

# Dump CompTIA CAS-004 Check - Latest CAS-004 Practice Materials



What's more, part of that ActualCollection CAS-004 dumps now are free: <https://drive.google.com/open?id=1M4vuxpJkr4nzu4Dq6HqIU3x8NNQho7S>

Our CAS-004 exam torrent will not only help you clear exam in your first try, but also enable you prepare exam with less time and effort. There are CAS-004 free download trials for your reference before you buy and you can check the accuracy of our questions and answers. Try to Practice CAS-004 Exam Pdf with our test engine and you will get used to the atmosphere of the formal test easily.

## What is the salary of an CompTIA CAS-004 Certified professional?

The Average salary of different countries of CompTIA CAS-004 Certified professional:

- United States \$85,400
- Germany €53,800
- United Kingdom £63,000
- Australia AUS \$58,000

>> **Dump CompTIA CAS-004 Check** <<

## Latest CAS-004 Practice Materials, PDF CAS-004 VCE

ActualCollection believes in customer satisfaction and strives hard to make the entire CompTIA CAS-004 exam preparation process simple, smart, and successful. These CompTIA CAS-004 exam questions formats are CompTIA CAS-004 Pdf Dumps file, desktop practice test software and web-based practice test software. All these three ActualCollection's CompTIA CAS-004 exam dumps formats contain the real and updated CAS-004 practice test.

## Why is the CompTIA CAS-004 certification difficult to write?

The CompTIA CAS-004 exam is difficult to write because it tests your knowledge of today's complex computer technologies not your knowledge of those technologies from 4 years ago. Many IT professionals have complained that the CompTIA CAS-004 certification exam doesn't adequately test your knowledge of today's complex computer technologies and as a result they end up having to retake the exam several times before they pass.

Preparing for the CompTIA CAS-004 Exam requires a significant amount of study and practice. Candidates are advised to use a variety of study materials, including textbooks, online courses, and practice exams. They should also gain hands-on experience in configuring and implementing security solutions in real-world environments. By passing the CompTIA CAS-004 exam, candidates can demonstrate their advanced skills and knowledge in cybersecurity, increase their career opportunities, and contribute to the protection of organizations against cyber threats.

## CompTIA Advanced Security Practitioner (CASP+) Exam Sample Questions (Q264-Q269):

### NEW QUESTION # 264

Which of the following BEST describes a common use case for homomorphic encryption?

- A. Transmitting confidential data to a CSP for processing on a large number of resources without revealing information
- B. Maintaining the confidentiality of data both at rest and in transit to and from a CSP for processing
- C. Processing data on a server after decrypting in order to prevent unauthorized access in transit
- D. Storing proprietary data across multiple nodes in a private cloud to prevent access by unauthenticated users

**Answer: A**

Explanation:

Homomorphic encryption is principally used to share privacy-sensitive data sets. When a company collects private data, it is responsible for keeping the data secure and respecting the privacy rights of individual data subjects. Companies often want to use third parties to perform analysis, however. Sharing unencrypted data in this scenario is a significant risk. Homomorphic encryption is a solution for this as it allows the receiving company to perform statistical calculations on fields within the data while keeping the data set as a whole encrypted. In another example, performing analysis on sensitive medical data (such as DNA) can be performed to reveal important statistical or other analytic information without exposing sensitive information.

### NEW QUESTION # 265

#### SIMULATION

You are a security analyst tasked with interpreting an Nmap scan output from company's privileged network.

The company's hardening guidelines indicate the following:

There should be one primary server or service per device.

Only default ports should be used.

Non-secure protocols should be disabled.

#### INSTRUCTIONS

Using the Nmap output, identify the devices on the network and their roles, and any open ports that should be closed.

For each device found by Nmap, add a device entry to the Devices Discovered list, with the following information:

The IP address of the device

The primary server or service of the device (Note that each IP should be associated with one service/port only) The protocol(s) that should be disabled based on the hardening guidelines (Note that multiple ports may need to be closed to comply with the hardening guidelines) If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

□

**Answer:**

Explanation:

10.1.45.65 SFTP Server Disable 8080

10.1.45.66 Email Server Disable 415 and 443

10.1.45.67 Web Server Disable 21, 80

10.1.45.68 UTM Appliance Disable 21

### NEW QUESTION # 266

A company is outsourcing to an MSSP that performs managed detection and response services.

The MSSP requires a server to be placed inside the network as a log aggregator and allows remote access to MSSP analyst. Critical devices send logs to the log aggregator, where data is stored for 12 months locally before being archived to a multitenant cloud. The data is then sent from the log aggregator to a public IP address in the MSSP datacenter for analysis. A security engineer is concerned about the security of the solution and notes the following.

- The critical device send cleartext logs to the aggregator.
- The log aggregator utilize full disk encryption.
- The log aggregator sends to the analysis server via port 80.
- MSSP analysis utilize an SSL VPN with MFA to access the log aggregator remotely.
- The data is compressed and encrypted prior to being achieved in the cloud.

Which of the following should be the engineer's GREATEST concern?

- A. Hardware vulnerabilities introduced by the log aggregate server
- **B. Encryption of data in transit**
- C. Multitenancy and data remnants in the cloud
- D. Network bridging from a remote access VPN

**Answer: B**

Explanation:

Encryption of data in transit should be the engineer's greatest concern regarding the security of the solution. Data in transit refers to data that is being transferred over a network or between devices. If data in transit is not encrypted, it can be intercepted, modified, or stolen by attackers who can exploit vulnerabilities in the network protocols or devices. The solution in the question sends logs from the critical devices to the aggregator in cleartext and from the aggregator to the analysis server via port 80, which are both insecure methods that expose the data to potential attacks.

### NEW QUESTION # 267

A security analyst is reviewing the following output:

Which of the following would BEST mitigate this type of attack?

- A. Deploying a honeypot
- **B. Placing a WAF inline**
- C. Installing a network firewall
- D. Implementing an IDS

**Answer: B**

Explanation:

The output shows a SQL injection attack that is trying to exploit a web application. A WAF (Web Application Firewall) is a security solution that can detect and block malicious web requests, such as SQL injection, XSS, CSRF, etc. Placing a WAF inline would prevent the attack from reaching the web server and database.

References: [https://owasp.org/www-community/attacks/SQL\\_Injection](https://owasp.org/www-community/attacks/SQL_Injection) <https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/>

### NEW QUESTION # 268

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

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

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

**Answer: A**

Explanation:

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