EDUSUM

#1 Online Certification Guide

COMPTIA CS0-002 STUDY GUIDE PDF

Grab the CompTIA CySA Plus Certification PDF Questions & Answers

Details of the Exam-Syllabus-Questions

CS0-002

CompTIA Cybersecurity Analyst (CySA+)

85 Questions Exam – 750/900 Cut Score – Duration of 165 minutes

Table of Contents:

Get an Overview of the CS0-002 Certification:

Who should take the **CS0-002 exam**? This is the first question that comes to a candidate's mind when preparing for the CySA Plus certification. The CS0-002 certification is suitable for candidates who are keen to earn knowledge on the Cybersecurity and grab their CompTIA Cybersecurity Analyst (CySA+). When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But CS0-002 study guide PDF is here to solve the problem. CS0-002 PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the CompTIA CS0-002 Certification?

There are several reasons why one should grab the CS0-002 certification.

- The CySA Plus certification proves to be one of the most recognized certifications.
- The certification badge proves the knowledge of the candidate regarding subject matters and makes his resume presentable to potential candidates.
- Thus earning the **CompTIA Cybersecurity Analyst (CySA+)** is a powerful qualification for a prosperous career.

What is the CompTIA CS0-002 CySA Plus Certification Exam Structure?

Exam Name	CompTIA Cybersecurity Analyst (CySA+)
Exam Code	CS0-002
Exam Price	$392 (USD)
Duration	165 mins
Number of Questions	85
Passing Score	750 / 900
Books / Training	**eLearning with CompTIA CertMaster Learn for CySA+ Interactive Labs with CompTIA CertMaster Labs for CySA+**
Schedule Exam	**CompTIA Marketplace**
Sample Questions	**CompTIA CySA+ Sample Questions**
Practice Exam	**CompTIA CS0-002 Certification Practice Exam**

Enhance Knowledge with CS0-002 Sample Questions:

Question: 1

A cybersecurity analyst receives a phone call from an unknown person with the number blocked on the caller ID. After starting conversation, the caller begins to request sensitive information.

Which of the following techniques is being applied?

a) Social engineering
b) Phishing
c) Impersonation
d) War dialing

Answer: a

Question: 2

Given the following logs:

Aug 18 11:00:57 comptia sshd[5657]: Failed password for root from 10.10.10.192 port 38980 ssh2
Aug 18 23:08:26 comptia sshd[5768]: Failed password for root from 18.70.0.160 port 38156 ssh2
Aug 18 23:08:30 comptia sshd[5770]: Failed password for admin from 18.70.0.160 port 38556 ssh2
Aug 18 23:08:34 comptia sshd[5772]: Failed password for invalid user asterisk from 18.70.0.160 port 38864 ssh2
Aug 18 23:08:38 comptia sshd[5774]: Failed password for invalid user sjobeck from 10.10.1.16 port 39157 ssh2
Aug 18 23:08:42 comptia sshd[5776]: Failed password for root from 18.70.0.160 port 39467 ssh2

Which of the following can be suspected?

a) An unauthorized user is trying to gain access from 10.10.10.192.
b) An authorized user is trying to gain access from 10.10.10.192.
c) An authorized user is trying to gain access from 18.70.0.160.
d) An unauthorized user is trying to gain access from 18.70.0.160.

Answer: d

Question: 3

After a security breach, it was discovered that the attacker had gained access to the network by using a brute-force attack against a service account with a password that was set to not expire, even though the account had a long, complex password.

Which of the following could be used to prevent similar attacks from being successful in the future?

a) Complex password policies
b) Account lockout
c) Self-service password reset portal
d) Scheduled vulnerability scans

Answer: b

Question: 4

A security analyst has been asked to review permissions on accounts within Active Directory to determine if they are appropriate to the user's role.

During this process, the analyst notices that a user from building maintenance is part of the Domain Admin group.

Which of the following does this indicate?

a) Cross-site scripting
b) Session hijack
c) Privilege escalation
d) Rootkit

Answer: c

Question: 5

A security analyst wants to capture data flowing in and out of a network. Which of the following would MOST likely assist in achieving this goal?

a) Taking a screenshot.
b) Analyzing network traffic and logs.
c) Analyzing big data metadata.
d) Capturing system image.

Answer: b

Question: 6

Which of the following tools should a cybersecurity analyst use to verify the integrity of a forensic image before and after an investigation?

a) strings
b) sha1sum
c) file
d) dd
e) gzip

Answer: b

Question: 7

In the last six months, a company is seeing an increase in credential-harvesting attacks. The latest victim was the chief executive officer (CEO).

Which of the following countermeasures will render the attack ineffective?

a) Use a complex password according to the company policy.
b) Implement an intrusion-prevention system.
c) Isolate the CEO's computer in a higher security zone.
d) Implement multifactor authentication.

Answer: d

Question: 8

The security analyst determined that an email containing a malicious attachment was sent to several employees within the company, and it was not stopped by any of the email filtering devices.
An incident was declared. During the investigation, it was determined that most users deleted the email, but one specific user executed the attachment.
Based on the details gathered, which of the following actions should the security analyst perform NEXT?

a) Obtain a copy of the email with the malicious attachment. Execute the file on another user's machine and observe the behavior. Document all findings.
b) Acquire a full backup of the affected machine. Reimage the machine and then restore from the full backup.
c) Take the affected machine off the network. Review local event logs looking for activity and processes related to unknown or unauthorized software.
d) Take possession of the machine. Apply the latest OS updates and firmware. Discuss the problem with the user and return the machine.

Answer: c

Question: 9

There are reports that hackers are using home thermostats to ping a national service provider without the provider's knowledge.

Which of the following attacks is occurring from these devices?

a) IoT
b) DDoS
c) MITM
d) MIMO

Answer: b

Question: 10

Which of the following is the main benefit of sharing incident details with partner organizations or external trusted parties during the incident response process?

a) It facilitates releasing incident results, findings and resolution to the media and all appropriate government agencies
b) It shortens the incident life cycle by allowing others to document incident details and prepare reports.
c) It enhances the response process, as others may be able to recognize the observed behavior and provide valuable insight.
d) It allows the security analyst to defer incident-handling activities until all parties agree on how to proceed with analysis.

Answer: c

What Study Guide Works Best in acing the CompTIA CS0-002 CySA Plus Certification?

The CS0-002 study guide is a combination of some proven study tips and the combination of all valuable study materials like sample questions, syllabus and practice tests in one place.

Explore the Syllabus Topics and Learn from the Core:

If you are determined to earn success in the CySA Plus exam, getting in full touch of the **syllabus** is mandatory. During preparation, you might not like all syllabus sections or topics, but try to get at least the fundamental knowledge from the sections you don't like. The more you possess knowledge on all syllabus sections, the more is the chance to attempt maximum number of questions during the actual exam.

Make Your Schedule:

Studying and completing the syllabus becomes easier, if you work on the syllabus topics after making a schedule. Your syllabus must mention what areas you want to cover and within what time. Once you make a schedule and follow it regularly, syllabus completion becomes easier and preparation becomes smoother.

Get Expert Advice from the Training:

Do not forget to join the CompTIA CS0-002 training if it is providing any. Training enhances the practical knowledge of a candidate, which helps them to work well in the practical field during projects.

Get Access to the PDF Sample Questions:

If your study material is in a **PDF format** or the materials are mobile-friendly, what could be better than that? Get access to the free sample questions and keep enhancing your knowledge beyond the syllabus.

Avoid Dumps and utilize the CompTIA CS0-002 Practice Test:

Why should you rely on practice tests? The reason is simple: you must get familiar with the exam pattern before reaching the exam hall. An aspirant aware of the exam structure and time management during the exam preparation can perform well in the actual exam and attempt the maximum number of questions during the exam.
Many aspirants prefer to read from dumps, but they miss out on the self assessment method. Therefore, CS0-002 practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven CS0-002 Practice Test for Success!!!

Do you want to pass the CS0-002 exam on your first attempt? Stop worrying; we, EduSum.com are here to provide you the best experience during your CompTIA Cybersecurity Analyst preparation. Try out our free mock tests to get a glimpse of our quality study materials, and build your confidence with the premium **CS0-002 practice tests**. Our expert-designed questions help you to improve performance and pass the exam on your first attempt.