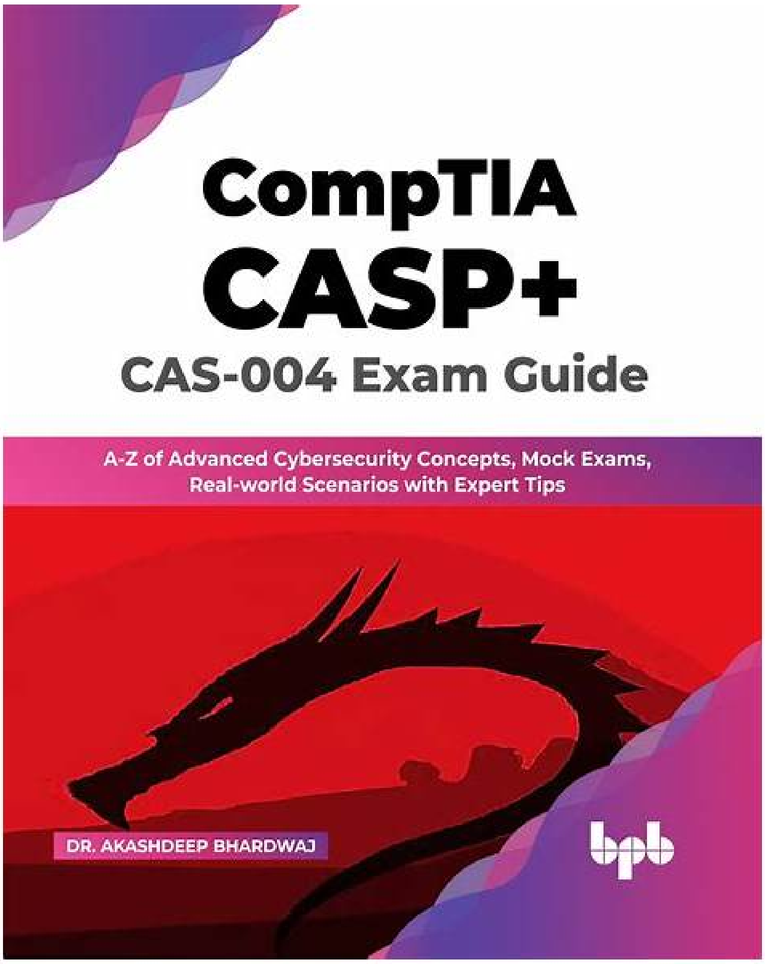
Ace CompTIA CAS-004 Exam Instantly with This Tried-and-Tested Method


CompTIA
CASP+
CAS-004 Exam Guide
A-Z of Advanced Cybersecurity Concepts, Mock Exams, Real-world Scenarios with Expert Tips
DR. AKASHDEEP BHARDWAJ
bpb

P.S. Free & New CAS-004 dumps are available on Google Drive shared by Real4test: https://drive.google.com/open?id=1XiTESVP7AVpqDHKQCsFo31r8IQpwJYWR

The Practice Exam software is specially made for the students so they can feel real-based examination scenarios and feel some pressure on their brains and don't feel excessive issues while giving the final CompTIA exam. There are a lot of customers that are currently using CompTIA Advanced Security Practitioner (CASP+) Exam (CAS-004) and are satisfied with it. Real4test has designed this product after getting positive feedback from professionals and is rated one of the best study materials for the preparation of the CompTIA CAS-004 exam.

CompTIA CAS-004 Exam is aimed at professionals who are looking to take their cybersecurity skills to the next level. CAS-004 exam is designed to test the candidate's ability to analyze and solve complex security problems, as well as their ability to design and implement advanced security solutions. CompTIA Advanced Security Practitioner (CASP+) Exam certification is ideal for individuals who are looking to advance their careers in the cybersecurity field, as it is recognized by a wide range of organizations and employers.

The CASP+ certification is recognized by major corporations and government agencies around the world. It is highly valued by employers who are looking for professionals with advanced cybersecurity skills. CompTIA Advanced Security Practitioner (CASP+) Exam certification is also recognized by the U.S. Department of Defense (DoD) and meets the requirements of the DoD 8570.01-M for Information Assurance Manager Level III and Information Assurance Technical Level III.

>> CAS-004 Guide <<

2025 CAS-004 Guide | High-quality CompTIA CAS-004: CompTIA Advanced

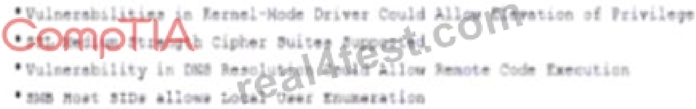
Security Practitioner (CASP+) Exam 100% Pass

Now, if you use CAS-004 preparation materials, you only need to learn twenty to thirty hours to go to the exam. And, you will have a 99% chance to pass the exam. Of course, you don't have to buy any other study materials. CAS-004 exam questions can satisfy all your learning needs. During this time, you must really be learning. If you just put CAS-004 Real Exam in front of them and didn't look at them, then we have no way. CAS-004 exam questions want to work with you to help you achieve your dreams.

CompTIA CAS-004 exam focuses on the latest trends and technologies in the field of IT security. CAS-004 exam covers topics such as risk management, enterprise security architecture, research and analysis, and integration of computing, communications, and business disciplines. CAS-004 Exam validates the candidate's ability to design, implement, and manage complex security solutions that meet the needs of their organization.

CompTIA Advanced Security Practitioner (CASP+) Exam Sample Questions (Q360-Q365):

NEW QUESTION # 360
An analyst execute a vulnerability scan against an internet-facing DNS server and receives the following report:



```
•Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege
•SSL Medium Strength Cipher Suites Supported
•Vulnerability in DNS Resolution Could Allow Remote Code Execution
•SMB Host SIDs allows Local User Enumeration
```

Which of the following tools should the analyst use FIRST to validate the most critical vulnerability?

- A. Account enumerator
- B. Password cracker
- C. Exploitation framework
- D. Port scanner

Answer: B

NEW QUESTION # 361
A vulnerability analyst identified a zero-day vulnerability in a company's internally developed software. Since the current vulnerability management system does not have any checks for this vulnerability, an engineer has been asked to create one.
Which of the following would be BEST suited to meet these requirements?

- A. OVAL
- B. ISACs
- C. Node.js
- D. ARF

Answer: A

Explanation:
Explanation
OVAL (Open Vulnerability and Assessment Language) is a standard that would be best suited for creating checks for a zero-day vulnerability in an organization's internally developed software. OVAL is a standard for expressing system configuration information and vulnerabilities in an XML format, allowing interoperability and automation among different security tools and platforms. An engineer can use OVAL to create definitions or tests for specific vulnerabilities or states in the software, and then use OVAL-compatible tools to scan or evaluate the software against those definitions or tests. ARF (Asset Reporting Format) is not a standard for creating checks for vulnerabilities, but a standard for expressing information about assets and their characteristics in an XML format, allowing interoperability and automation among different security tools and platforms. ISACs (Information Sharing and Analysis Centers) are not standards for creating checks for vulnerabilities, but organizations that collect, analyze, and disseminate information about threats, vulnerabilities, incidents, or best practices among different sectors or communities. Node.js is not a standard for creating checks for vulnerabilities, but a runtime environment that allows executing JavaScript code outside of a web browser, enabling the development of scalable web applications or services. Verified References:
https://www.comptia.org/blog/what-is-oval
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION # 362

A developer wants to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users. Which of the following would be BEST for the developer to perform? (Choose two.)

- A. Make the DACL read-only.
- B. Compress the program with a password.
- C. Implement certificate-based authentication.
- D. Encrypt with 3DES.
- E. Verify MD5 hashes.
- F. Utilize code signing by a trusted third party.

Answer: A,F

Explanation:
Utilizing code signing by a trusted third party and making the DACL (discretionary access control list) read- only are actions that the developer can perform to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users. Code signing is a technique that uses digital signatures to verify the authenticity and integrity of code, preventing unauthorized modifications or tampering. A trusted third party, such as a certificate authority, can issue and validate digital certificates for code signing. A DACL is an attribute of an object that defines the permissions granted or denied to users or groups for accessing or modifying the object. Making the DACL read-only can prevent unauthorized users or groups from changing the permissions or accessing the code. Implementing certificate-based authentication is not an action that the developer can perform to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users, but a method for verifying the identity of users or devices based on digital certificates, preventing unauthorized access or impersonation. Verifying MD5 hashes is not an action that the developer can perform to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users, but a method for checking the integrity of files based on cryptographic hash functions, detecting accidental or intentional changes or corruption. Compressing the program with a password is not an action that the developer can perform to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users, but a method for reducing the size of files and protecting them with a password, preventing unauthorized access or extraction. Encrypting with 3DES is not an action that the developer can perform to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users, but a method for protecting the confidentiality of data based on symmetric-key encryption algorithms, preventing unauthorized disclosure or interception. Verified References: https://www.comptia.org/blog/what-is-code-signing
https://partners.comptia.org/docs/default- source/resources/casp-content-guide

NEW QUESTION # 363

The risk subcommittee of a corporate board typically maintains a master register of the most prominent risks to the company. A centralized holistic view of risk is particularly important to the corporate Chief Information Security Officer (CISO) because:

- A. risks introduced by a system in one business unit can affect other business units in ways in which the individual business units have no awareness
- B. major risks identified by the subcommittee merit the prioritized allocation of scare funding to address cybersecurity concerns
- C. corporate general counsel requires a single system boundary to determine overall corporate risk exposure
- D. IT systems are maintained in silos to minimize interconnected risks and provide clear risk boundaries used to implement compensating controls

Answer: A

Explanation:
A - No - "Risk" does not necessarily mean IT systems, the Risk committee addresses all forms of risk.
B - Yes - For example, one entity outsourcing the management of some systems that other entities may have strict controls over access (PII for example) C - No - The GC can consolidate individual IT risks from the individual entities with their overall risk and then consolidate the entities for themselves.
D - No - Prioritising risks is the job of the sub-committee, but does not require a CISO for this.

NEW QUESTION # 364

Due to internal resource constraints, the management team has asked the principal security architect to recommend a solution that shifts most of the responsibility for application-level controls to the cloud provider. In the shared responsibility model, which of the following levels of service meets this requirement?

- A. PaaS
- B. SaaS
- C. IaaS
- D. FaaS

Answer: B

Explanation:
Software as a Service (SaaS) is a cloud computing model in which a third-party provider hosts and manages the application and makes it available to customers over the internet. In a SaaS model, the cloud provider is responsible for the security of the infrastructure and the application itself, while the customer is responsible for securing their data and user access to the application. This means that the customer can shift partial responsibility for application-level controls to the cloud provider.

NEW QUESTION # 365
......