



CISSP

(Certified Information Systems Security Professional)

Total Questions: 1,375

Last Updated: Aug 18, 2008

Document version: 8.27.11

Thanks for purchasing techXams' Study Guide,

techXams' CISSP study guide is a comprehensive compilation of questions and answers that have been developed by our team of certified professionals. In order to prepare for the actual exam, all you need is to study the content of this guide. An average of approximately 10 to 20 hours should be spent to study this guide and you will surely pass your exam. It's our guarantee.

Disclaimer

Neither this guide nor any material in this guide is sponsored, endorsed or affiliated with any of the respective vendor. All trademarks are properties of their respective owners.

Guarantee

If you study this guide properly and still unable to pass the exam, please send us a scanned copy of your official score at: refund@techeXams.ws. We will happily reimburse the cost of this study guide or send you an exchange of study guide of your choice free of cost.

Feedback

If you find any possible improvement, then please do let us know. We are always interested in improving the quality of this product. Feedback can be send at: feedback@techeXams.ws

Copyright

techXams holds the copyright of this material. techXams grants you a limited license to view and study this material, either for personal or commercial use. Unauthorized reproduction or distribution of this material, or any portion thereof, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Question: 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

Explanation:

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: 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

Explanation:

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: 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

2

Answer: B

Explanation:

An ISO and ITU standard defines the OSI model and supports protocols for serial and dial-up lines. - ht

conforms to layer 7 of the OSI model. Ethernet, X.25, TCP/IP,

Question: 4.

Which of the following is NOT a characteristic of a security policy?

...tion and pattern

- A. Lack of ability to change
- B. Lack of learning capability
- C. Inability to run on a variety of operating systems
- D. Requirement to be updated

Answer: B

Explanation:

Disadvantages of Knowledge-based Intrusion Detection (KID) include: Knowledge-based attacks continually change and are often unnoticed. Disadvantages include high false alarm rates. High positive alarm rates make the system unusable. Knowledge-based attacks might not be static errors. -CISSP PREP Guide (go

...ive; the knowledge-based attacks often go undetected. They are characterized by high false alarm rates. They create data noise that makes it difficult to manage a networked system. -Ronald Krutz The

Question: 5.

Digital signature uses a hash function to create a unique digital signature, which is then encrypted with the sender's private key.

...hority, which is then encrypted with the sender's private key.

Which of the following is NOT a characteristic of a digital signature?

- A. Certificate-based
- B. User's private key
- C. Name of secure channel
- D. Key authorization and identification

CISSP Demo Exam

Answer: A

Explanation:

The key word is 'In cr
 following data: Versio
 certificate creator); S
 authority to digitally
 certificate authority t
 starting date and tim
 Subject's name (cont
 contained in the cert
 of the certificate own

m to X.509 contain the
 ver (from the
 d by the certificate
 cation of the
 tes and times - a
 te is valued);
 s the public key
 the actual public key
 SP Study Guide by title

Question: 6.

Why are macro viru

- A. Active content
- B. The underlying
- C. Only a few ass
- D. Office templat

Explanation:

Macro Languages ena
 so easy to use, many
 Certification Guide p

these languages are
 II-in-one CISSP

Answer: B

Question: 7.

Tracing violations,

function of

- B. acc
- C. integrity
- D. accountability

er responsible is a

Answer: D

CISSP Demo Exam

Explanation:

Auditing capabilities ensure that users are accountable for their actions, verify that the security policies are enforced, and help determine the cause of an incident and provide as investigation tools.
 - Shon Harris All-in-one

Question: 8.

Which one of the following is a pattern analysis technique?

- A. Masking analysis
- B. Protocol analysis
- C. Traffic analysis
- D. Pattern analysis

Explanation:

Traffic analysis, which involves analyzing the patterns of transmission to infer information that is not explicitly stated (e.g., frequency, and so forth) and information transmitted) to the analyst. (CISSP Study Guide (gold edition) pg 323)

Question: 9.

In which situation would a traffic analysis be most useful?

- A. Where high availability is required
- B. Where the confidentiality of data is important
- C. Where counterintelligence is a concern
- D. Where data integrity is a concern



length, and origin?
 ?

Answer: C

employed by an intruder (e.g., frequency, and so forth) and information transmitted) to the analyst. (CISSP Study Guide (gold edition) pg 323)

interest?

B

Explanation:

Emanation eavesdropping. Receipt and display of information, which is resident on computers or terminals, through the interception of radio frequency (RF) signals emitted by those computers or terminals. The U.S. government addressed this problem by requiring a shielding technology employed on computers processing sensitive information. The CISSP PREP Guide (gold edition) pg 416

Question: 10.

In which state must

- A. User mode
- B. Stateful inspection
- C. Interprocess communication
- D. Supervisor mode

Explanation:

A computer is in a supervisor mode when instructions are executed on those instructions.)

Question: 11.

All of the following

- A. definition of the
- B. statement of ro
- C. statement of a
- D. statement of p

CISSP Demo Exam

...t instructions?

Answer: D

...ctions. (privileged
 ...is authorized to use
 ...255

...ne

...D

Explanation:

Policies are considered the first and highest level of documentation, from which the lower level elements of standards, procedures, and guidelines flow. This order, however, does not mean that policies are more important than procedures and guidelines, which are the more general policies that apply for strategic reasons, and then the more tactical procedures and guidelines. (CISSP Guide (gold edition) pg 13)

Question: 12.

What set of principles is used to guide the development of security policies?

- A. Authentication, authorization, and accounting
- B. Individual accountability, nonrepudiation, and confidentiality
- C. Need to know, least privilege, and separation of duties
- D. Audit trails, limited access, and least privilege

Answer: C

Explanation:

“In addition to the CIA triad, security policies should be based on the following concepts, principles, and tenants that should be followed when developing, implementing, and deploying a security solution. The principles of security are: least privilege, need to know, separation of duties, accountability, nonrepudiation, and confidentiality.”

Question: 13.

Why do vendors push updates to their customers to download patches for their software?

- A. Recipients can verify the integrity of the patch.
- B. Recipients can ensure the patch is not tampered with.

Why do vendors push updates to their customers to download patches for their software?

Why do vendors push updates to their customers to download patches for their software?

Answer: A

CISSP Demo Exam

Answer: A

Explanation:

TBSEC provides guidance to address basic security requirements of a system and how trust is established. The criteria developed later are used to design necessary functions. Pg. 413.

TBSEC guidelines ensure the functionality of a system is not separated, as in the case of products or by vendors. Pg.

Question: 16.

Which factor is critical to system integrity?

- A. Data classification
- B. Information ownership
- C. Change control
- D. System design

CISSP Demo Exam

Answer: A

Explanation:

A Integrity is dependent on the model relies on data control against possible threats. Confidentiality cannot include sensitivity, disclosure. 145 Tittel: CISSP Study following goals: 1.) The protected from unauth

Also Biba integrity ensure confidentiality, adding, strict access personnel object integrity, of confidentiality, on, and isolation." Pg erized by the three ers.2.) The data is internally and

Question: 17

Audit trails based upon

- A. intrusion detection threshold
- B. individual accountability
- C. audit review criteria
- D. individual authentication

Answer: B

Explanation:

Accountability is another... responsible for their actions. This accountability is supported by the proper individuals. Accountability is supported by... on the network. Audit trails can be used to... most events. -Ronald Krutz The CISSP PREP

responsible for their actions. This accountability is supported by the proper individuals. Accountability is supported by... on the network. Audit trails can be used to... most events. -Ronald Krutz The CISSP PREP

Question: 18.

Which one of the following is not an IPSEC (IPSEC) based virtual private network (VPN) security protocol?

- A. Brute force
- B. Man-in-the-middle
- C. Traffic analysis
- D. Replay

Which one of the following is not an IPSEC (IPSEC) based virtual private network (VPN) security protocol?

Answer: B

Explanation:

Active attacks find identification through negotiation. The attacker has revealed its identity before the attacker has revealed its identity to the system. The attacker has revealed its identity before it gave its identity to the system. The attacker has all legitimate access to the system. <http://msgs.securepo>

Active attacks find identification through negotiation. The attacker has revealed its identity before the attacker has revealed its identity to the system. The attacker has revealed its identity before it gave its identity to the system. The attacker has all legitimate access to the system. <http://msgs.securepo>

CISSP Demo Exam