



www.chinatag.com

CHINATAG

ISC CISSP

Certified Information Systems
Security Professional

Q&A

DEMO Version

Copyright (c) 2003 Chinatag LLC. All rights reserved.

Important Note Please Read Carefully

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website. Our IT certification products start at only **\$7.99**.

Study Tips

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 180 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to feedback@chinatag.com.

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team
Chinatag LLC.

Note:

Section A contains 250 questions.
Section B contains 183 questions.
Section C contains 245 questions.
The total number of questions is 678.

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/TERM/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

Section B

QUESTION NO: 1

In a discretionary mode, which of the following entities is authorized to grant information access to other people?

- A. Manager
- B. Group leader
- C. Security manager
- D. User

Answer: D

Explanation: Discretionary control is the most common type of access control mechanism implemented in computer systems today. The basis of this kind of security is that an individual user, or program operating on the user's behalf, is allowed to specify explicitly the types of access other users (or programs executing on their behalf) may have to information under the user's control. Discretionary security differs from mandatory security in that it implements the access control decisions of the user. Mandatory controls are driven by the results of a comparison between the user's trust level or clearance and the sensitivity designation of the information.

QUESTION NO: 2

Which DES mode of operation is best suited for database encryption?

- A. Cipher Block Chaining (CBC) mode
- B. Cycling Redundancy Checking (CRC) mode
- C. Electronic Code Book (ECB) mode
- D. Cipher Feedback (CFB) mode

Answer: C

Explanation: The DES algorithm in Electronic Codebook (ECB) mode is used for DEK and MIC encryption when symmetric key management is employed. The character string "DES-ECB" within an encapsulated PEM header field indicates use of this algorithm/mode combination.

A compliant PEM implementation supporting symmetric key management shall support this algorithm/mode combination. This mode of DES encryption is the best suited for database encryption because of its low overhead.

ECB Mode has some weakness, here they are:

1. ECB Mode encrypts a 64-bit block independently of all other 64-bit blocks
2. Given the same key, identical plaintext will encrypt the same way
3. Data compression prior to ECB can help (as with any mode)
4. Fixed block size of 64 bits therefore incomplete block must be padded

QUESTION NO: 3

Within the realm of IT security, which of the following combinations best defines risk?

- A. Threat coupled with a breach.
- B. Threat coupled with a vulnerability.
- C. Vulnerability coupled with an attack.
- D. Threat coupled with a breach of security.

Answer: B

Explanation: This is the main concept, when we talk about a possible risk we always have a possible vulnerability in the system attacked. This vulnerability can make a threat to be successful. We can say that the level of risk can be measured through the level of vulnerabilities in our current systems and the ability of the attackers to exploit them to make a threat successful.

QUESTION NO: 4

Which of the following would be the best reason for separating the test and development environments?

- A. To restrict access to systems under test.
- B. To control the stability of the test environment.
- C. To segregate user and development staff.
- D. To secure access to systems under development.

Answer: B

Explanation: This is the right answer, with a separation of the two environments (Test and development), we can get a more stable and more “in control” environment. Since we are making tests in the development environment, we don’t want our production processes there, we don’t want to experiment things in our production processes. With a separation of the environments we can get a more risk free production environment and more control and flexibility over the test environment for the developers.

QUESTION NO: 5

Which of the following statements pertaining to dealing with the media after a disaster occurred and disturbed the organizations activities is incorrect?

- A. The CEO should always be the spokesperson for the company during a disaster.
- B. The disaster recover plan must include how the media is to be handled during the disaster.

- C. The organization's spokesperson should report bad news before the press gets a hold of it through another channel.
- D. An emergency press conference site should be planned ahead.

Answer: A

Explanation: This is not a good practice, we cannot involve the CEO of the company to deal with the media in every case we have a disaster, depending on the severity of the disaster we can make the CEO talk, but the best practice in the real world is to have a well-known person with that role, with special speaking capabilities and knowledge about press methods. In general, the CEO always gets news of what happened, and he decides the company politics, then another designed employee (Usually from the disaster recovery team) deals with the media.

QUESTION NO: 6

Which Orange book security rating introduces security labels?

- A. C2
- B. B1
- C. B2
- D. B3

Answer: B

Explanation: Class (B1) or "Labeled Security Protection" systems require all the features required for class (C2). In addition, an informal statement of the security policy model, data labeling, and mandatory access control over named subjects and objects must be present. The capability must exist for accurately labeling exported information. Any flaws identified by testing must be removed.

QUESTION NO: 7

A Business Impact Analysis (BIA) does not:

- A. Recommend the appropriate recovery solution.
- B. Determine critical and necessary business functions and their resource dependencies.
- C. Identify critical computer applications and the associated outage tolerance.
- D. Estimate the financial impact of a disruption.

Answer: A

Explanation: Remember that when we talk about a BIA (Business Impact Analysis), we are analyzing and identifying possible issues about our infrastructure, in this kind of analysis we don't make suggestions about what to do to recover from them. This is not an action plan, It's an analysis about the business, the process

that it relays on, the level of the systems and a estimative of the financial impact, or in other words, how much many we loose with our systems down.

QUESTION NO: 8

Which access control model enables the owner of the resource to specify what subjects can access specific resources?

- A. Discretionary Access Control
- B. Mandatory Access Control
- C. Sensitive Access Control
- D. Role-based Access Control

Answer: A

Explanation: Discretionary Access Control (DAC) is used to control access by restricting a subject's access to an object. It is generally used to limit a user's access to a file. In this type of access control it is the owner of the file who controls other users' accesses to the file.

Using a DAC mechanism allows users control over access rights to their files. When these rights are managed correctly, only those users specified by the owner may have some combination of read, write, execute, etc. permissions to the file.

QUESTION NO: 9

What type of cable is used with 100Base-TX Fast Ethernet?

- A. Fiber-optic cable
- B. Four pairs of Category 3, 4 or 5 unshielded twisted-par (UTP) wires.
- C. Two pairs of Category 5 unshielded twisted-pair (UTP) or Category 1 shielded twisted-pair (STP) wires.
- D. RG.58 cable.

Answer: C

Explanation: 100BaseTX is a 100-Mbps baseband Fast Ethernet specification using two pairs of either UTP or STP wiring. The first pair of wires is used to receive data; the second is used to transmit. To guarantee proper signal timing, a 100BaseTX segment cannot exceed 100 meters in length. This specification of Ethernet is based on the IEEE 802.3 standard.

QUESTION NO: 10

Which of the following best describes the Secure Electronic Transaction (SET) protocol?

Section C - Practice questions

Study these questions as well.

QUESTION NO: 1

Covert channel is a communication channel that can be used for:

- A. Hardening the system.
- B. Violating the security policy.
- C. Protecting the DMZ.
- D. Strengthening the security policy.

Answer: B

Explanation:

Covert channel is a communication channel that allows transfer of information in a manner that violates the system's security policy.

QUESTION NO: 2

To ensure that integrity is attained through the Clark and Wilson model, certain rules are needed. These rules are:

- A. Processing rules and enforcement rules.
- B. Integrity-bouncing rules.
- C. Certification rules and enforcement rules.
- D. Certification rules and general rules.

Answer: C

Explanation:

To ensure that integrity is attained and preserved, Clark and Wilson assert, certain integrity-monitoring and integrity-preserving rules are needed. Integrity-monitoring rules are called certification rules, and integrity-preserving rules are called enforcement rules.

QUESTION NO: 3

What was introduced for circumventing difficulties in classic approaches to computer security by limiting damages produced by malicious programs?

- A. Integrity-preserving
- B. Ref Mon
- C. Integrity-monitoring
- D. Non-Interference

Answer: D

Explanation:

Non-Interference (NI for short) was introduced in order to circumvent difficulties in classic approaches to computer security. In order to limit, and possibly avoid, the damages produced by malicious programs (often called ``Trojan Horses") which try to leak secret information, it was suggested to impose some access control rules which limit the action of these programs.

QUESTION NO: 4

What is an indirect way to transmit information with no explicit reading of confidential information?

- A. Covert channels
- B. Backdoor
- C. Timing channels
- D. Overt channels

Answer: A

Explanation:

Covert channels: indirect ways for transmitting information with no explicit reading of confidential information. This kind of difficulties induced some researchers to re-think from scratch the whole problem of guaranteeing security in computer systems.

QUESTION NO: 5

Which of the following are the limitations of the BLP model?

- A. No policies for changing access data control.
- B. All of the choices.
- C. Contains covert channels.
- D. Static in nature.

Answer: B

Explanation:

Limitations of the BLP model:

Have no policies for changing access data control

Intended for systems with static security levels

Contains covert channels: a low subject can detect the existence of a high object when it is denied access. Sometimes it is not enough to hide the content of an object; also their existence may have to be hidden.

Restricted to confidentiality

QUESTION NO: 6

Which of the following are the two most well known access control models?

- A. Lattice and Biba
- B. Bell LaPadula and Biba
- C. Bell LaPadula and Chinese war
- D. Bell LaPadula and Info Flow

Answer: B

Explanation:

The two most well known models are Bell&LaPadula [1973] and Biba[1977]. Both were designed in and for military environments.

QUESTION NO: 7

What can be defined as a formal security model for the integrity of subjects and objects in a system?

- A. Biba
- B. Bell LaPadulaLattice
- C. Lattice
- D. Info Flow

Answer: A

The Handbook of Information System Management, 1999 Edition, ISBN: 0849399742 presents the following definition:

In studying the two properties of the Bell-LaPadula model, Biba discovered a plausible notion of integrity, which he defined as prevention of unauthorized modification. The resulting Biba integrity model states that maintenance of integrity requires that data not flow from a receptacle of given integrity to a receptacle of higher integrity. For example, if a process can write above its security level, trustworthy data could be contaminated by the addition of less trustworthy data. SANS glossary at <http://www.sans.org/newlook/resources/glossary.htm> define it as:

Formal security model for the integrity of subjects and objects in a system.

QUESTION NO: 8

Which of the following is best known for capturing security requirements of commercial applications?

- A. Lattice
- B. Biba
- C. Bell LaPadula
- D. Clark and Wilson

Answer: D

Explanation:

This model attempts to capture security requirements of commercial applications.

'Military' and 'Commercial' are shorthand for different ways of using computers. This model has emphasis on integrity:

Internal consistency: properties of the internal state of a system

External consistency: relation of the internal state of a system to the outside world

QUESTION NO: 9

The Clark Wilson model has its emphasis on:

- A. Security
- B. Integrity
- C. Accountability
- D. Confidentiality

Answer: B

Explanation:

This model attempts to capture security requirements of commercial applications.

'Military' and 'Commercial' are shorthand for different ways of using computers. This model has emphasis on integrity:

Internal consistency: properties of the internal state of a system

External consistency: relation of the internal state of a system to the outside world

QUESTION NO: 10

Which of the following is a state machine model capturing confidentiality aspects of access control?

- A. Clarke Wilson
- B. Bell-LaPadula
- C. Chinese Wall
- D. Lattice

Answer: B

Explanation:

Bell-LaPadula is a state machine model capturing confidentiality aspects of access control. Access permissions are defined through an Access Control matrix and through a partial ordering of security levels. Security policies prevent information flowing downwards from a high security level to a low security level. BLP only considers the information flow that occurs when a subject observes or alters an object.

Cissp1

1. Which of the following should be done with a classified document immediately after the document is printed? (Select the best choice.)

- a. It should be copied.
- b. It should be delivered.
- c. It should be shredded.
- d. It should be placed in an office mail box.

Answer: b

Section: 10. Physical Security

Choice b is correct. After a sensitive or classified document is printed, the document should be immediately taken out of the printer and delivered to the intended recipient. This practice will help protect the contents of a sensitive or classified document from being viewed by unauthorized personnel. Copying a sensitive or classified document might expose the contents of the document to unauthorized personnel because an increase in the number of copies of a document can decrease the security of a document. A document should not typically be shredded immediately after it is printed. A sensitive or classified document should not typically be placed in an office mail box because office mail boxes are typically in public areas that can be entered by anyone in an office.

Reference:

ISO/IEC 17799:2000, Section 7.3.1, Clear Desk and Clear Screen Policy.

2. Which of the following is an example of active misuse? (Select the best choice.)

- a. data diddling
- b. shoulder surfing
- c. eavesdropping
- d. sniffing

Answer: a

Section: 4. Application and Systems Development Security

Choice a is correct. Data diddling is an example of active misuse, which results in data alteration and affects the integrity of data. Active misuse is an attack on the integrity or availability of information. Shoulder surfing, eavesdropping, and sniffing are passive misuse, which can result in violation of the confidentiality of data without affecting the state of a computer or information stored on a computer.

Reference:

Summers, p. 82.

3. What is the mechanism that enables programming objects belonging to one class to acquire part of their definition from another class? (Select the best choice.)

- a. inheritance
- b. cohesion
- c. coupling
- d. polymorphism

Answer: a

Section: 4. Application and Systems Development Security

Choice a is correct. Inheritance is the mechanism that enables programming objects belonging to one class to acquire part of their definition from another class. Inheritance also enables objects belonging to one class to share the structure and behavior defined in another class. Cohesion is the degree to which functions or processing elements of a programming module are related or bound together. Coupling is the degree to which program modules depend on each other. Polymorphism enables a class method to be called without regard to the specific implementation of a method. For example, two classes, bicycle and motorcycle, each have a method named ride, which have different implementations in each class. The move class can call the ride method in either the motorcycle or bicycle class without regard to the specific implementation of the ride method in each class.

Reference:

Vallabhaneni, p. 217.

4. An attack that uses a misleading context to trick a user into making an inappropriate security-related decision is a _____. (Select the best choice.)

- a. spoofing attack
- b. surveillance attack
- c. DoS attack
- d. social engineering attack

Answer: a

Section: 9. Law, Investigation and Ethics

Choice a is correct. A spoofing attack involves an attacker creating a misleading context in order to trick a user into making an inappropriate security-related decision. An attacker might be able to use information gained in a spoofing attack to gain access to network resources. In a surveillance attack, an attacker passively monitors network traffic and records information provided by a user on web forms. A Denial of Service (DoS) attack occurs as a result of an attacker flooding a network with so many requests that a network ceases to respond to requests from legitimate users. In a social engineering attack, an attacker interacts directly with a user on a network to obtain network credentials or other secret or proprietary information.

Stephenson, p. 285.

5. Robert Morris designed the Internet Worm to do all of the following EXCEPT _____. (Select the best choice.)

- a. be undetectable
- b. spread
- c. degrade Internet performance
- d. remain undiscovered

Answer: c

Section: 4. Application and Systems Development Security

Choice c is correct. Robert Morris originally intended to use the Internet Worm to determine the extent to which the worm could spread without being detected. However, because of a programming bug, copies of the Internet Worm did not stop running as Morris had intended, which resulted in severe degradation of Internet performance and exhaustion of Internet resources.

Reference:

Pfleeger, p. 193.

6. Which of the following can encrypt remote access connections to a server? (Select the best choice.)

- a. SSL
- b. PGP
- c. S/MIME
- d. SSH

Answer: d

Section: 5. Cryptography

Choice d is correct. Secure Shell (SSH), an extension of the Unix shell, can encrypt remote access connections to a server. Typically, SSH replaces telnet. SSH can also replace the Unix r commands. **Secure Sockets Layer (SSL) is used to encrypt Hypertext Transfer Protocol (HTTP) traffic. Secure Multipurpose Internet Mail Extensions (S/MIME) and Pretty Good Privacy (PGP) are used to encrypt e-mail communications.**

Reference:

RFC 2504.

7. Which of the following is a reason that a device might be installed to reduce the vulnerability of a network resource? (Select the best choice.)

- a. safeguard
- b. precaution



- c. safety measure
- d. countermeasure

Answer: b

Section: 3. Security Management Practices

Choice b is correct. A precaution is a reason that a device might be installed to reduce the vulnerability of a network resource. For example, a firewall might be installed on a network as a precaution against attacks from the Internet. A countermeasure, which is sometimes referred to as a safeguard or a safety measure, is a device, procedure, action or technique that is designed to reduce the vulnerability of a computer or network from attack. Virus protection software is an example of a countermeasure.

Reference:

Fites and Kratz, p. 151.

8. What information is in an SA? (Select the best choice.)

- a. an SPI and a source address
- b. an SPI and an MD5 hash
- c. an MD5 hash and a source address
- d. an API and a destination address

Answer: d

Section: 5. Cryptography

Choice d is correct. A security association (SA) contains a security parameter index (SPI) and a destination address. An SA does not contain a source address or an MD5 hash. SAs are typically used in Internet Protocol Security (IPSec) to create an encrypted connection.

Reference:

RFC 1825.

9. There are three primary kinds of spoofing.

They are e-mail spoofing, Web site spoofing, and _____. (Select the best choice.)

- a. system masquerade
- b. spamming
- c. IP spoofing
- d. social engineering

Answer: c

Section: 9. Law, Investigation and Ethics

Choice c is correct. The three primary kinds of spoofing are e-mail spoofing, Web site spoofing and Internet Protocol (IP) spoofing. In a system masquerade attack, a legitimate computer is replaced in a communications stream with a masquerading computer. Masquerading is not considered spoofing.

Cissp2

1. A shared resource matrix is a technique commonly used to locate _____. (Select the best choice.)

- a. malicious code
- b. security flaws
- c. trap doors
- d. covert channels

Answer: d

Section: 4. Application and Systems Development Security

Choice d is correct. A shared resource matrix is a technique commonly used to locate covert channels. Analyzing resources of a system is one standard for locating covert channels, because the basis of a covert channel is a shared resource. The other choices are incorrect because a shared resource matrix will not normally lead to the identification of malicious code, security flaws or trap doors.

Reference:

Pfleeger, p. 204.

2. Which statement describes DES? (Select the best choice.)

- a. It is based upon public key cryptography.
- b. It uses stream ciphers.
- c. It was developed by the Department of Defense.
- d. It uses private key cryptography.

Answer: d

Section: 5. Cryptography

Choice d is correct. Data Encryption Standard (DES) uses private key cryptography. DES is a block cipher, and DES was developed by IBM.

Reference:

Fites and Kratz, p. 26.



3. Employees, contractors, or vendors of the company who use information systems resources as part of their job are known as _____. (Select the best choice.)

- a. owners
- b. custodians
- c. stewards
- d. end users

Answer: d

Section: 3. Security Management Practices

Choice d is correct. End users use information systems resources as part of their job. Owners are business executive or business manager who are responsible for company business information assets. Custodians and stewards are the entities designated by the owner to keep and protect information resources as prescribed by the owner.

Reference:

Tipton and Krause, p. 344.

4. Magnetic media requires environmental controls to protect it from the most common risks that include all **ECEPT** which of the following? (Select the best choice.)

- a. temperature
- b. liquids
- c. magnetism
- d. air

Answer: d

Section: 7. Operations Security

Choice d is correct. Air alone does not present a significant environmental risk to magnetic media. Temperature and liquid spillage can result in damage to the media itself, and magnetism can result in the loss of data contained on the media.

Reference:

Security Considerations in Computer Support and Operations, Special Publication 800-12.

The NIST Handbook, Chapter 14, p. 162.

5. The benefit of regularly testing DRPs include all but which of the following? (Select the best choice.)

- a. to train internal IT and off-site vendor personnel in configuring offsite backup systems and networks
- b. to assess whether the written DRP plans are accurate and up-to-date
- c. to determine recovery time objective to time-critical applications
- d. to ascertain that backup site systems, applications, databases and networks are sized properly to fit the circumstances

Answer: c

Section: 8. Business Continuity and Disaster Recovery Planning

Choice c is correct. Determining time criticality of applications should have been performed during the business impact assessment (BIA) phase of the methodology. The other choices are benefits of testing disaster recovery plans (DRPs).

Reference:

Devlin and Emerson, Chapter I-8, p. I-8-1.

Hutt, Bosworth and Hoyt, pp. 7-31.

6. If a CPU is in "*supervisor state*," it will access _____. (Select the best choice.)

- a. both privileged and non-privileged instructions
- b. only privileged instructions
- c. only non-privileged instructions
- d. interruptions but not execute instructions

Answer: a

Section: 6. Security Architecture and Models

Choice a is correct. If a central processing unit (CPU) is in *supervisor state*, it will access both privileged and non-privileged instructions. A CPU does not access only privileged instructions. In the *problem state* a CPU will access only non-privileged instructions. In the *wait state* a CPU will only access interruption but not execute instructions.

Reference:

Fites and Kratz, p. 169.

7. The custodian of information has the primary responsibility for _____. (Select the best choice.)

- a. logically ensuring that information is properly safeguarded from unauthorized access, modification or disclosure
- b. implementing safeguards such as ACLs to protect information
- c. accessing information in a manner controlled by ACL safeguards and supported by policy
- d. physically ensuring that information is safeguarded and maintained in a secure manner

Answer: b

Section: 1. Access Control Systems and Methodology

Choice b is correct. The custodian of information has the primary responsibility for implementing safeguards such as ACLs to protect information. The custodian is generally an application administrator or system administrator. It is a best-practice definition of information ownership to logically ensure that information is properly safeguarded from unauthorized access, modification or disclosure. Accessing information in a manner controlled by access control list (ACL) safeguards and supported by policy is more typical of a user or client than a custodian. Physically ensuring that information is safeguarded and maintained in a secure manner refers to an infrastructure support



service, such as a data center operations function.

Reference:

Tudor, pp. 41-42.

8. Layer 4 of the OSI model is known as the _____. (Select the best choice.)

- a. Data Link layer
- b. Transport layer
- c. Network layer
- d. Presentation layer

Answer: b

Section: 2. Telecommunications and Networking Security

Choice b is correct. Layer 4 of the Open Systems Interconnection (OSI) model is known as the Transport layer. The Data Link layer is known as OSI Layer 2. The Network layer is known as OSI Layer 3. The Presentation layer is known as OSI layer 6.

Reference:

Russell and Gangemi, p. 215.

9. A possible danger to a system, whether it is a person, thing or event that might exploit a vulnerability of the system is referred to as a _____. (Select the best choice.)

- a. problem
- b. danger
- c. concern
- d. threat

Answer: d

Section: 3. Security Management Practices

Choice d is correct. A threat is a possible danger to a system. The other choices are incorrect because they fail to reflect the level of severity that a threat poses to a system.

Reference:

Russell and Gangemi, p. 11.

10. A Trojan horse differs from a virus in the following two very important aspects.

Which of the following statements regarding a Trojan horse best describes this difference? (Select the best choice.)

- a. First, it is not found on Unix computers; second, it could stand alone as an independent executable file.



- b. First, it does not replicate or infect other files; second, it has a limit to how many times it can occur on a system.
- c. First, it does not replicate or infect other files; second, it cannot be found by anti-virus software using virus signature files.
- d. First, it does not replicate or infect other files; second, it can stand alone as an independent executable file.

Answer: d

Section: 9. Law, Investigation and Ethics

Choice d is correct. Trojan horses do not replicate or infect other files, and they can stand alone as independent executable files. Trojan horses can be found on Unix computers, and they can occur many times on a system. Trojan horses can not typically be found by using virus signature files.

Reference:

Stephenson, p. 36.

11. The characteristic of information being disclosed only to authorized persons, entities and processes at authorized times and in the authorized manner is known as _____. (Select the best choice.)

- a. integrity
- b. availability
- c. accountability
- d. confidentiality

Answer: d

Section: 3. Security Management Practices

Choice d is correct. Confidentiality is characterized by restrictions on the disclosure of information. Integrity is the characteristics of being accurate, availability is the characteristic of information being accessible and accountability is the ability to audit the possession of information.

Reference:

GASSP, 1997, p. 14.

12. The mandatory, step-by-step process that must be done in order to complete a task or assignment is known as _____. (Select the best choice.)

- a. policies
- b. standards
- c. guidelines
- d. procedures

Answer: d

Section: 3. Security Management Practices

Choice d is correct. The mandatory, step-by-step process that must be done in order to complete a task