CISSP模擬体験 & CISSP日本語

P.S. JpexamがGoogle Driveで共有している無料かつ新しいCISSPダンプ：https://drive.google.com/open?id=1kMeJ9dVMNYk_6LyXFq6AwqnyeGbJTEPt

ISCのCISSP認定試験に関連する知識を学んで自分のスキルを向上させ、CISSP認証資格を通して他人の認可を得たいですか。ISCの認定試験はあなたが自分自身のレベルを高めることができます。CISSP認定試験の資格を取ったら、あなたがより良く仕事をすることができます。この試験が非常に困難ですが、実は試験の準備時に一生懸命である必要はありません。JpexamのCISSP問題集を利用してから、一回で試験に合格することができるだけでなく、試験に必要な技能を身につけることもできます。

ISC CISSP認定は、情報セキュリティ分野で非常に尊敬され、認定された認定です。それは、専門知識を実証し、キャリアを促進したい専門家にとって貴重な資産です。認定には広範な準備と経験が必要ですが、報酬は努力する価値があります。資格のある情報セキュリティの専門家に対する需要の増加に伴い、CISSP認定を獲得することで、キャリアの成長と進歩の機会が多く開くことができます。

>> CISSP模擬体験 <<

ISC CISSP日本語、CISSP認定資格

弊社のソフトを利用して、あなたはISCのCISSP試験に合格するのが難しくないことを見つけられます。Jpexamの提供する資料と解答を通して、あなたはISCのCISSP試験に合格するコツを勉強することができます。あなたに安心でソフトを買わせるために、あなたは無料でISCのCISSPソフトのデモをダウンロードすることができます。

ISC CISSP認定試験を受ける資格を得るには、候補者は情報セキュリティの分野で最低5年間の専門的経験を持たなければなりません。あるいは、4年間の経験と関連分野の大学の学位を持つ候補者も適用できます。この試験は250の複数選択の質問で構成されており、候補者はそれを完了するのに最大6時間です。試験に合格するには、候補者は1000ポイントのうち最低700点を獲得する必要があります。

ISC Certified Information Systems Security Professional (CISSP) 認定 CISSP 試験問題 (Q735-Q740):

質問 # 735
Which of the following terms can be described as the process to conceal data into another file or media in a practice known as security through obscurity?

- A. Encryption
- B. NTFS ADS
- C. Steganography
- D. ADS - Alternate Data Streams

正解：C

解説：
It is the art and science of encoding hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message or could

claim there is a message.
It is a form of security through obscurity.
The word steganography is of Greek origin and means "concealed writing." It combines the Greek words steganos (), meaning "covered or protected," and graphei () meaning "writing."
The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages will appear to be (or be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter.
The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable, will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.
It is sometimes referred to as Hiding in Plain Sight. This image of trees blow contains in it another image of a cat using Steganography.

ADS Tree with Cat inside
This image below is hidden in the picture of the trees above:

Hidden Kitty As explained here the image is hidden by removing all but the two least significant bits of each color component and subsequent normalization.
ABOUT MSF and LSF One of the common method to perform steganography is by hiding bits within the Least Significant Bits of a media (LSB) or what is sometimes referred to as Slack Space. By modifying only the least significant bit, it is not possible to tell if there is an hidden message or not looking at the picture or the media. If you would change the Most Significant Bits (MSB) then it would be possible to view or detect the changes just by looking at the picture. A person can perceive only up to 6 bits of depth, bit that are changed past the first sixth bit of the color code would be undetectable to a human eye.
If we make use of a high quality digital picture, we could hide six bits of data within each of the pixel of the image. You have a color code for each pixel composed of a Red, Green, and Blue value. The color code is 3 sets of 8 bits each for each of the color. You could change the last two bit to hide your data. See below a color code for one pixel in binary format. The bits below are not real they are just example for illustration purpose:
RED GREEN BLUE 0101 0101 1100 1011 1110 0011 MSB LSB MSB LSB MSB LSB
Let's say that I would like to hide the letter A uppercase within the pixels of the picture. If we convert the letter "A" uppercase to a

decimal value it would be number 65 within the ASCII table , in binary format the value 65 would translet to 01000001
You can break the 8 bits of character A uppercase in group of two bits as follow: 01 00 00 01 Using the pixel above we will hide those bits within the last two bits of each of the color as follow:
RED GREEN BLUE 0101 0101 1100 1000 1110 0000 MSB LSB MSB LSB MSB LSB
As you can see above, the last two bits of RED was already set to the proper value of 01, then we move to the GREEN value and we changed the last two bit from 11 to 00, and finally we changed the last two bits of blue to 00. One pixel allowed us to hide 6 bits of data. We would have to use another pixel to hide the remaining two bits.
The following answers are incorrect:
-ADS - Alternate Data Streams: This is almost correct but ADS is different from steganography in that ADS hides data in streams of communications or files while Steganography hides data in a single file.
-Encryption: This is almost correct but Steganography isn't exactly encryption as much as using space in a file to store another file.
-NTFS ADS: This is also almost correct in that you're hiding data where you have space to do so. NTFS, or New Technology File System common on Windows computers has a feature where you can hide files where they're not viewable under normal conditions. Tools are required to uncover the ADS-hidden files.
The following reference(s) was used to create this question:
Steganography tool and http://en.wikipedia.org/wiki/Steganography

質問 # 736
What is the BEST approach to annual safety training?

- A. Safety training should address any gaps in a staff member's skill set.
- B. Ensure that all staff members are provided with identical safety training.
- C. Base safety training requirements on staff member job descriptions.
- D. Ensure that staff members in positions with known safety risks are given proper training.

正解：D

質問 # 737
How often should a Business Continuity Plan be reviewed?

- A. At least once a year
- B. At least Quarterly
- C. At least every six months
- D. At least once a month

正解：A

解説：
Explanation/Reference:
Explanation:
As stated in SP 800-34 Rev. 1: To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. During the Operation/Maintenance phase of the SDLC, information systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies. As a general rule, the plan should be reviewed for accuracy and completeness at an organization-defined frequency (at least once a year for the purpose of the exam) or whenever significant changes occur to any element of the plan. Certain elements, such as contact lists, will require more frequent reviews. Remember, there could be two good answers as specified above. Either once a year or whenever significant changes occur to the plan. You will of course get only one of the two presented within your exam.
References: NIST SP 800-34 Revision 1

質問 # 738
Which of the following is true?

- A. UDP guarantees delivers of data. TCP does not guarantee delivery of data.
- B. TCP is connection-oriented. UDP is not
- C. UDP is useful for longer messages
- D. UDP provides for Error Correction. TCP does not.

正解：B

質問 # 739
Proven application security principles include which of the following?

- A. Accepting infrastructure security controls
- B. Minimizing attack surface area
- C. Hardening the network perimeter
- D. Developing independent modules

正解：B

解説：
Minimizing the attack surface area is a core principle of application security. The attack surface refers to the various points (e.g., interfaces, inputs, and code paths) where an attacker could potentially gain access to a system. By minimizing the attack surface, you reduce the number of opportunities available for attackers to exploit vulnerabilities. This can be achieved by:
Removing unnecessary functionality.
Limiting user inputs.
Reducing the number of exposed services or components.
Ensuring that only essential parts of the application are accessible.
This principle is part of a broader approach to making applications more secure by focusing on reducing the exposure to threats.

質問 # 740
.....