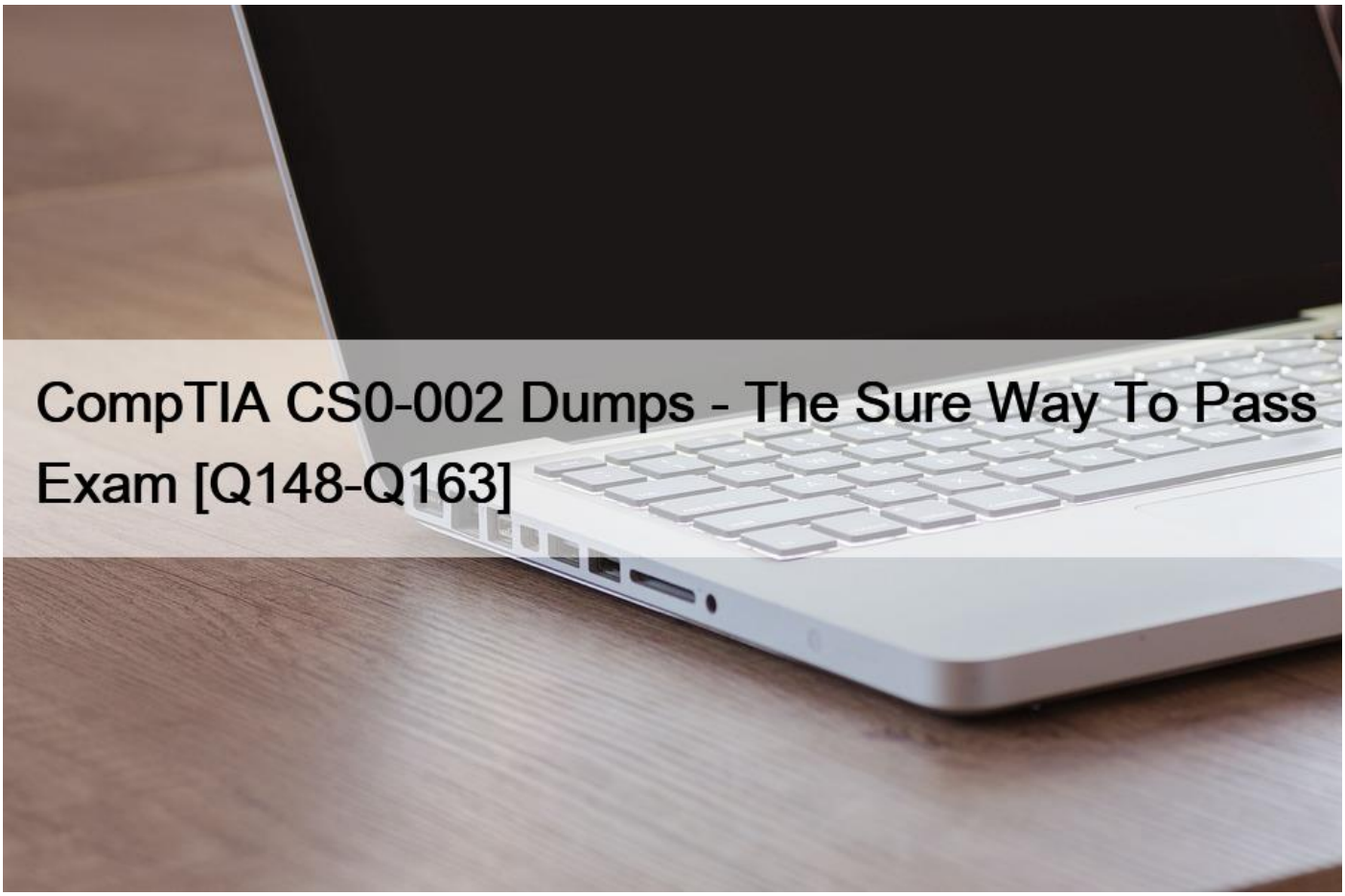
CompTIA CS0-002 Dumps - The Sure Way To Pass Exam [Q148-Q163



CompTIA CS0-002 Dumps - The Sure Way To Pass Exam
CS0-002 Exam Questions (Updated 2022) 100% Real Question Answers

NEW QUESTION 148

The security team at a large corporation is helping the payment-processing team to prepare for a regulatory compliance audit and meet the following objectives:

* Reduce the number of potential findings by the auditors.

* Limit the scope of the audit to only devices used by the payment-processing team for activities directly impacted by the regulations.

* Prevent the external-facing web infrastructure used by other teams from coming into scope.

* Limit the amount of exposure the company will face if the systems used by the payment-processing team are compromised.

Which of the following would be the MOST effective way for the security team to meet these objectives?

* Limit the permissions to prevent other employees from accessing data owned by the business unit.
* Segment the servers and systems used by the business unit from the rest of the network.
* Deploy patches to all servers and workstations across the entire organization.
* Implement full-disk encryption on the laptops used by employees of the payment-processing team.

NEW QUESTION 149

During an investigation, an incident responder intends to recover multiple pieces of digital media. Before removing the media, the responder should initiate:
* malware scans.
* secure communications.
* chain of custody forms.
* decryption tools.

NEW QUESTION 150

A cybersecurity professional wants to determine if a web server is running on a remote host with the IP address 192.168.1.100. Which of the following can be used to perform this task?
* nc 192.168.1.100 -1 80
* ps aux 192.168.1.100
* nmap 192.168.1.100 *p 80 *A
* dig www 192.168.1.100
* ping *p 80 192.168.1.100

NEW QUESTION 151

A company’s IDP/DLP solution triggered the following alerts:

A. 02/25-07:16:07.294705 SSH to Non-standard Port (TCP) 245.23.123.150:51533 -> 67.178.142.153:1234
B. 02/25-08:16:24.637829 E-mail sent containing text pattern 9999 9999 9999 9999 (TCP) 192.168.123.150:36543 -> 209.34.[illegible]:25
C. 02/25-08:23:53.367782 Malformed DNS Packet, size exceeded (UDP) 192.168.84.150:45513 -> 172.16.32.12:53
D. 02/25-09:01:34.335672 XMAS packet detected {TCP} 192.168.233.18:61412 -> 172.16.15.233:445
E. 02/25-09:12:51.564607 Attempted FTP Connection, clear text auth {TCP} 192.168.12.45:47654 ->172.16.222.12:21

Which of the following alerts should a security analyst investigate FIRST?
* A
* B
* C
* D
* E

NEW QUESTION 152

Which of the following assessment methods should be used to analyze how specialized software performs during heavy loads?

* Stress test
* API compatibility lest
* Code review
* User acceptance test
* Input validation

NEW QUESTION 153

A security analyst is investigating a system compromise. The analyst verities the system was up to date on OS patches at the time of the compromise. Which of the following describes the type of vulnerability that was MOST likely expiated?
* Insider threat
* Buffer overflow
* Advanced persistent threat
* Zero day

NEW QUESTION 154

A security analyst has been asked to scan a subnet. During the scan, the following output was generated:

```
[root@scanbox ~]# nmap 192.168.100.*

Starting Nmap 4.11 (http://www.insecure.org/nmap/) at 2015-10-10 19:10 EST
Interesting ports on purple.company.net (192.168.100.145):
Not shown: 1677 closed ports
PORT        STATE             SERVICE
22/tcp      open              ssh
53/tcp      open              domain
111/tcp     open              rpcbind

Interesting ports on lemonyellow.company.net (192.168.100.214):
Not shown: 1676 closed ports
PORT        STATE             SERVICE
22/tcp      open              ssh
80/tcp      open              http
111/tcp     open              rpcbind
443/tcp     open              ssl/http

Nmapfinished: 256IPaddresses (2hostsup) scannedin7.223 seconds
```


Based on the output above, which of the following is MOST likely?
* 192.168.100.214 is a secure FTP server
* 192.168.100.214 is a web server
* Both hosts are mail servers
* 192.168.100.145 is a DNS server

NEW QUESTION 155

A security analyst is investigating a malware infection that occurred on a Windows system. The system was not connected to a network and had no wireless capability Company policy prohibits using portable media or mobile storage The security analyst is trying to determine which user caused the malware to get onto the system Which of the following registry keys would MOST likely have this information?
* HKEY_USERS<user SID>SoftwareMicrosoftWindowsCurrentVersionRun

* HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionRun
* HKEY_USERS<user SID>SoftwareMicrosoftWindowsexplorerMountPoints2
* HKEY_USERS<user SID>SoftwareMicrosoftInternet ExplorerTyped URLs
* HKEY_LOCAL_MACHINESYSTEMControlSet001serviceseventlogSystemiusb3hub

NEW QUESTION 156

A developer wrote a script to make names and other Pll data unidentifiable before loading a database export into the testing system.

Which of the following describes the type of control that is being used?
* Data encoding
* Data masking
* Data loss prevention
* Data classification

NEW QUESTION 157

An incident response team is responding to a breach of multiple systems that contain PII and PHI. Disclosing the incident to external entities should be based on:
* the responder’s discretion
* the public relations policy
* the communication plan
* senior management’s guidance

NEW QUESTION 158

A company wants to update its acceptable use policy (AUP) to ensure it relates to the newly implemented password standard, which requires sponsored authentication of guest wireless devices. Which of the following is MOST likely to be incorporated in the AUP?
* Sponsored guest passwords must be at least ten characters in length and contain a symbol.
* The corporate network should have a wireless infrastructure that uses open authentication standards.
* Guests using the wireless network should provide valid identification when registering their wireless devices.
* The network should authenticate all guest users using 802.1x backed by a RADIUS or LDAP server.

NEW QUESTION 159

The Chief Information Officer (CIO) of a large healthcare institution is concerned about all machines having direct access to sensitive patient information. Which of the following should the security analyst implement to BEST mitigate the risk of sensitive data exposure?
* A cloud access service broker system
* NAC to ensure minimum standards are met
* MFA on all workstations
* Network segmentation

NEW QUESTION 160

A general contractor has a list of contract documents containing critical business data that are stored at a public cloud provider. The organization’s security analyst recently reviewed some of the storage containers and discovered most of the containers are not encrypted. Which of the following configurations will provide the MOST security to resolve the vulnerability?
* Upgrading TLS 1.2 connections to TLS 1.3
* Implementing AES-256 encryption on the containers

* Enabling SHA-256 hashing on the containers
* Implementing the Triple Data Encryption Algorithm at the file level

NEW QUESTION 161

industry partners from critical infrastructure organizations were victims of attacks on their SCADA devices. The attacks used privilege escalation to gain access to SCADA administration and access management solutions would help to mitigate this risk?
* Multifactor authentication
* Manual access reviews
* Endpoint detection and response
* Role-based access control

NEW QUESTION 162

The help desk has reported that users are reusing previous passwords when prompted to change them.

Which of the following would be the MOST appropriate control for the security analyst to configure to prevent password reuse? (Choose two.)
* Implement mandatory access control on all workstations.
* Implement role-based access control within directory services.
* Deploy Group Policy Objects to domain resources.
* Implement scripts to automate the configuration of PAM on Linux hosts.
* Deploy a single-sing-on solution for both Windows and Linux hosts.

NEW QUESTION 163

The help desk informed a security analyst of a trend that is beginning to develop regarding a suspicious email that has been reported by multiple users. The analyst has determined the email includes an attachment named invoice.zip that contains the following files:

Locky.js

xerty.ini

xerty.lib

Further analysis indicates that when the .zip file is opened, it is installing a new version of ransomware on the devices. Which of the following should be done FIRST to prevent data on the company NAS from being encrypted by infected devices?
* Disable access to the company VPN.
* Email employees instructing them not to open the invoice attachment.
* Set permissions on file shares to read-only.
* Add the URL included in the .js file to the company’s web proxy filter.

Pass CompTIA CS0-002 Exam Quickly With ValidExam: https://www.validexam.com/CS0-002-latest-dumps.html]