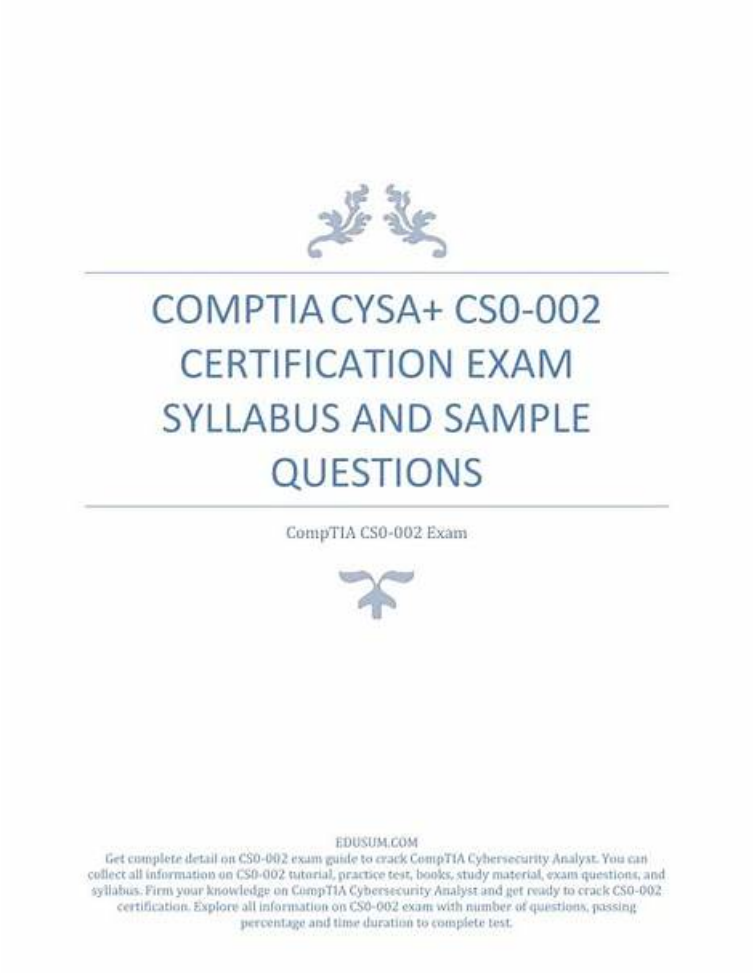
Exam CS0-002 Sample & CS0-002 Pass4sure Dumps Pdf



2025 Latest ActualtestPDF CS0-002 PDF Dumps and CS0-002 Exam Engine Free Share: https://drive.google.com/open?id=1bo8J-OhiiINvo9QvjFTZ8k4b8dqWiskb

Contemporarily, social competitions stimulate development of modern science, technology and business, which revolutionizes our society's recognition to CS0-002 exam and affect the quality of people's life. According to a recent report, those who own more than one skill certificate are easier to be promoted by their boss. To be out of the ordinary and seek an ideal life, we must master an extra skill to get high scores and win the match in the workplace. Our CS0-002 Exam Question can help make your dream come true. What's more, you can have a visit of our website that provides you more detailed information about the CS0-002 guide torrent.

CompTIA CS0-002 Exam consists of 85 multiple-choice and performance-based questions that candidates must answer in 165 minutes. CS0-002 exam is available in English and Japanese, and candidates must achieve a passing score of 750 out of 900 to earn the certification. CS0-002 exam can be taken at any Pearson VUE testing center globally, and candidates can register for the exam on the CompTIA website.

How can you prepare for CompTIA CS0-002 exam?

The candidates can find a wealth of resources to prepare for the CS0-002 exam on the official website. They can purchase the CompTIA Training Bundle directly from the certification webpage. The content of the bundle includes:

- CompTIA CertMaster Learn for Cybersecurity Analyst
- Exam Retake
- Exam Voucher
- CompTIA CertMaster Practice for Cybersecurity Analyst
- Official CySA+ Self-Paced Study Guide (eBook)

CompTIA also offers alternative training options, which include virtual labs, instructor-led training, and video tutorials. The details and links to these learning resources can be found on the official website. Before commencing the preparation process, it is recommended that the applicants first go through the study guide to be able to understand the comprehensive knowledge areas that will be evaluated during the delivery of the exam.

>> Exam CS0-002 Sample <<

100% Pass CS0-002 Marvelous Exam CompTIA Cybersecurity Analyst (CySA+) Certification Exam Sample

Achieving the CompTIA Cybersecurity Analyst (CySA+) Certification Exam (CS0-002) certification can significantly impact your career progression and earning potential. This certification showcases your expertise and knowledge to employers, making you a valuable asset in the CompTIA CS0-002 industry. With the rapidly evolving nature of the CompTIA world, staying up-to-date with the latest technologies and trends is crucial. The CS0-002 Certification Exam enables you to learn these changes and ensures you remain current in your field.

To prepare for the CySA+ certification exam, candidates can take advantage of various training resources available online or in-person. CompTIA offers official training courses and study materials to help candidates prepare for the exam. Additionally, there are several online communities and study groups that candidates can join to get support and guidance from other cybersecurity professionals.

CompTIA Cybersecurity Analyst (CySA+) Certification Exam Sample Questions (Q347-Q352):

NEW QUESTION # 347
An organization has a strict policy that if elevated permissions are needed, users should always run commands under their own account, with temporary administrator privileges if necessary. A security analyst is reviewing syslog entries and sees the following:

```
<100>2 2020-01-10T19:33:41.002Z webserver [illegible] BOM 'su vi httpd.conf' failed for joe
<100>2 2020-01-10T19:33:48.002Z webserver sudo 201 32001 - BOM 'sudo vi httpd.conf' success
<100>2 2020-01-10T20:36:01.010Z financeserver sudo 201 32001 - BOM 'sudo vi users.txt' success
<100>2 2020-01-10T21:18:34.002Z financeserver su 201 32001 - BOM 'su' success
<100>2 2020-01-10T21:53:11.002Z financeserver su 201 32001 - BOM 'su vi syslog.conf failed for joe
```

Which of the following entries should cause the analyst the MOST concern?

- A. <100>2 2020-01-10T20:36:36.0010z financeserver su 201 32001 = BOM ' sudo vi users.txt success
- B. <100> 2020-01-10T19:34..002z financeserver su 201 32001 = BOM ' su vi success
- C. <100> 2020-01-10T19:33:48.002z webserver sudo 201 32001 = BOM ' su vi httpd.conf' success
- D. <100> 2020-01-10T19:33:48.002z webserver sudo 201 32001 = BOM ' su vi syslog.conf failed for jos
- E. <100>2 2020-01-10T19:33:41.002z webserver su 201 32001 = BOM ' su vi httpd.conf' failed for joe

Answer: E

NEW QUESTION # 348
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)
B)
```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
```
C)
D)
```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\System\iusb3hub
```

- A. Option A

- B. Option C
- C. Option B
- D. Option D

Answer: B

NEW QUESTION # 349
When investigating a report of a system compromise, a security analyst views the following /var/log/secure log file:

```
rightness 3484]
Jun 25 11:22:10 localhost gdm-password]: gkr-pam: unlocked login keyring
Jun 25 11:23:02 localhost sudo: pam_unix(sudo:auth): conversation failed
Jun 25 11:23:02 localhost sudo: pam_unix(sudo:auth): auth could not identify password for [comptia]
Jun 25 11:23:04 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; COMMAND=/bin/bash
Jun 25 11:23:09 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; CONMAND=/bin/bash
Jun 25 11:23:16 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=xoot ; COMMAND=/bin/bash
Jun 25 11:23:29 localhost sudo: comptia ; user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; COMMAND=/bin/bash
Jun 25 11:24:13 localhost su: pam_unix(su-l:session): session opened for user root by comptia(uid=1000)
Jun 26 09:50:41 localhost gdm-password]: gkr-pam: unlocked login keyring
```

Which of the following can the analyst conclude from viewing the log file?

- A. The comptia user executed the sudo su command.
- B. The comptia user knows the root password.
- C. The comptia user added himself or herself to the /etc/sudoers file.
- D. The comptia user knows the sudo password.

Answer: B

Explanation:
the user is not in the sudoers file. you use your own password for that. the user used the su command to switch user accounts. when no user is specified, the su command defaults to the root account. the user is now logged into the root account. you need to know the root password to log into the root account.

NEW QUESTION # 350
A security analyst implemented a solution that would analyze the attacks that the organization's firewalls failed to prevent. The analyst used the existing systems to enact the solution and executed the following command:
$ sudo nc -l -v -e maildaemon.py 25 > caplog.txt
Which of the following solutions did the analyst implement?

- A. Log correlation
- B. Crontab mail script
- C. Honeypot
- D. Sinkhole

Answer: C

Explanation:
A) Log correlation is not correct. Log correlation is a process of analyzing and correlating data from multiple sources, such as firewalls, servers, applications, or devices, to identify patterns, trends, or anomalies. Log correlation can help to improve security visibility, detection, and response, but it does not describe the solution that the analyst implemented.
B) Crontab mail script is not correct. Crontab is a tool that allows users to schedule commands or scripts to run at specified times or intervals on a Linux system. A mail script is a script that can send or receive email messages using a mail server. A crontab mail script could be used to automate email tasks, such as sending reports or alerts, but it does not describe the solution that the analyst implemented.
C) Sinkhole is not correct. A sinkhole is a technique that redirects malicious or unwanted traffic to a controlled destination, such as a fake or isolated server. A sinkhole can help to prevent or mitigate the impact of attacks, such as botnets, malware, or phishing, by blocking or capturing the traffic. However, a sinkhole does not describe the solution that the analyst implemented.
1: CompTIA CySA+ Exam: Implementing a Firewall Analysis Solution
Explanation:
The correct answer is D. Honeypot. A honeypot is a security mechanism designed to detect and deflect attempts at unauthorized use of information systems. In this case, the analyst has set up a system to listen on a network port that is commonly used for email traffic. The purpose of this honeypot is to attract attackers and allow the security analyst to observe their behavior and tactics. By monitoring the traffic that is captured in the caplog.txt file, the analyst can identify attacks that were not blocked by the organization's firewalls1.

NEW QUESTION # 351
An application developer needs help establishing a digital certificate for a new application. Which of the following illustrates a certificate management best practice?

- A. Ensure the certificate is requested from a trusted CA.
- B. Ensure the certificate Is applied to the certificate revocation list.
- C. Ensure the developer has self-signed the certificate.
- D. Ensure the certificate key is less than 1028 bits long.
- E. Ensure the certificate key algorithm is SHA-1 compliant.

Answer: A

Explanation:
The best practice for establishing a digital certificate for a new application is to ensure the certificate is requested from a trusted CA. A CA stands for Certificate Authority, and it is an entity that issues and verifies digital certificates, which are electronic documents that contain a public key and a digital signature that prove the identity and authenticity of an application, a website, or a person. Requesting a certificate from a trusted CA can help ensure that the certificate is valid, secure, and recognized by other parties.

NEW QUESTION # 352
.....