

Note: Section A 250 questions, Section B 183 questions, Section C 245 questions, total 678 questions.

Section A

Question No: 1

Ensuring the integrity of business information is the PRIMARY concern of

- A. Encryption Security
- B. Procedural Security.
- C. Logical Security
- D. On-line Security

Answer: B

Procedures are looked at as the lowest level in the policy chain because they are closest to the computers and provide detailed steps for configuration and installation issues. They provide the steps to actually implement the statements in the policies, standards, and guidelines... Security procedures, standards, measures, practices, and policies cover a number of different subject areas. - Shon Harris All-in-one CISSP Certification Guide pg 44-45

Question No: 2

Which one of the following actions should be taken FIRST after a fire has been detected?

- A. Turn off power to the computers
- B. Call the fire department
- C. Notify management
- D. Evacuate all personnel

Answer: D

Protection of life is of the utmost importance and should be dealt with first before looking to save material objects.. - Shon Harris All-in-one CISSP Certification Guide pg 625

Question No: 3

Which one of the following is the Open Systems Interconnection (OSI) protocol for message handling?

- A. X.25
- B. X.400
- C. X.500
- D. X.509

Answer: B

An ISO and ITU standard for addressing and transporting e-mail messages. It conforms to layer 7 of the OSI model and supports several types of transport mechanisms, including Ethernet, X.25, TCP/IP, and dial-up lines. - <http://www.webopedia.com/ITERM/X!X 400.html>

Not A: This is wrong X25 is the method that defines transport of point-to-point packet switching networks.

Question No: 4

Which of the following is a weakness of both statistical anomaly detection and pattern matching?

- A. Lack of ability to scale.
- B. Lack of learning model.
- C. Inability to run in real time.
- D. Requirement to monitor every event.

Answer: B

Explanation: Disadvantages of Knowledge-based ID systems:

This system is resources-intensive; the knowledge database continually needs maintenance and updates. New, unique, or original attacks often go unnoticed.

Disadvantages of Behavior-based ID systems: The system is characterized by high false alarm rates. High positives are the most common failure of ID systems and can create data noise that makes the system unusable.

The activity and behavior of the users while in the networked system might not be static enough to effectively implement a behavior-based ID system. -Ronald Krutz The CISSP PREP Guide (gold edition) pg 88

Question No: 5

Digital signature users register their public keys with a certification authority, which distributes a certificate containing the user's public key and digital signature of the certification authority. In create the certificate, the user's public key and the validity period are combined with what other information before computing the digital signature?

- A. Certificate issuer and the Digital Signature Algorithm identifier
- B. User's private key and the identifier of the master key code
- C. Name of secure channel and the identifier of the protocol type
- D. Key authorization and identifier of key distribution center

Answer: B

.This means that a one-way hashing function would be run on the message and then Kevin would encrypt that has value with his private key.. .The act of signing just means that value was encrypted with a private key...- Shon Harris All-in-one CISSP Certification Guide pg 548

Question No: 6

Why are macro viruses easy to write?

- A. Active contents controls can make direct system calls
- B. The underlying language is simple and intuitive to apply.
- C. Only a few assembler instructions are needed to do damage.
- D. Office templates are fully API compliant.

Answer: B

Macro Languages enable programmers to edit, delete, and copy files. Because these languages are so easy to use, many more types of macro viruses are possible. - Shon Harris All-in-one CISSP Certification Guide pg 785

Question No: 7

Tracing violations, or attempted violations of system security to the user responsible is a function of