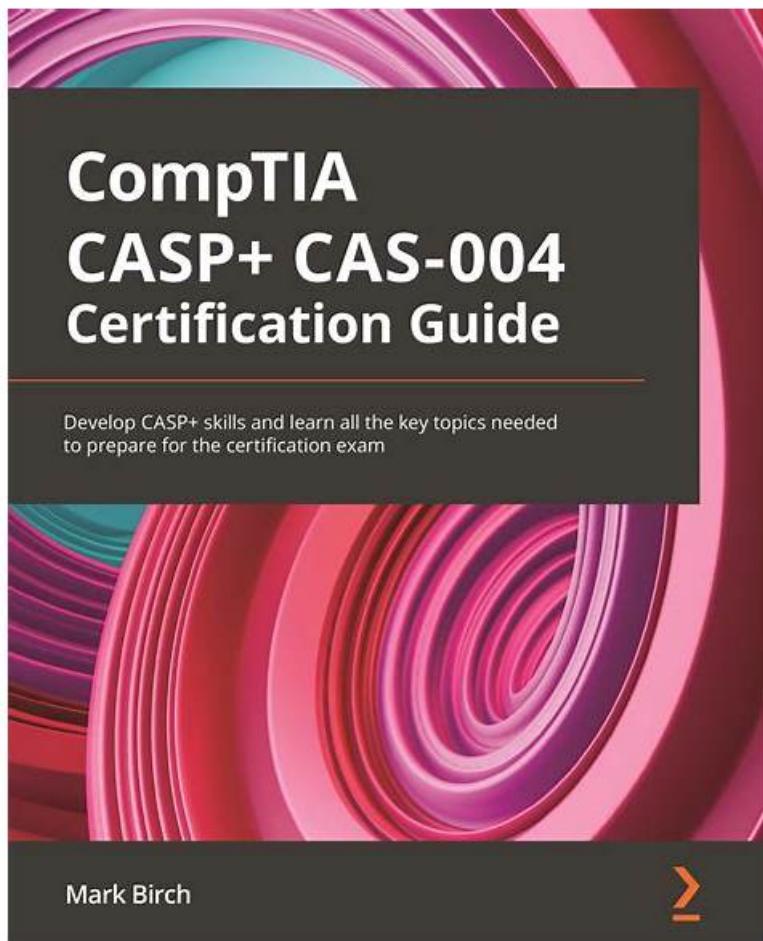


# CompTIA - CAS-004–High Pass-Rate Visual Cert Test



P.S. Free 2025 CompTIA CAS-004 dumps are available on Google Drive shared by PDFTorrent: <https://drive.google.com/open?id=1O38uz1fufyRjXsXoowWcJcOtxGKh-YI>

Get the CompTIA certification to validate your IT expertise and broaden your network to get more improvement in your career. PDFTorrent will help you with its valid and high quality CAS-004 prep torrent. CAS-004 questions & answers are compiled by our senior experts who with rich experience. Besides, we check the update about CAS-004 Training Pdf every day. If there is any update, the newest and latest information will be added into the CAS-004 complete dumps, while the old and useless questions will be removed of the CAS-004 torrent. The hiogh quality and high pass rate can ensure you get high scores in the CAS-004 actual test.

CompTIA CASP+ certification is designed for IT professionals who have at least ten years of experience in IT administration, including at least five years of hands-on technical security experience. CompTIA Advanced Security Practitioner (CASP+) Exam certification is vendor-neutral, which means that it is not tied to any specific technology or product. This makes the certification program ideal for IT professionals who work with a wide range of technologies and systems.

Achieving the CompTIA CASP+ certification demonstrates a high level of expertise in cybersecurity and can open up new career opportunities. CompTIA Advanced Security Practitioner (CASP+) Exam certification is recognized by many employers and government agencies around the world as a valuable credential for cybersecurity professionals.

**>> CAS-004 Visual Cert Test <<**

## Free PDF Quiz CompTIA - Newest CAS-004 Visual Cert Test

These CAS-004 exam questions braindumps are designed in a way that makes it very simple for the candidates. Each and every CAS-004 topic is elaborated with examples clearly. Use PDFTorrent top rate CompTIA CAS-004 Exam Testing Tool for making your success possible. CAS-004 exam preparation is a hard subject. Plenty of concepts get mixed up together due to which student

feel difficult to identify them. There is no similar misconception in CAS-004 Dumps because we have made it more interactive for you. The candidates who are less skilled may feel difficult to understand the CAS-004 questions can take help from these braindumps. The tough topics of CAS-004 certification have been further made easy with examples, simulations and graphs. Candidates can avail the opportunity of demo of free CAS-004 dumps.

## CompTIA Advanced Security Practitioner (CASP+) Exam Sample Questions (Q253-Q258):

### NEW QUESTION # 253

A security architect is designing a solution for a new customer who requires significant security capabilities in its environment. The customer has provided the architect with the following set of requirements:

- \* Capable of early detection of advanced persistent threats.
- \* Must be transparent to users and cause no performance degradation.
- + Allow integration with production and development networks seamlessly.
- + Enable the security team to hunt and investigate live exploitation techniques.

Which of the following technologies BEST meets the customer's requirements for security capabilities? A.

- A. Threat Intelligence
- B. Sandbox detonation
- **C. Deception software**
- D. Centralized logging

### Answer: C

Explanation:

Deception software is a technology that creates realistic but fake assets (such as servers, applications, data, etc.) that mimic the real environment and lure attackers into interacting with them. By doing so, deception software can help detect advanced persistent threats (APTs) that may otherwise evade traditional security tools

12. Deception software can also provide valuable insights into the attacker's tactics, techniques, and procedures (TTPs) by capturing their actions and behaviors on the decoys. Deception software can meet the customer's requirements for security capabilities because:

It is capable of early detection of APTs by creating attractive targets for them and alerting security teams when they are engaged12. It is transparent to users and causes no performance degradation because it does not interfere with legitimate traffic or resources13. It allows integration with production and development networks seamlessly because it can create decoys that match the network topology and configuration. It enables the security team to hunt and investigate live exploitation techniques because it can record and analyze the attacker's activities on the decoys13.

### NEW QUESTION # 254

Device event logs sources from MDM software as follows:

Device	Date/Time	Location	Event	Description
ANDROID_1022	01JAN21 0255	39.9072N, 77.0369W	PUSH	APPLICATION 1220 INSTALLED QUEUED
ANDROID_1022	01JAN21 0301	39.9072N, 77.0369W	INVENTORY	APPLICATION 1220 ADDED
ANDROID_1022	01JAN21 0701	39.0067N, 77.4291W	CHECK-IN	NORMAL
ANDROID_1022	01JAN21 0701	25.2854N, 51.5310E	CHECK-IN	NORMAL
ANDROID_1022	01JAN21 0900	39.0067N, 77.4291W	CHECK-IN	NORMAL
ANDROID_1022	01JAN21 1030	39.0067N, 77.4291W	STATUS	LOCAL STORAGE REPORTING 85% FULL

Which of the following security concerns and response actions would BEST address the risks posed by the device in the logs?

- A. Malicious installation of an application; change the MDM configuration to remove application ID 1220.
- B. Falsified status reporting; remotely wipe the device.
- C. Resource leak; recover the device for analysis and clean up the local storage.
- **D. Impossible travel; disable the device's account and access while investigating.**

### Answer: D

Explanation:

The device event logs show that the device was in two different locations (New York and London) within a short time span (one hour), which indicates impossible travel. This could be a sign of a compromised device or account. The best response action is to disable the device's account and access while investigating the incident. Malicious installation of an application is not evident from the logs, nor is resource leak or falsified status reporting. Verified References: <https://www.comptia.org/blog/what-is-impossible-travel> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

## NEW QUESTION # 255

An analyst reviews the following output collected during the execution of a web application security assessment:

```
Start 2022-08-30 12:23:02 --> 10.5.1.66:443 <--  
rDNS (10.5.1.66): HRdatabase.int.comptia.org  
Service detected: HTTP  
Testing protocols via sockets except NPN+ALPN  
SSLv3 not offered (OK)  
TLS 1 offered (deprecated)  
TLS 1.1 not offered  
TLS 1.2 not offered and downgraded to a weaker protocol  
TLS 1.3 offered and downgraded to a weaker protocol  
NPN/SPDY not offered  
ALPN/HTTP2 not offered  
Testing cipher categories  
NULL ciphers (no encryption) not offered  
Anonymous NULL Ciphers (no authentication) not offered  
Export ciphers (w/o ADH+NULL) not offered  
LOW: 64 Bit + DES, RC[2,4] (*/* export) not offered  
Triple DES Ciphers / 3DES not offered  
Obsolete CBC ciphers (AES, ARIA etc.) offered  
Strong encryption (AES ciphers) not offered  
Testing robust (perfect) forward secrecy, (P)FS  
No ciphers supporting Forward Secrecy offered  
Testing server preferences  
Has server cipher order? no  
Negotiated protocol TLSv1  
Negotiated cipher AES256-SHA (limited sense as client will pick)
```

Which of the following attacks would be most likely to succeed, given the output?

- A. On-path forced renegotiation to insecure ciphers
- B. Availability attack from manipulation of associated authentication data
- C. NULL and unauthenticated cipher downgrade attack
- D. Padding oracle attack

**Answer: D**

Explanation:

Based on the output in the image, which shows weak cipher suites and vulnerabilities related to encryption padding, the padding oracle attack is the most likely. This type of attack exploits the way padding errors are handled during decryption, potentially allowing an attacker to decrypt sensitive information. The weak cipher suites and lack of forward secrecy further increase the likelihood of such an attack succeeding. CASP+ highlights padding oracle attacks as critical vulnerabilities, particularly in environments where weak encryption protocols are used.

References:

CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Encryption and Padding Oracle Attacks)  
CompTIA CASP+ Study Guide: Cryptographic Attacks and Cipher Vulnerabilities

## NEW QUESTION # 256

Which of the following provides the best solution for organizations that want to securely back up the MFA seeds for its employees in a central, offline location with minimal management overhead?

- A. Secrets management
- B. Key escrow service
- C. Encrypted database
- D. Hardware security module

**Answer: D**

Explanation:

A Hardware Security Module (HSM) provides the best solution for securely backing up MFA seeds in a central, offline location with minimal management overhead. HSMs are specialized hardware devices designed for cryptographic key management, including storing sensitive data like MFA seeds securely. HSMs offer high levels of protection against tampering and provide offline security, making them an ideal choice for backing up cryptographic materials. CASP+ recognizes HSMs as critical components for managing and securing cryptographic keys in centralized, secure environments.

References:

\* CASP+ CAS-004 Exam Objectives: Domain 3.0 - Enterprise Security Architecture (HSM and Secure Key Management)

### NEW QUESTION # 257

A remote user reports the inability to authenticate to the VPN concentrator.

During troubleshooting, a security administrate captures an attempted authentication and discovers the following being presented by the user's VPN client:

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      10:e6:fc:62:b7:41:8a:d5:00:5e:45:b6
    Signature Algorithm: sha256WithRSAEncryption
      Issuer: C=BE, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation
      CA - SHA256 - G2
    Validity
      Not Before: Nov 21 08:00:00 2017 GMT
      Not After: Nov 22 07:59:59 2021 GMT
    Subject: C=US, ST=Illinois, L=Chicago, O=Employee1
    Subject Public Key Info:
      Public Key Algorithm: id-ecPublicKey
        Public-Key: (256 bit)
        pub:
          04:c9:22:69:31:8a:d6:6c:ea:da:c3:7f:2c:ac:a5:
          af:c0:02:ea:81:cb:65:b9:fd:0c:6d:46:5b:c9:1e:
          ed:b2:ac:2a:1b:4a:ec:80:7b:e7:1a:51:e0:df:f7:
          c7:4a:20:7b:91:4b:20:07:21:ce:cf:68:65:8c:c6:
          9d:3b:ef:d5:c1
        ASN1 OID: prime256v1
        NIST CURVE: p-256
  X509v3 extensions:
    X509v3 Key Usage: critical
      Certificate Sign, CRL Sign
    Authority Information Access:
      CA Issuers - URI:http://secure.globalsign.com/cacert/
      gsorganizationvalsha2g2r1.crt
      OCSP - URI: http://ocsp2.globalsign.com/gsorganizationvalsha2g2
  X509v3 Certificate Policies:
    Policy: 1.3.6.1.4.1.4146.1.20
    CPS: https://www.globalsign.com/repository
    Policy: 2.23.140.1.2.2
  X509v3 Basic Constraints:
    CA:FALSE
  X509v3 CRL Distribution Points:
    Full Name:
      URI:http://crl.globalsign.com/gs/gsorganizationvalsha2g2r1.crl
  X509v3 Subject Key Identifier:
    11:2A:23:2A:33:8B:1B:CE:B1:D6:AB:55:EF:D7:67:21:2C:94:5C:54
  X509v3 Authority Key Identifier:
    keyid:12:DE:51:F1:BD:1C:11:22:33:1C:C0:CC:7D:2B:38:00:30:E6:1A:7C
  Signature Algorithm: sha256WithRSAEncryption
  5b:c2:ed:d1:39:6f:af:40:27:bd:1e:18:3e:30:54:23:53:
  ...

```

Which of the following BEST describes the reason the user is unable to connect to the VPN service?

- A. The user's certificate was created using insecure encryption algorithms
- B. The user's certificate has been compromised and should be revoked.
- C. The user's certificate is not signed by the VPN service provider
- D. The user's certificate was not created for VPN use

**Answer: B**

### NEW QUESTION # 258

.....

Therefore, you have the option to use CompTIA CAS-004 PDF questions anywhere and anytime. CAS-004 dumps are designed according to the CompTIA Advanced Security Practitioner (CASP+) Exam (CAS-004) certification exam standard and have

hundreds of questions similar to the actual CAS-004 Exam. PDFTorrent CompTIA Advanced Security Practitioner (CASP+) Exam (CAS-004) web-based practice exam software also works without installation.

**Guaranteed CAS-004 Passing:** <https://www.pdftorrent.com/CAS-004-exam-prep-dumps.html>

- 100% Pass 2025 CAS-004 Visual Cert Test - CompTIA Advanced Security Practitioner (CASP+) Exam Guaranteed Passing □ Open website ➔ [www.itcerttest.com](http://www.itcerttest.com) □□□ and search for 「 CAS-004 」 for free download □Exam CAS-004 Simulations
- CAS-004 Exam Consultant □ CAS-004 Trustworthy Exam Torrent □ CAS-004 Valid Test Book □ Copy URL ➔ [www.pdfvce.com](http://www.pdfvce.com) □ open and search for □ CAS-004 □ to download for free □CAS-004 Exam Consultant
- CAS-004 Dumps Questions □ Exam CAS-004 Simulations □ CAS-004 Simulated Test □ Search on [ [www.tests dumps.com](http://www.tests dumps.com) ] for ➤ CAS-004 □ to obtain exam materials for free download □CAS-004 Trustworthy Exam Torrent
- Exam Sample CAS-004 Questions □ Exam Dumps CAS-004 Zip □ Hot CAS-004 Spot Questions \* Open website ➔ [www.pdfvce.com](http://www.pdfvce.com) □ and search for ➔ CAS-004 □ for free download □CAS-004 Dumps Questions
- Free PDF Quiz CompTIA - Unparalleled CAS-004 Visual Cert Test \* Easily obtain free download of 【 CAS-004 】 by searching on ➤ [www.examsreviews.com](http://www.examsreviews.com) □ □Reliable Test CAS-004 Test
- Exam CAS-004 Simulations □ Reliable Test CAS-004 Test □ Test CAS-004 Sample Questions □ Search for ➔ CAS-004 □ and download it for free immediately on □ [www.pdfvce.com](http://www.pdfvce.com) □ □Reliable CAS-004 Braindumps
- CAS-004 CompTIA Advanced Security Practitioner (CASP+) Exam For Guaranteed Success □ Enter 《 [www.getvalidtest.com](http://www.getvalidtest.com) 》 and search for ➤ CAS-004 □ to download for free □Exam Dumps CAS-004 Zip
- Pass Guaranteed Professional CompTIA - CAS-004 Visual Cert Test □ Search for ➔ CAS-004 □□□ and easily obtain a free download on □ [www.pdfvce.com](http://www.pdfvce.com) □ □CAS-004 Dumps Questions
- Reliable CAS-004 Braindumps Book □ Reliable CAS-004 Braindumps ✧ CAS-004 Pass Leader Dumps □ Open ➔ [www.testkingpdf.com](http://www.testkingpdf.com) ≈ enter ▷ CAS-004 ◁ and obtain a free download □Reliable CAS-004 Braindumps
- CAS-004 exams questions and answers - dumps PDF for CompTIA Advanced Security Practitioner (CASP+) Exam □ Immediately open □ [www.pdfvce.com](http://www.pdfvce.com) □ and search for ➔ CAS-004 □ to obtain a free download □Reliable CAS-004 Braindumps
- CAS-004 Dumps Questions □ Exam Dumps CAS-004 Zip □ Test CAS-004 Sample Questions □ The page for free download of ➔ CAS-004 □ on “ [www.itcerttest.com](http://www.itcerttest.com) ” will open immediately □Braindumps CAS-004 Pdf
- cursuri-serviciihr.ro, studison.kakdemo.com, daotao.wisebusiness.edu.vn, kalamlearning.com, shortcourses.russellcollege.edu.au, knowara.com, mikemil988.develop-blog.com, ncon.edu.sa, learning.cynaris.click, dataclick.in

P.S. Free 2025 CompTIA CAS-004 dumps are available on Google Drive shared by PDFTorrent: <https://drive.google.com/open?id=1O38uz1fufyRjXsXoowWcJcOtxGKh-YI>