CISSP試験番号 & CISSP練習問題集

BONUS！！！ ShikenPASS CISSPダンプの一部を無料でダウンロード：https://drive.google.com/open?id=1aHrqrR0QixJlxl-1jkis2ZqWRX5uN5fD

CISSPテストトレントは高品質で、主に合格率に反映されます。 CISSPテストトレントは、過去数年間の試験問題と業界動向に基づいて、業界の専門家によって慎重に編集されています。さらに重要なことは、時間の変化に基づいてCISSP試験資料を速やかに更新し、タイムリーに送信することです。教材を使用している人の99％が試験に合格し、証明書に合格しています。これは、間違いなく、CISSPテストトレントの合格率が99％であることを示しています。

ISC CISSP（認定情報システムセキュリティプロフェッショナル）認定試験は、情報セキュリティの専門家向けの世界的に認められた認定です。認定試験は、情報セキュリティの分野での個人の知識、スキル、および経験をテストするように設計されています。認定試験では、リスク管理、資産セキュリティ、セキュリティエンジニアリング、コミュニケーション、ネットワークセキュリティなど、幅広いトピックをカバーしています。

CISSP認定を取得することは、個人のキャリアの見通しを高め、収益の可能性を高めることができる重要な成果です。雇用主とクライアントに、個人が包括的な情報セキュリティプログラムの設計、開発、管理に必要な知識とスキルを持っていることを示しています。この認定は、チーフ情報セキュリティ責任者（CISO）やセキュリティコンサルタントなど、多くの高レベルの情報セキュリティの役割の要件でもあります。全体として、CISSP認定は、情報セキュリティのキャリアを追求している人にとって貴重な資産です。

>> CISSP試験番号 <<

信頼できるCISSP試験番号 & 合格スムーズCISSP練習問題集 | 実際的なCISSP資格講座

当代社会の競争が激しいとともに、自分の生きがいを探すために、できるだけ自分の能力を生かさなければならない。IT業界でのあなたは自分の能力を高めるために、CISSP試験を準備しているのでしょう。我々はCISSP試験に参加するつもりのあなたに最高のサービスを提供します。我々の提供するCISSP問題集を利用して、あなたは試験に合格することができると信じています。

ISC Certified Information Systems Security Professional (CISSP) 認定 CISSP 試験問題 (Q1211-Q1216):

質問 # 1211
An attacker has intruded into the source code management system and is able to download but not modify the code. Which of the following aspects of the code theft has the HIGHEST security impact?

- A. Administrative credentials or keys hard-coded within the stolen code could be used to access sensitive data.
- B. Competitors might be able to steal the organization's ideas by looking at the stolen code.
- C. The attacker could publicly share confidential comments found in the stolen code.
- D. A competitor could run their own copy of the organization's website using the stolen code.

正解：A

解説：

The aspect of the code theft that has the highest security impact is that administrative credentials or keys hard-coded within the stolen code could be used to access sensitive data. Administrative credentials or keys are the usernames, passwords, or encryption keys that grant access to the system or the application, and that allow the execution of privileged or critical functions, such as configuration, backup, update, or troubleshooting. Hard-coding is a practice of embedding the administrative credentials or keys within the source code of the system or the application, rather than storing them in a separate or external file or database. Hard-coding is considered as a bad or insecure practice, as it exposes the administrative credentials or keys to anyone who can view or access the source code, and it makes them difficult to change or update. If an attacker has intruded into the source code management system and is able to download the code, they could find the administrative credentials or keys hard-coded within the code, and use them to access sensitive data or compromise the system or the application. This is the aspect of the code theft that has the highest security impact, as it could result in data breach, data loss, data corruption, or system damage. The attacker could publicly share confidential comments found in the stolen code, competitors might be able to steal the organization's ideas by looking at the stolen code, or a competitor could run their own copy of the organization's website using the stolen code are not the aspects of the code theft that have the highest security impact, as they are not directly related to the access or the protection of the sensitive data or the system. The attacker could publicly share confidential comments found in the stolen code, which could reveal some information or insights about the organization's plans, strategies, or challenges, but this would not compromise the data or the system. Competitors might be able to steal the organization's ideas by looking at the stolen code, which could affect the organization's competitive advantage, innovation, or reputation, but this would not compromise the data or the system. A competitor could run their own copy of the organization's website using the stolen code, which could create confusion, deception, or infringement, but this would not compromise the data or the system. References: Official (ISC)2 Guide to the CISSP CBK, Fifth Edition, Chapter 21: Software Development Security, page 2015.

質問 # 1212
Data which is properly secured and can be described with terms like genuine or not corrupted from the original refers to data that has a high level of what?

- A. Authenticity
- B. Availability
- C. Authorization
- D. Non-Repudiation

正解：A

解説：
Explanation/Reference:
Explanation:
Authenticity is a close relative of authentication. Authenticity is the process of ensuring that a message received is the same message that was sent and has not been tampered with or altered. Lawyers, as a real-world case in point, are fanatical about ensuring that evidence is authentic and has not been tampered with or altered in any way to ensure a fair hearing for the accused.
Incorrect Answers:
B: Authorization is the rights and permissions granted to an individual (or process), which enable access to a computer resource. Once a user's identity and authentication are established, authorization levels determine the extent of system rights that an operator can hold. This is not what is described in the question.
C: Availability ensures the reliable and timely access to data or computing resources by the appropriate personnel. In other words, availability guarantees that the systems are up and running when they are needed. In addition, this concept guarantees that the security services needed by the security practitioner are in working order. This is not what is described in the question.
D: Nonrepudiation is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated. This is not what is described in the question.
References:
http://www.yourdictionary.com/authenticity

質問 # 1213
Which access control model is BEST suited in an environment where a high security level is required and where it is desired that only the administrator grants access control?

- A. TACACS
- B. MAC
- C. Access control matrix

- D. DAC

正解：B

解説：
Explanation/Reference:
Explanation:
MAC systems are generally very specialized and are used to protect highly classified data. Users require the correct security clearance to access a specific classification of data.
Incorrect Answers:
A: Discretionary Access Control (DAC) allows data owners to dictate what subjects have access to the files and resources they own.
C: An access control matrix is a table of subjects and objects indicating the actions individual subjects are allowed to take on individual objects.
D: TACACS is a remote access protocol, not an access control model.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, pp. 220-237

質問 # 1214
Which one of the following security mechanisms provides the BEST way to restrict the execution of privileged procedures?

- A. Application hardening
- B. Federated Identity Management (IdM)
- C. Role Based Access Control (RBAC)
- D. Biometric access control

正解：C

質問 # 1215
Which choice below MOST accurately describes the organization's responsibilities during an unfriendly termination?

- A. System access should be removed as quickly as possible after termination.
- B. Physical removal from the offices would never be necessary.
- C. The employee should be given time to remove whatever files he needs from the network.
- D. Cryptographic keys can remain the employee's property.

正解：A

解説：
Friendly terminations should be accomplished by implementing a standard set of procedures for outgoing or transferring employees.
This normally includes:
Removal of access privileges, computer accounts, authentication tokens.
The control of keys.
The briefing on the continuing responsibilities for confidentiality and privacy.
Return of property.
Continued availability of data. In both the manual and the electronic worlds this may involve documenting procedures or filing schemes, such as how documents are stored on the hard disk, and how they are backed up. Employees should be instructed whether or not to clean up their PC before leaving.
If cryptography is used to protect data, the availability of cryptographic keys to management personnel must be ensured.
Given the potential for adverse consequences during an unfriendly termination, organizations should do the following:

System access should be terminated as quickly as possible when an employee is leaving a position under less-than-friendly terms.
If employees are to be fired, system access should be removed at the same time (or just before) the employees are notified of their dismissal.
When an employee notifies an organization of the resignation and it can be reasonably expected that it is on unfriendly terms, system access should be immediately terminated.
During the notice of termination period, it may be necessary to assign the individual to a restricted area and function. This may be particularly true for employees capable of changing programs or modifying the system or applications.
In some cases, physical removal from the offices may be necessary.
Source: NIST Special Publication 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems.

質問 # 1216
......

id=1aHrqrR0QixJlxl-1jkis2ZqWRX5uN5fD