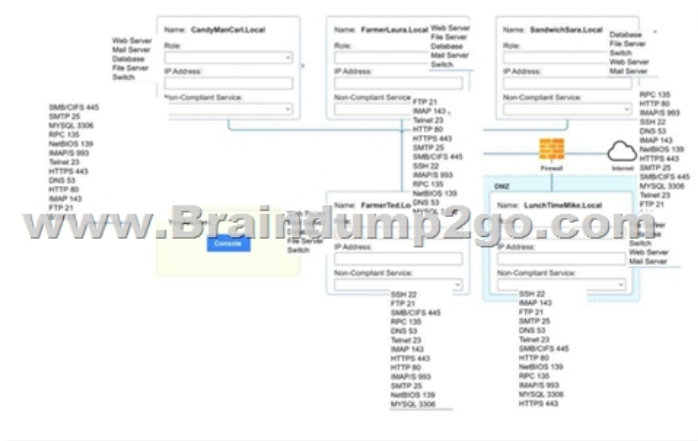
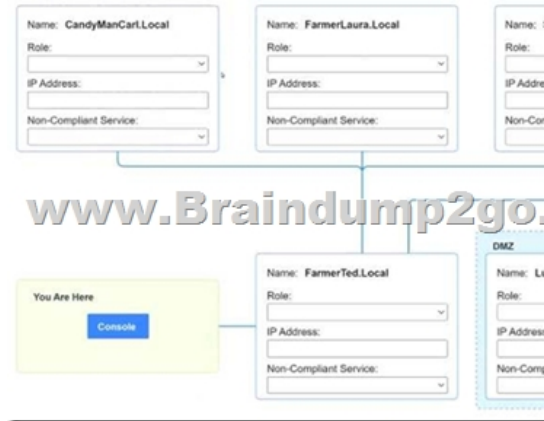
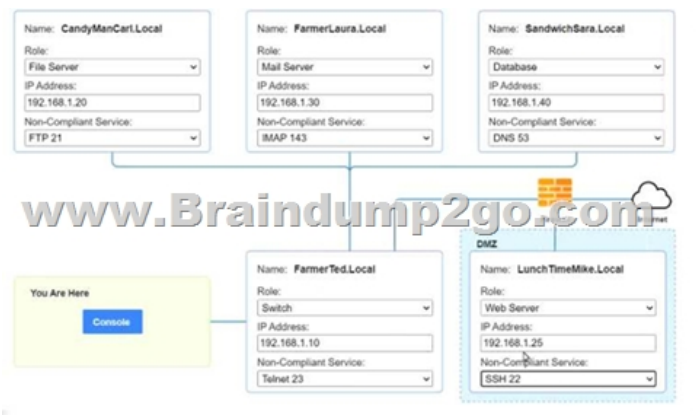


[August-2022Braindump2go CS0-002 (PDF and VCE)Dumps CS0-002 806Q Free Offer[Q807-Q853

August/2022 Latest Braindump2go CS0-002 Exam Dumps with PDF and VCE Free Updated Today! Following are some new Braindump2go CS0-002 Real Exam Questions!
QUESTION 807 You are a penetration tester who is reviewing the system hardening guidelines for a company. Hardening guidelines indicate the following.- There must be one primary server or service per device.- Only default port should be used.- Non-secure protocols should be disabled.- The corporate internet presence should be placed in a protected subnet. Instructions:- Using the available tools, discover devices on the corporate network and the services running on these devices. You must determine:- ip address of each device- The primary server or service each device- The protocols that should be disabled based on the hardening guidelines If at any time you would like to bring back.



Answer:



QUESTION 808A security analyst is reviewing the following server statistics:

% CPU	Disk KB in	Disk KB out	Net KB in	Net KB out
99	3122	43	456	34
100	123	56	87	7
99	2	234	3	245
100	345	867	8243	85
98	22	3	5634	42326
100	435	345	54	42
99	0	4	575	3514

Which of the following is MOST likely occurring?
 A. Race condition
 B. Privilege escalation
 C. Resource exhaustion
 D. VM escape
 Answer: C
 QUESTION 809
 A software developer is correcting the error-handling capabilities of an application following the initial coding of the fix. Which of the following would the software developer MOST likely perform to validate the code prior to pushing it to production?
 A. Web-application vulnerability scan
 B. Static analysis
 C. Packet inspection
 D. Penetration test
 Answer: B
 QUESTION 810
 Forming a hypothesis, looking for indicators of compromise, and using the findings to proactively improve detection capabilities are examples of the value of:
 A. vulnerability scanning
 B. threat hunting
 C. red learning
 D. penetration testing
 Answer: A
 QUESTION 811
 Which of the following BEST explains the function of a managerial control?
 A. To help design and implement the security planning, program development, and maintenance of the security life cycle
 B. To guide the development of training, education, security awareness programs, and system maintenance
 C. To create data classification, risk assessments, security control reviews, and contingency planning
 D. To ensure tactical design, selection of technology to protect data, logical access reviews, and the implementation of audit trails
 Answer: A
 QUESTION 812
 Which of the following types of controls defines placing an ACL on a file folder?
 A. Technical control
 B. Confidentiality control
 C. Managerial control
 D. Operational control
 Answer: A
 QUESTION 813
 A code review reveals a web application is using lime-based cookies for session management. This is a security concern because lime-based cookies are easy to:
 A. parameterize
 B. decode
 C. guess
 D. decrypt
 Answer: C
 QUESTION 814
 A security analyst discovers suspicious host activity while performing monitoring activities. The analyst pulls a packet capture for the activity and sees the following:

```

Date/time  Destination  Protocol  Host  Info
2020-08-20  92.168.4.52  HTTP     utoftor.com  POST /210/gate.php HTTP/1.1 (Application/octet-stream)

Follow TCP stream:
POST /210/gate.php HTTP/1.1
Cache-Control: no-cache
Content-Type: application/octet-stream
Pragma: no-cache
Content-Type: application/octet-stream
User-Agent: Mozilla/4.0
Host: utoftor.com
Ss.0.k.-4.4.RQ.6..HTTP/1.1 200 OK
Server: nginx/1.6.2
    
```

Which of the following describes what has occurred?
 A. The host attempted to download an application from utoftor.com.
 B. The host downloaded an application from utoftor.com.
 C. The host attempted to make a secure connection to utoftor.com.
 D. The host rejected the connection from utoftor.com.
 Answer: B
 QUESTION 815
 A security analyst is reviewing the following Internet usage trend report:

Username	Week #10	Week #9	Week #8	Week #7
User 1	58Gb	51Gb	59Gb	55Gb
User 2	65Gb	62Gb	67Gb	63Gb
User 3	173Gb	157Gb	197Gb	182Gb
User 4	38Gb	46Gb	29Gb	41Gb

Which of the following usernames should the security analyst investigate further?
 A. User 1
 B. User 2
 C. User 3
 D. User 4
 Answer: C
 QUESTION 816
 A consultant evaluating multiple threat intelligence leads to assess potential risks for a client. Which of the following is the BEST approach for the consultant to consider when modeling the client's attack surface?
 A. Ask for external scans from industry peers, look at the open ports, and compare information with the client.
 B. Discuss potential tools the client can purchase to reduce the likelihood of an attack.
 C. Look at attacks against similar industry peers and assess the probability of the same attacks happening.
 D. Meet with the senior management team to determine if funding is available for recommended solutions.
 Answer: A
 QUESTION 817
 Which of the following BEST explains the function of TPM?
 A. To provide hardware-based security features using unique keys
 B. To ensure platform confidentiality by storing security measurements
 C. To improve

management of the OS installation.D. To implement encryption algorithms for hard drivesAnswer: AQUESTION 818A manufacturing company uses a third-party service provider for Tier 1 security support. One of the requirements is that the provider must only source talent from its own country due to geopolitical and national security interests. Which of the following can the manufacturing company implement to ensure the third-party service provider meets this requirement?A. Implement a secure supply chain program with governance.B. Implement blacklisting for IP addresses from outside the country.C. Implement strong authentication controls for contractors.D. Implement user behavior analytics for key staff members.Answer: AQUESTION 819 A company's application development has been outsourced to a third-party development team.Based on the SLA. The development team must follow industry best practices for secure coding. Which of the following is the BEST way to verify this agreement?A. Input validationB. Security regression testingC. Application fuzzingD. User acceptance testingE. Stress testingAnswer: DQUESTION 820A security administrator needs to provide access from partners to an Isolated laboratory network inside an organization that meets the following requirements:- The partners' PCs must not connect directly to the laboratory network.- The tools the partners need to access while on the laboratory network must be available to all partners- The partners must be able to run analyses on the laboratory network, which may take hours to completeWhich of the following capabilities will MOST likely meet the security objectives of the request?A. Deployment of a jump box to allow access to the laboratory network and use of VDI in persistent mode to provide the necessary tools for analysisB. Deployment of a firewall to allow access to the laboratory network and use of VDI in non- persistent mode to provide the necessary tools for analysisC. Deployment of a firewall to allow access to the laboratory network and use of VDI in persistent mode to provide the necessary tools for analysisD. Deployment of a jump box to allow access to the Laboratory network and use of VDI in non- persistent mode to provide the necessary tools for analysisAnswer: CQUESTION 821Which of the following are the MOST likely reasons to include reporting processes when updating an incident response plan after a breach? (Select TWO).A. To establish a clear chain of commandB. To meet regulatory requirements for timely reportingC. To limit reputation damage caused by the breachD. To remediate vulnerabilities that led to the breachE. To isolate potential insider threatsF. To provide secure network design changesAnswer: BFQUESTION 822Which of the following is MOST dangerous to the client environment during a vulnerability assessment penetration test?A. There is a longer period of time to assess the environment.B. The testing is outside the contractual scopeC. There is a shorter period of time to assess the environmentD. No status reports are included with the assessment.Answer: BQUESTION 823Which of the following is MOST important when developing a threat hunting program?A. Understanding penetration testing techniquesB. Understanding how to build correlation rules within a SIEMC. Understanding security software technologiesD. Understanding assets and categories of assetsAnswer: DQUESTION 824Which of the following are considered PH by themselves? (Select TWO).A. Government IDB. Job titleC. Employment start dateD. Birth certificateE. Employer addressF. Mother's maiden nameAnswer: ADQUESTION 825Which of the following BEST describes HSM?A. A computing device that manages cryptography, decrypts traffic, and maintains library callsB. A computing device that manages digital keys, performs encryption/decryption functions, and maintains other cryptographic functionsC. A computing device that manages physical keys, encrypts devices, and creates strong cryptographic functionsD. A computing device that manages algorithms, performs entropy functions, and maintains digital signaturesAnswer: BQUESTION 826A threat hunting team received a new IoC from an ISAC that follows a threat actor's profile and activities. Which of the following should be updated NEXT?A. The whitelistB. The DNSC. The blocklistD. The IDS signatureAnswer: DQUESTION 827Which of the following BEST describes what an organization's incident response plan should cover regarding how the organization handles public or private disclosures of an incident?A. The disclosure section should focus on how to reduce the likelihood customers will leave due to the incident.B. The disclosure section should contain the organization's legal and regulatory requirements regarding disclosures.C. The disclosure section should include the names and contact information of key employees who are needed for incident resolutionD. The disclosure section should contain language explaining how the organization will reduce the likelihood of the incident from happening in the future.Answer: BQUESTION 828 An IT security analyst has received an email alert regarding vulnerability within the new fleet of vehicles the company recently purchased. Which of the following attack vectors is the vulnerability MOST likely targeting?A. SCADAB. CAN busC. ModbusD. IoTAnswer: DQUESTION 829After examining a header and footer file, a security analyst begins reconstructing files by scanning the raw data bytes of a hard disk and rebuilding them. Which of the following techniques is the analyst using?A. Header analysisB. File carvingC. Metadata analysisD. Data recoveryAnswer: BQUESTION 831A company's domain has been spoofed in numerous phishing campaigns. An analyst needs to determine the company is a victim of domain spoofing, despite having a DMARC record that should tell mailbox providers to ignore any email that fails DMARC upon review of the record, the analyst finds the following: Which of the following BEST explains the reason why the company's requirements are not being processed correctly by mailbox providers?A. The DMARC record's DKIM alignment tag is incorrectly configured.B. The

DMARC record's policy tag is incorrectly configured.C. The DMARC record does not have an SPF alignment lag.D. The DMARC record's version tag is set to DMARC1 instead of the current version, which is DMARC3.
QUESTION 832 Which of the following BEST explains the function of trusted firmware updates as they relate to hardware assurance?
A. Trusted firmware updates provide organizations with development, compilation, remote access, and customization for embedded devices.
B. Trusted firmware updates provide organizations with security specifications, open-source libraries, and custom toots for embedded devices.
C. Trusted firmware updates provide organizations with remote code execution, distribution, maintenance, and extended warranties for embedded devices.
D. Trusted firmware updates provide organizations with secure code signing, distribution, installation, and attestation for embedded devices.
QUESTION 833 A help desk technician inadvertently sent the credentials of the company's CRM n clear text to an employee's personal email account. The technician then reset the employee's account using the appropriate process and the employee's corporate email, and notified the security team of the incident According to the incident response procedure, which of the following should the security team do NEXT?
A. Contact the CRM vendor.
B. Prepare an incident summary report.
C. Perform postmortem data correlation.
D. Update the incident response plan.
QUESTION 834 A developer downloaded and attempted to install a file transfer application in which the installation package is bundled with acKvare. The next-generation antivirus software prevented the file from executing, but it did not remove the file from the device. Over the next few days, more developers tried to download and execute the offending file. Which of the following changes should be made to the security tools to BEST remedy the issue?
A. Blacklist the hash in the next-generation antivirus system.
B. Manually delete the file from each of the workstations.
C. Remove administrative rights from all developer workstations.
D. Block the download of the fie via the web proxy
QUESTION 835 After detecting possible malicious external scanning, an internal vulnerability scan was performed, and a critical server was found with an outdated version of JBoss. A legacy application that is running depends on that version of JBoss. Which of the following actions should be taken FIRST to prevent server compromise and business disruption at the same time?
A. Make a backup of the server and update the JBoss server that is running on it.
B. Contact the vendor for the legacy application and request an updated version.
C. Create a proper DMZ for outdated components and segregate the JBoss server.
D. Apply visualization over the server, using the new platform to provide the JBoss service for the legacy application as an external service.
QUESTION 836 An incident response team detected malicious software that could have gained access to credit card data. The incident response team was able to mitigate significant damage and implement corrective actions. By having incident response mechanisms in place. Which of the following should be notified for lessons learned?
A. The human resources department
B. Customers
C. Company leadership
D. The legal team
QUESTION 837 In SIEM software, a security analysis selected some changes to hash signatures from monitored files during the night followed by SMB brute-force attacks against the file servers Based on this behavior, which of the following actions should be taken FIRST to prevent a more serious compromise?
A. Fully segregate the affected servers physically in a network segment, apart from the production network.
B. Collect the network traffic during the day to understand if the same activity is also occurring during business hours
C. Check the hash signatures, comparing them with malware databases to verify if the files are infected.
D. Collect all the files that have changed and compare them with the previous baseline
QUESTION 838 While implementing a PKI for a company, a security analyst plans to utilize a dedicated server as the certAcate authority that is only used to sign intermediate certificates. Which of the following are the MOST secure states for the certificate authority server when it is not in use? (Select TWO)
A. On a private VLAN
B. Full disk encrypted
C. Powered off
D. Backed up hourly
E. VPN accessible only
F. Air gapped
QUESTION 839 Which of the following BEST identifies the appropriate use of threat intelligence as a function of detection and response?
A. To identify weaknesses in an organization's security posture
B. To identify likely attack scenarios within an organization
C. To build a business security plan for an organization
D. To build a network segmentation strategy
QUESTION 840 While conoXicting a cloud assessment, a security analyst performs a Prowler scan, which generates the following within the report:

```
7.74 [extra774] Ensure credentials unused for 30 days or greater are disabled
PASS: User admin has logged into the console in the past 30 days
INFO: User h...
INFO: User c...
FAIL: User BusinessUser has never used access key 1 and not rotated it in 30 days
PASS: No users found with access key 2 enabled
```

Based on the Prowler report, which of the following is the BEST recommendation?
A. Delete Cloud Dev access key 1
B. Delete BusinessUsr access key 1
C. Delete access key 1
D. Delete access key 2
QUESTION 841 An internally developed file-monitoring system identified the following except as causing a program to crash often:

```
char filedata[100];
fp = fopen("access.log", "a");
strncpy(filedata, fp, 100);
printf("%s\n", filedata);
```


Set up an FTP server that both companies can access and export the required financial data to a folder. B. Set up a VPN between Company A and Company B, granting access only to the ERPs within the connection. C. Set up a PKI between Company A and Company B and Intermediate shared certificates between the two entities. D. Create static NATs on each entity's firewalls that map to the ERP systems and use native ERP authentication to allow access.

Answer: B

QUESTION 851 A company has alerted planning the implemented a vulnerability management procedure. However, its security maturity level is low, so there are some prerequisites to complete before risk calculation and prioritization. Which of the following should be completed FIRST?

A. A business Impact analysis
B. A system assessment
C. Communication of the risk factors
D. A risk identification process

Answer: D

QUESTION 852 A security team implemented a SIEM as part of its security-monitoring program. There is a requirement to integrate a number of sources into the SIEM to provide better context relative to the events being processed. Which of the following BEST describes the result the security team hopes to accomplish by adding these sources?

A. Data enrichment
B. Continuous integration
C. Machine learning
D. Workflow orchestration

Answer: A

QUESTION 853 A security analyst is investigating an alert from the threat detection platform on a host (10.0.1.25) in a staging environment that could be running a cryptomining tool because it is sending traffic to an IP address that is related to Bitcoin. The network rules for the instance are the following:

Rule	Direction	Protocol	SR
1	inbound	tcp	any
2	inbound	tcp	any
3	inbound	tcp	10.
4	outbound	udp	10.
5	outbound	tcp	10.

Which of the following is the BEST way to isolate and triage the host?

A. Remove rules 1, 2, and 3.
B. Remove rules 1, 2, 4, and 5.
C. Remove rules 1, 2, 3, 4, and 5.
D. Remove rules 1, 2, and 5.
E. Remove rules 1, 4, and 5.
F. Remove rules 4 and 5

Answer: D

Resources From: 1. 2022 Latest Braindump2go CS0-002 Exam Dumps (PDF & VCE) Free Share: <https://www.braindump2go.com/cs0-002.html>
2. 2022 Latest Braindump2go CS0-002 PDF and CS0-002 VCE Dumps Free Share: <https://drive.google.com/drive/folders/1ijxiiJOyOJ7Z8VAogjAysf7iznDnjE46?usp=sharing>
3. 2021 Free Braindump2go CS0-002 Exam Questions Download: [https://www.braindump2go.com/free-online-pdf/CS0-002-PDF-Dumps\(807-853\).pdf](https://www.braindump2go.com/free-online-pdf/CS0-002-PDF-Dumps(807-853).pdf)
Free Resources from Braindump2go, We Devoted to Helping You 100% Pass All Exams!