[CySA+ CS0-001 DumpsFull Version CS0-001 Exam Dumps (PDF and VCE) 321Q for Free Download(Q264-Q275)

2019/Feb Braindump2go CS0-001 Exam Dumps with PDF and VCE New Updated Today! Following are some new CS0-001 Real Exam Questions:1.|2019 Latest CS0-001 Exam Dumps (PDF & VCE) 321Q&As Instant Download:https://www.braindump2go.com/cs0-001.html2.|2019 Latest CS0-001 ExamQuestions & Answers Instant Download:https://drive.google.com/drive/folders/0B75b5xYLjSSNclFka2Z1NWtOaG8?usp=sharingQUESTION 264A company allows employees to work remotely. The security administration is configuring services that will allow remote help desk personnel to work secure outside the company's headquarters. Which of the following presents the BEST solution to meet this goal?A. Configure a VPN concentrator to terminate in the DMZ to allow help desk personnel access to resources.B. Open port 3389 on the firewall to the server to allow users to connect remotely.C. Set up a jump box for all help desk personnel to remotely access system resources.D. Use the company's existing web server for remote access and configure over port 8080.**Answer: A**QUESTION 265In order to leverage the power of data correlation within Nessus, a cybersecurity analyst needs to write an SQL statement that will provide how long a vulnerability has been present on the network.Given the following output table:

ScanDate	IP	P
2015-06-01	192.168.1.224	System
2015-09-01	192.168.1.224	Syste
2016-01-01	192.168.1.224	System

Which of the following SQL statements would provide the resulted output needed for this correlation?A. SELECT Port, ScanDate, IP, PlugIn FROM MyResults WHERE PluginID=`1000'B. SELECT ScanDate, IP, Port, PlugIn FROM MyResults WHERE PluginID=`1000'C. SELECT IP, PORT, PlugIn, ScanDate FROM MyResults SET PluginID=`1000'D. SELECT ScanDate, IP, Port, PlugIn SET MyResults WHERE PluginID=`1000'**Answer: B**QUESTION 266After an internal audit, it was determined that administrative logins need to use multifactor authentication or a 15-character key with complexity enabled. Which of the following policies should be updates to reflect this change? (Choose two.)A. Data ownership policyB. Password policyC. Data classification policyD. Data retention policyE. Acceptable use policyF. Account management policy**Answer: BF** QUESTION 267Management wants to scan servers for vulnerabilities on a periodic basis. Management has decided that the scan frequency should be determined only by vendor patch schedules and the organization's application deployment schedule. Which of the following would force the organization to conduct an out-of- cycle vulnerability scan?A. Newly discovered PII on a serverB. A vendor releases a critical patch updateC. A critical bug fix in the organization's applicationD. False positives identified in production**Answer: B**QUESTION 268A security administrator recently deployed a virtual honeynet. The honeynet is not protected by the company's firewall, while all production networks are protected by a stateful firewall. Which of the following would BEST allow an external penetration tester to determine which one is the honeynet's network?A. Banner grabB. Packet analyzerC. FuzzerD. TCP ACK scan**Answer: D**QUESTION 269A security analyst is conducting a vulnerability assessment of older SCADA devices on the corporate network. Which of the following compensating controls is likely to prevent the scans from providing value?A. Access control list network segmentation that prevents access to the SCADA devices inside the network.B. Detailed and tested firewall rules that effectively prevent outside access of the SCADA devices.C. Implementation of a VLAN that allows all devices on the network to see all SCADA devices on the network.D. SCADA systems configured with `SCADA SUPPORT'=ENABLE**Answer: B**QUESTION 270A logistics company's vulnerability scan identifies the following vulnerabilities on Internet-facing devices in the DMZ: SQL injection on an infrequently used web server that provides files to vendors SSL/TLS not used for a website that contains promotional informationThe scan also shows the following vulnerabilities on internal resources: Microsoft Office Remote Code Execution on test server for a human resources system TLS downgrade vulnerability on a server in a development networkIn order of risk, which of the following should be patched FIRST?A. Microsoft Office Remote Code ExecutionB. SQL injectionC. SSL/TLS not usedD. TLS downgrade**Answer: A**QUESTION 271A cybersecurity analyst is reviewing Apache logs on a web server and finds that some logs are missing. The analyst has identified that the systems administrator accidentally deleted some log files. Which of the following actions or rules should be implemented to prevent this incident from reoccurring?A. Personnel trainingB. Separation of dutiesC. Mandatory vacationD. Backup server**Answer: D** QUESTION 272While reviewing three months of logs, a security analyst notices probes from random company laptops going to SCADA equipment at the company's manufacturing location. Some of the probes are getting responses from the equipment even though firewall rules are in place, which should block this type of unauthorized activity. Which of the following should the analyst recommend to keep this activity from originating from company laptops?A. Implement a group policy on company systems to block access to SCADA networks.B. Require connections to the SCADA network to go through a forwarding proxy.C. Update

the firewall rules to block SCADA network access from those laptop IP addresses.D. Install security software and a host-based firewall on the SCADA equipment.**Answer: A**QUESTION 273NOTE: Question IP must be 192.168.192.123During a network reconnaissance engagement, a penetration tester was given perimeter firewall ACLs to accelerate the scanning process. The penetration tester has decided to concentrate on trying to brute force log in to destination IP address 192.168.192.132 via secure shell.

```
access-list outside-acl permit tcp any host 192.168.192.123 eq https
access-list outside-acl permit tcp 10.10.10.0 mask 255.255.255.0 host 192.168.192.123 eq ssh
```

Given a source IP address of 10.10.10.30, which of the following ACLs will permit this access?A.

```
access-list outside-acl permit tcp any host 192.168.192.123 eq https
```

B.

```
access-list outside-acl
```

C.

```
access-list outside-acl permit tcp 10.10.10.0 mask 255.255.255.0 host 192.168.192.123 eq ssh
```

D.

```
access-list outside-acl permit tcp host 10.10.10.0 mask 255.255.255.0 host 192.168.192.123 eq
```

Answer: CQUESTION 274An analyst is preparing for a technical security compliance check on all Apache servers. Which of the following will be the BEST to use?A. CIS benchmarkB. NagiosC. OWASPD. UntidyE. Cain & Abel**Answer: A** QUESTION 275A company provides wireless connectivity to the internal network from all physical locations for company- owned devices. Users were able to connect the day before, but now all users have reported that when they connect to an access point in the conference room, they cannot access company resources. Which of the following BEST describes the cause of the problem?A. The access point is blocking access by MAC address. Disable MAC address filtering.B. The network is not available. Escalate the issue to network support.C. Expired DNS entries on users' devices. Request the affected users perform a DNS flush.D. The access point is a rogue device. Follow incident response procedures.**Answer: D**!!!RECOMMEND!!!1.|2019 Latest CS0-001 Exam Dumps (PDF & VCE) 321Q&As Instant Download:https://www.braindump2go.com/cs0-001.html2.|2019 Latest CS0-001 Study Guide Video Instant Download: YouTube Video: YouTube.com/watch?v=ZV4LytVliIk