EDUSUM

#1 Online Certification Guide

COMPTIA CAS-004 STUDY GUIDE PDF

Grab the CompTIA CASP+ Certification PDF Questions & Answers

Details of the Exam-Syllabus-Questions

CAS-004

CompTIA Advanced Security Practitioner (CASP+)

90 Questions Exam – Duration of 165 minutes

Table of Contents:

Get an Overview of the CAS-004 Certification:

Who should take the **CAS-004 exam**? This is the first question that comes to a candidate’s mind when preparing for the CASP+ certification. The CAS-004 certification is suitable for candidates who are keen to earn knowledge on the Cybersecurity and grab their CompTIA Advanced Security Practitioner (CASP+). When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But CAS-004 study guide PDF is here to solve the problem. CAS-004 PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the CompTIA CAS-004 Certification?

There are several reasons why one should grab the CAS-004 certification.

- The CASP+ 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 Advanced Security Practitioner (CASP+)** is a powerful qualification for a prosperous career.

What is the CompTIA CAS-004 CASP+ Certification Exam Structure?

Exam Name	CompTIA Advanced Security Practitioner (CASP+)
Exam Code	CAS-004
Exam Price	$494 (USD)
Duration	165 mins
Number of Questions	90
Passing Score	Pass / Fail
Books / Training	**CASP+ CAS-004**
Schedule Exam	**CompTIA Marketplace** **Pearson VUE**
Sample Questions	**CompTIA CASP+ Sample Questions**
Practice Exam	**CompTIA CAS-004 Certification Practice Exam**

Enhance Knowledge with CAS-004 Sample Questions:

Question: 1

During a security assessment, activities were divided into two phases: internal and external exploitation. The security assessment team set a hard time limit on external activities before moving to a compromised box within the enterprise perimeter.

Which of the following methods is the assessment team most likely to employ NEXT?

a) Pivoting from the compromised, moving laterally through the enterprise, and trying to exfiltrate data and compromise devices
b) Conducting a social engineering attack attempt with the goal of accessing the compromised box physically
c) Exfiltrating network scans from the compromised box as a precursor to social media reconnaissance
d) Open-source intelligence gathering to identify the network perimeter and scope to enable further system compromises

Answer: a

Question: 2

A security engineer is managing operational, excess, and available equipment for a customer. Three pieces of expensive leased equipment, which are supporting a highly confidential portion of the customer network, have recently been taken out of operation. The engineer determines the equipment lease runs for another 18 months.

Which of the following is the BEST course of action for the engineer to take to decommission the equipment properly?

a) Remove any labeling indicating the equipment was used to process confidential data and mark it as available for reuse.
b) Return the equipment to the leasing company and seek a refund for the unused time.
c) Redeploy the equipment to a less sensitive part of the network until the lease expires.
d) Securely wipe all device memory and store the equipment in a secure location until the end of the lease.

Answer: d

Question: 3

Which of the following is the GREATEST security concern with respect to BYOD?

a) The filtering of sensitive data out of data flows at geographic boundaries
b) Removing potential bottlenecks in data transmission paths
c) The transfer of corporate data onto mobile corporate devices
d) The migration of data into and out of the network in an uncontrolled manner

Answer: d

Question: 4

The Chief Information Security Officer (CISO) is concerned that certain systems administrators with privileged access may be reading other users' emails. Review of a tool's output shows the administrators have used web mail to log into other users' inboxes.

Which of the following tools would show this type of output?

a) Log analysis tool
b) Password cracker
c) Command-line tool
d) File integrity monitoring tool

Answer: a

Question: 5

While attending a meeting with the human resources department, an organization's information security officer sees an employee using a username and password written on a memo pad to log into a specific service.

When the information security officer inquires further as to why passwords are being written down, the response is that there are too many passwords to remember for all the different services the human resources department is required to use. Additionally, each password has specific complexity requirements and different expiration time frames.

Which of the following would be the BEST solution for the information security officer to recommend?

a) Utilizing MFA
b) Implementing SSO
c) Deploying 802.1X
d) Pushing SAML adoption
e) Implementing TACACS

Answer: b

Question: 6

Which of the following describes a contract that is used to define the various levels of maintenance to be provided by an external business vendor in a secure environment?

a) NDA
b) MOU
c) BIA
d) SLA

Answer: d

Question: 7

A power outage is caused by a severe thunderstorm and a facility is on generator power. The CISO decides to activate a plan and shut down non-critical systems to reduce power consumption.

Which of the following is the CISO activating to identify critical systems and the required steps?

a) BIA
b) CERT
c) IRP
d) COOP

Answer: c

Question: 8

A Chief Information Security Officer (CISO) is reviewing the controls in place to support the organization's vulnerability management program. The CISO finds patching and vulnerability scanning policies and procedures are in place.

However, the CISO is concerned the organization is siloed and is not maintaining awareness of new risks to the organization. The CISO determines systems administrators need to participate in industry security events.

Which of the following is the CISO looking to improve?

a) Vendor diversification
b) System hardening standards
c) Bounty programs
d) Vulnerability signatures
e) Threat awareness

Answer: e

Question: 9

A pharmaceutical company is considering moving its technology operations from on-premises to externally-hosted to reduce costs while improving security and resiliency.

These operations contain data that includes the prescription records, medical doctors' notes about treatment options, and the success rates of prescribed drugs. The company wants to maintain control over its operations because many custom applications are in use.

Which of the following options represent the MOST secure technical deployment options?

(Select THREE).

a) Single tenancy
b) Multi-tenancy
c) Community
d) Public
e) Private
f) Hybrid
g) Saas
h) Iaas
i) Paas

Answer: a, e, h

Question: 10

During the decommissioning phase of a hardware project, a security administrator is tasked with ensuring no sensitive data is released inadvertently.

All paper records are scheduled to be shredded in a crosscut shredder, and the waste will be burned. The system drives and removable media have been removed prior to e-cycling the hardware.

Which of the following would ensure no data is recovered from the system drives once they are disposed of?

a) Overwriting all HDD blocks with an alternating series of data
b) Physically disabling the HDDs by removing the drive head
c) Demagnetizing the hard drive using a degausser
d) Deleting the UEFI boot loaders from each HDD

Answer: c

What Study Guide Works Best in acing the CompTIA CAS-004 CASP+ Certification?

The CAS-004 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 CASP+ 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 CAS-004 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 CAS-004 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, CAS-004 practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven CAS-004 Practice Test for Success!!!

Do you want to pass the CAS-004 exam on your first attempt? Stop worrying; we, EduSum.com are here to provide you the best experience during your CompTIA Advanced Security Practitioner preparation. Try out our free mock tests to get a glimpse of our quality study materials, and build your confidence with the premium **CAS-004 practice tests**. Our expert-designed questions help you to improve performance and pass the exam on your first attempt.