ISC.CISSP.v2021-08-21.q483

Exam Code:	CISSP
Exam Name:	Certified Information Systems Security Professional (CISSP)
Certification Provider:	ISC
Free Question Number:	483
Version:	v2021-08-21
# of views:	7616
# of Questions views:	4830
https://www.freepdfdumps.com/ISC.CISSP.v2021-08-21.q483.html	

NEW QUESTION: 1
What can be defined as a momentary low voltage?
A. Spike
B. Sag
C. Fault
D. Brownout
Answer: B (LEAVE A REPLY)
A sag is a momentary low voltage. A spike is a momentary high voltage. A fault is a momentary power out and a brownout is a prolonged power supply that is below normal voltage.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 6: Physical security (page 299).

NEW QUESTION: 2
Which choice below is the first priority in an emergency?
A. Notifying external support resources for recovery and restoration
B. Warning customers and contractors of a potential interruption of service
C. Communicating with employees families the status of the emergency
D. Protecting the health and safety of everyone in the facility
Answer: D (LEAVE A REPLY)
Life safety, or protecting the health and safety of everyone in the facility is the first priority in an emergency or disaster. Evacuation routes, assembly areas, and accounting for personnel (head counts and last-known locations) are the most important function of emergency procedures, before anything else. Once all personnel have been accounted for and emergency teams have arrived to prevent further damage or hazard, family members should be notified of the status of the event. Providing restoration and recovery, and implementing alternative production methods also comes later. Source: Emergency Management Guide for Business and Industry, Federal Emergency Management Agency, August, 1998.

NEW QUESTION: 3
Identification usually takes the form of:
A. Login ID.
B. User password.
C. None of the choices.
D. Passphrase
Answer: A (LEAVE A REPLY)
Identification is a means to verify who you are. Authentication is what you are authorized to perform, access, or do. User identification enables accountability. It enables you to trace activities to individual users that may be held responsible for their actions. Identification usually takes the form of Logon ID or User ID. Some of the Logon ID characteristics are: they must be unique, not shared, and usually non descriptive of job function

NEW QUESTION: 4
What is the FIRST step required in establishing a records retention program?
A. Classify records based on sensitivity.
B. Identify and inventory all records storage locations.
C. Draft a records retention policy.
D. Identify and inventory all records.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 5
Which of the following is a connection-orientated protocol?
A. IP
B. UDP
C. TCP
D. ICMP
E. SNMP
F. TFTP
Answer: (SHOW ANSWER)
TCP is a connection-orientated protocol.

NEW QUESTION: 6
Which of the following is the MAIN reason that system re-certification and re-accreditation are needed?
A. To assist data owners in making future sensitivity and criticality determinations
B. To help the security team accept or reject new systems for implementation and production
C. To assure the software development team that all security issues have been addressed
D. To verify that security protection remains acceptable to the organizational security policy
Answer: D (LEAVE A REPLY)

NEW QUESTION: 7

Which of the following would NOT be considered a penetration testing technique?

A. Sniffing

B. Scanning

C. War dialing

D. Data manipulation

Answer: D (LEAVE A REPLY)

The correct answer is Data manipulation. Data manipulation describes the corruption of data integrity to perform fraud for personal gain or other reasons.

External penetration testing should not alter the data in any way. The other three are common penetration techniques.

NEW QUESTION: 8

Intrusion detection systems can be all of the following types EXCEPT:

A. Signature-based.

B. Statistical anomaly-based.

C. Network-based.

D. Defined-based.

Answer: D (LEAVE A REPLY)

The correct answer is Defined-based. All the other answers are types of IDSs.

NEW QUESTION: 9

The Secure Hash Algorithm (SHA-1) of the Secure Hash Standard (NIST FIPS PUB 180) processes data in block lengths of:

A. 128 bits.

B. 256 bits.

C. 512 bits.

D. 1024 bits.

Answer: C (LEAVE A REPLY)

The correct answer is 512 bits. If a block length is fewer than 512 bits, padding bits are added to make the block length equal to 512 bits. The other answers are distracters.

NEW QUESTION: 10

Which one of the following is an advantage of an effective release control strategy from a configuration control standpoint?

A. Ensures that a trace for all deliverables is maintained and auditable

B. Enforces backward compatibility between releases

C. Ensures that there is no loss of functionality between releases

D. Allows for future enhancements to existing features

Answer: A (LEAVE A REPLY)

NEW QUESTION: 11
Which of the following binds a subject name to a public key value?
A. A public-key certificate
B. A public key infrastructure
C. A secret key infrastructure
D. A private key certificate
Answer: (SHOW ANSWER)
Remember the term Public-Key Certificate is synonymous with Digital Certificate or Identity certificate.
The certificate itself provides the binding but it is the certificate authority who will go through the Certificate Practice Statements (CPS) actually validating the bindings and vouch for the identity of the owner of the key within the certificate.
As explained in Wikipedia:
In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document which uses a digital signature to bind together a public key with an identity
- information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.
In a typical public key infrastructure (PKI) scheme, the signature will be of a certificate authority (CA). In a web of trust scheme such as PGP or GPG, the signature is of either the user (a self-signed certificate) or other users ("endorsements") by getting people to sign each other keys. In either case, the signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together. RFC 2828 defines the certification authority (CA) as:
An entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.
An authority trusted by one or more users to create and assign certificates. Optionally, the certification authority may create the user's keys.
X509 Certificate users depend on the validity of information provided by a certificate. Thus, a CA should be someone that certificate users trust, and usually holds an official position created and granted power by a government, a corporation, or some other organization. A CA is responsible for managing the life cycle of certificates and, depending on the type of certificate and the CPS that applies, may be responsible for the life cycle of key pairs associated with the certificates
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
and http://en.wikipedia.org/wiki/Public_key_certificate

NEW QUESTION: 12
What name is given to the study and control of signal emanations from electrical and electromagnetic equipment?
A. Cross Talk
B. EMI
C. TEMPEST
D. EMP
Answer: (SHOW ANSWER)

NEW QUESTION: 13
Which model, based on the premise that the quality of a software product is a direct function of the quality of it's associated software development and maintenance processes, introduced five levels with which the maturity of an organization involved in the software process is evaluated?
A. The Spiral Model
B. The total Quality Model (TQM)
C. The Software Capability Maturity Model
D. The IDEAL Model
Answer: (SHOW ANSWER)

NEW QUESTION: 14
Which of the following items is NOT a benefit of cold sites?
A. Quick Recovery
B. A secondary location is available to reconstruct the environment
C. No resource contention with other organization
D. Low Cost
Answer: (SHOW ANSWER)

NEW QUESTION: 15
To what does logon abuse refer?
A. Legitimate users accessing networked services that would normally be restricted to them
B. Nonbusiness or personal use of the Internet
C. Intrusions via dial-up or asynchronous external network connections
D. Breaking into a network primarily from an external source
Answer: A (LEAVE A REPLY)
The correct answer is "Legitimate users accessing networked services that would normally be restricted to them". Logon abuse entails an otherwise proper user attempting to access areas of the network that are deemed offlimits. Answer "Breaking into a network primarily from an external source" is called network intrusion, and d refers to backdoor remote access.

NEW QUESTION: 16
Refer to the information below to answer the question.
Desktop computers in an organization were sanitized for re-use in an equivalent security environment. The data was destroyed in accordance with organizational policy and all marking and other external indications of the sensitivity of the data that was formerly stored on the magnetic drives were removed.
Organizational policy requires the deletion of user data from Personal Digital Assistant (PDA) devices before disposal. It may not be possible to delete the user data if the device is malfunctioning. Which destruction method below provides the BEST assurance that the data has been removed?
A. Knurling
B. Grinding

C. Degaussing
D. Shredding
Answer: (SHOW ANSWER)

NEW QUESTION: 17
In a multilevel security system (MLS), the Pump is:
A. A one-way information flow device
B. A two-way information flow device
C. A device that implements role-based access control
D. Compartmented Mode Workstation (CMW)
Answer: A (LEAVE A REPLY)
The Pump (M.h. Kang, I.S. Moskowitz, APump for Rapid, Reliable,
Secure Communications, The 1st ACM Conference on Computer and Communications
Security, Fairfax, VA, 1993) was developed at the US Naval
Research Laboratory (NRL). It permits information flow in one direction only, from a lower level of security classification or sensitivity to a higher level. It is a convenient approach to multilevel security in that it can be used to put together systems with different security levels.
* Answer "A two-way information flow device" is a distracter.
* Answer "Compartmented Mode Workstation (CMW)", the CMW, refers to windows-based workstations that require users to work with information at different classification levels.
Thus, users may work with multiple windows with
different classification levels on their workstations. When data is
attempted to be moved from one window to another, mandatory access
control policies are enforced. This prevents information of a higher classification from being deposited to a location of lower classification.
* Answer "A device that implements role-based access control", role-based access control, is an access control mechanism and is now being considered for mandatory access control based on users' roles in their organizations.

NEW QUESTION: 18
What would be the Annualized Rate of Occurrence (ARO) of the threat "user input error", in the case where a company employs 100 data entry clerks and every one of them makes one input error each month?
A. 100

B. 120
C. 1
D. 1200
Answer: D (LEAVE A REPLY)
If every one of the 100 clerks makes 1 error 12 times per year, it makes a total of 1200 errors. The Annnualized Rate of Occurence (ARO) is a value that represents the estimated frequency in which a threat is expected to occur. The range can be from 0.0 to a large number. Having an average of 1200 errors per year means an ARO of 1200.

NEW QUESTION: 19
An international medical organization with headquarters in the United States (US) and branches in France wants to test a drug in both countries. What is the organization allowed to do with the test subject's data?
A. Aggregate it into one database in the US
B. Process it in the US, but store the information in France
C. Share it with a third party
D. Anonymize it and process it in the US
Answer: B (LEAVE A REPLY)
Explanation
Section: Security Assessment and Testing

NEW QUESTION: 20
A code, as is pertains to cryptography:
A. Is a generic term for encryption.
B. Is specific to substitution ciphers.
C. Deals with linguistic units.
D. Is specific to transposition ciphers.
Answer: C (LEAVE A REPLY)
Historically, a code refers to a cryptosystem that deals with linguistic units:
words, phrases, sentences, and so forth. Codes are only useful for specialized circumstances where the message to transmit has an already defined equivalent ciphertext word.
Source: DUPUIS, Cl?ment, CISSP Open Study Guide on domain 5, cryptography, April 1999.

NEW QUESTION: 21
What is one of the most common drawbacks to using a dual-homed host firewall?
A. The examination of the packet at the Network layer introduces latency.
B. The examination of the packet at the Application layer introduces latency.
C. The ACLs must be manually maintained on the host.

D. Internal routing may accidentally become enabled.

Answer: D (LEAVE A REPLY)

A dual-homed host uses two NICs to attach to two separate networks,
commonly a trusted network and an untrusted network. It's
important that the internal routing function of the host be disabled to create an application-layer chokepoint and filter packets. Many systems come with routing enabled by default, such as IP forwarding, which makes the firewall useless. The other answers are distracters. Source:
Hacker Proof by Lars Klander (Jamsa Press, 1997).

NEW QUESTION: 22

In the days before CIDR (Classless Internet Domain Routing), networks were commonly organized by classes. Which of the following would have been true of a Class C network?

A. The first bit of the IP address would be set to zero.

B. The first bit of the IP address would be set to one and the second bit set to zero.

C. The first two bits of the IP address would be set to one, and the third bit set to zero.

D. The first three bits of the IP address would be set to one.

Answer: C (LEAVE A REPLY)

Each Class C network address has a 24-bit network prefix, with the three highest
order bits set to 1-1-0
The following answers are incorrect:
The first bit of the IP address would be set to zero. Is incorrect because, this would be a Class A network address.
The first bit of the IP address would be set to one and the second bit set to zero. Is incorrect because, this would be a Class B network address .
The first three bits of the IP address would be set to one. Is incorrect because, this is a distractor.
Class D & E have the first three bits set to 1. Class D the 4th bit is 0 and for Class E the 4th bit to 1.Classless Internet Domain Routing (CIDR)
High Order bits are shown in bold below.
For Class A, the addresses are 0.0.0.0 - 127.255.255.255
The lowest Class A address is represented in binary as 00000000.00000000.0000000.00000000
For Class B networks, the addresses are 128.0.0.0 - 191.255.255.255.
The lowest Class B address is represented in binary as 10000000.00000000.00000000.00000000
For Class C, the addresses are 192.0.0.0 - 223.255.255.255
The lowest Class C address is represented in binary as 11000000.00000000.00000000.00000000
For Class D, the addresses are 224.0.0.0 - 239.255.255.255 (Multicast)
The lowest Class D address is represented in binary as 11100000.00000000.00000000.00000000
For Class E, the addresses are 240.0.0.0 - 255.255.255.255 (Reserved for future usage)
The lowest Class E address is represented in binary as 11110000.00000000.00000000.00000000
Classful IP Address Format
References:
3Com http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf

NEW QUESTION: 23
Which of the following are the three types of NIACAP accreditation?
A. Site, type, and location
B. Site, type, and general
C. Site, type, and system
D. Type, system, and location
Answer: C (LEAVE A REPLY)

NEW QUESTION: 24
Which of the following is the PRIMARY benefit of implementing data-in-use controls?
A. If the data is lost, it must be decrypted to be opened.
B. When the data is being viewed, it can only be printed by authorized users.
C. If the data is lost, it will not be accessible to unauthorized users.
D. When the data is being viewed, it must be accessed using secure protocols.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 25
What is the MAIN purpose of a change management policy?
A. To assure management that changes to the Information Technology (IT) infrastructure are necessary
B. To verify that changes to the Information Technology (IT) infrastructure are approved
C. To identify the changes that may be made to the Information Technology (IT) infrastructure
D. To determine the necessary for implementing modifications to the Information Technology (IT) infrastructure
Answer: B (LEAVE A REPLY)

NEW QUESTION: 26
With SQL Relational databases where is the actual data stored?
A. Views
B. Tables
C. Schemas and sub-schemas
D. Index-sequential tables
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: SQL is a relational database Query language. SQL stands for structured query language. Schemas describe how the tables and views are structured - careful design is required so that the SQL database runs in an efficient manner. Tables are made up of rows and columns and contain the actual data. Views represent how you want to look at the data. They are not concerned with where the data is, but rather what data you want to view and how you want to see it. You can even join more than one table together.

However, the less efficient the views, the longer it takes to retrieve your report. Sub- schemas may be used to establish user privileges to see data.

NEW QUESTION: 27
This type of attack is generally most applicable to public-key cryptosystems, what type of attack am I?
A. Chosen-Ciphertext attack
B. Ciphertext-only attack
C. Plaintext Only Attack
D. Adaptive-Chosen-Plaintext attack
Answer: A (LEAVE A REPLY)
A chosen-ciphertext attack is one in which cryptanalyst may choose a piece of ciphertext and attempt to obtain the corresponding decrypted plaintext. This type of attack is generally most applicable to public-key cryptosystems.
A chosen-ciphertext attack (CCA) is an attack model for cryptanalysis in which the cryptanalyst gathers information, at least in part, by choosing a ciphertext and obtaining its decryption under an unknown key. In the attack, an adversary has a chance to enter one or more known ciphertexts into the system and obtain the resulting plaintexts. From these pieces of information the adversary can attempt to recover the hidden secret key used for decryption.
A number of otherwise secure schemes can be defeated under chosen-ciphertext attack. For example, the El Gamal cryptosystem is semantically secure under chosen-plaintext attack, but this semantic security can be trivially defeated under a chosen-ciphertext attack. Early versions of RSA padding used in the SSL protocol were vulnerable to a sophisticated adaptive chosen-ciphertext attack which revealed SSL session keys. Chosen-ciphertext attacks have implications for some self-synchronizing stream ciphers as well. Designers of tamper-resistant cryptographic smart cards must be particularly cognizant of these attacks, as these devices may be completely under the control of an adversary, who can issue a large number of chosen-ciphertexts in an attempt to recover the hidden secret key.
According to RSA: Cryptanalytic attacks are generally classified into six categories that distinguish the kind of information the cryptanalyst has available to mount an attack. The categories of attack are listed here roughly in increasing order of the quality of information available to the cryptanalyst, or, equivalently, in decreasing order of the level of difficulty to the cryptanalyst. The objective of the cryptanalyst in all cases is to be able to decrypt new pieces of ciphertext without additional information. The ideal for a cryptanalyst is to extract the secret key.
A ciphertext-only attack is one in which the cryptanalyst obtains a sample of ciphertext, without the plaintext associated with it. This data is relatively easy to obtain in many scenarios, but a successful ciphertext-only attack is generally difficult, and requires a very large ciphertext sample. Such attack was possible on cipher using Code Book Mode where frequency analysis was being used and even thou only the ciphertext was available, it was still possible to eventually collect enough data and decipher it without having the key.
A known-plaintext attack is one in which the cryptanalyst obtains a sample of ciphertext and the corresponding plaintext as well. The known-plaintext attack (KPA) or crib is an attack model for cryptanalysis where the attacker has samples of both the plaintext and its encrypted version (ciphertext), and is at liberty to make use of them to reveal further secret information such as secret keys and code books.

A chosen-plaintext attack is one in which the cryptanalyst is able to choose a quantity of plaintext and then obtain the corresponding encrypted ciphertext. A chosen-plaintext attack (CPA) is an attack model for cryptanalysis which presumes that the attacker has the capability to choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts. The goal of the attack is to gain some further information which reduces the security of the encryption scheme. In the worst case, a chosen-plaintext attack could reveal the scheme's secret key.

This appears, at first glance, to be an unrealistic model; it would certainly be unlikely that an attacker could persuade a human cryptographer to encrypt large amounts of plaintexts of the attacker's choosing. Modern cryptography, on the other hand, is implemented in software or hardware and is used for a diverse range of applications; for many cases, a chosen-plaintext attack is often very feasible. Chosen-plaintext attacks become extremely important in the context of public key cryptography, where the encryption key is public and attackers can encrypt any plaintext they choose.

Any cipher that can prevent chosen-plaintext attacks is then also guaranteed to be secure against known-plaintext and ciphertext-only attacks; this is a conservative approach to security.

Two forms of chosen-plaintext attack can be distinguished:

Batch chosen-plaintext attack, where the cryptanalyst chooses all plaintexts before any of them are encrypted. This is often the meaning of an unqualified use of "chosen-plaintext attack".

Adaptive chosen-plaintext attack, is a special case of chosen-plaintext attack in which the cryptanalyst is able to choose plaintext samples dynamically, and alter his or her choices based on the results of previous encryptions. The cryptanalyst makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions.

Non-randomized (deterministic) public key encryption algorithms are vulnerable to simple "dictionary"-type attacks, where the attacker builds a table of likely messages and their corresponding ciphertexts. To find the decryption of some observed ciphertext, the attacker simply looks the ciphertext up in the table. As a result, public-key definitions of security under chosen-plaintext attack require probabilistic encryption (i.e., randomized encryption). Conventional symmetric ciphers, in which the same key is used to encrypt and decrypt a text, may also be vulnerable to other forms of chosen-plaintext attack, for example, differential cryptanalysis of block ciphers.

An adaptive-chosen-ciphertext is the adaptive version of the above attack. A cryptanalyst can mount an attack of this type in a scenario in which he has free use of a piece of decryption hardware, but is unable to extract the decryption key from it.

An adaptive chosen-ciphertext attack (abbreviated as CCA2) is an interactive form of chosen-ciphertext attack in which an attacker sends a number of ciphertexts to be decrypted, then uses the results of these decryptions to select subsequent ciphertexts. It is to be distinguished from an indifferent chosen-ciphertext attack (CCA1).

The goal of this attack is to gradually reveal information about an encrypted message, or about the decryption key itself. For public-key systems, adaptive-chosen-ciphertexts are generally applicable only when they have the property of ciphertext malleability - that is, a ciphertext can be modified in specific ways that will have a predictable effect on the decryption of that message.

A Plaintext Only Attack is simply a bogus detractor. If you have the plaintext only then there is no need to perform any attack.
References:
RSA Laboratories FAQs about today's cryptography: What are some of the basic types of cryptanalytic attack?
also see:
http://www.giac.org/resources/whitepaper/cryptography/57.php
and
http://en.wikipedia.org/wiki/Chosen-plaintext_attack

NEW QUESTION: 28
When are security requirements the LEAST expensive to implement?
A. During the application rollout phase
B. When built into application design
C. During each phase of the project cycle
D. When identified by external consultants
Answer: B (LEAVE A REPLY)

NEW QUESTION: 29
Which of the following protects a password from eavesdroppers and supports the encryption of communication?
A. Challenge Handshake Authentication Protocol (CHAP)
B. Challenge Handshake Identification Protocol (CHIP)
C. Challenge Handshake Encryption Protocol (CHEP)
D. Challenge Handshake Substitution Protocol (CHSP)
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
One approach to remote access security is the Challenge Handshake Authentication Protocol (CHAP). CHAP protects the password from eavesdroppers and supports the encryption of communication. Challenge Handshake Authentication Protocol (CHAP) addresses some of the vulnerabilities found in PAP. It uses a challenge/response mechanism to authenticate the user instead of sending a password. When a user wants to establish a PPP connection and both ends have agreed that CHAP will be used for authentication purposes, the user's computer sends the authentication server a logon request. The server sends the user a challenge (nonce), which is a random value. This challenge is encrypted with the use of a predefined password as an encryption key, and the encrypted challenge value is returned to the server. The authentication server also uses the predefined password as an encryption key and decrypts the challenge value, comparing it to the original value sent. If the two results are the same, the authentication server deduces that the user must have entered the correct password, and authentication is granted.
Incorrect Answers:

B: The correct name for the protocol is Challenge Handshake Authentication Protocol (CHAP), not Challenge Handshake Identification Protocol (CHIP).
C: The correct name for the protocol is Challenge Handshake Authentication Protocol (CHAP), not Challenge Handshake Encryption Protocol (CHEP).
D: The correct name for the protocol is Challenge Handshake Authentication Protocol (CHAP), not Challenge Handshake Substitution Protocol (CHSP).
References:
Krutz, Ronald L and Russell Dean Vines, The CISSP and CAP Prep Guide: Mastering CISSP and CAP, Wiley Publishing, Indianapolis, 2007, p. 66 Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 710

NEW QUESTION: 30
Which of the following processes is used to align security controls with business functions?
A. Data mapping
B. Standards selection
C. Scoping
D. Tailoring
Answer: B (LEAVE A REPLY)
Section: Mixed questions

NEW QUESTION: 31
Which of the following usually provides reliable, real-time information without consuming network or host resources?
A. network-based IDS
B. host-based IDS
C. application-based IDS
D. firewall-based IDS
Answer: A (LEAVE A REPLY)
"A network-based IDS has little negative affect on overall network performance, and because it is deployed on a single-purpose system, it doesn't adversely affect the performance of any other computer." Pg 34 Krutz: CISSP Prep Guide: Gold Edition.

NEW QUESTION: 32

To what does covert channel eavesdropping refer?
A. Using a hidden, unauthorized network connection to communicate unauthorized information
B. The use of two-factor passwords
C. Nonbusiness or personal use of the Internet
D. Socially engineering passwords from an ISP
Answer: A (LEAVE A REPLY)
The correct answer is "Using a hidden, unauthorized network connection to communicate unauthorized information". A Covert Channel is a connection intentionally created to transmit unauthorized information from inside a trusted network to a partner at an outside, untrusted node.
Answer "Socially engineering passwords from an ISP" is called masquerading.

NEW QUESTION: 33
Which of the following keys has the SHORTEST lifespan?
A. Secret key
B. Public key
C. Session key
D. Private key
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A session key is a single-use symmetric key that is used to encrypt messages between two users during a single communication session.
If Tanya has a symmetric key she uses to always encrypt messages between Lance and herself, then this symmetric key would not be regenerated or changed. They would use the same key every time they communicated using encryption. However, using the same key repeatedly increases the chances of the key being captured and the secure communication being compromised. If, on the other hand, a new symmetric key were generated each time Lance and Tanya wanted to communicate, it would be used only during their one dialogue and then destroyed. If they wanted to communicate an hour later, a new session key would be created and shared.
A session key provides more protection than static symmetric keys because it is valid for only one session between two computers. If an attacker were able to capture the session key, she would have a very small window of time to use it to try to decrypt messages being passed back and forth.
Incorrect Answers:
A: A secret key is static in nature. It has no fixed lifespan and is used until someone decides to change the key. Session keys are used for single communication sessions so they have a much shorter lifespan.
B: A public key is issued by a CA and typically has a lifespan of one or two years. Session keys are used for single communication sessions so they have a much shorter lifespan.
D: A private key is issued by a CA and typically has a lifespan of one or two years. Session keys are used for single communication sessions so they have a much shorter lifespan.
References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, pp. 798-799

NEW QUESTION: 34
Which of the following is needed to securely distribute symmetric cryptographic keys?
A. Officially approved Public-Key Infrastructure (PKI) Class 3 or Class 4 certificates
B. Officially approved and compliant key management technology and processes
C. An organizationally approved communication protection policy and key management plan
D. Hardware tokens that protect the user's private key.
Answer: C (LEAVE A REPLY)
Section: Software Development Security

NEW QUESTION: 35
What physical characteristic does a retinal scan biometric device measure?
A. The pattern of blood vessels at the back of the eye
B. The amount of light reflected by the retina
C. The size, curvature, and shape of the retina
D. The pattern of light receptors at the back of the eye
Answer: (SHOW ANSWER)

NEW QUESTION: 36
Which of the following focuses on the basic features and architecture of a system?
A. operational assurance
B. life cycle assurance
C. covert channel assurance
D. level A1
Answer: (SHOW ANSWER)
"The operational assurance requirements specified in the Orange Book are as follows:
System Architecture System integrity Covert channel analysis Trusted facility management Trusted recovery"
Pg. 301 Krutz: The CISSP Prep Guide: Gold Edition

NEW QUESTION: 37
Which of the following techniques BEST prevents buffer overflows?
A. Boundary and perimeter offset
B. Character set encoding
C. Code auditing
D. Variant type and bit length
Answer: B (LEAVE A REPLY)
Section: Mixed questions
Explanation:

Some products installed on systems can also watch for input values that might result in buffer overflows, but the best countermeasure is proper programming. This means use bounds checking. If an input value is only sup-posed to be nine characters, then the application should only accept nine characters and no more. Some languages are more susceptible to buffer overflows than others, so programmers should understand these issues, use the right languages for the right purposes, and carry out code review to identify buffer overflow vulnerabilities.

NEW QUESTION: 38
Which of the following System and Organization Controls (SOC) report types should an organization request if they require a period of time report covering security and availability for a particular system?
A. SOC 2 Type 2
B. SOC 1 Type1
C. SOC 1Type2
D. SOC 2 Type 1
Answer: (SHOW ANSWER)

NEW QUESTION: 39
Which of the following best ensures accountability of users for the actions taken within a system or domain?
A. Identification
B. Authentication
C. Authorization
D. Credentials
Answer: (SHOW ANSWER)
The only way to ensure accountability is if the subject is uniquely identified and authenticated. Identification alone does not provide proof the user is who they claim to be. After showing proper credentials, a user is authorized access to resources.
References:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 4: Access Control (page 126).

NEW QUESTION: 40
Sensitivity labels are an example of what application control type?
A. Preventive security controls
B. Detective security controls
C. Compensating administrative controls
D. Preventive accuracy controls
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Sensitivity (Security) labels are attached to all objects; thus, every file, directory, and device has its own security label with its classification information. A user may have a security clearance of secret, and the data

he requests may have a security label with the classification of top secret. In this case, the user will be denied (prevented) because his clearance is not equivalent or does not dominate (is not equal or higher than) the classification of the object.
The terms "security labels" and "sensitivity labels" can be used interchangeably.
Incorrect Answers:
B: Sensitivity labels are preventive, not detective, as the label may prevent the user or process from accessing the resource.
C: A compensating control is a data security measure that is designed to satisfy the requirement for some other security measure that is deemed too difficult or impractical to implement. Sensitive controls are preventive, not compensating.
D: Sensitivity labels have nothing to do with accuracy. They are preventive.
References:
Conrad, Eric, Seth Misenar and Joshua Feldman, CISSP Study Guide, 2nd Edition, Syngress, Waltham, 2012, p. 222

NEW QUESTION: 41
What does it mean to say that sensitivity labels are "incomparable"?
A. The number of classification in the two labels is different.
B. Neither label contains all the classifications of the other.
C. the number of categories in the two labels are different.
D. Neither label contains all the categories of the other.
Answer: (SHOW ANSWER)
If a category does not exist then you cannot compare it. Incomparable is when you
have two disjointed sensitivity labels, that is a category in one of the labels is not in the other label.
"Because neither label contains all the categories of the other, the labels can't be compared.
They're said to be incomparable"
COMPARABILITY:
The label:
TOP SECRET [VENUS ALPHA]
is "higher" than either of the labels:
SECRET [VENUS ALPHA] TOP SECRET [VENUS]
But you can't really say that the label:
TOP SECRET [VENUS]
is higher than the label:
SECRET [ALPHA]
Because neither label contains all the categories of the other, the labels can't be compared.
They're said to be incomparable. In a mandatory access control system, you won't be allowed
access to a file whose label is incomparable to your clearance.
The Multilevel Security policy uses an ordering relationship between labels known as the
dominance relationship. Intuitively, we think of a label that dominates another as being "higher"
than the other. Similarly, we think of a label that is dominated by another as being "lower" than the

other. The dominance relationship is used to determine permitted operations and information flows.
DOMINANCE
The dominance relationship is determined by the ordering of the Sensitivity/Clearance component of the label and the intersection of the set of Compartments.
Sample Sensitivity/Clearance ordering are:
Top Secret > Secret > Confidential > Unclassified
s3 > s2 > s1 > s0
Formally, for label one to dominate label 2 both of the following must be true:
The sensitivity/clearance of label one must be greater than or equal to the sensitivity/clearance of label two.
The intersection of the compartments of label one and label two must equal the compartments of label two.
Additionally:
Two labels are said to be equal if their sensitivity/clearance and set of compartments are exactly equal. Note that dominance includes equality.
One label is said to strictly dominate the other if it dominates the other but is not equal to the other.
Two labels are said to be incomparable if each label has at least one compartment that is not included in the other's set of compartments.
The dominance relationship will produce a partial ordering over all possible MLS labels, resulting in what is known as the MLS Security Lattice.
The following answers are incorrect:
The number of classification in the two labels is different. Is incorrect because the categories are what is being compared, not the classifications.
Neither label contains all the classifications of the other. Is incorrect because the categories are what is being compared, not the classifications.
the number of categories in the two labels is different. Is incorrect because it is possibe a category exists more than once in one sensitivity label and does exist in the other so they would be comparable.
Reference(s) used for this question:
OReilly - Computer Systems and Access Control (Chapter 3)
http://www.oreilly.com/catalog/csb/chapter/ch03.html and http://rubix.com/cms/mls_dom

NEW QUESTION: 42
Which one of the following affects the classification of data?
A. Passage of time
B. Multilevel Security (MLS) architecture
C. Minimum query size
D. Assigned security label
Answer: A (LEAVE A REPLY)

NEW QUESTION: 43

Which of the following components are considered part of the Trusted Computing Base?

A. trusted hardware and firmware

B. trusted hardware and software

C. trusted hardware, software and firmware

D. trusted computer operators and system managers

Answer: C (LEAVE A REPLY)

The trusted computing base (TCB) is a collection of all the hardware, software, and firmware components within a system that provide some type of security and enforce the system's security policy. The TCB does not address only operating system components, because a computer system is not made up of only an operating system.

Hardware, software components, and firmware components can affect the system in a negative or positive manner, and each has a responsibility to support and enforce the security policy of that particular system. Some components and mechanisms have direct responsibilities in supporting the security policy, such as firmware that will not let a user boot a computer from a USB drive, or the memory manager that will not let processes overwrite other processes' data. Then there are components that do not enforce the security policy but must behave properly and not violate the trust of a system. Examples of the ways in which a component could violate the system's security policy include an application that is allowed to make a direct call to a piece of hardware instead of using the proper system calls through the operating system, a process that is allowed to read data outside of its approved memory space, or a piece of software that does not properly release resources after use.

To assist with the evaluation of secure products, TCSEC introduced the idea of the Trusted Computing Base (TCB) into product evaluation. In essence, TCSEC starts with the principle that there are some functions that simply must be working correctly for security to be possible and consistently enforced in a computing system. For example, the ability to define subjects and objects and the ability to distinguish between them is so fundamental that no system could be secure without it. The TCB then are these fundamental controls implemented in a given system, whether that is in hardware, software, or firmware. Each of the TCSEC levels describes a different set of fundamental functions that must be in place to be certified to that level.

The link below will take you to a one page document that describes the high-level requirements that any TCB would need to meet to achieve each division or class (essentially a subdivision) of the TCSEC rating. See details at:

https://www.freepracticetests.org/documents/TCB.pdf

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (pp. 359-360). McGraw-Hill. Kindle Edition.

and

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17936-17943). Auerbach Publications. Kindle Edition.

NEW QUESTION: 44

Which model, based on the premise that the quality of a software product is a direct function of the quality of its associated software development and maintenance processes, introduced five levels with which the maturity of an organization involved in the software process is evaluated?

A. The Total Quality Model (TQM)

B. The IDEAL Model

C. The Software Capability Maturity Model

D. The Spiral Model

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation:

The Software Capability Maturity Model (CMM) is based on the premise that the quality of a software product is a direct function of the quality of its associated software development and maintenance processes. It introduces five maturity levels that serve as a foundation for conducting continuous process improvement and as an ordinal scale for measuring the maturity of the organization involved in the software processes.

CMM has Five Maturity Levels of Software Processes:

- The initial level: processes are disorganized, even chaotic. Success is likely to depend on individual efforts, and is not considered to be repeatable as processes would not be sufficiently defined and documented to allow them to be replicated.
- The repeatable or managed level: basic project management techniques are established, and successes could be repeated as the requisite processes would have been made established, defined, and documented.
- The defined level: an organization has developed its own standard software process through greater attention to documentation, standardization, and integration.
- The quantatively managed level: an organization monitors and controls its own processes through data collection and analysis.
- The optimized level: processes are constantly being improved through monitoring feedback from current processes and introducing innovative processes to better serve the organization's particular needs.

Incorrect Answers:

A: Total Quality Management (TQM) is a management approach of an organization centered on quality, based on the participation of all its members and aiming at long term success through customer satisfaction.

B: The Integrated Design, Evaluation, and Assessment of Loadings (IDEAL) model is a post-construction water quality model for designing storm water best management practices. It is not a software development model.

D: The Spiral model uses an iterative approach to software development with an emphasis on risk analysis. The iterative approach allows new requirements to be addressed as they are uncovered. It is a good model for complex projects that have fluid requirements.

The spiral model has four main phases:

- Planning
- Risk analysis: ensures that all issues are actively reviewed and analyzed.
-

- Development and testing: prototype testing takes place early in the development project, and feedback based upon these tests is integrated into the following iteration of steps.
- Evaluation: the customer evaluates the product in its current state and provides feedback, which is an input value for the following iteration of steps.

References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, pp. 62, 1115-1116, 1120-1122

http://en.wikipedia.org/wiki/Capability_Maturity_Model

https://en.wikipedia.org/wiki/Total_quality_management

https://en.wikipedia.org/wiki/IDEAL_model

NEW QUESTION: 45

Another name for a VPN is a:

A. tunnel

B. one-time password

C. pipeline

D. bypass

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

A virtual private network (VPN) is a secure, private connection through an untrusted network. VPN technology requires a tunnel to work and it assumes encryption.

Incorrect Answers:

B: A one-time password is not the same as a VPN.

C: Tunnel, not pipeline, can be used as a name for a VPN.

D: Tunnel, not bypass, can be used as a name for a VPN.

References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 702

NEW QUESTION: 46

The "revocation request grace period" is defined as:

A. Time period between the arrival of a revocation reason and the publication of the revocation information

B. The period for to the user within he must make a revocation request upon a revocation reason

C. Minimum response time for performing a revocation by the CA

D. Maximum response time for performing a revocation by the CA

Answer: D (LEAVE A REPLY)

NEW QUESTION: 47
Which of the following phases of a software development life cycle normally addresses Due Care and Due Diligence?
A. Implementation
B. System feasibility
C. Product design
D. Software plans and requirements
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Information security best practice is a consensus of the best way to protect the confidentiality, integrity, and availability of assets. Following best practices is a way to demonstrate due care and due diligence.
Due Care and Due Diligence should therefore be a part of the Software plans and requirements phase.
Note: Due care is doing what a reasonable person would do. It is sometimes called the "prudent man" rule. The term derives from "duty of care. Due diligence is the management of due care. Expecting your staff to keep their systems patched means you expect them to exercise due care. Verifying that your staff has patched their systems is an example of due diligence.
Incorrect Answers:
A: Due Care and Due Diligence would be a part of the requirements of a project, and not a part of the implementation phase.
B: Due Care and Due Diligence would be a part of the requirements of a project, and not a part of the System feasibility phase.
C: Due Care and Due Diligence would be a part of the requirements of a project, and not a part of the design phase.
References:
Conrad, Eric, Seth Misenar and Joshua Feldman, CISSP Study Guide, 2nd Edition, Syngress, Waltham, 2012, p. 161

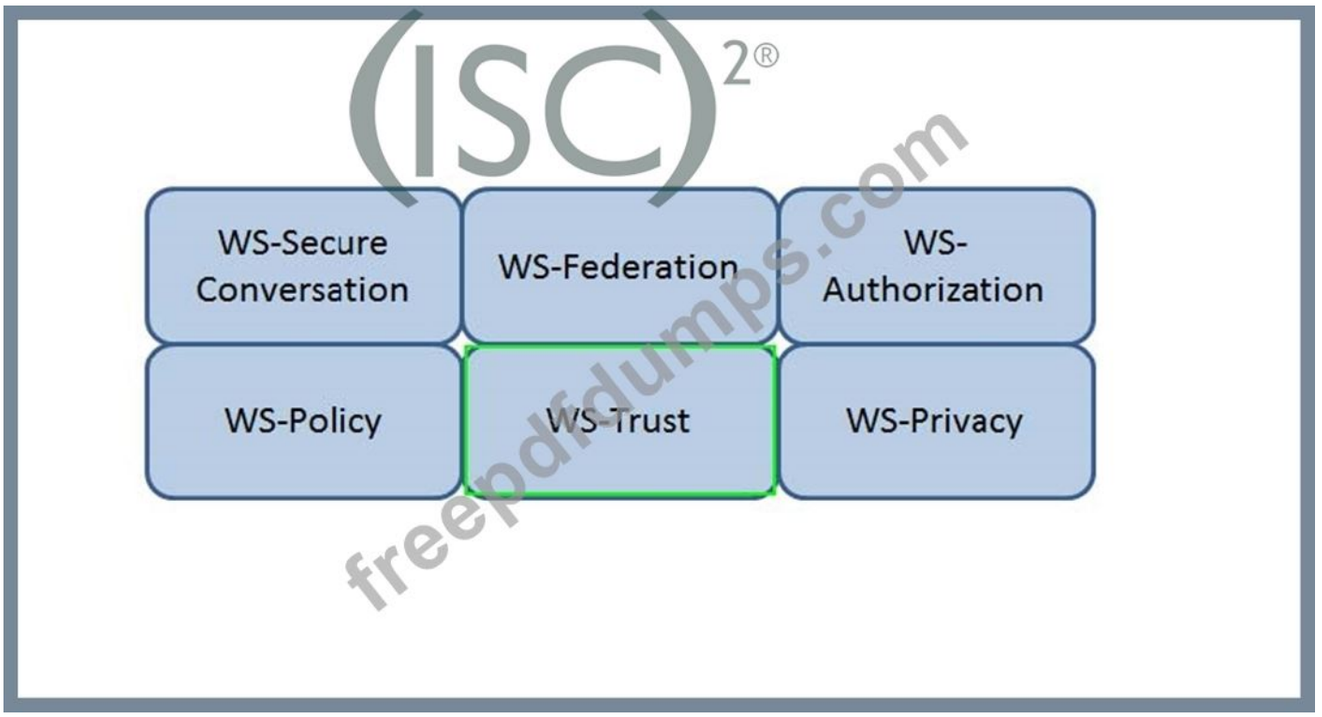
NEW QUESTION: 48
What process determines who is trusted for a given purpose?
A. Identification
B. Authorization
C. Authentication
D. Accounting

Answer: B (LEAVE A REPLY)
Authorization determines who is trusted for a given purpose. More precisely, it determines whether a particular principal, who has been authenticated as the source of a request to do something, is trusted for that operation. Authorization may also include controls on the time at which something can be done (e.g. only during working hours) or the computer terminal from which it can be requested (e.g. only the one on the system administrator desk).

NEW QUESTION: 49
Which choice is NOT an accurate description of C.I.A.?
A. A stands for authorization.
B. A stands for availability.
C. I stands for integrity.
D. C stands for confidentiality.
Answer: (SHOW ANSWER)

NEW QUESTION: 50
HOTSPOT
Which Web Services Security (WS-Security) specification negotiates how security tokens will be issued, renewed and validated? Click on the correct specification in the image below.

Answer:



NEW QUESTION: 51
On which port is POP3 usually run?
A. 109
B. 139
C. 119
D. 110
Answer: (SHOW ANSWER)

NEW QUESTION: 52
Which of the following statements pertaining to Kerberos is true?
A. Kerberos uses public key cryptography.
B. Kerberos uses X.509 certificates.
C. Kerberos is a credential-based authentication system.
D. Kerberos was developed by Microsoft.
Answer: (SHOW ANSWER)
Kerberos is a trusted, credential-based, third-party authentication protocol that was developed at MIT and that uses symmetric (secret) key cryptography to authenticate clients to other entities on a network for access to services. It does not use X.509 certificates, which are used in public key cryptography. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 40).

NEW QUESTION: 53
Which of the following are the steps usually followed in the development of documents such as security policy, standards and procedures?

A. design, development, publication, coding, and testing.
B. design, evaluation, approval, publication, and implementation.
C. initiation, evaluation, development, approval, publication, implementation, and maintenance.
D. feasibility, development, approval, implementation, and integration.
Answer: (SHOW ANSWER)
The common steps used the development of security policy are initiation of the project, evaluation, development, approval, publication, implementation, and maintenance. The other choices listed are the phases of the software development life cycle and not the step used to develop ducuments such as Policies, Standards, etc...
Reference: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 3, 2002, Auerbach Publications.

NEW QUESTION: 54
In IPSec, if the communication is to be gateway-to-gateway or host-to-gateway:
A. Tunnel mode of operation is required
B. Only transport mode can be used
C. Encapsulating Security Payload (ESP) authentication must be used
D. Both tunnel and transport mode can be used
Answer: A (LEAVE A REPLY)
Transport mode is established when the enpoint is a host. If the gateway in a gateway-to-host communication was to use transport mode, it would act as a host system, which is acceptable for direct protocols to that gateway. Otherwise, TUNNEL mode is required for gateway services... This is the most common mode of operation and is required for gateway-togateway and host-to-gateway communications.
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, page 167.

NEW QUESTION: 55
In which one of the following documents is the assignment of individual roles and responsibilities MOST appropriately defined?
A. Security policy
B. Enforcement guidelines
C. Acceptable use policy
D. Program manual
Answer: (SHOW ANSWER)
An acceptable use policy is a document that the employee signs in which the expectations, roles and responsibilities are outlined. Issue -specific policies address specific security issues that management feels need more detailed explanation and attention to make sure a comprehensive structure is built and all employees understand how they are to comply to these security issues. - Shon Harris All-in-one CISSP Certification Guide pg 62

NEW QUESTION: 56

A weak key of an encryption algorithm has which of the following properties?
A. It can only be used as a public key
B. It facilitates attacks against the algorithm
C. It has much more zeroes than ones
D. It is too short, and thus easily crackable
Answer: B (LEAVE A REPLY)

NEW QUESTION: 57
Which attack type below does NOT exploit TCP vulnerabilities?
A. Sequence Number attack
B. Ping of Death
C. SYN attack
D. land.c attack
Answer: (SHOW ANSWER)
The Ping of Death exploits the fragmentation vulnerability of large
ICMP ECHO request packets by sending an illegal packet with more
than 65K of data, creating a buffer overflow.
* a TCP sequence number attack, which exploits the nonrandom predictable pattern of TCP connection sequence numbers to spoof a session.
* a TCP SYN attack, is a DoS attack that exploits the TCP threeway
handshake. The attacker rapidly generates randomly sourced SYN
packets filling the target's connection queue before the connection can timeout.
* land.c attack, is also a DoS attack that exploits TCP
SYN packets. The attacker sends a packet that gives both the source and destination as the target's address, and uses the same source and destination port. Sources: Designing Network Security by Merike Kaeo (Cisco Press, 1999) and Mastering Network Security by Chris Brenton (Sybex,
1999).

NEW QUESTION: 58
Which of the following would be best suited to oversee the development of an information security policy?
A. System Administrators
B. End User
C. Security Officers
D. Security administrators
Answer: (SHOW ANSWER)
The security officer would be the best person to oversea the development of such policies. Security officers and their teams have typically been charged with the responsibility of creating the security policies. The policies must be written and communicated appropriately to ensure that they can be understood by the end users. Policies that are poorly written, or written at too high of an education level (common industry practice is to focus the content for general users at the sixth- to eighth-grade reading level), will not be understood.

Implementing security policies and the items that support them shows due care by the company and its management staff. Informing employees of what is expected of them and the consequences of noncompliance can come down to a liability issue. While security officers may be responsible for the development of the security policies, the effort should be collaborative to ensure that the business issues are addressed. The security officers will get better corporate support by including other areas in policy development. This helps build buy-in by these areas as they take on a greater ownership of the final product. Consider including areas such as HR, legal, compliance, various IT areas and specific business area representatives who represent critical business units.

When policies are developed solely within the IT department and then distributed without business input, they are likely to miss important business considerations. Once policy documents have been created, the basis for ensuring compliance is established. Depending on the organization, additional documentation may be necessary to support policy. This support may come in the form of additional controls described in standards, baselines, or procedures to help personnel with compliance. An important step after documentation is to make the most current version of the

documents readily accessible to those who are expected to follow them. Many organizations place the documents on their intranets or in shared file folders to facilitate their accessibility. Such placement of these documents plus checklists, forms, and sample documents can make awareness more effective.

For your exam you should know the information below:

End User - The end user is responsible for protecting information assets on a daily basis through adherence to the security policies that have been communicated.

Executive Management/Senior Management - Executive management maintains the overall responsibility for protection of the information assets. The business operations are dependent upon information being available, accurate, and protected from individuals without a need to know.

Security Officer - The security officer directs, coordinates, plans, and organizes information security activities throughout the organization. The security officer works with many different individuals, such as executive management, management of the business units, technical staff, business partners, auditors, and third parties such as vendors. The security officer and his or her team are responsible for the design, implementation, management, and review of the organization's security policies, standards, procedures, baselines, and guidelines.

Information Systems Security Professional- Drafting of security policies, standards and supporting guidelines, procedures, and baselines is coordinated through these individuals. Guidance is provided for technical security issues, and emerging threats are considered for the adoption of new policies. Activities such as interpretation of government regulations and industry trends and analysis of vendor solutions to include in the security architecture that advances the security of the organization are performed in this role.

Data/Information/Business/System Owners - A business executive or manager is typically responsible for an information asset. These are the individuals that assign the appropriate classification to information assets. They ensure that the business information is protected with appropriate controls. Periodically, the information asset owners need to review the classification and access rights associated with information assets. The owners, or their delegates, may be

required to approve access to the information. Owners also need to determine the criticality, sensitivity, retention, backups, and safeguards for the information. Owners or their delegates are responsible for understanding the risks that exist with regards to the information that they control.
Data/Information Custodian/Steward - A data custodian is an individual or function that takes care of the information on behalf of the owner. These individuals ensure that the information is available to the end users and is backed up to enable recovery in the event of data loss or corruption. Information may be stored in files, databases, or systems whose technical infrastructure must be managed, by systems administrators. This group administers access rights to the information assets.
Information Systems Auditor- IT auditors determine whether users, owners, custodians, systems, and networks are in compliance with the security policies, procedures, standards, baselines, designs, architectures, management direction, and other requirements placed on systems. The auditors provide independent assurance to the management on the appropriateness of the security controls. The auditor examines the information systems and determines whether they are designed, configured, implemented, operated, and managed in a way ensuring that the organizational objectives are being achieved. The auditors provide top company management with an independent view of the controls and their effectiveness.
Business Continuity Planner - Business continuity planners develop contingency plans to prepare for any occurrence that could have the ability to impact the company's objectives negatively. Threats may include earthquakes, tornadoes, hurricanes, blackouts, changes in the economic/political climate, terrorist activities, fire, or other major actions potentially causing significant harm. The business continuity planner ensures that business processes can continue through the disaster and coordinates those activities with the business areas and information technology personnel responsible for disaster recovery.
Information Systems/ Technology Professionals- These personnel are responsible for designing security controls into information systems, testing the controls, and implementing the systems in production environments through agreed upon operating policies and procedures. The information systems professionals work with the business owners and the security professionals to ensure that the designed solution provides security controls commensurate with the acceptable criticality, sensitivity, and availability requirements of the application.
Security Administrator - A security administrator manages the user access request process and ensures that privileges are provided to those individuals who have been authorized for access by application/system/data owners. This individual has elevated privileges and creates and deletes accounts and access permissions. The security administrator also terminates access privileges when individuals leave their jobs or transfer between company divisions. The security administrator maintains records of access request approvals and produces reports of access rights for the auditor during testing in an access controls audit to demonstrate compliance with the policies.
Network/Systems Administrator - A systems administrator (sysadmin/netadmin) configures network and server hardware and the operating systems to ensure that the information can be available and accessible. The administrator maintains the computing infrastructure using tools and utilities such as patch management and software distribution mechanisms to install updates and test patches on organization computers. The administrator tests and implements system upgrades to ensure the continued reliability of the servers and network devices. The administrator provides vulnerability management through either commercial off the

shelf (COTS) and/or non-COTS solutions to test the computing environment and mitigate vulnerabilities appropriately.

Physical Security - The individuals assigned to the physical security role establish relationships with external law enforcement, such as the local police agencies, state police, or the Federal Bureau of Investigation (FBI) to assist in investigations. Physical security personnel manage the installation, maintenance, and ongoing operation of the closed circuit television (CCTV) surveillance systems, burglar alarm systems, and card reader access control systems. Guards are placed where necessary as a deterrent to unauthorized access and to provide safety for the company employees. Physical security personnel interface with systems security, human resources, facilities, and legal and business areas to ensure that the practices are integrated.

Security Analyst - The security analyst role works at a higher, more strategic level than the previously described roles and helps develop policies, standards, and guidelines, as well as set various baselines. Whereas the previous roles are "in the weeds" and focus on pieces and parts of the security program, a security analyst helps define the security program elements and follows through to ensure the elements are being carried out and practiced properly. This person works more at a design level than at an implementation level.

Administrative Assistants/Secretaries - This role can be very important to information security; in many companies of smaller size, this may be the individual who greets visitors, signs packages in and out, recognizes individuals who desire to enter the offices, and serves as the phone screener for executives. These individuals may be subject to social engineering attacks, whereby the potential intruder attempts to solicit confidential information that may be used for a subsequent attack. Social engineers prey on the goodwill of the helpful individual to gain entry. A properly trained assistant will minimize the risk of divulging useful company information or of providing unauthorized entry.

Help Desk Administrator - As the name implies, the help desk is there to field questions from users that report system problems. Problems may include poor response time, potential virus infections, unauthorized access, inability to access system resources, or questions on the use of a program. The help desk is also often where the first indications of security issues and incidents will be seen. A help desk individual would contact the computer security incident response team (CIRT) when a situation meets the criteria developed by the team. The help desk resets passwords, resynchronizes/reinitializes tokens and smart cards, and resolves other problems with access control.

Supervisor - The supervisor role, also called user manager, is ultimately responsible for all user activity and any assets created and owned by these users. For example, suppose Kathy is the supervisor of ten employees. Her responsibilities would include ensuring that these employees understand their responsibilities with respect to security; making sure the employees' account information is up-to-date; and informing the security administrator when an employee is fired,
suspended, or transferred. Any change that pertains to an employee's role within the company usually affects what access rights they should and should not have, so the user manager must inform the security administrator of these changes immediately.

Change Control Analyst Since the only thing that is constant is change, someone must make sure changes happen securely. The change control analyst is responsible for approving or rejecting requests to make changes to the network, systems, or software. This role must make certain that

the change will not introduce any vulnerabilities, that it has been properly tested, and that it is properly rolled out. The change control analyst needs to understand how various changes can affect security, interoperability, performance, and productivity. Or, a company can choose to just roll out the change and see what happens.
The following answers are incorrect:
Systems Administrator - A systems administrator (sysadmin/netadmin) configures network and server hardware and the operating systems to ensure that the information can be available and accessible. The administrator maintains the computing infrastructure using tools and utilities such as patch management and software distribution mechanisms to install updates and test patches on organization computers. The administrator tests and implements system upgrades to ensure the continued reliability of the servers and network devices. The administrator provides vulnerability management through either commercial off the shelf (COTS) and/or non-COTS solutions to test the computing environment and mitigate vulnerabilities appropriately.
End User - The end user is responsible for protecting information assets on a daily basis through adherence to the security policies that have been communicated.
Security Administrator - A security administrator manages the user access request process and ensures that privileges are provided to those individuals who have been authorized for access by application/system/data owners. This individual has elevated privileges and creates and deletes accounts and access permissions. The security administrator also terminates access privileges when individuals leave their jobs or transfer between company divisions. The security administrator maintains records of access request approvals and produces reports of access rights for the auditor during testing in an access controls audit to demonstrate compliance with the policies.
Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 109
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 108). McGraw-Hill. Kindle Edition.

NEW QUESTION: 59
Which of the following is not a component of a Operations Security "triples"?
A. Asset
B. Threat
C. Vulnerability
D. Risk
Answer: (SHOW ANSWER)
The Operations Security domain is concerned with triples - threats, vulnerabilities and assets. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 216.

NEW QUESTION: 60

Which of the following ensures that security is not breached when a system crash or other system failure occurs?

A. trusted recovery

B. hot swappable

C. redundancy

D. secure boot

Answer: (SHOW ANSWER)

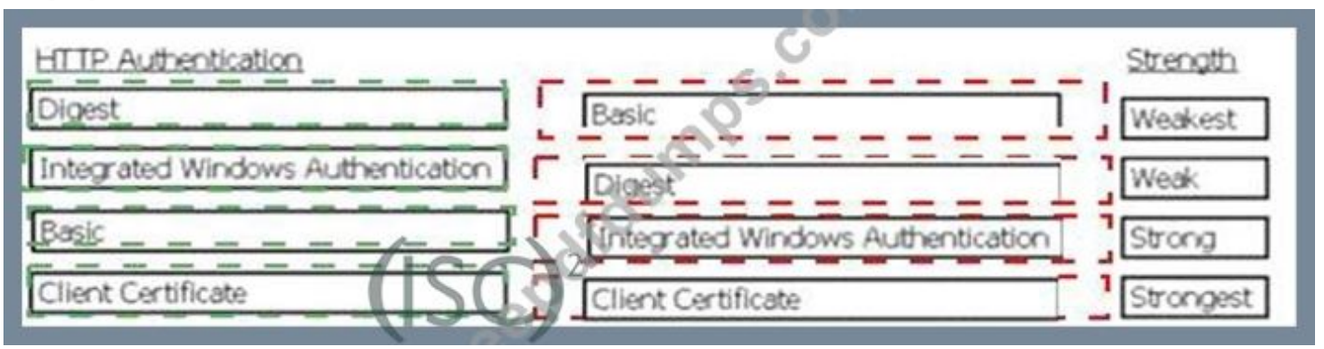
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, page 222.

"System crash" and "system failure" are the key words. One "recovers" from a crash or failure.

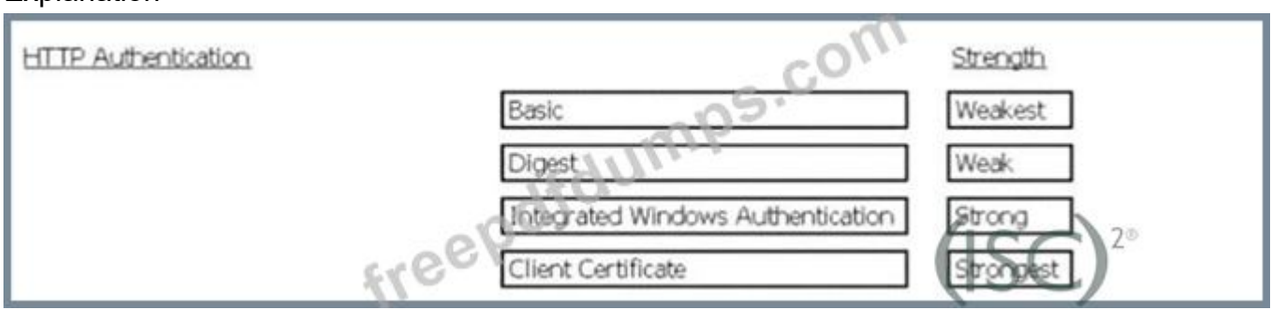
NEW QUESTION: 61

Rank the Hypertext Transfer protocol (HTTP) authentication types shows below in order of relative strength. Drag the authentication type on the correct positions on the right according to strength from weakest to strongest.

Answer:



Explanation



NEW QUESTION: 62
How do the Information Labels of Compartmented Mode Workstation differ from the Sensitivity Levels of B3 evaluated systems?
A. Information Labels in CMW are homologous to Sensitivity Labels, but a different term was chosen to emphasize that CMW's are not described in the Orange Book.
B. Information Labels contain more information than Sensitivity Labels, thus allowing more granular access decisions to be made.
C. Sensitivity Labels contain more information than Information Labels because B3+ systems should store more sensitive data than workstations.
D. Information Labels contain more information than Sensitivity Labels, but are not used by the Reference Monitor to determine access permissions.
Answer: D (LEAVE A REPLY)
The primary goal of the compartmented mode workstation (CMW) project was to articulate the security requirements that workstations must meet to process highly classified intelligence data. As a basis for the validity of the requirements developed, a prototype was implemented which demonstrated that workstations could meet the requirements in an operationally useful manner while still remaining binary compatible with off-the-shelf software. The security requirements not only addressed traditional security concerns but also introduced concepts in areas such as labeling and the use of a trusted window management system. The CMW labeling paradigm is based on associating two types of security labels with objects: sensitivity levels and information labels. Sensitivity levels describe the levels at which objects must be protected. Information labels are used to prevent data over classification and also provide a mechanism for associating with data those markings that are required for accurate data labeling, but which play no role in access control decisions. The use of a trusted window manager allows users to easily operate at multiple sensitivity levels and provides a convenient mechanism for communicating security information to users in a relatively unobtrusive manner. Information labels are not used by reference monitor, permissions are referenced in Sensibility labels.

NEW QUESTION: 63
A Security Operations Center (SOC) receives an incident response notification on a server with an active intruder who has planted a backdoor. Initial notifications are sent and communications are established. What MUST be considered or evaluated before performing the next step?
A. Notifying law enforcement is crucial before hashing the contents of the server hard drive
B. Identifying who executed the incident is more important than how the incident happened
C. Removing the server from the network may prevent catching the intruder

D. Copying the contents of the hard drive to another storage device may damage the evidence
Answer: (SHOW ANSWER)
Section: Security Operations

NEW QUESTION: 64
Which of the following is the PRIMARY reason a sniffer operating on a network is collecting packets only from its own host?
A. The network is connected using switches.
B. The network's firewall does not allow sniffing.
C. An Intrusion Detection System (IDS) has dropped the packets.
D. The network is connected using hubs.
Answer: (SHOW ANSWER)

NEW QUESTION: 65
Which standard defines the International Standard for the Common
Criteria?
A. CSC-STD-002-85
B. IS15408
C. BS7799
D. DoD 5200.28-STD
Answer: B (LEAVE A REPLY)
ISO/IEC 15408-1 is the International Standards version of the Common CriteriA. The ISO approved and published the CC text as the new International Standard (IS) 15408 on December 1, 19994. As of this writing the Common Criteria version is 2.1. Answer b is the Code of Practice for Information Security Management (BS7799) developed by the British Standards Institute. The BS7799 standard effectively comes in two parts: ISO/IEC 17799:2000 (Part 1) is the standard code of practice and can be regarded as a comprehensive catalogue of recommended security policy. BS7799-2:1999 (Part 2) is a standard specification for an Information Security Management System (ISMS). An ISMS is the means by which Senior Management monitors and controls their security, minimizing the residual business risk and ensuring that security continues to fulfill corporate, customer, and legal requirements.5 *Answer DoD 5200.28-STD is the Orange Book, the DoD Trusted Computer System Evaluation Criteria. *Answer CSC-STD-002-85 is the Green Book, the DoD Password Management Guidelines. Source: The Common Criteria Project.

NEW QUESTION: 66
Which of the following is an unintended communication path that is NOT protected by the system's normal security mechanisms?
A. A trusted path
B. A protection domain
C. A covert channel
D. A maintenance hook
Answer: C (LEAVE A REPLY)

A covert channel is an unintended communication path within a system, therefore it is not protected by the system's normal security mechanisms. Covert channels are a secret way to convey information.
Covert channels are addressed from TCSEC level B2.
The following are incorrect answers:
A trusted path is the protected channel that allows a user to access the Trusted Computing Base (TCB) without being compromised by other processes or users.
A protection domain consists of the execution and memory space assigned to each process.
A maintenance hook is a hardware or software mechanism that was installed to permit system maintenance and to bypass the system's security protections.
Reference used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 6: Operations Security (page 219).

NEW QUESTION: 67
When attempting to establish liability, which of the following would be described as performing the ongoing maintenance necessary to keep something in proper working order, updated, effective, or to abide by what is commonly expected in a situation?
A. Due care
B. Due concern
C. Due diligence
D. Due practice
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Due care is performing the ongoing maintenance necessary to keep something in proper working order, or to abide by what is commonly expected in a situation. This is especially important if the due care situation exists because of a contract, regulation, or law. The opposite of due care is "negligence." EXAM TIP:
The Due Diligence refers to the steps taken to identify risks that exist within the environment. This is based on best practices, standards such as ISO 27001, ISO 17799, and other consensus. The first letter of the word Due and the word Diligence should remind you of this. The two letters are DD = Do Detect.
In the case of due care, it is the actions that you have taken (implementing, designing, enforcing, updating) to reduce the risks identified and keep them at an acceptable level. The same apply here, the first letters of the work Due and the work Care are DC. Which should remind you that DC = Do correct.
Incorrect Answers:
B: Due concern is not a valid answer. Due Care is what is described in the question.
C: Due diligence is performing reasonable examination and research before committing to a course of action. Basically, "look before you leap." In law, you would perform due diligence by researching the terms of a contract before signing it. The opposite of due diligence might be "haphazard" or "not doing your homework." This is not what is described in the question.
D: Due practice is not a valid answer. Due Care is what is described in the question.

NEW QUESTION: 68
Which of the following describes the sequence of steps required for a Kerberos session to be established between a user (Principal P1), and an application server (Principal P2)?
A. Principals P1 and Principals P2 authenticate to the Key Distribution Center (KDC),
B. Principal P1 receives a Ticket Granting Ticket (TGT), and then Principal P2 requests a service ticket from the KDC.
C. Principal P1 authenticates to the Key Distribution Center(KDC), Principal P1 receives a Ticket Granting Ticket (TGT), and Principal P1 requests a service ticket from the Ticket Granting Service (TGS) in order to access the application server P2
D. Principal P1 authenticates to the Key Distribution Center (KDC),
E. Principal P1 requests a Ticket Granting Ticket (TGT) from the authentication server, and then Principal P1 requests a service ticket from the application server P2
F. Principals P1 and P2 authenticate to the Key Distribution Center (KDC), Principal P1 requests a Ticket Granting Ticket (TGT) from the authentication server, and application server P2 requests a service ticket from P1
Answer: C (LEAVE A REPLY)
Principles P1 and P2 authenticate to the Key Distribution Center (KDC), principle P1 receives a Ticket Granting Ticket (TGT), and principle P2 requests a service ticket from the KDC.
The principle P2 does not request a service ticket. P1 would request a service ticket.
Principles P1 and P2 authenticate to the Key Distribution Center (KDC), principle P1 requests a Ticket Granting Ticket (TGT) from the authentication server, and application server P2 requests a service ticket from P1
A request by P1 to access P2 will fail without a service ticket, but this is not the best answer.
Principle P1 authenticates to the Key Distribution Center (KDC), principle P1 requests a Ticket Granting Ticket (TGT) from the authentication server, and principle P1 requests a service ticket from the application server P2
The request for a service ticket is made to the KDC, not to P2 P2 does not proxy authentication requests for the principle P1
The following reference(s) were/was used to create this question:
Sybex CISSP Study Guide, Third Edition. pg 21
Kerberos logon process: User types in username and password, a symmetric key is derive from the password, the user sends a Kerberos Authentication requrest to KDC, which returns a TGT showing the user was identified.
"1) The client sends its TGT back to Ticket Granting Service (TGS) on the KDC with request for access to a server or service"
"3) A service ticket (ST) is granted and sent to the client. The service ticket includes a session key encrypted with the client symmetric key and also encrypted with the service or server symmetric key"
"4) The client sends the ST to the server or service host."

NEW QUESTION: 69
Which of the following is the BEST mitigation from phishing attacks?
A. Strong file and directory permissions
B. Security awareness training
C. Network activity monitoring
D. Corporate policy and procedures
Answer: B (LEAVE A REPLY)

NEW QUESTION: 70
Which of the following services is provided by S-RPC?
A. Availability
B. Accountability
C. Integrity
D. Authentication
Answer: D (LEAVE A REPLY)
Secure RPC provides authentication services. Secure RPC (Remote Procedure Call) protects remote procedures with an authentication mechanism. The Diffie-Hellman authentication mechanism authenticates both the host and the user who is making a request for a service. The authentication mechanism uses Data Encryption Standard (DES) encryption. Applications that use Secure RPC include NFS and the naming services, NIS and NIS+.
WHAT IS RPC?
Remote Procedure Call (RPC) is a protocol that one program can use to request a service from a program located in another computer in a network without having to understand network details. (A procedure call is also sometimes known as a function call or a subroutine call.) RPC uses the client/server model. The requesting program is a client and the service-providing program is the server. Like a regular or local procedure call, an RPC is a synchronous operation requiring the requesting program to be suspended until the results of the remote procedure are returned. However, the use of lightweight processes or threads that share the same address space allows multiple RPCs to be performed concurrently. When program statements that use RPC are compiled into an executable program, a stub is included in the compiled code that acts as the representative of the remote procedure code. When the program is run and the procedure call is issued, the stub receives the request and forwards it to a client runtime program in the local computer. The client runtime program has the knowledge of how to address the remote computer and server application and sends the message across the network that requests the remote procedure. Similarly, the server includes a runtime program and stub that interface with the remote procedure itself. Results are returned the same way. There are several RPC models and implementations. A popular model and implementation is the Open Software Foundation's Distributed Computing Environment (DCE). The Institute of Electrical and Electronics Engineers defines RPC in its ISO Remote Procedure Call Specification, ISO/IEC CD 11578 N6561, ISO/IEC, November 1991. RPC spans the Transport layer and the Application layer in the Open Systems Interconnection (OSI) model of network communication. RPC makes it easier to develop an application that includes multiple programs distributed in a network. All of the other answers are not features of S/RPC.

Reference(s) used for this Question: http://docs.sun.com/app/docs/doc/816-4883/6mb2joane?a=view and http://docs.oracle.com/cd/E23823_01/html/816-4557/auth-2.html and

NEW QUESTION: 71

Which of the following is NOT a known type of Message Authentication Code (MAC)?

A. Keyed-hash message authentication code (HMAC)

B. DES-CBC

C. Signature-based MAC (SMAC)

D. Universal Hashing Based MAC (UMAC)

Answer: (SHOW ANSWER)

There is no such thing as a Signature-Based MAC. Being the wrong choice in the list, it is the best answer to this question.

WHAT IS A Message Authentication Code (MAC)?

In Cryptography, a MAC (Message Authentication Code) also known as a cryptographic checksum, is a small block of data that is generated using a secret key and then appended to the message. When the message is received, the recipient can generate their own MAC using the secret key, and thereby know that the message has not changed either accidentally or intentionally in transit. Of course, this assurance is only as strong as the trust that the two parties have that no one else has access to the secret key.

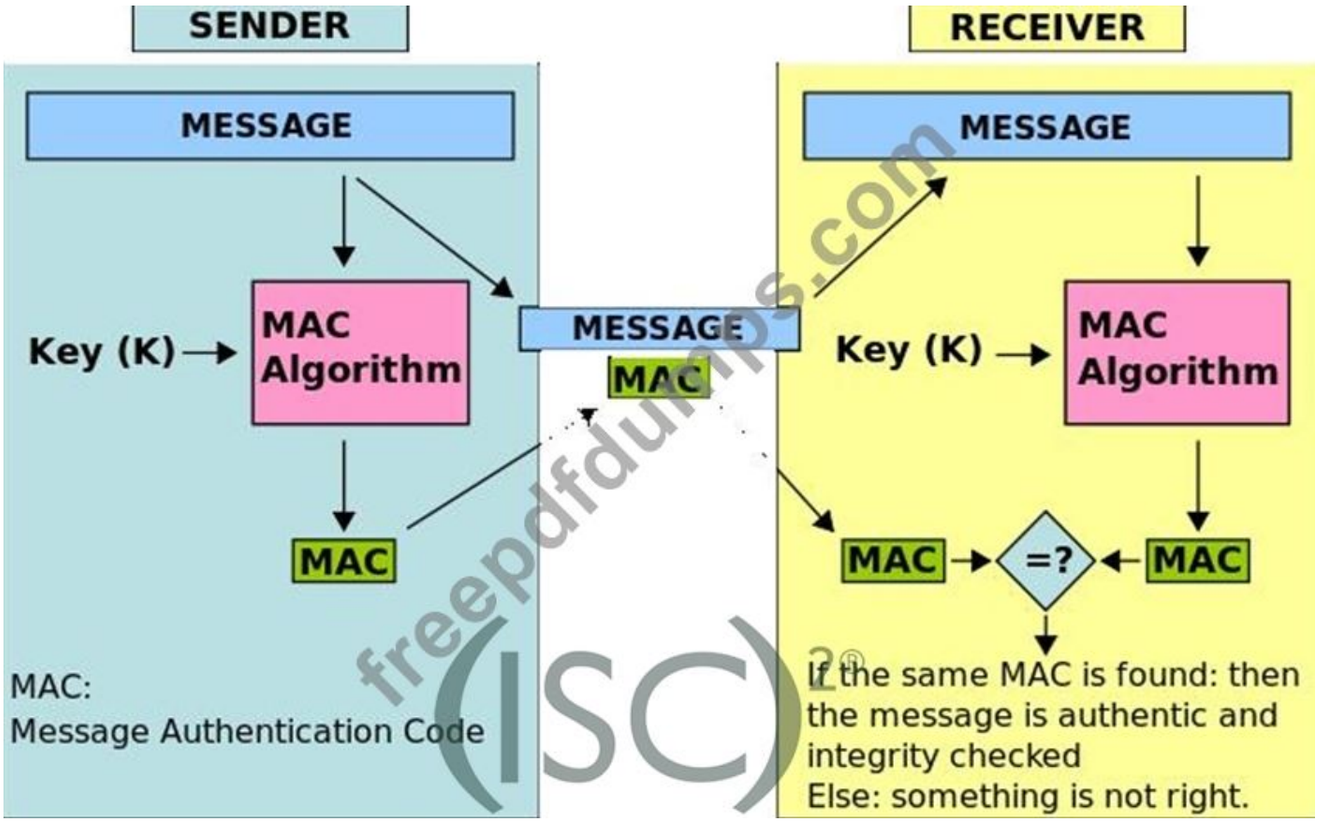
A MAC is a small representation of a message and has the following characteristics:

A MAC is much smaller than the message generating it.

Given a MAC, it is impractical to compute the message that generated it.

Given a MAC and the message that generated it, it is impractical to find another message generating the same MAC.

See the graphic below from Wikipedia showing the creation of a MAC value:



Message Authentication Code MAC HMAC

In the example above, the sender of a message runs it through a MAC algorithm to produce a MAC data tag. The message and the MAC tag are then sent to the receiver. The receiver in turn runs the message portion of the transmission through the same MAC algorithm using the same key, producing a second MAC data tag. The receiver then compares the first MAC tag received in the transmission to the second generated MAC tag. If they are identical, the receiver can safely assume that the integrity of the message was not compromised, and the message was not altered or tampered with during transmission.

However, to allow the receiver to be able to detect replay attacks, the message itself must contain data that assures that this same message can only be sent once (e.g. time stamp, sequence number or use of a one-time MAC). Otherwise an attacker could - without even understanding its content - record this message and play it back at a later time, producing the same result as the original sender.

NOTE: There are many ways of producing a MAC value. Below you have a short list of some implementation.

The following were incorrect answers for this question:

They were all incorrect answers because they are all real type of MAC implementation.

In the case of DES-CBC, a MAC is generated using the DES algorithm in CBC mode, and the secret DES key is shared by the sender and the receiver. The MAC is actually just the last block of ciphertext generated by the algorithm. This block of data (64 bits) is attached to the unencrypted message and transmitted to the far end. All previous blocks of encrypted data are discarded to prevent any attack on the MAC itself. The receiver can just generate his own MAC using the secret DES key he shares to ensure message integrity and authentication. He knows that the message has not changed because the chaining function of CBC would significantly alter the last block of data if any bit had changed anywhere in the message. He knows the source of the message (authentication) because only one other person holds the secret key.

A Keyed-hash message authentication code (HMAC) is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret cryptographic key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authentication of a message. Any cryptographic hash function, such as MD5, SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA1 accordingly.
The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output, and on the size and quality of the key.
A message authentication code based on universal hashing, or UMAC, is a type of message authentication code (MAC) calculated choosing a hash function from a class of hash functions according to some secret (random) process and applying it to the message.
The resulting digest or fingerprint is then encrypted to hide the identity of the hash function used. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message.
UMAC is specified in RFC 4418, it has provable cryptographic strength and is usually a lot less computationally intensive than other MACs.
What is the MicMac (confusion) with MIC and MAC?
The term message integrity code (MIC) is frequently substituted for the term MAC, especially in communications, where the acronym MAC traditionally stands for Media
Access Control when referring to Networking. However, some authors use MIC as a distinctly different term from a MAC; in their usage of the term the MIC operation does not use secret keys. This lack of security means that any MIC intended for use gauging message integrity should be encrypted or otherwise be protected against tampering. MIC algorithms are created such that a given message will always produce the same MIC assuming the same algorithm is used to generate both. Conversely, MAC algorithms are designed to produce matching MACs only if the same message, secret key and initialization vector are input to the same algorithm. MICs do not use secret keys and, when taken on their own, are therefore a much less reliable gauge of message integrity than
MACs. Because MACs use secret keys, they do not necessarily need to be encrypted to provide the same level of assurance.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third
Edition ((ISC)2 Press) (Kindle Locations 15799-15815). Auerbach Publications. Kindle
Edition.
and
http://en.wikipedia.org/wiki/Message_authentication_code
and
http://tools.ietf.org/html/rfc4418

NEW QUESTION: 72
Which choices below are roles or responsibility of the person
designated to manage the contingency planning process? Select three
A. Providing direction to senior management
B. Ensuring the identification of all critical business functions

C. Integrating the planning process across business units
D. Providing stress reduction programs to employees after an event
Answer: (SHOW ANSWER)
Contingency planners have many roles and responsibilities when planning business continuity, disaster recovery, emergency management, or business resumption processes. In addition to correct answers some of these roles and responsibilities can include: Ensuring executive management compliance with the contingency plan program Providing periodic management reports and status Coordinating and integrating the activation of emergency response organizations Answer "Providing stress reduction programs to employees after an event", providing stress reduction programs to employees after an event, is a responsibility of the human resources area. Source: Contingency Planning and Management, Contingency Planning 101, by Kelley Goggins, March 1999.

NEW QUESTION: 73
The information security staff's participation in which of the following system development life cycle phases provides maximum benefit to the organization?
A. project initiation and planning phase
B. system design specifications phase
C. development and documentation phase
D. in parallel with every phase throughout the project
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
A system has a developmental life cycle, which is made up of the following phases: initiation, acquisition/ development, implementation, operation/maintenance, and disposal. Collectively these are referred to as a system development life cycle (SDLC).
Security is critical in each phase of the life cycle.
In the initiation phase the company establishes the need for a specific system. The company has figured out that there is a problem that can be solved or a function that can be carried out through some type of technology. A preliminary risk assessment should be carried out to develop an initial description of the confidentiality, integrity, and availability requirements of the system.
The Acquisition/Development phase should include security analysis such as Security functional requirements analysis and Security assurance requirements analysis
In the Implementation phase, it may be necessary to carry out certification and accreditation (C&A) processes before a system can be formally installed within the production environment. Certification is the technical testing of a system.
In the Operation and Maintenance phase, continuous monitoring needs to take place to ensure that security baselines are always met. Vulnerability assessments and penetration testing should also take place in this phase. These types of periodic testing allow for new vulnerabilities to be identified and remediated.
Disposal phase: When a system no longer provides a needed function, plans for how the system and its data will make a transition should be developed. Data may need to be moved to a different system, archived,

discarded, or destroyed. If proper steps are not taken during the disposal phase, unauthorized access to sensitive assets can take place.
Incorrect Answers:
A: Security staff should participate in all phases of the system development life cycle, not just the project initiation and planning phases.
B: Security staff should participate in all phases of the system development life cycle, not just the development phase. Documentation is not one of the phases in the system development life cycle.
C: System design specifications would happen in the development phase. 'System design specifications' is not a recognized phase in itself. Security staff should participate in all phases of the system development life cycle, not just the development phase.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, pp. 1087-1093

NEW QUESTION: 74
Which of the following statements pertaining to biometrics is FALSE?
A. User can be authenticated based on behavior.
B. User can be authenticated based on unique physical attributes.
C. User can be authenticated by what he knows.
D. A biometric system's accuracy is determined by its crossover error rate (CER).
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Biometrics is based on "what you are" or "what you do". It is not based on what you know.
Incorrect Answers:
A: Behavioral (what you do), is one of the two categories that biometrics are divided into.
B: The physiological biometric category refers to traits that are physical attributes unique to a specific individual.
D: When determining a biometric system's accuracy, the CER metric is the most important measurement.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, pp. 187, 188

NEW QUESTION: 75
What is the effective key size of DES?
A. 56 bits
B. 64 bits
C. 128 bits
D. 1024 bits
Answer: A (LEAVE A REPLY)
Data Encryption Standard (DES) is a symmetric key algorithm. Originally developed by IBM, under project name Lucifer, this 128-bit algorithm was accepted by the NIST in 1974, but the total key size was reduced to 64 bits, 56 of which make up the effective key, plus and extra 8 bits for parity. It somehow became a national

cryptographic standard in 1977, and an American National Standard Institute (ANSI) standard in 1978. DES was later replaced by the Advanced Encryption Standard (AES) by the NIST. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 8: Cryptography (page 525).

NEW QUESTION: 76
What does the directive of the European Union on Electronic Signatures deal with?
A. Encryption of classified data
B. Encryption of secret data
C. Non repudiation
D. Authentication of web servers
Answer: (SHOW ANSWER)
Explanation/Reference:
Reference:
FORD, Warwick & BAUM, Michael S., Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption (2nd Edition), 2000, Prentice Hall PTR, Page 589; Directive 1999/93/

NEW QUESTION: 77
Which layer of the OSI/ISO model handles physical addressing, network topology, line discipline, error notification, orderly delivery of frames, and optional flow control?
A. Physical
B. Data link
C. Network
D. Session
Answer: B (LEAVE A REPLY)
The Data Link layer provides data transport across a physical link. It handles
physical addressing, network topology, line discipline, error notification, orderly delivery of frames,
and optional flow control.
Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 2, August 1999.

NEW QUESTION: 78
Which of the following is NOT part of user provisioning?
A. Creation and deactivation of user accounts
B. Business process implementation

C. Maintenance and deactivation of user objects and attributes
D. Delegating user administration
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
User provisioning involves the creation, maintenance, and deactivation of user objects and attributes as they exist in one or more systems, directories, or applications, in response to business processes.
Business process implementation is not part of this.
Incorrect Answers:
A: User provisioning involves creating, maintaining, and deactivating accounts as necessary according to business requirements.
C: User provisioning involves the creation, maintenance, and deactivation of user objects and attributes as they exist in one or more systems, directories, or applications, in response to business processes.
D: Delegated user administration is a component of user provisioning software.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 179

NEW QUESTION: 79
Refer to the information below to answer the question.
A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns.
In the plan, what is the BEST approach to mitigate future internal client-based attacks?
A. Screen for harmful exploits of client-side services before implementation.
B. Remove all non-essential client-side web services from the network.
C. Harden the client image before deployment.
D. Block all client side web exploits at the perimeter.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 80
Which answer best describes a computer software attack that takes advantage of a previously unpublished vulnerability?
A. Zero-Day Attack
B. Exploit Attack
C. Vulnerability Attack
D. Software Crack
Answer: A (LEAVE A REPLY)
A zero-day (or zero-hour, or Oday, or day zero) attack or threat is a computer threat that tries to exploit computer application vulnerabilities that are unknown to others or the software developer. Zero-day exploits (actual software that uses a security hole to carry out an attack) are used or shared by attackers before the developer of the target software knows about the vulnerability. The term derives from the age of the exploit. A "zero day" attack occurs on or before the first or "zeroth" day of developer awareness, meaning the developer

has not had any opportunity to distribute a security fix to users of the software. Zero-day attacks occur during the vulnerability window that exists in the time between when a vulnerability is first exploited and when software developers start to develop a counter to that threat.
For viruses, Trojans and other zero-day attacks, the vulnerability window follows this time line:
The developer creates software containing an unknown vulnerability The attacker finds the vulnerability before the developer does The attacker writes and distributes an exploit while the vulnerability is not known to the developer The developer becomes aware of the vulnerability and starts developing a fix.
The following answers are incorrect:
Exploit Attack An exploit (from the verb to exploit, in the meaning of using something to one's own advantage) is a piece of software, a chunk of data, or sequence of commands that takes advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerised). This frequently includes such things as gaining control of a computer system or allowing privilege escalation or a denial-ofservice attack.
Vulnerability Attack There is no such thing as the term Vulnerability Attack. However a vulnerability is synonyous with a weakness, it could be bad quality of software, a weakness within your physical security, or a weakness in your policies and procedures. An attacker will take advantage of a weakness and usually use an exploit to gain access to your systems without proper authorization or privilege.
Software Crack Software cracking is the modification of software to remove or disable features which are considered undesirable by the person cracking the software, usually related to protection methods: copy protection, trial/demo version, serial number, hardware key, date checks, CD check or software annoyances like nag screens and adware.
A crack is the software tool used to remove the need to insert a serial number or activation key.
The following reference(s) were/was used to create this question: 2011, Ethical Hacking and Countermeasures, EC-Council Official Curriculum, Book 1, Page 9
https://en.wikipedia.org/wiki/Zero_day_attack https://en.wikipedia.org/wiki/Exploit_%28computer_security%29 https://en.wikipedia.org/wiki/Software_cracking

NEW QUESTION: 81
As part of an application penetration testing process, session hijacking can BEST be achieved by which of the following?
A. Known-plaintext attack
B. Denial of Service (DoS)
C. Structured Query Language (SQL) injection
D. Cookie manipulation
Answer: (SHOW ANSWER)

NEW QUESTION: 82
How does a Host Based Intrusion Detection System (HIDS) identify a potential attack?
A. Monitors alarms sent to the system administrator
B. Examines the Access Control List (ACL)
C. Examines log messages or other indications on the system.

D. Matches traffic patterns to virus signature files

Answer: (SHOW ANSWER)

NEW QUESTION: 83

Which division of the Orange Book deals with discretionary protection (need-to-know)?

A. D

B. C

C. B

D. A

Answer: B (LEAVE A REPLY)

C deals with discretionary protection. See metric below:

TNI/TCSEC MATRIX

	A1	B3	B2	B1	C2	C1
DISCRETIONARY ACCESS						
Discretionary Access Control						
Identification and Authentication						
System Integrity						
System Architecture						
Security Testing						
Security Features User's Guide Trusted Facility Manual Design Documentation Test Documentation						
CONTROLLED ACCESS						
Protect Audit Trails						
Object Reuse						
MANDATORY ACCESS CONTROL						
Labels						
Mandatory Access Control						
Process isolation in system architecture						
Design Specification & Verification						
Device labels						
Subject Sensitivity Labels						
Trusted Path						
Separation of Administrator and User functions						
Covert Channel Analysis (Only Covert Storage Channel at B2)						
Trusted Facility Management						
Configuration Management						
Trusted Recovery						
Covert Channel Analysis (Both Timing and Covert Channel analysis at B3)						
Security Administrator Role Defined						
Monitor events and notify security personnel						
Trusted Distribution						
Formal Methods						
	A1	B3	B2	B1	C2	C1

TCSEC Metric

The following are incorrect answers:

D is incorrect. D deals with minimal security.

B is incorrect. B deals with mandatory protection.

A is incorrect. A deals with verified protection.

Reference(s) used for this question:
CBK, p. 329 - 330
and
Shon Harris, CISSP All In One (AIO), 6th Edition , page 392-393

NEW QUESTION: 84
Which of the following is the BEST reason for the use of security metrics?
A. They provide an appropriate framework for Information Technology (IT) governance.
B. They quantify the effectiveness of security processes.
C. They ensure that the organization meets its security objectives.
D. They speed up the process of quantitative risk assessment.
Answer: (SHOW ANSWER)

NEW QUESTION: 85
Which of the following is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism?
A. OAKLEY
B. Internet Security Association and Key Management Protocol (ISAKMP)
C. Simple Key-management for Internet Protocols (SKIP)
D. IPsec Key exchange (IKE)
Answer: B (LEAVE A REPLY)
RFC 2828 (Internet Security Glossary) defines the Internet Security Association and Key Management Protocol (ISAKMP) as an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism. Simple Key-management for Internet Protocols (SKIP) is a key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets. OAKLEY is a key establishment protocol (proposed for IPsec but superseded by IKE) based on the Diffie-Hellman algorithm and designed to be a compatible component of ISAKMP. IPsec Key Exchange (IKE) is an Internet, IPsec, key-establishment protocol [R2409] (partly based on OAKLEY) that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations, such as in AH and ESP. Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 86
In what security mode can a system be operating if all users have the clearance or authorization and need-to-know to all data processed within the system?
A. Dedicated security mode.
B. System-high security mode.
C. Compartmented security mode.

D. Multilevel security mode.

Answer: A (LEAVE A REPLY)

An information-system (IS) security mode of operation wherein each user with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has all of the following: (a) a valid security clearance for all information within the system; (b) formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, sub compartments, and/or special access programs); and (c) a valid need-to-know for all information contained within the IS. When in the dedicated security mode, a system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time.

NEW QUESTION: 87

Which of the following answers presents the MOST significant threat to network based IDS or IPS systems?

A. Encrypted Traffic

B. Complex IDS/IPS Signature Syntax

C. Digitally Signed Network Packets

D. Segregated VLANs

Answer: A (LEAVE A REPLY)

Discussion: Encrypted network packets present the biggest threat to an effective IDS/IPS plan because the network cannot easily (Or quickly) be decoded and examined.

Encrypted packets can't be examined by the IDS to determine if there is a threat there so in most cases the traffic is just forwarded along with the potential threat.

There is an industry where a company provides examination services for your network traffic, acting like a proxy server for all your network traffic.

You simply send them copies of your certificates so they can decode the traffic. This is common in the financial industry where violating federal law or being sued by federal investigators for insider trading can lead to business collapse.

The external company examines all the network traffic coming and going from your network for potential liabilities.

The following answers are incorrect:

-Complex IDS/IPS Signature syntax: IDS/IPS signatures can be complex but this isn't the MOST significant threat to the functionality of an IDS/IPS system.

-Digitally Signed Network Packets: This is an incorrect answer because it isn't a threat to IDS/IPS systems looking for dangerous network traffic. Foremost because we don't commonly digitally sign each network packet we send.

-Segregated VLANs: This is not a correct answer but VLANs can present barriers to IDS/IPS systems spotting dangerous traffic. There is an easy solution to VLANs and IDS/IPS systems and that would be simply placing an IDS/IPS sensor on that VLAN and set it up to send its traffic to the IDS/IPS management system.

The following reference(s) was used to create this question:

Gregg, Michael; Haines, Billy (2012-02-16). CASP: CompTIA Advanced Security Practitioner Study Guide Authorized Courseware: Exam CAS-001 (Pg. 138) Wiley. Kindle Edition.

NEW QUESTION: 88
Which of the following is TRUE regarding Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)?
A. TCP is connection-oriented, UDP is not.
B. UDP provides for Error Correction, TCP does not.
C. UDP is useful for longer messages, rather than TCP.
D. TCP does not guarantee delivery of data, while UDP does guarantee data delivery.
Answer: A (LEAVE A REPLY)
TCP is a reliable connection-oriented transport for guaranteed delivery of data.
Protocols represent certain rules and regulations that are essential in order to have data communication between two entities. Internet Protocols work in sending and receiving data packets. This type of communication may be either connection-less or connection-oriented.
In a connection-oriented scenario, an acknowledgement is being received by the sender from the receiver in support of a perfect transfer. Transmission Control Protocol or TCP is such a protocol.
On the other hand, UDP or User Datagram Protocol is of the connection-less type where no feedback is being forwarded to the sender after delivery and the data transfer have taken place or not. Though, it's not a guaranteed method, but, once a connection is established, UDP works much faster than TCP as TCP has to rely on a feedback and accordingly, the entire 3-way handshaking takes place.
The following answers are incorrect:
UDP provides for Error Correction, TCP does not: UDP does not provide for error correction, while TCP does.
UDP is useful for longer messages, rather than TCP: UDP is useful for shorter messages due to its connectionless nature.
TCP does not guarantee delivery of data, while UDP does guarantee data delivery: The opposite is true.
References Used for this question:
http://www.cyberciti.biz/faq/key-differences-between-tcp-and-udp-protocols/
http://www.skullbox.net/tcpudp.php
James's TCP-IP FAQ - Understanding Port Numbers.

NEW QUESTION: 89
Which of the following statements pertaining to a security policy is incorrect?
A. Its main purpose is to inform the users, administrators and managers of their obligatory requirements for protecting technology and information assets.
B. It specifies how hardware and software should be used throughout the organization.
C. It needs to have the acceptance and support of all levels of employees within the organization in order for it to be appropriate and effective.
D. It must be flexible to the changing environment.
Answer: B (LEAVE A REPLY)
A security policy would NOT define how hardware and software should be used throughout the organization.
A standard or a procedure would provide such details but not a policy.

A security policy is a formal statement of the rules that people who are given access to anorganization's technology and information assets must abide. The policy communicates the security goals to all of the users, the administrators, and the managers. The goals will be largely determined by the following key tradeoffs: services offered versus security provided, ease of use versus security, and cost of security versus risk of loss.

The main purpose of a security policy is to inform the users, the administrators and the managers of their obligatory requirements for protecting technology and information assets.

The policy should specify the mechanisms through which these requirements can be met.

Another purpose is to provide a baseline from which to acquire, configure and audit computer systems and networks for compliance with the policy. In order for a security policy to be appropriate and effective, it needs to have the acceptance and support of all levels of employees within the organization. A good security policy must:

* Be able to be implemented through system administration procedures, publishing of acceptable use guidelines, or other appropriate methods
* Be able to be enforced with security tools, where appropriate, and with sanctions, where actual prevention is not technically feasible
* Clearly define the areas of responsibility for the users, the administrators, and the managers
* Be communicated to all once it is established
* Be flexible to the changing environment of a computer network since it is a living document

Reference(s) used for this question:

National Security Agency, Systems and Network Attack Center (SNAC),The 60 Minute Network Security Guide, February 2002, page 7.

or

A local copy is kept at:

https://www.freepracticetests.org/documents/The%2060%20Minute%20Network%20Security%20Guide.pdf

NEW QUESTION: 90

A portion of a Vigen?re cipher square is given below using five (1, 2, 14, 16, 22) of the possible 26 alphabets. Using the key word bow, which of the following is the encryption of the word advance using the Vigen?re cipher?

Exhibit:

Vigenère Cipher

PLAINTEXT	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
2	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
14	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
16	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
22	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v

A. b r r b b y f

B. b r r b b y h

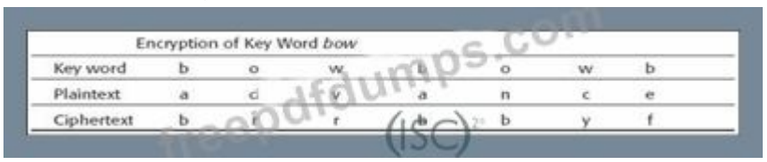
C. b r r b c y f

D. b r r b j y f

Answer: (SHOW ANSWER)

The Vigen?re cipher is a polyalphabetic substitution cipher. The key word bow indicates which alphabets to use. The letter b indicates the alphabet of row 1, the letter o indicates the alphabet of row 14, and the letter w indicates the alphabet of row 22. To encrypt, arrange the key word, repetitively over the plaintext as shown in Table.

Exhibit: Thus, the letter a of the plaintext is transformed into b of alphabet in row 1, the letter d is transformed into r of row 14, the letter v is transformed into r of row 22 and so on.



NEW QUESTION: 91

Of the following, which multiple access method for computer networks does 802.11 Wireless Local Area Network use?

A. CSMA/CA

B. CSMA/CD

C. 802.11 does not support multiple access methods

D. 802.11 RTS/CTS Exchange

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

802.11 Wireless Local Area Network uses CSMA\CA.

Note: Carrier sense multiple access with collision avoidance (CSMA/CA) is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by transmitting only when the channel is sensed to be "idle".

Incorrect Answers:

B: While Ethernet uses CSMA/CD, 802.11 Wireless does not. In wireless networks the collision detection of the alternative CSMA/CD is unreliable due to the hidden node problem.

C: 802.11 uses Carrier sense multiple access (CSMA/CA).

D: Wireless network uses CSMA/CA, not 802.11 RTS/CTS Exchange.

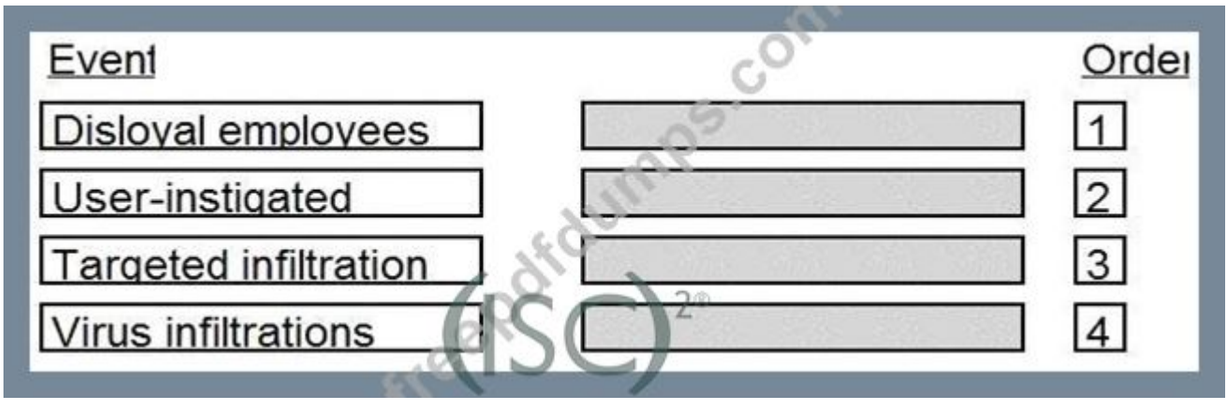
References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 578

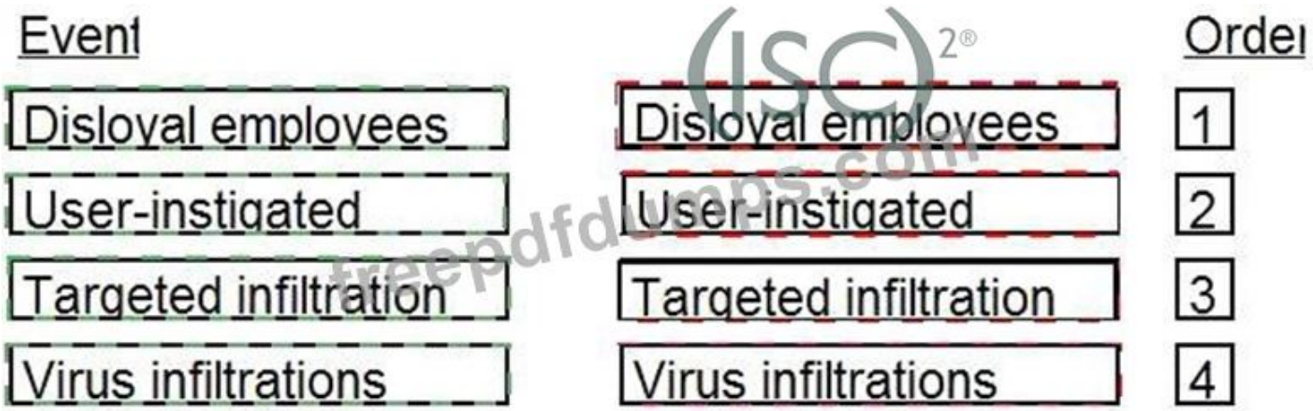
NEW QUESTION: 92
Which of the following practices provides the development team with a definition of security and identification of threats in designing software?
A. Threat modeling
B. Requirements review
C. Penetration testing
D. Stakeholder review
Answer: (SHOW ANSWER)

NEW QUESTION: 93
Which statement below is the BEST definition of need-to-know?
A. Need-to-know requires that the operator have the minimum knowledge of the system necessary to perform his task.
B. Need-to-know ensures that no single individual (acting alone) can compromise security controls.
C. Need-to-know grants each user the lowest clearance required for their tasks.
D. Need-to-know limits the time an operator performs a task.
Answer: (SHOW ANSWER)
The concept of need-to-know means that, in addition to whatever
specific object or role rights a user may have on the system, the
user has also the minimum amount of information necessary to perform
his job function.
* Answer "Need-to-know ensures that no single individual (acting alone) can compromise security controls." is separation of duties, assigning parts of tasks to different personnel.
*Answer "Need-to-know grants each user the lowest clearance required for their tasks." is least privilege, the user has the minimum security level required to perform his job function.
*Answer "Need-to-know limits the time an operator performs a task." is rotation of duties, wherein the amount of time an operator is assigned a security-sensitive task is limited before being moved to a different task with a different security classification.

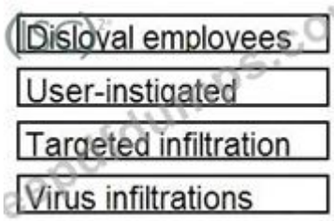
NEW QUESTION: 94
In which order, from MOST to LEAST impacted, does user awareness training reduce the occurrence of the events below?



Answer:



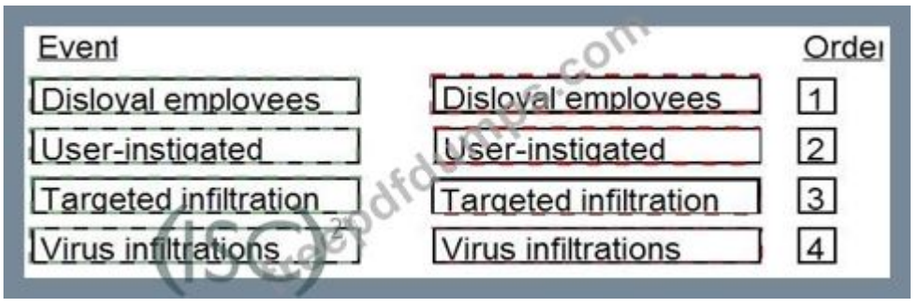
Explanation



NEW QUESTION: 95

In which order, from MOST to LEAST impacted, does user awareness training reduce the occurrence of the events below?

Answer:



Explanation

NEW QUESTION: 96

Which choice below MOST accurately describes partitioned security mode?

A. The only state in which certain privileged instructions may beexecuted.

B. A system containing information accessed by personnel with different security clearances.

C. All personnel have the clearance but not necessarily formal access approval.

D. All personnel have the clearance and formal access approval.

Answer: C (LEAVE A REPLY)

A partitioned security mode is a mode of operation wherein all personnel have the clearance but not necessarily formal access approval and need-to-know for all information contained in the system. *Answer "All personnel have the clearance and formal access approval" is a compartmented security modE. A compartmented security mode is a mode of operation wherein all personnel have a valid personnel clearance, formal access approval and signed nondisclosure agreements, and valid need-to-know for that information to which he/she is to have access. *Answer "The only state in which certain privileged instructions may beexecuted" is executive statE. Executive state is one of several states in which a system may operate and the only one in which certain privileged instructions may be executeD. Such instructions cannot be executed when the system is operating in other (e.g., user) states.

Synonymous with supervisor state. *Answer "A system containing information accessed by personnel with different security clearances" is multilevel securE. Multilevel secure is a class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and needs-to-know, but prevents users from obtaining access to information for which they lack

authorization. Source: DoD 5200.28-STD Department of Defense Trusted Computer System Evaluation Criteria.

NEW QUESTION: 97
RAID Level 1 mirrors the data from one disk to set of disks using which of the following techniques?
A. Copying the data onto another disk or set of disks.
B. Moving the data onto another disk or set of disks.
C. Establishing dual connectivity to another disk or set of disks.
D. Establishing dual addressing to another disk or set of disks.
Answer: (SHOW ANSWER)
Explanation: RAID 1 or Mirroring is a technique in which data is written to two duplicate disks simultaneously through a copy process. This way if one of the disk drives fails, the system can instantly switch to the other disk without any loss of data or service. Disk mirroring is used commonly in on-line database systems where it's critical that the data be accessible at all times. RAID means "Redundant Array of Inexpensive Disks".

NEW QUESTION: 98
Which of the following logical access exposures involvers changing data before, or as it is entered into the computer?
A. Data diddling
B. Salami techniques
C. Trojan horses
D. Viruses
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Data diddling refers to the alteration of existing data. Many times, this modification happens before the data is entered into an application or as soon as it completes processing and is outputted from an application. For instance, if a loan processor is entering information for a customer's loan of $100,000, but instead enters $150,000 and then moves the extra approved money somewhere else, this would be a case of data diddling. Another example is if a cashier enters an amount of $40 into the cash register, but really charges the customer $60 and keeps the extra $20.
This type of crime is extremely common and can be prevented by using appropriate access controls and proper segregation of duties. It will more likely be perpetrated by insiders, who have access to data before it is processed.
Incorrect Answers:
B: Salami techniques: A salami attack is the one in which an attacker commits several small crimes with the hope that the overall larger crime will go unnoticed. This is not what is described in the question.
C: A Trojan Horse is a program that is disguised as another program. This is not what is described in the question.
D: A Virus is a small application or a string of code that infects applications. This is not what is described in the question.

References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 1059

NEW QUESTION: 99
Which of the following processes has the PRIMARY purpose of identifying outdated software versions, missing patches, and lapsed system updates?
A. Penetration testing
B. Vulnerability management
C. Software Development Life Cycle (SDLC)
D. Life cycle management
Answer: (SHOW ANSWER)
Reference:
https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-operations/vulnerab

NEW QUESTION: 100
Which choice below is NOT an example of a media control?
A. Printing to a printer in a secured room
B. Conducting background checks on individuals
C. Sanitizing the media before disposition
D. Physically protecting copies of backup media
Answer: B (LEAVE A REPLY)
The answer is a personnel control. Most support and operations
staff have special access to the system. Some organizations conduct
background checks on individuals filling these positions to screen
out possibly untrustworthy individuals.
*Answer "Sanitizing the media before disposition": The process of removing information from media before disposition is called sanitization. Three techniques are commonly used
for media sanitization: overwriting, degaussing, and destruction.
*Answer "Printing to a printer in a secured room": It may be necessary to actually output data to the media in a secure location, such as printing to a printer in a locked room
instead of to a general-purpose printer in a common area.
*Answer "Physically protecting copies of backup media": Physical protection of copies of backup media stored offsite should be accorded a level of protection equivalent to media
containing the same information stored onsite.
Source: National Institute of Standards and Technology, An Introduction to Computer Security: The NIST Handbook Special Publication 800-12.

NEW QUESTION: 101
Which one of the following considerations has the LEAST impact when considering transmission security?
A. Network availability

B. Node locations
C. Network bandwidth
D. Data integrity
Answer: C (LEAVE A REPLY)
Section: Software Development Security

NEW QUESTION: 102
The use of strong authentication, the encryption of Personally Identifiable Information (PII) on database servers, application security reviews, and the encryption of data transmitted across networks provide
A. data integrity.
B. defense in depth.
C. data availability.
D. non-repudiation.
Answer: (SHOW ANSWER)

NEW QUESTION: 103
In computing what is the name of a non-self-replicating type of malware program containing malicious code that appears to have some useful purpose but also contains code that has a malicious or harmful purpose imbedded in it, when executed, carries out actions that are unknown to the person installing it, typically causing loss or theft of data, and possible system harm.
A. virus.
B. worm.
C. Trojan horse.
D. trapdoor.
Answer: C (LEAVE A REPLY)
A trojan horse is any code that appears to have some useful purpose but also
contains code that has a malicious or harmful purpose imbedded in it. A Trojan often also includes a trapdoor as a means to gain access to a computer system bypassing security controls.
Wikipedia defines it as:
A Trojan horse, or Trojan, in computing is a non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm. The term is derived from the story of the wooden horse used to trick defenders of Troy into taking concealed warriors into their city in ancient Greece, because computer Trojans often employ a form of social engineering, presenting themselves as routine, useful, or interesting in order to persuade victims to install them on their computers.
The following answers are incorrect:
virus. Is incorrect because a Virus is a malicious program and is does not appear to be harmless, it's sole purpose is malicious intent often doing damage to a system. A computer virus is a type of malware that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds,

the affected areas are then said to be "infected".
worm. Is incorrect because a Worm is similiar to a Virus but does not require user intervention to execute. Rather than doing damage to the system, worms tend to self-propagate and devour the resources of a system. A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
trapdoor. Is incorrect because a trapdoor is a means to bypass security by hiding an entry point into a system. Trojan Horses often have a trapdoor imbedded in them.
References:
http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29
and
http://en.wikipedia.org/wiki/Computer_virus
and
http://en.wikipedia.org/wiki/Computer_worm
and
http://en.wikipedia.org/wiki/Backdoor_%28computing%29

NEW QUESTION: 104
When building a data center, site location and construction factors that increase the level of vulnerability to physical threats include
A. adequate distance from and lack of access to adjacent buildings.
B. hardened building construction with consideration of seismic factors.
C. curved roads approaching the data center.
D. proximity to high crime areas of the city.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 105
What principle requires that changes to the plaintext affect many parts of the ciphertext?
A. Encapsulation
B. Permutation
C. Diffusion
D. Obfuscation
Answer: (SHOW ANSWER)
Section: Mixed questions
Explanation:
Diffusion, on the other hand, means that a single plaintext bit has influence over several of the ciphertext bits.

Changing a plaintext value should change many ciphertext values, not just one. In fact, in a strong block cipher, if one plaintext bit is changed, it will change every ciphertext bit with the probability of 50 percent. This means that if one plaintext bit changes, then about half of the ciphertext bits will change.

NEW QUESTION: 106
After a company is out of an emergency state, what should be moved back to the original site first?
A. Executives
B. Least critical components
C. IT support staff
D. Most critical components
Answer: B (LEAVE A REPLY)
This will expose any weaknesses in the plan and ensure the primary site has been properly repaired before moving back. Moving critical assets first may induce a second disaster if the primary site has not been repaired properly.
The first group to go back would test items such as connectivity, HVAC, power, water, improper procedures, and/or steps that has been overlooked or not done properly. By moving these first, and fixing any problems identified, the critical operations of the company are not negatively affected.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 621).

NEW QUESTION: 107
The control measures that are intended to reveal the violations of security policy using software and hardware are associated with:
A. Preventive/physical
B. Detective/technical
C. Detective/physical
D. Detective/administrative
Answer: (SHOW ANSWER)
The detective/technical control measures are intended to reveal the violations of security policy using technical means. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35

NEW QUESTION: 108
_____ are the step-by-step instructions used to satisfy control requirements.
A. Standard
B. Procedure
C. Guideline
D. Outline
E. Policy
Answer: B (LEAVE A REPLY)

NEW QUESTION: 109
Which choice below is incorrect regarding when a BCP, DRP, or emergency management plan should be evaluated and modified?
A. Annually, in a scheduled review.
B. Never; once it has been tested it should not be changed.
C. After an emergency or disaster response.
D. After training drills, tests, or exercises.
Answer: A (LEAVE A REPLY)
Emergency management plans, business continuity plans, and disaster recovery plans should be regularly reviewed, evaluated, modified, and updated. At a minimum, the plan should be reviewed at an annual audit. It should also be re-evaluated: After tests or training exercises, to adjust any discrepancies between the test results and the plan After a disaster response or an emergency recovery, as this is an excellent time to amend the parts of the plan that were not effective When personnel, their responsibilities, their resources, or organizational structures change, to familiarize new or reorganized personnel with procedures When polices, procedures, or infrastructures change Source: Emergency Management Guide for Business and Industry Federal Emergency Management Agency, August, 1998 and NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity National Fire Protection Association, 2000 edition.

NEW QUESTION: 110
Without proper signal protection, embedded systems may be prone to which type of attack?
A. Denial of Service (DoS)
B. Information disclosure
C. Tampering
D. Brute force
Answer: (SHOW ANSWER)

NEW QUESTION: 111
What is the main focus of the Bell-LaPadula security model?
A. Accountability
B. Integrity
C. Confidentiality
D. Availability

Answer: (SHOW ANSWER)

The Bell-LaPadula model is a formal model dealing with confidentiality.

The Bell-LaPadula Model (abbreviated BLP) is a state machine model used for enforcing access control in government and military applications. It was developed by David Elliott

Bell and Leonard J. LaPadula, subsequent to strong guidance from Roger R. Schell to formalize the U.S. Department of Defense (DoD) multilevel security (MLS) policy. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects.

Security labels range from the most sensitive (e.g."Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public").

The Bell-LaPadula model focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity. In this formal model, the entities in an information system are divided into subjects and objects.

The notion of a "secure state" is defined, and it is proven that each state transition preserves security by moving from secure state to secure state, thereby inductively proving that the system satisfies the security objectives of the model. The Bell-LaPadula model is built on the concept of a state machine with a set of allowable states in a computer network system. The transition from one state to another state is defined by transition functions.

A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a security policy. To determine whether a specific access mode is allowed, the clearance of a subject is compared to the classification of the object

(more precisely, to the combination of classification and set of compartments, making up the security level) to determine if the subject is authorized for the specific access mode.

The clearance/classification scheme is expressed in terms of a lattice. The model defines two mandatory access control (MAC) rules and one discretionary access control (DAC) rule with three security properties:

The Simple Security Property - a subject at a given security level may not read an object at a higher security level (no read-up).

The -property (read "star"-property) - a subject at a given security level must not write to any object at a lower security level (no write-down). The -property is also known as the

Confinement property.

The Discretionary Security Property - use of an access matrix to specify the discretionary access control.

The following are incorrect answers:

Accountability is incorrect. Accountability requires that actions be traceable to the user that performed them and is not addressed by the Bell-LaPadula model.

Integrity is incorrect. Integrity is addressed in the Biba model rather than Bell-Lapadula.

Availability is incorrect. Availability is concerned with assuring that data/services are available to authorized users as specified in service level objectives and is not addressed by the Bell-Lapadula model.

References:

CBK, pp. 325-326

AIO3, pp. 279 - 284

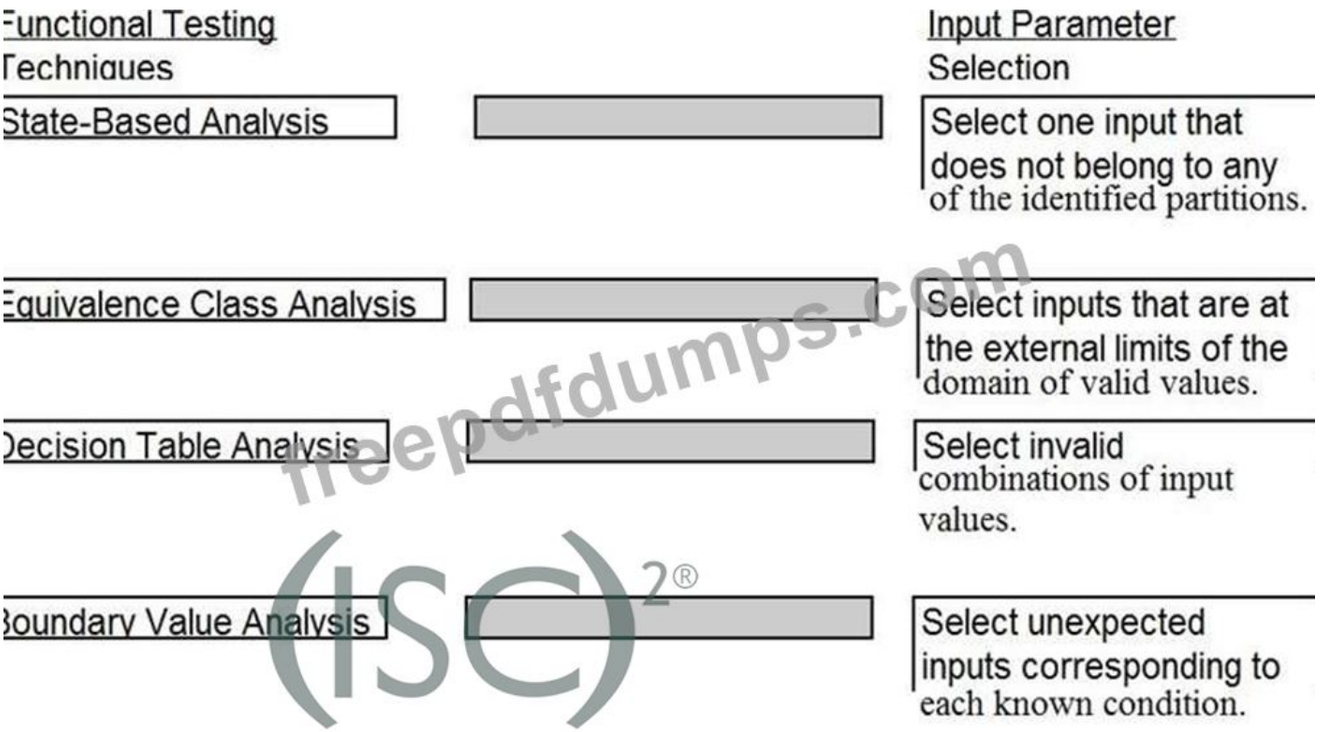
AIOv4 Security Architecture and Design (pages 333 - 336)

AIOv5 Security Architecture and Design (pages 336 - 338)
Wikipedia at https://en.wikipedia.org/wiki/Bell-La_Padula_model

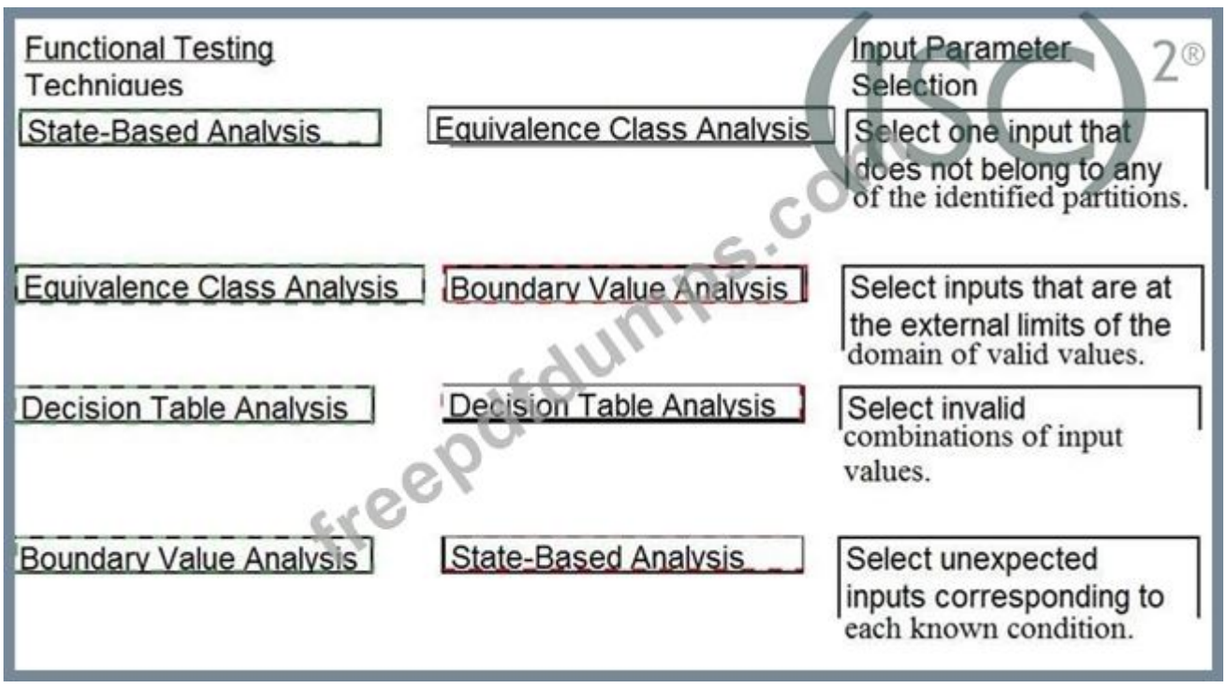
NEW QUESTION: 112
How do covert timing channels convey information?
A. By generating noise and traffic with the data
B. By modifying the timing of a system resource in some measurable way
C. By changing a system's stored data characteristics
D. By performing a covert channel analysis
Answer: B (LEAVE A REPLY)
The correct answer is "By modifying the timing of a system resource in some measurable way". A covert timing channel alters the timing of parts of the system to enable it to be used to communicate information covertly (outside the normal security function).
* Answer "By changing a system's stored data characteristics" is the description of the use of a covert storage channel.
* "By generating noise and traffic with the data" is a technique to combat the use of covert channels.
* Answer "By performing a covert channel analysis" is the Orange Book requirement for B3,
B2, and A1 evaluated systems.

NEW QUESTION: 113
What physical characteristic does a retinal scan biometric device measure?
A. The size, curvature, and shape of the retina
B. The pattern of blood vessels at the back of the eye
C. The pattern of light receptors at the back of the eye
D. The amount of light reflected by the retina
Answer: B (LEAVE A REPLY)

NEW QUESTION: 114
DRAG DROP
A software security engineer is developing a black box-based test plan that will measure the system's reaction to incorrect or illegal inputs or unexpected operational errors and situations. Match the functional testing techniques on the left with the correct input parameters on the right.



Answer:



NEW QUESTION: 115

Good forensics requires the use of a bit level copy?(True/False)

A. True

B. False

Answer: (SHOW ANSWER)

Good forensics requires the use of a bit level copy. A bit level copy duplicates all information on the suspect's disk. This includes slack space and free space.

NEW QUESTION: 116
Biometrics is used for identification in the physical controls and for authentication in the:
A. Detective controls.
B. Corrective controls.
C. Logical controls.
D. Preventive controls.
Answer: C (LEAVE A REPLY)
The correct answer is "Logical controls". The other answers are different categories of controls where preventive controls attempt to eliminate or reduce vulnerabilities before an attack occurs; detective controls attempt to
determine that an attack is taking place or has taken place; and corrective controls involve taking action to restore the system to normal operation after a successful attack.

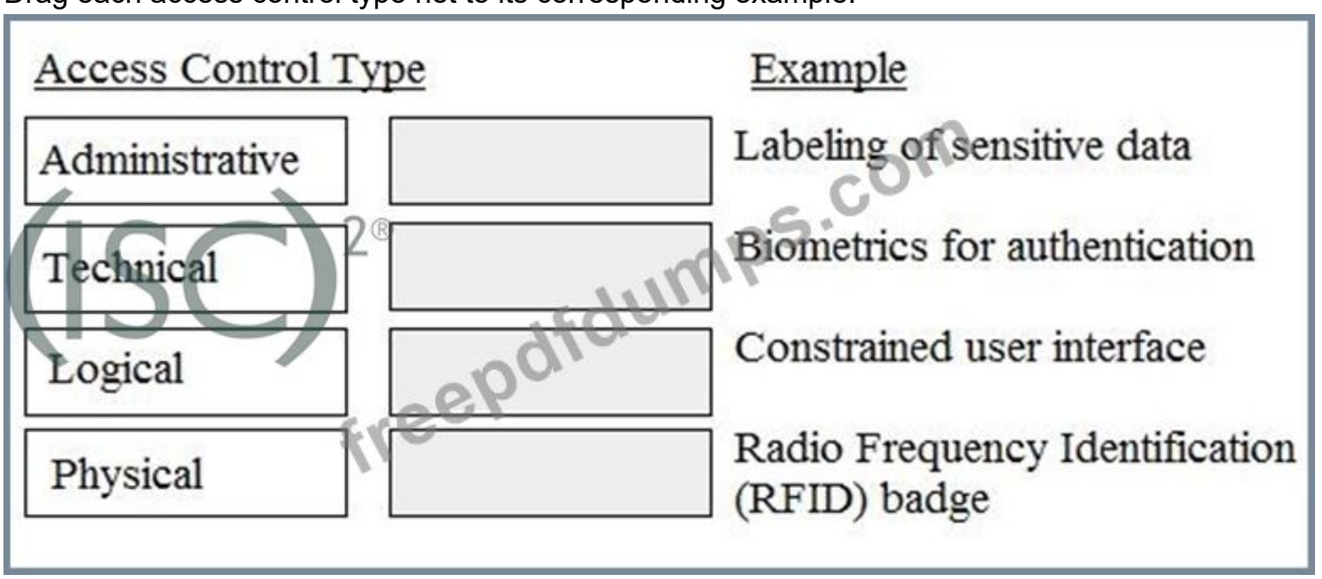
NEW QUESTION: 117
With what frequency should monitoring of a control occur when implementing Information Security Continuous Monitoring (ISCM) solutions?
A. Continuously without exception for all security controls
B. Before and after each change of the control
C. At a rate concurrent with the volatility of the security control
D. Only during system implementation and decommissioning
Answer: B (LEAVE A REPLY)
Section: Security Operations

NEW QUESTION: 118
Which choice below most accurately describes a business impact analysis (BIA)?
A. Activities designed to return an organization to an acceptable operating condition
B. A management-level analysis that identifies the impact of losing an entitys resources
C. A prearranged agreement between two or more entities to provide assistance
D. A program that implements the strategic goals of the organization
Answer: B (LEAVE A REPLY)
A business impact analysis (BIA) measures the effect of resource loss and escalating losses over time in order to provide the entity with reliable data upon which to base decisions on hazard mitigation and continuity planning. A BIA is performed as one step during the creation of a Business Continuity Plan (BCP). A common five-step approach to a BCP could consist of:

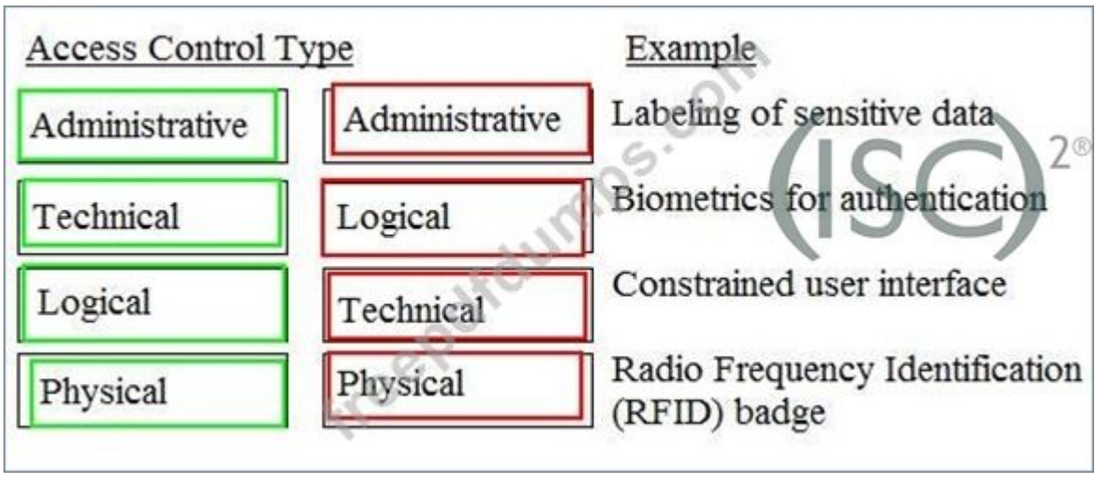
BCP project scope creation
Business impact assessment
Recovery strategy development
Recovery plan development
Implementation, testing, and maintenance.
Answer a is a definition of a disaster/emergency management program. Answer c describes a mutual aid agreement. Answer d is the definition of a recovery program. Source: NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity, National Fire Protection Association, 2000 edition and Handbook of Information Security Management, by Micki Krause and Harold F. Tipton, Auerback, 1999 edition.

NEW QUESTION: 119
When dealing with compliance with the Payment Card Industry-Data Security Standard (PCI-DSS), an organization that shares card holder information with a service provider MUST do which of the following?
A. Validate that the service providers security policies are in alignment with those of the organization.
B. Validate the service provider's PCI-DSS compliance status on a regular basis.
C. Perform a service provider PCI-DSS assessment on a yearly basis.
D. Ensure that the service provider updates and tests its Disaster Recovery Plan (DRP) on a yearly basis.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 120
Match the access control type to the example of the control type.
Drag each access control type net to its corresponding example.



Answer:



NEW QUESTION: 121
In a wireless General Packet Radio Services (GPRS) Virtual Private Network (VPN) application, which of the following security protocols is commonly used?
A. SSL
B. IPSEC
C. TLS
D. WTP
Answer: B (LEAVE A REPLY)
An example is the use of a GPRS-enabled laptop that connects to a corporate intranet via a VPN. The laptop is given an IP address and a RADIUS server authenticates the user. IPSEC is used to create the VPN. As background, GPRS is a second-generation (2G) packet data technology that is overlaid on existing Global System for Mobile communications (GSM). GSM is the wireless analog of the ISDN landline system. The key features of GPRS are that it is always on line (no dial-up needed), existing GSM networks can be upgraded with GPRS, and it can serve as the packet data core of third generation (3G) systems.
Answers SSL and TLS are similar security protocols that are used on the Internet side of the Wireless Application Protocol (WAP) Gateway.
For answer WTP is the Wireless Transaction Protocol that is part of the WAP suite of protocols. WTP is a lightweight, message-oriented, transaction protocol that provides more reliable connections than UDP, but does not have the robustness of TCP.

NEW QUESTION: 122
Which of the following could illegally capture network user passwords?
A. Data diddling
B. Sniffing
C. Spoofing
D. Smurfing
Answer: B (LEAVE A REPLY)
Sniffing is the action of capture the information going over the network. Most popular way of connecting computers is through Ethernet. Ethernet protocol works by sending packet information to all the hosts on the same circuit. The packet header contains the proper address of the destination machine. Only the machine with the matching address is suppose to accept the packet. A machine that is accepting all packets, no matter what the packet header says, is said to be in promiscuous mode. Because, in a normal networking environment, account and password information is passed along Ethernet in clear-text, it is not hard for an intruder to put a machine into promiscuous mode and by sniffing, compromise all the machines on the net by capturing password in an illegal fashion.

NEW QUESTION: 123
Which Orange book security rating is the FIRST to be concerned with covert channels?
A. A1
B. B3
C. B2
D. B1
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
In the Orange Book, covert channels in operating systems are not addressed until security level B2 and above because these are the systems that would be holding data sensitive enough for others to go through all the necessary trouble to access data in this fashion.
B2: Structured Protection: The security policy is clearly defined and documented, and the system design and implementation are subjected to more thorough review and testing procedures. This class requires more stringent authentication mechanisms and well-defined interfaces among layers. Subjects and devices require labels, and the system must not allow covert channels. A trusted path for logon and authentication processes must be in place, which means the subject communicates directly with the application or operating system, and no trapdoors exist. There is no way to circumvent or compromise this communication channel. Operator and administration functions are separated within the system to provide more trusted and protected operational functionality. Distinct address spaces must be provided to isolate processes, and a covert

channel analysis is conducted. This class adds assurance by adding requirements to the design of the system.
The type of environment that would require B2 systems is one that processes sensitive data that require a higher degree of security. This type of environment would require systems that are relatively resistant to penetration and compromise.
Incorrect Answers:
A: Level B2, not A1 is the FIRST to be concerned with covert channels.
B: Level B2, not B3 is the FIRST to be concerned with covert channels.
D: Level B2, not B1 is the FIRST to be concerned with covert channels.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, pp. 395-396

NEW QUESTION: 124
Which of the following computer design approaches is based on the fact that in earlier technologies, the instruction fetch was the longest part of the cycle?
A. Pipelining
B. Reduced Instruction Set Computers (RISC)
C. Complex Instruction Set Computers (CISC)
D. Scolar processors
Answer: (SHOW ANSWER)
Reference: pg 255 Krutz: CISSP Prep Guide: Gold Edition

NEW QUESTION: 125
In the days before CIDR (Classless Internet Domain Routing), networks were commonly organized by classes. Which of the following would have been true of a Class A network?
A. The first bit of the IP address would be set to zero.
B. The first bit of the IP address would be set to one and the second bit set to zero.
C. The first two bits of the IP address would be set to one, and the third bit set to zero.
D. The first three bits of the IP address would be set to one.
Answer: A (LEAVE A REPLY)
Each Class A network address has a 8-bit network prefix, with the first bit of the ipaddress set to zero. See the diagram below for more details.
The following answers are incorrect:
The first bit of the IP address would be set to one and the second bit set to zero. Is incorrect because this would be a Class B network address.
The first two bits of the IP address would be set to one, and the third bit set to zero. Is incorrect because, this would be a Class C network address.
The first three bits of the ipaddress would be set to one. Is incorrect because, this is a distractor.
Class D & E have the first three bits set to 1.
Class D the 4th bit is 0 and for
Class E the 4th bit to 1.

See diagram below from the 3COM tutorial on everything you ever wanted to know about
IP addressing:
Classful IP addressing format
Classless Internet Domain Routing (CIDR)
Classless Inter-Domain Routing (CIDR) is a method for allocating IP addresses and routing
Internet Protocol packets. The Internet Engineering Task Force introduced CIDR in 1993 to replace the previous addressing architecture of classful network design in the Internet.
Their goal was to slow the growth of routing tables on routers across the Internet, and to help slow the rapid exhaustion of IPv4 addresses.
For Class A, the addresses are 0.0.0.0 - 127.255.255.255.
For Class B networks, the addresses are 128.0.0.0 - 191.255.255.255.
For Class C, the addresses are 192.0.0.0 - 223.255.255.255.
For Class D, the addresses are 224.0.0.0 - 239.255.255.255.
For Class E, the addresses are 240.0.0.0 - 255.255.255.255.
References:
3 Com http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf
and
AIOv3 Telecommunications and Networking Security (page 438)
and
https://secure.wikimedia.org/wikipedia/en/wiki/Classless_Inter-Domain_Routing

NEW QUESTION: 126
_____ are the technical ways of restricting who or what can access system resources.
A. Preventive Manual Controls
B. Detective Technical Controls
C. Preventive Circuit Controls
D. Preventive Technical Controls
Answer: (SHOW ANSWER)
Preventive Technical Controls are the technical ways of restricting who or what can access system resources and what type of access is permitted. Its purpose is to protect the OS and other systems from unauthorized modification or manipulation. It is usually built into an operating system, or it can be a part of an application or program, or an add-on security package, or special components to regulate communication between computers. It also protects the integrity and availability by limiting the number of users and/or processes. These controls also protect confidential information from being disclosed to unauthorized persons.

NEW QUESTION: 127
Which answer below is the BEST description of a Single Loss
Expectancy (SLE)?
A. An algorithm that determines the expected annual loss to an
organization from a threat
B. An algorithm that represents the magnitude of a loss to an asset

from a threat
C. An algorithm used to determine the monetary impact of each occurrence of a threat
D. An algorithm that expresses the annual frequency with which a threat is expected to occur
Answer: C (LEAVE A REPLY)
The correct answer is "An algorithm used to determine the monetary impact of each occurrence of a threat". The Single Loss Expectancy (or Exposure) figure may be created as a result of a Business Impact Assessment (BIA). The SLE represents only the estimated monetary loss of a single occurrence of a specified threat event. The SLE is determined by multiplying the value of the asset by its exposure factor. This gives the expected loss the threat will cause for one occurrence.
Answer a describes the Exposure Factor (EF). The EF is expressed as a percentile of the expected value or functionality of the asset to be lost due to the realized threat event. This figure is used to calculate the SLE, above.
Answer "An algorithm that expresses the annual frequency with which a threat is expected to occur" describes the Annualized Rate of Occurrence (ARO). This is an estimate of how often a given threat event may occur annually. For example, a threat expected to occur weekly would have an ARO of 52. A threat expected to occur once every five years has an ARO of 1/5 or .2. This figure is used to determine the ALE.
Answer d describes the Annualized Loss Expectancy (ALE). The ALE is derived by multiplying the SLE by its ARO. This value represents the expected risk factor of an annual threat event. This figure is then integrated into the risk management process.

NEW QUESTION: 128
Which of the following testing method examines the functionality of an application without peering into its internal structure or knowing the details of it's internals?
A. Black-box testing
B. Parallel Test
C. Regression Testing
D. Pilot Testing
Answer: A (LEAVE A REPLY)
Black-box testing is a method of software testing that examines the functionality of an application (e.g. what the software does) without peering into its internal structures or workings (see white-box testing). This method of test can be applied to virtually every level of software testing: unit, integration, system and acceptance. It typically comprises most if not all higher level testing, but can also dominate unit testing as well.
For your exam you should know the information below: Alpha and Beta Testing - An alpha version is early version is an early version of the application system submitted to the internal user for testing. The alpha

version may not contain all the features planned for the final version. Typically software goes to two stages testing before it consider finished.The first stage is called alpha testing is often performed only by the user within the organization developing the software. The second stage is called beta testing, a form of user acceptance testing, generally involves a limited number of external users. Beta testing is the last stage of testing, and normally involves real world exposure, sending the beta version of the product to independent beta test sites or offering it free to interested user.

Pilot Testing - A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests - usually over interim platform and with only basic functionalities.

White box testing - Assess the effectiveness of a software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's specific logic path. However testing all possible logical path in large information system is not feasible and would be cost prohibitive, and therefore is used on selective basis only.

Black Box Testing - An integrity based form of testing associated with testing components of an information system's "functional" operating effectiveness without regards to any specific internal program structure. Applicable to integration and user acceptance testing.

Function/validation testing - It is similar to system testing but it is often used to test the functionality of the system against the detailed requirements to ensure that the software that has been built is traceable to customer requirements.

Regression Testing - The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

Parallel Testing - This is the process of feeding test data into two systems - the modified system and an alternative system and comparing the result.

Sociability Testing - The purpose of these tests is to confirm that new or modified system can operate in its target environment without adversely impacting existing system. This should cover not only platform that will perform primary application processing and interface with other system but , in a client server and web development, changes to the desktop environment. Multiple application may run on the users desktop, potentially simultaneously , so it is important to test the impact of installing new dynamic link libraries (DLLs), making operating system registry or configuration file modification, and possibly extra memory utilization.

The following answers are incorrect:

Parallel Testing - This is the process of feeding test data into two systems - the modified system and an alternative system and comparing the result.

Regression Testing - The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

Pilot Testing - A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests - usually over interim platform and with only basic functionalities

The following reference(s) were/was used to create this question: CISA review manual 2014 Page number 167 Official ISC2 guide to CISSP CBK 3rd Edition Page number 176

NEW QUESTION: 129
Several analysis methods can be employed by an IDS, each with its own strengths and weaknesses, and their applicability to any given situation should be carefully considered. There are two basic IDS analysis methods that exist.
Which of the basic method is more prone to false positive?
A. Pattern Matching (also called signature analysis)
B. Anomaly Detection
C. Host-based intrusion detection
D. Network-based intrusion detection
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Anomaly Detection IDS learns about the normal activities and events on your system by watching and tracking what it sees. Once it has accumulated enough data about normal activity, it can detect abnormal and possibly malicious activities or events. There is a small risk that some non-harmful activity is classified as anomaly by mistake - false positives can occur.
Incorrect Answers:
A: A Pattern Matching IDS uses a signature database and attempts to match all monitored events to its contents. Only activities present in the database will be detected. There will be no false positives.
C: Host-based intrusion detection is not an IDS analysis method. It is a classification on information source. A host - based IDS watches for questionable activity on a single computer system, especially by watching audit trails, event logs, and application logs.
D: Network-based intrusion detection is not an IDS analysis method. It is a classification on information course. Here the source is a network segment.
References:
Stewart, James M., Ed Tittel, and Mike Chapple, CISSP: Certified Information Systems Security Professional Study Guide, 5th Edition, Sybex, Indianapolis, 2011, p. 56

NEW QUESTION: 130
The communication to an object to carry out an operation in an objectoriented system is called a:
A. Note.
B. Method.
C. Message.
D. Behavior.
Answer: C (LEAVE A REPLY)
Answer Note is a distracter.
A method is the code that defines the actions an object performs in response to a messagE.
Behavior is the result exhibited by an object upon receipt of a message.

NEW QUESTION: 131
An organization implements a remote access server (RAS), Once users connect to the server, digital certificates are used to authenticate their identity. What type of extensible Authentication protocol (EAP) would the organization use during this authentication?
A. Message Digest 5 (MD5)
B. Subscriber Identity Module (SIM)
C. Transport layer security (TLS)
D. Lightweight Extensible Authentication Protocol (EAP)
Answer: (SHOW ANSWER)

NEW QUESTION: 132
A form of digital signature where the signer is not privy to the content
of the message is called a:
A. Encrypted signature
B. Zero knowledge proof
C. Masked signature
D. Blind signature
Answer: (SHOW ANSWER)
A blind signature algorithm for the message M uses a blinding factor, f; a modulus m; the private key, s, of the signer and the public key, q, of the signer. The sender, who generates f and knows q, presents the message to the signer in the form: Mf q (mod m) Thus, the message is not in a form readable by the signer since the signer does not know f. The signer signs Mf q (mod m) with his/her private key, returning (Mf q)s (mod m) This factor can be reduced to fMs (mod m) since s and q are inverses of each other. The sender then divides fMs (mod m) by the blinding factor, f, to obtain Ms (mod m) Ms (mod m) is, therefore, the message, M, signed with the private key, s, of the signer.
Answer Zero knowledge proof refers to a zero knowledge proof. In general, a zero knowledge proof involves a person, A, trying to prove that he/she knows something, S, to another person, B, without revealing S or anything about S.Answers Masked signature and Encrypted signature are distracters.

NEW QUESTION: 133
In an object-oriented system, the situation wherein objects with a common
name respond differently to a common set of operations is called:
A. Polyinstantiation.
B. Delegation.
C. Polyresponse.
D. Polymorphism.
Answer: D (LEAVE A REPLY)
Delegation is the forwarding of a request by one object to another object.
Answer Polyresponse is a distracter.
Polyinstantiationis the development of a detailed version

of an object from another object. The new object uses values that are
different from those in the original object.

NEW QUESTION: 134
In computing what is the name of a non-self-replicating type of malware program containing malicious code that appears to have some useful purpose but also contains code that has a malicious or harmful purpose imbedded in it, when executed, carries out actions that are unknown to the person installing it, typically causing loss or theft of data, and possible system harm.
A. virus.
B. worm.
C. Trojan horse.
D. trapdoor.
Answer: C (LEAVE A REPLY)
A trojan horse is any code that appears to have some useful purpose but also contains code that has a malicious or harmful purpose imbedded in it. A Trojan often also includes a trapdoor as a means to gain access to a computer system bypassing security controls.
Wikipedia defines it as:
A Trojan horse, or Trojan, in computing is a non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm. The term is derived from the story of the wooden horse used to trick defenders of Troy into taking concealed warriors into their city in ancient Greece, because computer Trojans often employ a form of social engineering, presenting themselves as routine, useful, or interesting in order to persuade victims to install them on their computers.
The following answers are incorrect:
virus. Is incorrect because a Virus is a malicious program and is does not appear to be harmless, it's sole purpose is malicious intent often doing damage to a system. A computer virus is a type of malware that, when executed, replicates by inserting copies of itself
(possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected".
worm. Is incorrect because a Worm is similiar to a Virus but does not require user intervention to execute. Rather than doing damage to the system, worms tend to self- propagate and devour the resources of a system. A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers.
Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
trapdoor. Is incorrect because a trapdoor is a means to bypass security by hiding an entry point into a system. Trojan Horses often have a trapdoor imbedded in them.
References:
http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29

and
http://en.wikipedia.org/wiki/Computer_virus
and
http://en.wikipedia.org/wiki/Computer_worm
and
http://en.wikipedia.org/wiki/Backdoor_%28computing%29

NEW QUESTION: 135
Which of the following would be the BEST criterion to consider in determining the classification of an information asset?
A. Value
B. Age
C. Useful life
D. Personal association
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The 'value' of an information asset should be used to classify the information asset.
The rationale behind assigning values to different types of data is that it enables a company to gauge the amount of funds and resources that should go toward protecting each type of data, because not all data has the same value to a company. After identifying all important information, it should be properly classified. A company has a lot of information that is created and maintained. The reason to classify data is to organize it according to its sensitivity to loss, disclosure, or unavailability. Once data is segmented according to its sensitivity level, the company can decide what security controls are necessary to protect different types of data. This ensures that information assets receive the appropriate level of protection, and classifications indicate the priority of that security protection.
Incorrect Answers:
B: The age of an information asset is not the best criterion to consider in determining the classification of the information asset.
C: The useful life of an information asset is not the best criterion to consider in determining the classification of the information asset.
D: The personal association of an information asset is not the best criterion to consider in determining the classification of the information asset.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 109

NEW QUESTION: 136
Which choice below is a role of the Information Systems Security
Officer?
A. The ISO is responsible for examining systems to see whether they
are meeting stated security requirements.

B. The ISO is responsible for day-to-day security administration.
C. The ISO is responsible for following security procedures and
reporting security problems.
D. The ISO establishes the overall goals of the organization's computer security program.
Answer: B (LEAVE A REPLY)
Answer "The ISO establishes the overall goals of the organization's computer security program" is a responsibility of senior management. Answer "The ISO is responsible for examining systems to see whether they are meeting stated security requirements" is a description of the role of auditing. Answer "The ISO is responsible for following security procedures and reporting security problems" is the role of the user, or consumer, of security in an organization.

NEW QUESTION: 137
What is called the use of technologies such as fingerprint, retina, and iris scans to authenticate the individuals requesting access to resources?
A. Micrometrics
B. Macrometrics
C. Biometrics
D. MicroBiometrics
Answer: C (LEAVE A REPLY)
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide:
Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35

NEW QUESTION: 138
Which of the following steps is NOT one of the four steps of a Business Impact Analysis (BIA)?
A. Notifying senior management
B. Gathering the needed assessment materials
C. Performing the vulnerability assessment
D. Analyzing the information compiled
Answer: A (LEAVE A REPLY)
"A BIA generally takes the form of these four steps:
Pg. 383 Krutz: CISSP Prep Guide: Gold Edition.

NEW QUESTION: 139

Which of the following backup methods makes a complete backup of every file on the server every time it is run?

A. full backup method.

B. incremental backup method.

C. differential backup method.

D. tape backup method.

Answer: (SHOW ANSWER)

The Full Backup Method makes a complete backup of every file on the server every time it is run. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

NEW QUESTION: 140

Digital cash refers to the electronic transfer of funds from one party to another. When digital cash is referred to as anonymous or identified, it means that:

A. Anonymous the identity of the bank is withheld; Identified the identity of the bank is not withheld

B. Anonymous the identity of the cash holder is not known; Identified the identity of the cash holder is known

C. Anonymous the identity of the cash holder is not known; Identified the identity of the merchant is known

D. Anonymous the identity of merchant is withheld; Identified the identity of the merchant is not withheld

Answer: B (LEAVE A REPLY)

Anonymous implementations of digital cash do not identify the cash holder and use blind signature schemes; identified implementations use conventional digital signatures to identify the cash holder.

In looking at these two approaches, anonymous schemes are analogous to cash since cash does not allow tracing of the person who made the cash payment while identified approaches are the analog of credit or debit card transactions.

NEW QUESTION: 141

Under MAC, who may grant a right of access that is explicitly forbidden in the access control policy?

A. None of the choices.

B. All users.

C. Administrators only.

D. All managers.

Answer: A (LEAVE A REPLY)

MAC is defined as follows in the Handbook of Information Security Management: With mandatory controls, only administrators and not owners of resources may make decisions that bear on or derive from policy. Only

an administrator may change the category of a resource, and no one may grant a right of access that is explicitly forbidden in the access control policy.

NEW QUESTION: 142
Which of the following is the most reliable authentication method for remote access?
A. Variable callback system
B. Synchronous token
C. Fixed callback system
D. Combination of callback and caller ID
Answer: B (LEAVE A REPLY)
A Synchronous token generates a one-time password that is only valid for a short period of time. Once the password is used it is no longer valid, and it expires if not entered in the acceptable time frame.
The following answers are incorrect:
Variable callback system. Although variable callback systems are more flexible than fixed callback systems, the system assumes the identity of the individual unless two-factor authentication is also implemented. By itself, this method might allow an attacker access as a trusted user.
Fixed callback system. Authentication provides assurance that someone or something is who or what he/it is supposed to be. Callback systems authenticate a person, but anyone can pretend to be that person. They are tied to a specific place and phone number, which can be spoofed by implementing call-forwarding.
Combination of callback and Caller ID. The caller ID and callback functionality provides greater confidence and auditability of the caller's identity. By disconnecting and calling back only authorized phone numbers, the system has a greater confidence in the location of the call. However, unless combined with strong authentication, any individual at the location could obtain access.
The following reference(s) were/was used to create this question: Shon Harris AIO v3 p. 140, 548 ISC2 OIG 2007 p. 152-153, 126-127

NEW QUESTION: 143
Which backup method is additive because the time and tape space required for each night's backup grows during the week as it copies the day's changed files and the previous days' changed files up to the last full backup?
A. differential backup method.
B. full backup method.
C. incremental backup method.
D. tape backup method.
Answer: A (LEAVE A REPLY)
The Differential Backup Method is additive because the time and tape space required for each night's backup grows during the week as it copies the day's changed files and the previous days' changed files up to the last full backup. Archive Bits

Unless you've done a lot of backups in your time you've probably never heard of an Archive Bit. An archive bit is, essentially, a tag that is attached to every file. In actuality, it is a binary digit that is set on or off in the file, but that's crummy technical jargon that doesn't really tell us anything. For the sake of our discussion, just think of it as the flag on a mail box. If the flag is up, it means the file has been changed. If it's down, then the file is unchanged.
Archive bits let the backup software know what needs to be backed up. The differential and incremental backup types rely on the archive bit to direct them. Backup Types Full or Normal The "Full" or "normal" backup type is the most standard. This is the backup type that you would use if you wanted to backup every file in a given folder or drive. It backs up everything you direct it to regardless of what the archive bit says. It also resets all archive bits (puts the flags down). Most backup software, including the built-in Windows backup software, lets you select down to the individual file that you want backed up. You can also choose to backup things like the "system state".
Incremental When you schedule an incremental backup, you are in essence instructing the software to only backup files that have been changed, or files that have their flag up. After the incremental backup of that file has occured, that flag will go back down. If you perform a normal backup on Monday, then an incremental backup on Wednesday, the only files that will be backed up are those that have changed since Monday. If on Thursday someone deletes a file by accident, in order to get it back you will have to restore the full backup from Monday, followed by the Incremental backup from Wednesday.
Differential Differential backups are similar to incremental backups in that they only backup files with their archive bit, or flag, up. However, when a differential backup occurs it does not reset those archive bits which means, if the following day, another differential backup occurs, it will back up that file again regardless of whether that file has been changed or not. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.
And: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (pages 617-619). And:
http://www.brighthub.com/computing/windows-platform/articles/24531.aspx

NEW QUESTION: 144
What does an Exposure Factor (EF) describe?
A. The annual expected financial loss to an organization from a threat
B. The percentage of loss that a realized threat event would have on a
specific asset
C. Anumber that represents the estimated frequency of the occurrence of an expected threat
D. Adollar figure that is assigned to a single event
Answer: B (LEAVE A REPLY)
The correct answer is "The percentage of loss that a realized threat event would have on a specific asset". Answer "Adollar figure that is assigned to a single event" is an SLE,
"Anumber that represents the estimated frequency of the occurrence of
an expected threat" is an ARO, and "The annual expected financial loss to an organization from a threat" is an ALE.

NEW QUESTION: 145
Attack trees are MOST useful for which of the following?
A. Evaluating Denial of Service (DoS) attacks
B. Generating attack libraries
C. Enumerating threats
D. Determining system security scopes
Answer: (SHOW ANSWER)

NEW QUESTION: 146
In the National Information Assurance Certification and Accreditation
Process (NIACAP), a type accreditation performs which one of the following functions?
A. Evaluates the applications and systems at a specific, self-contained location
B. Evaluates a major application or general support system
C. Verifies the evolving or modified system's compliance with the information agreed on in the System Security Authorization Agreement (SSAA)
D. Evaluates an application or system that is distributed to a number of different locations
Answer: D (LEAVE A REPLY)
* Answer "Evaluates a major application or general support system" is the NIACAP system accreditation.
* Answer "Verifies the evolving or modified system's compliance with the information agreed on in the System Security Authorization Agreement (SSAA)" is the Phase 2 or
Verification phase of the Defense Information Technology Security Certification and
Accreditation Process (DITSCAP). The objective is to use the SSAA to establish an evolving yet binding agreement on the level of security required before the system development begins or changes to a system are made. After accreditation, the SSAA becomes the baseline security configuration document.
* Answer "Evaluates the applications and systems at a specific, self-contained location" is the NIACAP site accreditation.

NEW QUESTION: 147
Which of the following answers BEST indicates the most important part of a data backup plan?
A. Testing the backups with restore operations
B. An effective backup plan
C. A reliable network infrastructure
D. Expensive backup hardware
Answer: A (LEAVE A REPLY)
If you can't restore lost files from your backup system then your backup plan is useless. You could have the best backup system and plan available but if you are unable to restore files then the system can't assure data availability.
Develop an effective disaster recovery plan and include in that plan a good backup strategy that meets the needs of your organization. Be sure to include periodic recovery practice operations to prove the effectiveness of the system.
The following answers are incorrect:

-An effective backup plan: This is vital but testing the plan with restores is vital to operate a network safely.
-A reliable network infrastructure: This is incorrect because it is only part of what you need to have an effective backup and restore plan.
-Expensive backup hardware: This is good to have but if you don't rest your restore plan and it doesn't work when you need it, it is useless.
The following reference(s) was used to create this question: 2013. Official Security+ Curriculum.

NEW QUESTION: 148
Which of the following is NOT a media viability control used to protect the viability of data storage media?
A. clearing
B. marking
C. handling
D. storage
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Clearing is not an example of a media viability control used to protect the viability of data storage media.
Media viability controls are implemented to preserve the proper working state of the media, particularly to facilitate the timely and accurate restoration of the system after a failure.
Many physical controls should be used to protect the viability of the data storage media. The goal is to protect the media from damage during handling and transportation, or during short-term or long-term storage. Proper marking and labeling of the media is required in the event of a system recovery process:
Marking. All data storage media should be accurately marked or labeled. The labels can be used to
- identify media with special handling instructions, or to log serial numbers or bar codes for retrieval during a system recovery.

Handling. Proper handling of the media is important. Some issues with the handling of media include
- cleanliness of the media and the protection from physical damage to the media during transportation to the archive sites.

Storage. Storage of the media is very important for both security and environmental reasons. A proper
- heat- and humidity-free, clean storage environment should be provided for the media. Data media is sensitive to temperature, liquids, magnetism, smoke, and dust.

Incorrect Answers:
B: Marking is a media viability control used to protect the viability of data storage media.
C: Handling is a media viability control used to protect the viability of data storage media.
D: Storage is a media viability control used to protect the viability of data storage media.
References:
Krutz, Ronald L. and Russell Dean Vines, The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 324

NEW QUESTION: 149

Which software development model is actually a meta-model that incorporates a number of the software development models?

A. The Waterfall model

B. The modified Waterfall model

C. The Spiral model

D. The Critical Path Model (CPM)

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

The spiral model is a risk-driven process model generator for software projects. Thus, the incremental, waterfall, prototyping, and other process models are special cases of the spiral model that fit the risk patterns of certain projects.

Incorrect Answers:

A: The Waterfall model is a special case of the Spiral model, not the opposite way around.

B: The modified Waterfall model is a special case of the Spiral model, not the opposite way around.

D: A critical path model is not a meta-model. The critical path model requires you to establish the time frame for a project and schedule start and end times for each task in the project.

References:

https://en.wikipedia.org/wiki/Spiral_model

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, pp. 1112, 1115-1116

NEW QUESTION: 150

Which of the following statements pertaining to using Kerberos without any extension is false?

A. A client can be impersonated by password-guessing.

B. Kerberos is mostly a third-party authentication protocol.

C. Kerberos uses public key cryptography.

D. Kerberos provides robust authentication.

Answer: C (LEAVE A REPLY)

Kerberos is a trusted, credential-based, third-party authentication protocol that uses symmetric (secret) key cryptography to provide robust authentication to clients accessing services
on a network.

Because a client's password is used in the initiation of the Kerberos request for the service
protocol, password guessing can be used to impersonate a client.

Here is a nice overview of HOW Kerberos is implement as described in RFC 4556:

1 Introduction

The Kerberos V5 protocol [RFC4120] involves use of a trusted third
party known as the Key Distribution Center (KDC) to negotiate shared
session keys between clients and services and provide mutual
authentication between them.

The corner-stones of Kerberos V5 are the Ticket and the

Authenticator. A Ticket encapsulates a symmetric key (the ticket session key) in an envelope (a public message) intended for a specific service. The contents of the Ticket are encrypted with a symmetric key shared between the service principal and the issuing KDC. The encrypted part of the Ticket contains the client principal name, among other items. An Authenticator is a record that can be shown to have been recently generated using the ticket session key in the associated Ticket. The ticket session key is known by the client who requested the ticket. The contents of the Authenticator are encrypted with the associated ticket session key. The encrypted part of an Authenticator contains a timestamp and the client principal name, among other items.

As shown in Figure 1, below, the Kerberos V5 protocol consists of the following message exchanges between the client and the KDC, and the client and the application service:

-

The Authentication Service (AS) Exchange

The client obtains an "initial" ticket from the Kerberos authentication server (AS), typically a Ticket Granting Ticket (TGT). The AS-REQ message and the AS-REP message are the request and the reply message, respectively, between the client and the AS.

-

The Ticket Granting Service (TGS) Exchange

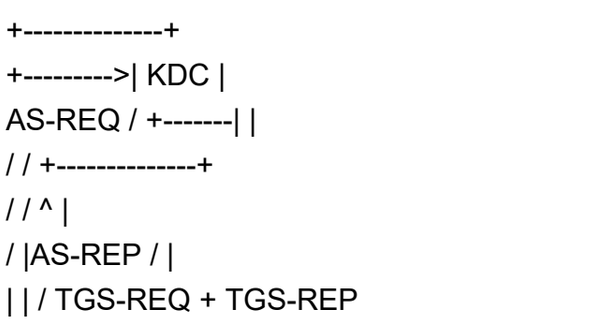
The client subsequently uses the TGT to authenticate and request a service ticket for a particular service, from the Kerberos ticket-granting server (TGS). The TGS-REQ message and the TGS-REP message are the request and the reply message respectively between the client and the TGS.

-

The Client/Server Authentication Protocol (AP) Exchange

The client then makes a request with an AP-REQ message, consisting of a service ticket and an authenticator that certifies the client's possession of the ticket session key. The server may optionally reply with an AP-REP message. AP exchanges typically negotiate session-specific symmetric keys.

Usually, the AS and TGS are integrated in a single device also known as the KDC.



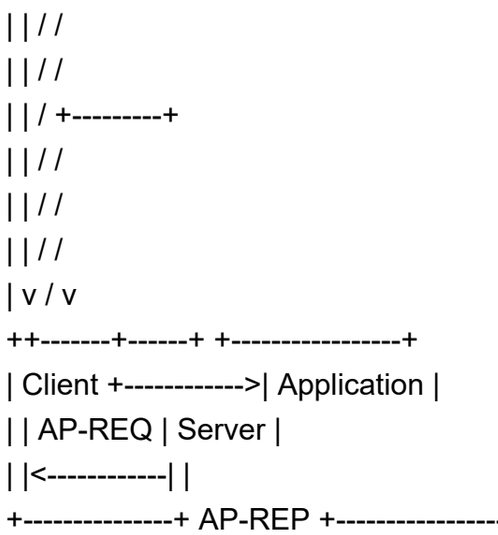


Figure 1: The Message Exchanges in the Kerberos V5 Protocol
In the AS exchange, the KDC reply contains the ticket session key,
among other items, that is encrypted using a key (the AS reply key)
shared between the client and the KDC. The AS reply key is typically derived from the client's password for human users. Therefore, for human users, the attack resistance strength of the Kerberos protocol is no stronger than the strength of their passwords.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 40).
And
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 147-151). and http://www.ietf.org/rfc/rfc4556txt

NEW QUESTION: 151
Which of the following monitors network traffic in real time?
A. network-based IDS
B. firewall-based IDS
C. host-based IDS
D. application-based IDS
Answer: (SHOW ANSWER)

NEW QUESTION: 152

Which one of the following is an effective communications error-control technique usually implemented in software?

A. Bit stuffing

B. Packet filtering

C. Redundancy check

D. Packet checksum

Answer: D (LEAVE A REPLY)

NEW QUESTION: 153

Business Associates

A. are entities that perform services that require the use of Protected Health Information on behalf of Covered Entities. One covered entity may be a business partner of another covered entity

B. are entities that perform services that require the use of Protected Health Information on behalf of Covered Entities. One covered entity cannot be a business partner of another covered entity.

C. are entities that perform services that require the use of Encrypted Insurance Information on behalf of Covered Entities. One covered entity may be a business partner of another covered entity

D. are entities that do not perform services that require the use of Protected Health Information on behalf of Covered Entities. One covered entity may be a business partner of another covered entity

Answer: A (LEAVE A REPLY)

NEW QUESTION: 154

A protection mechanism to limit inferencing of information in statistical
database queries is:

A. Specifying a maximum query set size

B. Specifying a minimum query set size, but prohibiting the querying of all but one of the records in the database

C. Specifying a minimum query set size

D. Specifying a maximum query set size, but prohibiting the querying of all but one of the records in the database

Answer: B (LEAVE A REPLY)

When querying a database for statistical information, individually identifiable information should be protected. Thus, requiring a minimum size for the query set (greater than one) offers protection against gathering information on one individual. However, an attack may consist of gathering statistics on a query set size M, equal to or greater than the minimum query set size, and then requesting the same statistics on a query set size of M + 1. The second query set would be designed to include the individual whose information is being sought surreptitiously.

*Thus with answer "Specifying a minimum query set size, but prohibiting the querying of all but one of the records in the database", this type of attack could not take place.

* Answer "Specifying a minimum query set size" is, therefore, incorrect since it leaves open the loophole of the M+1 set size query. Answers "Specifying a maximum query set size" and "Specifying a maximum query set size, but prohibiting the querying of all but one of the records in the database" are incorrect since the

critical metric is the minimum query set size and not the maximum size. Obviously, the maximum query set size cannot be set to a value less than the minimum set size.

NEW QUESTION: 155
Which of the following security controls might force an operator into collusion with personnel assigned organizationally within a different function in order to gain access to unauthorized data?
A. Limiting the local access of operations personnel
B. Job rotation of operations personnel
C. Management monitoring of audit logs
D. Enforcing regular password changes
Answer: A (LEAVE A REPLY)
The questions specifically said: "within a different function" which eliminate Job
Rotation as a choice.
Management monitoring of audit logs is a detective control and it would not prevent collusion.
Changing passwords regularly would not prevent such attack.
This question validates if you understand the concept of separation of duties and least privilege.
By having operators that have only the minimum access level they need and only what they need to do their duties within a company, the operations personnel would be force to use collusion to defeat those security mechanism.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 156
The organization would like to deploy an authorization mechanism for an Information Technology (IT) infrastructure project with high employee turnover.
Which access control mechanism would be preferred?
A. Role-Based Access Control (RBAC)
B. Attribute Based Access Control (ABAC)
C. Mandatory Access Control (MAC)
D. Discretionary Access Control (DAC)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 157
An online retail company has formulated a record retention schedule for customer transactions. Which of the following is a valid reason a customer transaction is kept beyond the retention schedule?
A. Useful for future business initiatives
B. Long term data mining needs
C. Customer makes request to retain
D. Pending legal hold
Answer: D (LEAVE A REPLY)

NEW QUESTION: 158

Why do vendors publish MD5 hash values when they provide software patches for their customers to download from the Internet?

A. Recipients can verify the software's integrity after downloading.

B. Recipients can confirm the authenticity of the site from which they are downloading the patch.

C. Recipients can request future updates to the software by using the assigned hash value.

D. Recipients need the hash value to successfully activate the new software.

Answer: A (LEAVE A REPLY)

If the two values are different, Maureen knows that the message was altered, either intentionally or unintentionally, and she discards the message...As stated in an earlier section, the goal of using a one-way hash function is to provide a fingerprint of the message. MD5 is the newer version of MD4. IT still produces a 128-bit hash, but the algorithm is a bit more complex to make it harder to break than MD4. The MD5 added a fourth round of operations to be performed during the hash functions and makes several of its mathematical operations carry steps or more complexity to provide a higher level of security . - Shon Harris All-in-one CISSP Certification Guide pg 182-185

NEW QUESTION: 159

The software maintenance phase controls consist of:

A. Request control, configuration control, and change control.

B. Request control, release control, and access control.

C. Request control, change control, and release control.

D. Change control, security control, and access control.

Answer: (SHOW ANSWER)

The software maintenance phase controls
consist of request control, change control, and release control by definition.
The other answers are, therefore, incorrect.
Topic 16, Exam SET D

NEW QUESTION: 160

Which of the following is the MOST effective practice in managing user accounts when an employee is terminated?

A. Delete employee network and system IDs upon termination.

B. Implement processes for automated removal of access for terminated employees.

C. Manually remove terminated employee user-access to all systems and applications.

D. Disable terminated employee network ID to remove all access.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 161

Who is ultimately responsible for the security of an organization?

A. Management

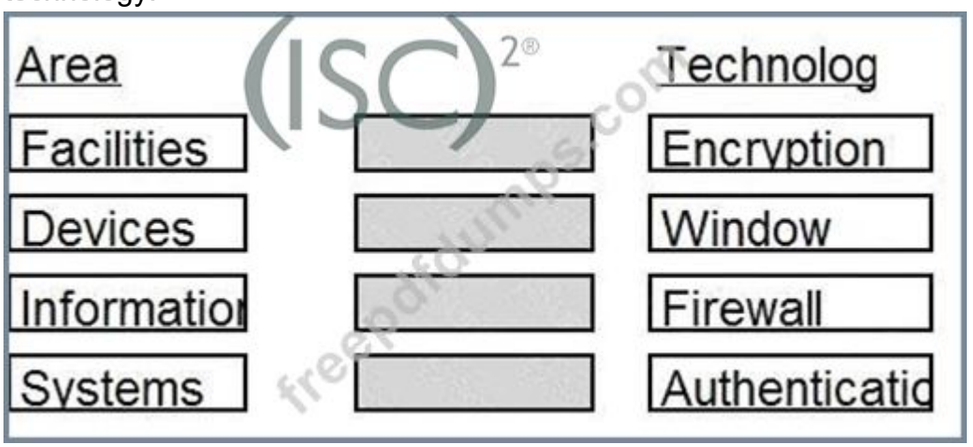
B. Senior management

C. The chief security officer

D. Department heads
E. Employees
Answer: B (LEAVE A REPLY)
Senior management is ultimately responsible for the security of an organization. Policy flows from the top down.

NEW QUESTION: 162
The criteria for evaluating the legal requirements for implementing safeguards is to evaluate the cost (C) of instituting the protection versus the estimated loss (L) resulting from the exploitation f the corresponding vulnerability. Therefore, a legal liability exists when?
A. C < L
B. C > L
C. C < L - (residual risk)
D. C > L - (residual risk)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 163
Given the various means to protect physical and logical assets, match the access management area to the technology.



Answer:

Explanation

NEW QUESTION: 164
The Telecommunications Security Domain of information security is also concerned with the prevention and detection of the misuse or abuse of systems, which poses a threat to the tenets of:
A. Confidentiality, Integrity, and Entity (C.I.E.).
B. Confidentiality, Integrity, and Authenticity (C.I.A.).
C. Confidentiality, Integrity, and Availability (I.A.).
D. Confidentiality, Integrity, and Liability (C.I.L.).
Answer: (SHOW ANSWER)
The CIA acronym stands for Confidentiality, Integrity and Availability.
"Confidentiality, Integrity and Entity (CIE)" is incorrect. "Entity" is not part of the telecommunications domain definition.
"Confidentiality, Integrity and Authenticity (CIA)" is incorrect. While authenticity is included in the telecommunications domain, CIA is the acronym for confidentiality, integrity and availability.
"Confidentiality, Integrity, and Liability (CIL)" is incorrect. Liability is not part of the telecommunications domain definition.
References:
CBK, pp. 407 - 408

NEW QUESTION: 165
Which one of the following authentication mechanisms creates a problem for mobile users?
A. one-time password mechanism
B. address-based mechanism
C. challenge response mechanism
D. reusable password mechanism
Answer: (SHOW ANSWER)

NEW QUESTION: 166
Which of the following is an advantage of using a high-level programming language?
A. It decreases execution times for programs
B. It allows programmers to define syntax
C. It requires programmer-controlled storage management
D. It enforces coding standards
Answer: D (LEAVE A REPLY)

Coding standards are enforced because a specific order to statements are required and there is required syntax that also must be used. High-Level languages are easier to read because of the english like statements.

See extract below from the Official ISC2 Guide (OIG) to the CISSP CBK :

In the development phase, programmers have the option of writing code in several different programming languages. A programming language is a set of rules telling the computer what operations to perform.

Programming languages have evolved in generations, and each language is characterized into one of the generations. Those in the lower level are closer in form to the binary language of the computer. Both machine and assembly languages are considered low-level languages.

As the languages become easier and more similar to the language people use to communicate, they become higher level. High-level languages are easier to use than low-level languages and can be used to produce programs more quickly.

In addition, high-level languages may be said to be beneficial because they enforce coding standards and can provide more security. On the other hand, higher level languages automate certain functions, and provide complicated operations for the program, implemented by the programming environment or tool, the internal details of which may be poorly understood by the programmer. Therefore, it is possible that high-level languages may introduce security vulnerabilities in ways that are not apparent to the developer.

Programming languages are frequently referred to by generations.

The first generation is generally held to be the machine language, opcodes (operating codes), and object code used by the computer itself. These are very simple instructions that can be executed directly by the CPU of a computer. Each type of computer has its own machine language. However, the blizzard of hexadecimal or binary code is difficult for people to understand.

A second generation of assembly language was created, which uses symbols as abbreviations for major instructions.

The third generation, usually known as high-level language, uses meaningful words (generally English) as the commands. COBOL, FORTRAN, BASIC, and C are examples of this type.

Above this point there may be disagreement on definitions. Fourth-generation languages, sometimes known as very high-level languages, are represented by query languages, report generators, and application generators.

Fifth-generation languages, or natural language interfaces, require expert systems and artificial intelligence. The intent is to eliminate the need for programmers to learn a specific vocabulary, grammar, or syntax. The text of a natural language statement very closely resembles human speech.

NOTE FROM CLEMENT:

The use of the word Standard above is synonymous with Conventions

Code conventions are important to programmers for a number of reasons:

80% of the lifetime cost of a piece of software goes to maintenance.

Hardly any software is maintained for its whole life by the original author.

Code conventions improve the readability of the software, allowing engineers to understand new

code more quickly and thoroughly.
If you ship your source code as a product, you need to make sure it is as well packaged and clean as any other product you create.
The following statements are incorrect:
It decreases execution times for programs. This is incorrect because high-level languages need to be converted into code that the computer understands. The programs are either compiled or run through an interpreter and converted into machine language.
It allows programmers to define syntax. Is incorrect because there is a required syntax for high-level languages.
It requires programmer-controlled storage management. Is incorrect because whether it is a high-level language or not this would not be an advantage.
Reference(s) used for this question:
OIG CBK Application Security (pages 545 - 547)
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 13030-13035). Auerbach Publications. Kindle Edition.
and
Example of Java Code Conventions

NEW QUESTION: 167
Which of the following floors would be most appropriate to locate information processing facilities in a 6-stories building?
A. Basement
B. Ground floor
C. Third floor
D. Sixth floor
Answer: (SHOW ANSWER)
You data center should be located in the middle of the facility or the core of a building to provide protection from natural disasters or bombs and provide easier access to emergency crewmembers if necessary. By being at the core of the facility the external wall would act as a secondary layer of protection as well. Information processing facilities should not be located on the top floors of buildings in case of a fire or flooding coming from the roof. Many crimes and theft have also been conducted by simply cutting a large hole on the roof.

They should not be in the basement because of flooding where water has a natural tendancy to flow down :-) Even a little amount of water would affect your operation considering the quantity of electrical cabling sitting directly on the cement floor under under your raise floor.
The data center should not be located on the first floor due to the presence of the main entrance where people are coming in and out. You have a lot of high traffic areas such as the elevators, the loading docks, cafeteria, coffee shopt, etc.. Really a bad location for a data center.
So it was easy to come up with the answer by using the process of elimination where the top, the bottom, and the basement are all bad choices. That left you with only one possible answer which is the third floor.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 5th Edition, Page 425.

NEW QUESTION: 168
The National Computer Security Center (NCSC) is:
A. An activity within the US Department of Commerce that provides information security awareness training and develops standards for protecting sensitive but unclassified information
B. A joint enterprise between the NSA and NIST for developing cryptographic algorithms and standards
C. A division of the National Institute of Standards and Technology (NIST) that issues standards for cryptographic functions and publishes them as Federal Information Processing Standards (FIPS)
D. A branch of the National Security Agency (NSA) that initiates research and develops and publishes standards and criteria for trusted information systems
Answer: D (LEAVE A REPLY)
The NCSC promotes information systems security awareness and technology transfer through many channels, including the annual National Information Systems Security Conference. It was founded in 1981 as the Department of Defense Computer Security Center , and its name was change in 1985 to NCSc. It developed the Trusted Computer Evaluation Program Rainbow series for evaluating commercial products against information system security criteria. All the other answers are, therefore incorrect since they refer to NIST, which is under the US Department of Commerce.

NEW QUESTION: 169
In the following choices there is one that is a typical biometric characteristics that is not used to uniquely authenticate an individual's identity?
A. Retina scans
B. Iris scans
C. Palm scans
D. Skin scans

Answer: D (LEAVE A REPLY)
Answer A, B and C can be used to uniquely identify a person, but in the case of the Skin, there are no unique characteristics that can differentiate two distinct individuals in an acceptable accurate way. In the case of the IRIS and the
Retina, there are not two of them equal. In the case of the palm, every person has different marks on it. The skin is common to all and does not have specific textures or marks to make it unique in comparison to another individual.

NEW QUESTION: 170
Attributes that characterize an attack are stored for reference using which of the following Intrusion Detection System (IDS)?
A. signature-based IDS
B. statistical anomaly-based IDS
C. event-based IDS
D. inferent-based IDS
Answer: (SHOW ANSWER)
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49

NEW QUESTION: 171
Frame relay uses a public switched network to provide:
A. Local Area Network (LAN) connectivity.
B. Metropolitan Area Network (MAN) connectivity.
C. Wide Area Network (WAN) connectivity.
D. World Area Network (WAN) connectivity.
Answer: C (LEAVE A REPLY)
Frame relay uses a public switched network to provide Wide Area Network (WAN) connectivity.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the
Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 73.

NEW QUESTION: 172
Between which pair of Open System Interconnection (OSI) Reference Model layers are routers used as a communications device?
A. Data-Link and Transport
B. Transport and Session
C. Physical and Data-Link
D. Network and Session
Answer: A (LEAVE A REPLY)

NEW QUESTION: 173

An application developer is deciding on the amount of idle session time that the application allows before a timeout. The BEST reason for determining the session timeout requirement is

A. organization policy.

B. industry best practices.

C. industry laws and regulations.

D. management feedback.

Answer: A (LEAVE A REPLY)

Section: Software Development Security

NEW QUESTION: 174

Which of the following is NOT a basic component of security architecture?

A. Motherboard

B. Central Processing Unit (CPU)

C. Storage Devices

D. Peripherals (input/output devices)

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Explanation:

The system architecture aspect of security architecture includes the following:

CPU - Central Processing Unit

- Storage devices - includes both long and short-term storage, such as memory and disk
- Peripherals - includes both input and output devices, such as keyboards and printer

The components and devices connect to the motherboard. However, the motherboard is not considered a basic component of security architecture.

Incorrect Answers:

B: The Central Processing Unit (CPU) is a basic component of security architecture.

C: Storage Devices are a basic component of security architecture.

D: Peripherals (input/output devices) are a basic component of security architecture.

NEW QUESTION: 175

What are high-level policies?

A. They are step-by-step procedures to implement a safeguard.

B. They are the instructions on how to perform a Quantitative Risk Analysis.

C. They are recommendations for procedural controls.

D. They are statements that indicate a senior management's intention to support InfoSec.

Answer: D (LEAVE A REPLY)

The correct answer is "They are statements that indicate a senior management's intention to support InfoSec". High-level policies are senior management statements of recognition of the importance of InfoSec controls.

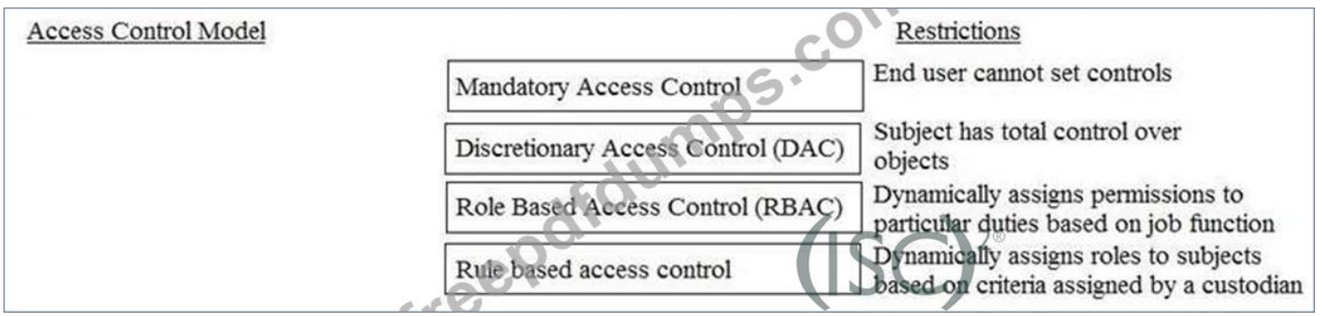
NEW QUESTION: 176

Drag and Drop Question

Match the name of access control model with its associated restriction.

Drag each access control model to its appropriate restriction access on the right.

Answer:



NEW QUESTION: 177

Which of the following biometrics methods provides the HIGHEST accuracy and is LEAST accepted by users?

A. Palm Scan

B. Hand Geometry

C. Fingerprint

D. Retina scan

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation:

A system that reads a person's retina scans the blood-vessel pattern of the retina on the backside of the eyeball. This pattern has shown to be extremely unique between different people. A camera is used to project a beam inside the eye and capture the pattern and compare it to a reference file recorded previously. Acceptability in terms of biometric systems refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system. For example, a concern with retina scanning systems may be the exchange of body fluids on the eyepiece or the feeling that a retinal scan could be harmful to the eye. Another concern would be the retinal pattern that could reveal changes in a person's health, such as diabetes or high blood pressure.

Incorrect Answers:

A: While requiring contact with a surface shared by others, a palm scan is generally considered more acceptable than sharing a surface with other parts of the anatomy. Therefore, this answer is incorrect.
B: A Hand Geometry scan is less accurate and more acceptable than a retina scan. Therefore, this answer is incorrect.
C: A fingerprint scan is more acceptable to users than a retina scan. Users are much more likely to prefer placing their fingers on a fingerprint scanner than looking into a retina scanner. Therefore, this answer is incorrect.
References:
Krutz, Ronald L and Russell Dean Vines, The CISSP and CAP Prep Guide: Mastering CISSP and CAP, Wiley Publishing, Indianapolis, 2007, p. 60 Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 191

NEW QUESTION: 178
What BEST describes the National Security Agency-developed
Capstone?
A. A one-way function for implementation of public key encryption
B. A device for intercepting electromagnetic emissions
C. A chip that implements the US Escrowed Encryption Standard
D. The PC Card implementation of the Clipper Chip system
Answer: C (LEAVE A REPLY)
Capstone is a Very Large Scale Integration (VLSI) chip that
employs the Escrowed Encryption Standard and incorporates the
Skipjack algorithm, similar to the Clipper Chip. As such, it has a
LEAf. Capstone also supports public key exchange and digital signatures.
At this time, Capstone products have their LEAF function suppressed
and a Certifying Authority provides for key recovery.
*Answer "A device for intercepting electromagnetic emissions" is then, obviously, incorrect.
For information purposes, though, the US Government program to study and control the interception of electromagnetic emissions that may compromise classified information is called TEMPEST.
* Answer "The PC Card implementation of the Clipper Chip system" is also, obviously, incorrect.
However, Capstone was first implemented on a PC card called
Fortezza.
* Answer "A one-way function for implementation of public key encryption" is incorrect since Capstone is not a mathematical function, but it incorporates mathematical functions for key
exchange, authentication and encryption.

NEW QUESTION: 179
In the days before CIDR (Classless Internet Domain Routing), networks were commonly organized by classes. Which of the following would have been true of a Class B network?
A. The first three bits of the ip address would be set to one
B. The first two bits of an ip address would be set to one, and the third bit set to zero

C. The first bit of the ip address would be set to one and the second bit set to zero
D. The first bit of the ip address would be set to zero
Answer: (SHOW ANSWER)

NEW QUESTION: 180
What is RAD?
A. A development methodology
B. A project management technique
C. A measure of system complexity
D. Risk-assessment diagramming
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The Rapid Application Development (RAD) model is a software development model or methodology that relies on the use of rapid prototyping and enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality.
Incorrect Answers:
B: RAD, or Rapid Application Development, is a software development model that relies on the use of rapid prototyping and enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality. It is not a project management technique.
C: RAD, or Rapid Application Development, is a software development model that relies on the use of rapid prototyping and enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality. It is not a measure of system complexity D: RAD, or Rapid Application Development, is a software development model that relies on the use of rapid prototyping and enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality. It is not Risk-assessment diagramming.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, pp. 1116-1118

NEW QUESTION: 181
What are the primary approaches IDS takes to analyze events to detect attacks?
A. Misuse detection and anomaly detection.
B. Log detection and anomaly detection.
C. Misuse detection and early drop detection.
D. Scan detection and anomaly detection.
Answer: A (LEAVE A REPLY)
There are two primary approaches to analyzing events to detect attacks: misuse detection and anomaly detection. Misuse detection, in which the analysis targets something known to be "bad", is the technique used by most commercial systems. Anomaly detection, in which the analysis looks for abnormal patterns of activity, has been, and continues to be, the subject of a great deal of research. Anomaly detection is used in limited form by a number of IDSs. There are strengths and weaknesses associated with each approach, and

it appears that the most effective IDSs use mostly misuse detection methods with a smattering of anomaly detection components.

NEW QUESTION: 182
Which of the following identifies the encryption algorithm selected by NIST for the new Advanced Encryption Standard?
A. Twofish
B. Serpent
C. RC6
D. Rijndael
Answer: (SHOW ANSWER)
The Answer: Rijndael. Rijndael is the new approved method of encrypting sensitive but unclassified information for the U.S. government. It has been accepted by and is also widely used in the public arena as well. It has low memory requirements and has been constructed to easily defend against timing attacks.
The following answers are incorrect: Twofish. Twofish was among the final candidates chosen for AES, but was not selected.
Serpent. Serpent was among the final candidates chosen for AES, but was not selected.
RC6. RC6 was among the final candidates chosen for AES, but was not selected.
The following reference(s) were/was used to create this question:
ISC2 OIG, 2007 p. 622, 629-630
Shon Harris AIO, v.3 p 247-250

NEW QUESTION: 183
What is a programmable logic device (PLD)?
A. Random Access Memory (RAM) that contains the software to perform specific tasks
B. An integrated circuit with connections or internal logic gates that can be changed through a programming process
C. A volatile device
D. A program resident on disk memory that executes a specific function
Answer: B (LEAVE A REPLY)
*Answer A volatile device is incorrect because a PLD is non-volatile.
*Answer "Random Access Memory (RAM) that contains the software to perform specific tasks" is incorrect because random access memory is volatile memory that is not a nonvolatile logic device.

*Answer "A program resident on disk memory that executes a specific function" is a distracter.

NEW QUESTION: 184
The goals of integrity do NOT include:
A. Accountability of responsible individuals
B. Prevention of the unauthorized or unintentional modification of information by authorized users
C. Preservation of internal and external consistency
D. Prevention of the modification of information by unauthorized users
Answer: (SHOW ANSWER)
The correct answer is "Accountability of responsible individuals". Accountability is holding individuals responsible for their actions. The other options are the three goals of
integrity.

NEW QUESTION: 185
For the purpose of classification, which of the following is used to divide trust domain and trust boundaries?
A. Network architecture
B. Integrity
C. Identity Management (IdM)
D. Confidentiality management
Answer: (SHOW ANSWER)
Section: Mixed questions

NEW QUESTION: 186
The Data Encryption Standard (DES) encryption algorithm has which of the following characteristics?
A. 64 bits of data input results in 56 bits of encrypted output
B. 128 bit key with 8 bits used for parity
C. 64 bit blocks with a 64 bit total key length
D. 56 bits of data input results in 56 bits of encrypted output
Answer: C (LEAVE A REPLY)
DES works with 64 bit blocks of text using a 64 bit key (with 8 bits used for parity, so
the effective key length is 56 bits).
Some people are getting the Key Size and the Block Size mixed up. The block size is usually a specific length. For example DES uses block size of 64 bits which results in 64 bits of encrypted data for each block. AES uses a block size of 128 bits, the block size on AES can only be 128 as per the published standard FIPS-197.
A DES key consists of 64 binary digits ("0"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each 8-bit byte1. Authorized users of encrypted computer data must have the key that was used to encipher the data in order to decrypt it.
IN CONTRAST WITH AES

The input and output for the AES algorithm each consist of sequences of 128 bits (digits with values of 0 or 1). These sequences will sometimes be referred to as blocks and the number of bits they contain will be referred to as their length. The Cipher Key for the AES algorithm is a sequence of 128, 192 or 256 bits. Other input, output and Cipher Key lengths are not permitted by this standard.
The Advanced Encryption Standard (AES) specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Rijndael was designed to handle additional block sizes and key lengths, however they are not adopted in the AES standard.
The AES algorithm may be used with the three different key lengths indicated above, and therefore these different "flavors" may be referred to as "AES-128", "AES-192", and "AES-256".
The other answers are not correct because:
"64 bits of data input results in 56 bits of encrypted output" is incorrect because while DES does work with 64 bit block input, it results in 64 bit blocks of encrypted output.
"128 bit key with 8 bits used for parity" is incorrect because DES does not ever use a 128 bit key.
"56 bits of data input results in 56 bits of encrypted output" is incorrect because DES always works with 64 bit blocks of input/output, not 56 bits.
Reference(s) used for this question:
Official ISC2 Guide to the CISSP CBK, Second Edition, page: 336-343
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

NEW QUESTION: 187
In addition to providing an audit trail required by auditors, logging can be used to
A. provide backout and recovery information
B. prevent security violations
C. provide system performance statistics
D. identify fields changed on master files.
Answer: B (LEAVE A REPLY)
Auditing tools are technical controls that track activity within a network on a network device or on a specific computer. Even though auditing is not an activity that will deny an entity access to a network or computer, it will track activities so a network administrator can understand the types of access that took place, identify a security breach, or warn the administrator of suspicious activity. This can be used to point out weakness of their technical controls and help administrators understand where changes need to be made to preserve the necessary security level within the environment. . - Shon Harris All-in-one CISSP Certification Guide pg 179-180

NEW QUESTION: 188
IT security measures should:
A. Be complex
B. Be tailored to meet organizational security goals.

C. Make sure that every asset of the organization is well protected.
D. Not be developed in a layered fashion.
Answer: B (LEAVE A REPLY)
In general, IT security measures are tailored according to an organization's unique needs. While numerous factors, such as the overriding mission requirements, and guidance, are to be considered, the fundamental issue is the protection of the mission or business from IT security-related, negative impacts. Because IT security needs are not uniform, system designers and security practitioners should consider the level of trust when connecting to other external networks and internal sub-domains. Recognizing the uniqueness of each system allows a layered security strategy to be used - implementing lower assurance solutions with lower costs to protect less critical systems and higher assurance solutions only at the most critical areas.
The more complex the mechanism, the more likely it may possess exploitable flaws.
Simple mechanisms tend to have fewer exploitable flaws and require less maintenance.
Further, because configuration management issues are simplified, updating or replacing a simple mechanism becomes a less intensive process.
Security designs should consider a layered approach to address or protect against a specific threat or to reduce a vulnerability. For example, the use of a packet-filtering router in conjunction with an application gateway and an intrusion detection system combine to increase the work-factor an attacker must expend to successfully attack the system. Adding good password controls and adequate user training improves the system's security posture even more.
The need for layered protections is especially important when commercial-off-the-shelf
(COTS) products are used. Practical experience has shown that the current state-of-the-art for security quality in COTS products does not provide a high degree of protection against sophisticated attacks. It is possible to help mitigate this situation by placing several controls in series, requiring additional work by attackers to accomplish their goals.
Source: STONEBURNER, Gary & al, National Institute of Standards and Technology
(NIST), NIST Special Publication 800-27, Engineering Principles for Information
Technology Security (A Baseline for Achieving Security), June 2001 (pages 9-10).

NEW QUESTION: 189
How does security in a distributed file system using mutual authentication differ from file security in a multi-user host?
A. Access control can rely on the Operating System (OS), and eavesdropping is
B. Access control cannot rely on the Operating System (OS), and eavesdropping
C. Access control cannot rely on the Operating System (OS), and eavesdropping
D. Access control can rely on the Operating System (OS), but eavesdropping is
Answer: A (LEAVE A REPLY)

NEW QUESTION: 190
Which of the following is less likely to be used in creating a Virtual Private Network?
A. L2TP
B. PPTP

C. IPSec
D. L2F
Answer: (SHOW ANSWER)
"The following are the three most common VPN communications protocol standards:
Point-to-Point Tunneling Protocol(PPTP). PPTP works at the Data Link Layer of the OSI model. Designed for individual client to server connections, it enables only a single point-to-point connection per session. This standard is very common with asynchronous connections that use Win9x or NT clients. PPTP uses native Point-to-Point Protocol (PPP) authentication and encryption services.
Layer 2 Tunneling Protocol (L2TP). L2TP is a combination of PPTP and the earlier Layer 2 Forwarding (L2F) Protocol that works at the Data Link Layer like PPTP. It has become an accepted tunneling standard for VPN's. In fact, dial-up VPNs use this standard quite frequently. Like PPTP, this standard was designed for single point-to-point client to server connections. Not that multiple protocols can be encapsulated within the L2TP tunnel, but do not use encryption like PPTP. Also, L2TP supports TACACS+ and RADIUS, but PPTP does not.
IPSEC. IPSec operates at the Network Layer and it enables multiple and simultaneous tunnels, unlike the single connection of the previous standards. IPSec has the functionality to encrypt and authenticate IP data. It is built into the new Ipv6 standard, and is used as an add-on to the current Ipv4. While PPTP and L2TP are aimed more at dial-up VPNs, IPSec focuses more on network-tonetwork connectivity." Pg. 123-125 Krutz: The CISSP Prep Guide: Gold Edition.

NEW QUESTION: 191
Which of the following statements pertaining to fire suppression systems is TRUE?
A. Halon is today the most common choice as far as agent are concern because it is highly effective in the way that it interferes with the chemical reaction of the elements within a fire.
B. Gas masks provide an effective protection against use of CO2 systems. They are recommended for the protection of the employees within data centers.
C. CO2 systems are NOT effective because they suppress the oxygen supply required to sustain the fire.
D. Water Based extinguisher are NOT an effective fire suppression method for class C
(electrical) fires.
Answer: (SHOW ANSWER)
Water Based fire extinguishers should never be used on Electrical Fire. If you do so, it will probably the last time you use such an extinguisher to put out an electrical fire as you will be electrocuted. Any liquid based agent should be avoided for Electrical
Fire.
CO2 systems are effective because they suppress the oxygen supply required to sustain the fire. Since oxygen is removed, it can be potentially lethal to people and gas masks do not provide protection against CO2. These systems are more appropriate for unattended facilities.
The Montreal Protocol of 1987 states that Halon has been designated an ozone-depleting substance and due to the risk to the environment production was stopped January 1st,
1994. Companies that still have Halon systems have been asked to replace them with nontoxic extinguishers. The name of the agreement is called The Montreal Protocol.

Soda acid is an effective fire suppression method for common combustibles and liquids, but not for electrical fires.
TIP:
Do remember the name of the agreement that was signed in Montreal where countries have agreed to stop production of Halon, it is called: The Montreal Protocol
A student of mine told me that he thinks about me when he wish to remember the classes of fire, that scared me off a bit but his explanations made a lot of sense, here how he is using my first name to remember the classes of fire. My name is CLEMENT but he is using only the CLEM portion:
C = Common Combustible
L = Liquid Fire
E = Electrical Fire
M = Metals that are flammable
HERE IS ANOTHER WAY TO REMEMBER THEM FROM HARRISON:
A - Ash (common combustible)
B - Bubble/Boil (Liquid)
C - Circuit (Electrical)
D - Metal. (Just remember it :)
Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 6: Physical Security (page 313).

NEW QUESTION: 192
The US Government Tempest program was established to thwart which
one of the following types of attacks?
A. Emanation Eavesdropping
B. Denial of Service
C. Software Piracy
D. Dumpster Diving
Answer: A (LEAVE A REPLY)
The correct answer is Emanation Eavesdropping. The Tempest program required shielding and other emanation reducing safeguards to be employed on computers processing classified data. The other answers are types of attacks against computers, but are not the focus of the Tempest program.

NEW QUESTION: 193
What are cognitive passwords?
A. Passwords that can be used only once.
B. Fact or opinion-based information used to verify an individual's identity.
C. Password generators that use a challenge response scheme.
D. Passphrases.
Answer: B (LEAVE A REPLY)

Cognitive passwords are fact or opinion-based information used to verify an individual's identity. Passwords that can be used only once are one-time or dynamic passwords. Password generators that use a challenge response scheme refer to token devices.
A passphrase is a sequence of characters that is longer than a password and is transformed into a virtual password.
Source: WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#1 Access Control System & Methodology (page 2), /Documents/CISSP_Summary_2002/index.html.

NEW QUESTION: 194
Which of the following is true about Kerberos?
A. It is a second party authentication system
B. It depends upon symmetric ciphers
C. It encrypts data after a ticket is granted, but passwords are exchanged in plain text.
D. It utilizes public key cryptography
Answer: B (LEAVE A REPLY)

NEW QUESTION: 195
In Mandatory Access Control, sensitivity labels attached to object contain what information?
A. The item's classification
B. The item's classification and category set
C. The item's category
D. The items's need to know
Answer: B (LEAVE A REPLY)
The following is the correct answer: the item's classification and category set.
A Sensitivity label must contain at least one classification and one category set.
Category set and Compartment set are synonyms, they mean the same thing. The sensitivity label must contain at least one Classification and at least one Category. It is common in some environments for a single item to belong to multiple categories. The list of all the categories to which an item belongs is called a compartment set or category set.
The following answers are incorrect:
The item's classification. Is incorrect because you need a category set as well.
The item's category. Is incorrect because category set and classification would be both be required.
The item's need to know. Is incorrect because there is no such thing. The need to know is indicated by the catergories the object belongs to. This is NOT the best answer.
Reference(s) used for this question:
OIG CBK, Access Control (pages 186 - 188)
AIO, 3rd Edition, Access Control (pages 162 - 163)
AIO, 4th Edition, Access Control, pp 212-214
Wikipedia - http://en.wikipedia.org/wiki/Mandatory_Access_Control

NEW QUESTION: 196

During an audit of system management, auditors find that the system administrator has not been trained. What actions need to be taken at once to ensure the integrity of systems?

A. A review of all departmental procedures

B. A review of all systems by an experienced administrator

C. A review of hiring policies and methods of verification of new employees

D. A review of all training procedures to be undertaken

Answer: (SHOW ANSWER)

NEW QUESTION: 197

Which of the following can BEST prevent security flaws occurring in outsourced software development?

A. Contractual requirements for code quality

B. Certification of the quality and accuracy of the work done

C. Licensing, code ownership and intellectual property rights

D. Delivery dates, change management control and budgetary control

Answer: B (LEAVE A REPLY)

NEW QUESTION: 198

How should a risk be HANDLED when the cost of the countermeasure OUTWEIGHS the cost of the risk?

A. Reject the risk

B. Perform another risk analysis

C. Accept the risk

D. Reduce the risk

Answer: (SHOW ANSWER)

Which means the company understands the level of risk it is faced.

The following answers are incorrect because :

Reject the risk is incorrect as it means ignoring the risk which is dangerous.

Perform another risk analysis is also incorrect as the existing risk analysis has already shown the results.

Reduce the risk is incorrect is applicable after implementing the countermeasures.

Reference : Shon Harris AIO v3 , Chapter-3: Security Management Practices , Page : 39

NEW QUESTION: 199

Which of the following encryption methods is known to be unbreakable?

A. Symmetric ciphers.
B. DES codebooks.
C. One-time pads.
D. Elliptic Curve Cryptography.
Answer: (SHOW ANSWER)
A One-Time Pad uses a keystream string of bits that is generated completely at random that is used only once. Because it is used only once it is considered unbreakable.
The following answers are incorrect: Symmetric ciphers. This is incorrect because a Symmetric Cipher is created by substitution and transposition. They can and have been broken
DES codebooks. This is incorrect because Data Encryption Standard (DES) has been broken, it was replaced by Advanced Encryption Standard (AES).
Elliptic Curve Cryptography. This is incorrect because Elliptic Curve Cryptography or ECC is typically used on wireless devices such as cellular phones that have small processors. Because of the lack of processing power the keys used at often small. The smaller the key, the easier it is considered to be breakable. Also, the technology has not been around long enough or tested thourough enough to be considered truly unbreakable.

NEW QUESTION: 200
When considering all the reasons that buffer overflow vulnerabilities exist what is the real reason?
A. Human error
B. The Windows Operating system
C. Insecure programming languages
D. Insecure Transport Protocols
Answer: A (LEAVE A REPLY)
Discussion: Since computer program code is written by humans and there are proper and improper ways of writing software code it is clear that human errors create the conditions for buffer overflows to exist. Unfortunately as secure as any operating system is it becomes insecure when people install insecure code that can be host to buffer overflow attacks so it is human error that really causes these vulnerabilities.
Mitigation: The best mitigation against buffer overflow attacks is to:
- Be sure you keep your software updated with any patches released by the vendors.
- Have sensible configurations for your software. (e.g,. lock it down)
- Control access to your sensitive systems with network traffic normalizing systems like a filtering firewall or other devices that drops inappropriate network packets.
- If you don't need the software or service on a system, remove it. If it is useless it can only be a threat.
The following answers are incorrect:
The Windows Operating system: This isn't the intended answer.
Insecure programming languages: This isn't correct. Modern programming languages are capable of being used securely. It's only when humans make mistakes that any programming language becomes a threat.
Insecure Transport Protocols: This is partially correct. If you send logon ID and passwords over the network in clear text, no programming language will protect you from sniffers.
The following reference(s) were/was used to create this question:

2 011 EC-COUNCIL Official Curriculum, Ethical Hacking and Countermeasures, v71,
Module 17, Page 806

NEW QUESTION: 201
A smart Card that has two chips with the Capability of utilizing both Contact and Contactless formats is called:
A. Contact Smart Cards
B. Contactless Smart Cards
C. Hybrid Cards
D. Combi Cards
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
A smart Card that has two chips with the ability of utilizing both Contact and Contactless formats is called a combi card.
Incorrect Answers:
A: Contact Smart Cards are not configured for the Contactless format.
B: Contactless Smart Cards are not configured for the Contact format
C: The hybrid card makes use of two CPU chips for processing and includes both contact-oriented and contactless components.
D: The combi-card is similar to the hybrid card, but it only uses a single CPU chip for the processing.
References:
Miller, David R, CISSP Training Kit, O'Reilly Media, 2013, Sebastopol, p. 82
http://www.smartcardalliance.org/pages/smart-cards-intro-primer

NEW QUESTION: 202
Which of the following rules pertaining to a Business Continuity Plan/Disaster Recovery Plan is incorrect?
A. In order to facilitate recovery, a single plan should cover all locations.
B. There should be requirements to form a committee to decide a course of action. These decisions should be made ahead of time and incorporated into the plan.
C. In its procedures and tasks, the plan should refer to functions, not specific individuals.
D. Critical vendors should be contacted ahead of time to validate equipment can be obtained in a timely manner.
Answer: A (LEAVE A REPLY)
The first documentation rule when it comes to a BCP/DRP is "one plan, one building". Much of the plan revolves around reconstructing a facility and replenishing it with production contents. If more than one facility is involved, then the reader of the plan will find it difficult to identify quantities and specifications of replacement resource items. It is possible to have multiple plans for a single building, but those plans must be linked so that the identification and ordering of resource items is centralized. All other statements are correct.
Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 162).

NEW QUESTION: 203
What is the minimum static charge able to cause disk drive data loss?
A. 550 volts
B. 1000 volts
C. 1500 volts
D. 2000 volts
Answer: C (LEAVE A REPLY)
A static charge of 1500 volts is able to cause disk drive data loss.
A charge of 1000 volts is likely to scramble monitor display and a charge of 2000 volts can cause a system shutdown.
It should be noted that charges of up to 20,000 volts or more are possible under conditions of very low humidity with non-static-free carpeting.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 10: Physical Security (page 333).

NEW QUESTION: 204
Physical security is accomplished through proper facility construction, fire and water protection, anti-theft mechanisms, intrusion detection systems, and security procedures that are adhered to and enforced. Which of the following is not a component that achieves this type of security?
A. Administrative control mechanisms
B. Integrity control mechanisms
C. Technical control mechanisms
D. Physical control mechanisms
Answer: B (LEAVE A REPLY)
Integrity Controls Mechanisms are not part of physical security. All of the other detractors were correct this one was the wrong one that does not belong to Physical Security. Below you have more details extracted from the SearchSecurity web site:
Information security depends on the security and management of the physical space in which computer systems operate. Domain 9 of the CISSP exam's Common Body of Knowledge addresses the challenges of securing the physical space, its systems and the people who work within it by use of administrative, technical and physical controls. The following topics are covered:
Facilities management: The administrative processes that govern the maintenance and protection of the physical operations space, from site selection through emergency response.
Risks, issues and protection strategies: Risk identification and the selection of security protection components.
Perimeter security: Typical physical protection controls.
Facilities management
Facilities management is a complex component of corporate security that ranges from the planning of a secure physical site to the management of the physical information system environment. Facilities

management responsibilities include site selection and physical security planning (i.e. facility construction, design and layout, fire and water damage protection, antitheft mechanisms, intrusion detection and security procedures.) Protections must extend to both people and assets. The necessary level of protection depends on the value of the assets and data. CISSP candidates must learn the concept of critical-path analysis as a means of determining a component's business function criticality relative to the cost of operation and replacement. Furthermore, students need to gain an understanding of the optimal location and physical attributes of a secure facility. Among the topics covered in this domain are site inspection, location, accessibility and obscurity, considering the area crime rate, and the likelihood of natural hazards such as floods or earthquakes.

This domain also covers the quality of construction material, such as its protective qualities and load capabilities, as well as how to lay out the structure to minimize risk of forcible entry and accidental damage. Regulatory compliance is also touched on, as is preferred proximity to civil protection services, such as fire and police stations. Attention is given to computer and equipment rooms, including their location, configuration (entrance/egress requirements) and their proximity to wiring distribution centers at the site.

Physical risks, issues and protection strategies

An overview of physical security risks includes risk of theft, service interruption, physical damage, compromised system integrity and unauthorized disclosure of information.

Interruptions to business can manifest due to loss of power, services, telecommunications connectivity and water supply. These can also seriously compromise electronic security monitoring alarm/response devices. Backup options are also covered in this domain, as is a strategy for quantifying the risk exposure by simple formula.

Investment in preventive security can be costly. Appropriate redundancy of people skills, systems and infrastructure must be based on the criticality of the data and assets to be preserved. Therefore a strategy is presented that helps determine the selection of cost appropriate controls. Among the topics covered in this domain are regulatory and legal requirements, common standard security protections such as locks and fences, and the importance of establishing service level agreements for maintenance and disaster support. Rounding out the optimization approach are simple calculations for determining mean time between failure and mean time to repair (used to estimate average equipment life expectancy) - essential for estimating the cost/benefit of purchasing and maintaining redundant equipment.

As the lifeblood of computer systems, special attention is placed on adequacy, quality and protection of power supplies. CISSP candidates need to understand power supply concepts and terminology, including those for quality (i.e. transient noise vs. clean power); types of interference (EMI and RFI); and types of interruptions such as power excess by spikes and surges, power loss by fault or blackout, and power degradation from sags and brownouts. A simple formula is presented for determining the total cost per hour for backup power. Proving power reliability through testing is recommended and the advantages of three power protection approaches are discussed (standby UPS, power line conditioners and backup sources) including minimum requirements for primary and alternate power provided.

Environmental controls are explored in this domain, including the value of positive pressure water drains and climate monitoring devices used to control temperature, humidity and reduce static electricity. Optimal temperatures and humidity settings are provided.

Recommendations include strict procedures during emergencies, preventing typical risks

(such as blocked fans), and the use of antistatic armbands and hygrometers. Positive pressurization for proper ventilation and monitoring for air born contaminants is stressed.
The pros and cons of several detection response systems are deeply explored in this domain. The concept of combustion, the classes of fire and fire extinguisher ratings are detailed. Mechanisms behind smoke-activated, heat-activated and flame-activated devices and Automatic Dial-up alarms are covered, along with their advantages, costs and shortcomings. Types of fire sources are distinguished and the effectiveness of fire suppression methods for each is included. For instance, Halon and its approved replacements are covered, as are the advantages and the inherent risks to equipment of the use of water sprinklers.
Administrative controls
The physical security domain also deals with administrative controls applied to physical sites and assets. The need for skilled personnel, knowledge sharing between them, separation of duties, and appropriate oversight in the care and maintenance of equipment and environments is stressed. A list of management duties including hiring checks, employee maintenance activities and recommended termination procedures is offered.
Emergency measures include accountability for evacuation and system shutdown procedures, integration with disaster and business continuity plans, assuring documented procedures are easily available during different types of emergencies, the scheduling of periodic equipment testing, administrative reviews of documentation, procedures and recovery plans, responsibilities delegation, and personnel training and drills.
Perimeter security
Domain nine also covers the devices and techniques used to control access to a space.
These include access control devices, surveillance monitoring, intrusion detection and corrective actions. Specifications are provided for optimal external boundary protection, including fence heights and placement, and lighting placement and types. Selection of door types and lock characteristics are covered. Surveillance methods and intrusion-detection methods are explained, including the use of video monitoring, guards, dogs, proximity detection systems, photoelectric/photometric systems, wave pattern devices, passive infrared systems, and sound and motion detectors, and current flow sensitivity devices that specifically address computer theft. Room lock types - both preset and cipher locks (and their variations) -- device locks, such as portable laptop locks, lockable server bays, switch control locks and slot locks, port controls, peripheral switch controls and cable trap locks are also covered. Personal access control methods used to identify authorized users for site entry are covered at length, noting social engineering risks such as piggybacking. Wireless proximity devices, both user access and system sensing readers are covered (i.e. transponder based, passive devices and field powered devices) in this domain.
Now that you've been introduced to the key concepts of Domain 9, watch the Domain 9, Physical Security video
Return to the CISSP Essentials Security School main page
See all SearchSecurity.com's resources on CISSP certification training
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 280.

NEW QUESTION: 205
Which of the following is not a known type of Message Authentication Code (MAC)?

A. Block cipher-based MAC
B. Stream cipher-based MAC
C. Signature-based MAC
D. Hash function-based MAC
Answer: (SHOW ANSWER)

NEW QUESTION: 206
Which type of fire alarm system sensor is intended to detect fire at its earliest stage?
A. Ionization
B. Photoelectric
C. Infrared
D. Thermal
Answer: A (LEAVE A REPLY)

NEW QUESTION: 207
A DMZ is located:
A. right behind your first Internet facing firewall
B. right in front of your first Internet facing firewall
C. right behind your first network active firewall
D. right behind your first network passive Internet http firewall
Answer: (SHOW ANSWER)
While the purpose of systems in the DMZ is to allow public access to certain internal network resources (EMAIL, DNS, Web), it is a good practice to restrict that access to the minimum necessary to provide those services through use of a firewall. In computer security, a DMZ or Demilitarized Zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external attacker only has direct access to equipment in the DMZ, rather than any other part of the network. The name is derived from the term "demilitarized zone", an area between nation states in which military operation is not permitted.
The following are incorrect answers: "Right in front of your first Internet facing firewall" While the purpose of systems in the DMZ is to allow public access to certain internal network resources (EMAIL, DNS, Web), it is a good practice to restrict that access to the minimum necessary to provide those services through use of a firewall.
"Right behind your first network active firewall" This is an almost-right-sounding answer meant to distract the unwary.
"Right behind your first network passive Internet http firewall" This is an almost-right-sounding answer meant to distract the unwary.
References: CBK, p. 434 and AIO3, p. 483 and http://en.wikipedia.org/wiki/DMZ_%28computing%29

NEW QUESTION: 208

Which of the following would be MOST important to guarantee that the computer evidence will be admissible in court?

A. It must prove a fact that is immaterial to the case.

B. Its reliability must be proven.

C. The process for producing it must be documented and repeatable.

D. The chain of custody of the evidence must show who collected, secured, controlled, handled, transported the evidence, and that it was not tampered with.

Answer: D (LEAVE A REPLY)

The answer: The
chain of custody of the evidence must show who collected,
secured, controlled, handled, and transported the evidence, and that it was not tampered with.
It has to be material, relevant and reliable, and the chain of custody must be maintained, it is unlikely that it will be admissible in court if it has been tampered with.

The following answers are incorrect:

It must prove a fact that is immaterial to the case. Is incorrect because evidence must be relevant. If it is immaterial then it is not relevant.

Its reliability must be proven. Is incorrect because it is not the best answer. While evidence must be relevant if the chain of custody cannot be verified, then the evidence could lose it's credibility because there is no proof that the evidence was not tampered with. So, the correct answer above is the BEST answer.

The process for producing it must be documented and repeatable. Is incorrect because just because the process is documented and repeatable does not mean that it will be the same. This amounts to Corroborative Evidence that may help to support a case.

NEW QUESTION: 209

What is the process that RAID Level 0 uses as it creates one large disk by using several disks?

A. striping

B. mirroring

C. integrating

D. clustering

Answer: (SHOW ANSWER)

RAID Level 0 creates one large disk by using several disks. This process is called striping. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 65.

NEW QUESTION: 210

What is the BEST description of risk reduction?

A. Assuming all costs associated with the risk internally

B. Assigning any costs associated with risk to a third party

C. Removing all risk to the enterprise at any cost

D. Altering elements of the enterprise in response to a risk analysis

Answer: D (LEAVE A REPLY)
The correct answer is "Altering elements of the enterprise in response to a risk analysis". Answer "Removing all risk to the enterprise at any cost" is not possible or desirable, "Assigning any costs associated with risk to a third party" is risk transference, and "Assuming all costs associated with the risk internally" is risk acceptance.

NEW QUESTION: 211
According to FEMA, which choice below is NOT a recommended way
to purify water after a disaster?
A. Distilling the water for twenty minutes
B. Adding 16 drops per gallon of household liquid bleach to the water
C. Adding water treatment tablets to the water
D. Boiling from 3 to 5 minutes
Answer: C (LEAVE A REPLY)
FEMArecommends that water treatment products sold in camping
or surplus stores should not be used, unless the only active ingredient is 5.25 percent hypochloritE. When adding liquid bleach, it should contain 5.25 percent hypochlorite and no other added cleaners or scents. Distilling the water is the most highly recommended method,
as it also removes other chemicals and heavy metals, as well as most
microbes. Source: Emergency Water and Food Procedures, Federal Emergency
Management Agency, April, 1997.

NEW QUESTION: 212
Packet Filtering Firewalls can also enable access for:
A. only authorized application port or service numbers.
B. only unauthorized application port or service numbers.
C. only authorized application port or ex-service numbers.
D. only authorized application port or service integers.
Answer: A (LEAVE A REPLY)
Firewall rules can be used to enable access for traffic to specific ports or services. "Service numbers" is rather stilted English but you may encounter these types of wordings on the actual exam -- don't let them confuse you.

"Only unauthorized application port or service numbers" is incorrect. Unauthorized ports/services would be blocked in a properly installed firewall rather than permitting access.
"Only authorized application port or ex-service numbers" is incorrect. "Ex-service" numbers is a nonsense term meant to distract you.
"Only authorized application port or service integers." While service numbers are in fact integers, the more usual (and therefore better) answer is either service or "service number."
References
CBK, p. 464
AIO3, pp. 482 - 484

NEW QUESTION: 213
Due to system constraints, a group of system administrators must share a high-level access set of credentials.
Which of the following would be MOST appropriate to implement?
A. Increased console lockout times for failed logon attempts
B. Reduce the group in size
C. A credential check-out process for a per-use basis
D. Full logging on affected systems
Answer: C (LEAVE A REPLY)
Section: Security Operations

NEW QUESTION: 214
A security practitioner has just been assigned to address an ongoing Denial of Service (DoS) attack against the company's network, which includes an e-commerce web site. The strategy has to include defenses for any size of attack without rendering the company network unusable. Which of the following should be a PRIMARY concern when addressing this issue?
A. Deal with end user education and training.
B. Pay more for a dedicated path to the Internet.
C. Allow legitimate connections while blocking malicious connections.
D. Ensure the web sites are properly backed up on a daily basis.
Answer: C (LEAVE A REPLY)
Section: Mixed questions

NEW QUESTION: 215
Which of the following is a limitation of the Common Vulnerability Scoring System (CVSS) as it relates to conducting code review?
A. It aims to calculate the risk of published vulnerabilities.
B. It has many worksheets and practices to implement.
C. It requires a robust risk management framework to be put in place.
D. It has normalized severity ratings.
Answer: (SHOW ANSWER)

NEW QUESTION: 216
What is the length of an MD5 message digest?
A. 128 bits
B. 160 bits
C. 256 bits
D. varies depending upon the message size.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
MD5 is a message digest algorithm that was developed by Ronald Rivest in 1991. MD5 takes a message of an arbitrary length and generates a 128-bit message digest. In MD5, the message is processed in 512- bit blocks in four distinct rounds.
Incorrect Answers:
B: MD5 generates a 128-bit message digest, not 160-bit.
C: MD5 generates a 128-bit message digest, not 256-bit.
D: MD5 generates a 128-bit message digest regardless of the message size.
Krutz, Ronald L. and Russel Dean Vines, The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, New York, 2001, p. 153

NEW QUESTION: 217
Which approach to a security program ensures people responsible for protecting the company's assets are driving the program?
A. The Delphi approach.
B. The top-down approach.
C. The bottom-up approach.
D. The technology approach.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A security program should use a top-down approach, meaning that the initiation, support, and direction come from top management; work their way through middle management; and then reach staff members.
In contrast, a bottom-up approach refers to a situation in which staff members (usually IT) try to develop a security program without getting proper management support and direction. A bottom-up approach is commonly less effective, not broad enough to address all security risks, and doomed to fail. A top-down approach makes sure the people actually responsible for protecting the company's assets (senior management) are driving the program. Senior management are not only ultimately responsible for the protection of the organization, but also hold the purse strings for the necessary funding, have the authority to assign needed resources, and are the only ones who can ensure true enforcement of the stated security rules and policies.
Incorrect Answers:

A: Delphi is a group decision method used to ensure that each member of a group gives an honest and anonymous opinion pertaining to the company's risks.
C: The bottom-up approach is the opposite to the top-down approach. The bottom-up approach refers to a situation in which staff members (usually IT) try to develop a security program without getting proper management support and direction.
D: The technology approach is not a defined security program approach.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 63

NEW QUESTION: 218
Which of the following steps should be performed first in a business impact analysis (BIA)?
A. Estimate the Recovery Time Objectives (RTO)
B. Evaluate the criticality of business functions
C. Identify all business units within the organization
D. Evaluate the impact of the disruptive events
Answer: C (LEAVE A REPLY)

NEW QUESTION: 219
What is called an event or activity that has the potential to cause harm to the information systems or networks?
A. Vulnerability
B. Threat agent
C. Weakness
D. Threat
Answer: D (LEAVE A REPLY)
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the
Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 16, 32.

NEW QUESTION: 220
Which of the following will you consider as a "role" under a role based access control system?
A. Bank rules
B. Bank computer
C. Bank teller
D. Bank network
Answer: C (LEAVE A REPLY)
With role-based access control, access rights are grouped by role name, and the use of resources is restricted to individuals authorized to assume the associated role. For example, within a hospital system the role of doctor can include operations to perform diagnosis, prescribe medication, and order laboratory tests; and the role of researcher can be limited to gathering anonymous clinical information for studies.

NEW QUESTION: 221

A DMZ is located:
A. right behind your first Internet facing firewall
B. right in front of your first Internet facing firewall
C. right behind your first network active firewall
D. right behind your first network passive Internet http firewall
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
A demilitarized zone is shielded by two firewalls: one right behind the first Internet facing the Internet, and one facing the private network.
Incorrect Answers:
B: A demilitarized zone is shielded by the Internet facing firewall. It is not placed outside this firewall.
C: A demilitarized zone is placed behind the first Internet facing firewall, not behind the first network active firewall.
D: A demilitarized zone does not need to be placed behind a network passive Internet http firewall. It just needs to be place behind the first Internet facing firewall.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 629

NEW QUESTION: 222
Which of the following questions is less likely to help in assessing physical access controls?
A. Does management regularly review the list of persons with physical access to sensitive facilities?
B. Is the operating system configured to prevent circumvention of the security software and application controls?
C. Are keys or other access devices needed to enter the computer room and media library?
D. Are visitors to sensitive areas signed in and escorted?
Answer: B (LEAVE A REPLY)
Physical security and environmental security are part of operational controls, and are measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. All the questions above are useful in assessing physical access controls except for the one regarding operating system configuration, which is a logical access control. Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Pages A-21 to A-24).

NEW QUESTION: 223
Which of the following algorithms does NOT provide hashing?
A. SHA-1
B. MD2
C. RC4
D. MD5
Answer: (SHOW ANSWER)

As it is an algorithm used for encryption and does not provide hashing functions , it is also commonly implemented ' Stream Ciphers '.
The other answers are incorrect because :
SHA-1 was designed by NIST and NSA to be used with the Digital Signature Standard (DSS).
SHA was designed to be used in digital signatures and was developed when a more secure hashing algorithm was required for U.S. government applications.
MD2 is a one-way hash function designed by Ron Rivest that creates a 128-bit message digest value. It is not necessarily any weaker than the other algorithms in the "MD" family, but it is much slower.
MD5 was also created by Ron Rivest and is the newer version of MD4. It still produces a 128-bit hash, but the algorithm is more complex, which makes it harder to break.
Reference : Shon Harris , AIO v3 , Chapter - 8 : Cryptography , Page : 644 - 645

NEW QUESTION: 224
Which of the following best explains why computerized information systems frequently fail to meet the needs of users?
A. Constantly changing user needs
B. Inadequate quality assurance (QA) tools
C. Inadequate project management.
D. Inadequate user participation in defining the system's requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 225
Which of the following would not correspond to the number of primary keys values found in a table in a relational database?
A. Degree
B. Number of tuples
C. Cardinality
D. Number of rows
Answer: A (LEAVE A REPLY)
The degree of a table represents the number of columns in a table.
All other elements represent the number of rows, or records, thus the number of unique primary keys values within the table.
NOTE FROM DAN:
You can have multiple columns that in aggregate make up the Primary Key, but you only have one PK.
Primary Keys
The first type of key we'll discuss is the primary key. Every database table should have one or more columns designated as the primary key. The value this key holds should be unique for each record in the database. For example, assume we have a table called Employees that contains personnel information for every employee in our firm. We'd need to select an appropriate primary key that would uniquely identify each employee. Your first thought might be to use the employee's name.

This wouldn't work out very well because it's conceivable that you'd hire two employees with the same name. A better choice might be to use a unique employee ID number that you assign to each employee when they're hired. Some organizations choose to use Social
Security Numbers (or similar government identifiers) for this task because each employee already has one and they're guaranteed to be unique. However, the use of Social Security
Numbers for this purpose is highly controversial due to privacy concerns. (If you work for a government organization, the use of a Social Security Number may even be illegal under the Privacy Act of 1974.) For this reason, most organizations have shifted to the use of unique identifiers (employee ID, student ID, etc.) that don't share these privacy concerns.

Once you decide upon a primary key and set it up in the database, the database management system will enforce the uniqueness of the key. If you try to insert a record into a table with a primary key that duplicates an existing record, the insert will fail.

Most databases are also capable of generating their own primary keys. Microsoft Access, for example, may be configured to use the AutoNumber data type to assign a unique ID to each record in the table. While effective, this is a bad design practice because it leaves you with a meaningless value in each record in the table. Why not use that space to store something useful?

Foreign Keys

The other type of key that we'll discuss in this course is the foreign key. These keys are used to create relationships between tables. Natural relationships exist between tables in most database structures. Returning to our employees database, let's imagine that we wanted to add a table containing departmental information to the database. This new table might be called Departments and would contain a large amount of information about the department as a whole. We'd also want to include information about the employees in the department, but it would be redundant to have the same information in two tables
(Employees and Departments). Instead, we can create a relationship between the two tables.

Let's assume that the Departments table uses the Department Name column as the primary key. To create a relationship between the two tables, we add a new column to the
Employees table called Department. We then fill in the name of the department to which each employee belongs. We also inform the database management system that the
Department column in the Employees table is a foreign key that references the
Departments table. The database will then enforce referential integrity by ensuring that all of the values in the Departments column of the Employees table have corresponding entries in the Departments table.

Note that there is no uniqueness constraint for a foreign key. We may (and most likely do!) have more than one employee belonging to a single department. Similarly, there's no requirement that an entry in the Departments table have any corresponding entry in the
Employees table. It is possible that we'd have a department with no employees.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the
Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access Control
Systems (page 45).

also see:

http://databases.about.com/od/specificproducts/a/keys.htm

NEW QUESTION: 226
Which of the following is addressed by Kerberos?
A. Authorization and authentication.
B. Validation and integrity.
C. Confidentiality and integrity.
Answer: C (LEAVE A REPLY)
Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. A free implementation of this protocol is available from the Massachusetts Institute of Technology.
Kerberos is available in many commercial products as well. Kerberos was created by MIT as a solution to these network security problems. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server has used Kerberos to prove their identity, they can also encrypt (confidentiality) all of their communications to assure privacy and data integrity as they go about their business.

NEW QUESTION: 227
The European Union Electronic Signature Directive of January, 2000,
defines an advanced electronic signature. This signature must meet
all of the following requirements except that:
A. It must be created using means that are generally accessible and available.
B. It must be uniquely linked to the signatory.
C. It must be linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
D. It must be capable of identifying the signatory.
Answer: A (LEAVE A REPLY)
The Directive requires that the means be maintained under the sole control of the signatory. This requirement is a particularly difficult one to achieve. One approach is to use different tokens or smart cards for the different transactions involved. The other answers are typical characteristics of digital signatures that can be implemented with public key cryptography.

NEW QUESTION: 228
Theoretically, quantum computing offers the possibility of factoring the products of large prime numbers and calculating discreet logarithms in polynomial time. These calculations can be accomplished in such a

compressed time frame because:
A. A quantum computer takes advantage of quantum tunneling in molecular scale transistors. This mode permits ultra high-speed switching to take place, thus, exponentially increasing the speed of computations.
B. Information can be transformed into quantum light waves that travel through fiber optic channels. Computations can be performed on the associated data by passing the light waves through various types of optical filters and solid-state materials with varying indices of refraction, thus drastically increasing the throughput over conventional computations.
C. A quantum computer exploits the time-space relationship that changes as particles approach the speed of light. At that interface, the resistance of conducting materials effectively is zero and exponential speed computations are possible.
D. A quantum bit in a quantum computer is actually a linear superposition of both the one and zero states and, therefore, can theoretically represent both values in parallel. This phenomenon allows computation that usually takes exponential time to be accomplished in polynomial time since different values of the binary pattern of the solution can be calculated simultaneously.
Answer: D (LEAVE A REPLY)
In digital computers, a bit is in either a one or zero state. In a quantum computer, through linear superposition, a quantum bit can be in both states, essentially simultaneously. Thus, computations consisting of trail evaluations of binary patterns can take place simultaneously in exponential time. The probability of obtaining a correct result is increased through a phenomenon called constructive interference of light while the probability of obtaining an incorrect result is decreased through destructive interference. Answer a describes optical computing that is effective in applying Fourier and other transformations to data to perform high-speed computations. Light representing large volumes of data passing through properly shaped physical objects can be subjected to mathematical transformations and recombined to provide the appropriate results. However, this mode of computation is not defined as quantum computing. Answers c and d are diversionary answers that do not describe quantum computing.

NEW QUESTION: 229
Which of the following is a characteristic of the independent testing of a program?
A. Independent testing teams help identify functional requirements and Service Level Agreements (SLA)
B. Independent testing increases the likelihood that a test will expose the effect of a hidden feature.
C. Independent testing decreases the likelihood that a test will expose the effect of a hidden feature.
D. Independent testing teams help decrease the cost of creating test data and system design specification.
Answer: (SHOW ANSWER)

NEW QUESTION: 230
Which type of control is concerned with avoiding occurrences of risks?
A. Deterrent controls
B. Detective controls
C. Preventive controls
D. Compensating controls
Answer: C (LEAVE A REPLY)
Preventive controls are concerned with avoiding occurrences of risks while deterrent controls are concerned with discouraging violations. Detecting controls identify occurrences and compensating controls are alternative controls, used to compensate weaknesses in other controls. Supervision is an example of compensating control.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 231
Which of the following MUST be in place to recognize a system attack?
A. Passive honeypot
B. Stateful firewall
C. Log analysis
D. Distributed antivirus
Answer: B (LEAVE A REPLY)

NEW QUESTION: 232
An intranet provides more security and control than which of the following:
A. private posting on the Internet.
B. public posting on the Ethernet.
C. public posting on the Internet.
D. public posting on the Extranet.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A public posting on the internet is not secure. Compared to the internet, an intranet provides more control.
Incorrect Answers:
A: A private posting provides high security and control.
B: Ethernet is a link layer protocol in the TCP/IP stack. An Intranet is defined on the physical layer. The data link layer provides more control compared to the physical layer.
D: An extranet is a website that allows controlled access to partners, vendors and suppliers or an authorized set of customers - normally to a subset of the information accessible from an organization's intranet. As an extranet is a subset of an intranet is provides more security and control.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 661

NEW QUESTION: 233
The recommended optimal relative humidity range for computer operations is:
A. 40% to 60%
B. 10% to 30%
C. 30% to 40%
D. 60% to 80%
Answer: A (LEAVE A REPLY)
The correct answer is C. 40% to 60% relative humidity is recommended
for safe computer operations. Too low humidity can create
static discharge problems, and too high humidity can create condensation and electrical contact problems.

NEW QUESTION: 234
ICMP and IGMP belong to which layer of the OSI model?
A. Datagram Layer.
B. Network Layer.
C. Transport Layer.
D. Data Link Layer.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
ICMP and IGMP work at the network layer of the OSI model.
Incorrect Answers:
A: There is no Datagram Layer in the OSI model.
C: ICMP and IGMP do not belong to the Transport layer of the OSI model. TCP and UDP are examples of protocols working at the transport layer.
D: ICMP and IGMP do not belong to the Transport layer of the OSI model. ARP, OSOF, and MAC are examples of protocols workings at the data link layer.
References:
https://en.wikipedia.org/wiki/Network_layer

NEW QUESTION: 235
What is the proper term to refer to a single unit of IP data?
A. IP segment.
B. IP datagram.
C. IP frame.
D. IP fragment.
Answer: B (LEAVE A REPLY)
IP is a datagram based technology.
DIFFERENCE BETWEEN PACKETS AND DATAGRAM
As specified at: http://en.wikipedia.org/wiki/Packet_(information_technology)

In general, the term packet applies to any message formatted as a packet, while the term datagram is generally reserved for packets of an "unreliable" service.
A "reliable" service is one that notifies the user if delivery fails, while an "unreliable" one does not notify the user if delivery fails. For example, IP provides an unreliable service.
Together, TCP and IP provide a reliable service, whereas UDP and IP provide an unreliable one.
All these protocols use packets, but UDP packets are generally called datagrams.
If a network does not guarantee packet delivery, then it becomes the host's responsibility to provide reliability by detecting and retransmitting lost packets. Subsequent experience on the ARPANET indicated that the network itself could not reliably detect all packet delivery failures, and this pushed responsibility for error detection onto the sending host in any case. This led to the development of the end-to-end principle, which is one of the Internet's fundamental design assumptions.
The following answers are incorrect:
IP segment. Is incorrect because IP segment is a detractor, the correct terminology is TCP segment. IP is a datagram based technology.
IP frame. Is incorrect because IP frame is a detractor, the correct terminology is Ethernet frame. IP is a datagram based technology.
IP fragment. Is incorrect because IP fragment is a detractor.
References:
Wikipedia http://en.wikipedia.org/wiki/Internet_Protocol

NEW QUESTION: 236
A storage information architecture does not address which of the following?
A. collection of data
B. archiving of data
C. management of data
D. use of data
Answer: (SHOW ANSWER)

NEW QUESTION: 237
Which of the following needs to be taken into account when assessing vulnerability?
A. Risk identification and validation
B. Threat mapping
C. Risk acceptance criteria
D. Safeguard selection
Answer: A (LEAVE A REPLY)
Section: Mixed questions
Explanation/Reference: https://books.google.com.pk/books?id=9gCn86CmsNQC&pg=PA478&lpg=PA478&dq=CISSP+taken+into+account+when+assessing

+vulnerability&source=bl&ots=riGvVpNN7I&sig=ACfU3U1isazG0OJlZdAAy91LvAW_rbXdAQ&hl=en&sa=X&ved=2ahUKEwj6p9vg4qnpAhUNxYUKHdODDZ4Q6AEwDHoECBMQAQ#v=onepage&q=CISSP%20taken%20into%20account%20when%20assessing%20vulnerability&f=false

NEW QUESTION: 238

Which of the following is an extension to Network Address Translation that permits multiple devices providing services on a local area network (LAN) to be mapped to a single public IP address?

A. IP Spoofing

B. IP subnetting

C. Port address translation

D. IP Distribution

Answer: (SHOW ANSWER)

Port Address Translation (PAT), is an extension to network address translation (NAT) that permits multiple devices on a local area network (LAN) to be mapped to a single public IP address. The goal of PAT is to conserve IP addresses or to publish multiple hosts with service to the internet while having only one single IP assigned on the external side of your gateway. Most home networks use PAT. In such a scenario, the Internet Service Provider (ISP) assigns a single IP address to the home network's router. When Computer X logs on the Internet, the router assigns the client a port number, which is appended to the internal IP address. This, in effect, gives Computer X a unique address. If Computer Z logs on the Internet at the same time, the router assigns it the same local IP address with a different port number. Although both computers are sharing the same public IP address and accessing the Internet at the same time, the router knows exactly which computer to send specific packets to because each computer has a unique internal address.

Port Address Translation is also called porting, port overloading, port-level multiplexed NAT and single address NAT.

Shon Harris has the following example in her book:

The company owns and uses only one public IP address for all systems that need to communicate outside the internal network. How in the world could all computers use the exact same IP address? Good question. Here's an example: The NAT device has an IP address of 127.50.41.3. When computer A needs to communicate with a system on the Internet, the NAT device documents this computer's private address and source port number (10.10.44.3; port 43,887). The NAT device changes the IP address in the computer's packet header to 127.50.41.3, with the source port 40,000. When computer B also needs to communicate with a system on the Internet, the NAT device documents the private address and source port number (10.10.44.15; port 23,398) and changes the header information to 127.50.41.3 with source port 40,001. So when a system responds to computer A, the packet first goes to the NAT device, which looks up the port number 40,000 and sees that it maps to computer A's real information. So the NAT device changes the header information to address 10.10.44.3 and port 43,887 and sends it to computer A for processing. A company can save a lot more money by using PAT, because the company needs to buy only a few public IP addresses, which are used by all systems in the network.

As mentioned on Wikipedia:
NAT is also known as Port Address Translation: is a feature of a network device that translate TCP or UDP communications made between host on a private network and host on a public network. I allows a single public IP address to be used by many host on private network which is usually a local area network LAN
NAT effectively hides all TCP/IP-level information about internal hosts from the Internet.
The following were all incorrect answer:
IP Spoofing - In computer networking, the term IP address spoofing or IP spoofing refers to the creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing, with the purpose of concealing the identity of the sender or impersonating another computing system.
Subnetting - Subnetting is a network design strategy that segregates a larger network into smaller components. While connected through the larger network, each subnetwork or subnet functions with a unique IP address. All systems that are assigned to a particular subnet will share values that are common for both the subnet and for the network as a whole.
A different approach to network construction can be thought of as subnetting in reverse. Known as CIDR, or Classless Inter-Domain Routing, this approach also creates a series of subnetworks. Rather than dividing an existing network into small components, CIDR takes smaller components and connects them into a larger network. This can often be the case when a business is acquired by a larger corporation. Instead of doing away with the network developed and used by the newly acquired business, the corporation chooses to continue operating that network as a subsidiary or an added component of the corporation's network. In effect, the system of the purchased entity becomes a subnet of the parent company's network.
IP Distribution - This is a generic term which could mean distribution of content over an IP network or distribution of IP addresses within a Company. Sometimes people will refer to this as Internet Protocol address management (IPAM) is a means of planning, tracking, and managing the Internet Protocol address space used in a network. Most commonly, tools such as DNS and DHCP are used in conjunction as integral functions of the IP address management function, and true IPAM glues these point services together so that each is aware of changes in the other (for instance DNS knowing of the IP address taken by a client via DHCP, and updating itself accordingly). Additional functionality, such as controlling reservations in DHCP as well as other data aggregation and reporting capability, is also common. IPAM tools are increasingly important as new IPv6 networks are deployed with larger address pools, different subnetting techniques, and more complex 128-bit hexadecimal numbers which are not as easily human-readable as IPv4 addresses.
Reference(s) used for this question:
STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 1: Understanding Firewalls.
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Telecommunications and Network Security, Page 350.
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 12765-12774). Telecommunications and Network Security, Page 604-606

http://searchnetworking.techtarget.com/definition/Port-Address-Translation-PAT
http://en.wikipedia.org/wiki/IP_address_spoofing
http://www.wisegeek.com/what-is-subnetting.htm
http://en.wikipedia.org/wiki/IP_address_management

NEW QUESTION: 239
A system is developed so that its business users can perform business functions but not user administration functions. Application administrators can perform administration functions but not user business functions. These capabilities are BEST described as
A. rule based access controls.
B. least privilege.
C. Mandatory Access Control (MAC).
D. separation of duties.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 240
Which answer BEST describes information access permissions where, unless the user is specifically given access to certain data they are denied any access by default?
A. Implicit Deny
B. Explicit Deny
C. Implied Permissions
D. Explicit Permit
Answer: A (LEAVE A REPLY)
Discussion: Implicit Deny is a method of controlling access to data by denying access to ALL data then granting only to what the user needs to do their jobs.
The converse being Explicit Deny where you only deny access for users for a smaller set of data and permit access to all other data. (Worst practice)
Similar to the term of least privilege where users are only given access to data the must have in order to carry out their job duties, Implicit Deny principle denies by default access to information.
More simply put, access to ALL data is denied by default and only necessary access is given to data so they employee can carry out their job duties.
This term is common to firewalls or other filtering devices where, unless traffic is specifically permitted it is denied by default to enhance security.
The following answers are incorrect:
- Explicit Deny: Sorry, this is incorrect. Explicit Deny means users are given access to ALL data and only denied to a smaller subset of data. This a dangerous practice for information security.
- Implied Permissions: Sorry, incorrect answer. This isn't a commonly used term in risk reduction methodology.
- Explicit Permit: Sorry, also incorrect. Explicit means users are specifically given access but isn't used normally with the permit rule.
The following reference(s) was used to create this question:

2013. Official Security+ Curriculum.

NEW QUESTION: 241
Who should measure the effectiveness of Information System security related controls in an organization?
A. The local security specialist
B. The business manager
C. The systems auditor
D. The central security manager
Answer: C (LEAVE A REPLY)
It is the systems auditor that should lead the effort to ensure that the security controls are in place and effective. The audit would verify that the controls comply with polices, procedures, laws, and regulations where applicable. The findings would provide these to senior management.
The following answers are incorrect: the local security specialist. Is incorrect because an independent review should take place by a third party. The security specialist might offer mitigation strategies but it is the auditor that would ensure the effectiveness of the controls the business manager. Is incorrect because the business manager would be responsible that the controls are in place, but it is the auditor that would ensure the effectiveness of the controls the central security manager. Is incorrect because the central security manager would be responsible for implementing the controls, but it is the auditor that is responsibe for ensuring their effectiveness.

NEW QUESTION: 242
Which of the following would best describe a Concealment cipher?
A. Permutation is used, meaning that letters are scrambled.
B. Every X number of words within a text, is a part of the real message.
C. Replaces bits, characters, or blocks of characters with different bits, characters or blocks.
D. Hiding data in another message so that the very existence of the data is concealed.
Answer: B (LEAVE A REPLY)
When a concealment cipher is used, every X number of words within a text, is a part of the real message. The message is within another message.
A concealment cipher is a message within a message. If my other super-secret spy buddy and I decide our key value is every third word, then when I get a message from him, I will pick out every third word and write it down. Suppose he sends me a message that reads, "The saying, 'The time is right' is not cow language, so is now a dead subject." Because my key is every third word, I

come up with "The right cow is dead." This again means nothing to me, and I am now turning in my decoder ring.
Concealment ciphers include the plaintext within the ciphertext. It is up to the recipient to know which letters or symbols to exclude from the ciphertext in order to yield the plaintext. Here is an example of a concealment cipher:
i2l32i5321k34e1245ch456oc12ol234at567e
Remove all the numbers, and you'll have i like chocolate. How about this one?
Larry even appears very excited. No one worries.
The first letter from each word reveals the message leave now. Both are easy, indeed, but many people have crafted more ingenious ways of concealing the messages. By the way, this type of cipher doesn't even need ciphertext, such as that in the above examples.
Consider the invisible drying ink that kids use to send secret messages. In a more extreme example, a man named Histiaeus, during 5th century B.C., shaved the head of a trusted slave, then tattooed the message onto his bald head. When the slave's hair grew back, Histiaeus sent the slave to the message's intended recipient, Aristagoros, who shaved the slave's head and read the message instructing him to revolt.
The following answers are incorrect:
A transposition cipher uses permutations.
A substitution cipher replaces bits, characters, or blocks of characters with different bits, characters or blocks.
Steganography refers to hiding the very existence of the message.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 1).
and also see:
http://www.go4expert.com/forums/showthread.php?t=415

NEW QUESTION: 243
Which of the following is mobile device remote fingerprinting?
A. Identifying a device based on common characteristics shared by all devices of a certain type
B. Storing information about a remote device in a cookie file
C. Retrieving the serial number of the mobile device
D. Installing an application to retrieve common characteristics of the device
Answer: A (LEAVE A REPLY)

NEW QUESTION: 244
Which of the following violates identity and access management best practices?
A. Privileged accounts
B. System accounts
C. Generic accounts
D. User accounts
Answer: C (LEAVE A REPLY)

NEW QUESTION: 245
Which of the following can best be defined as a key distribution protocol that uses hybrid encryption to convey session keys. This protocol establishes a long-term key once, and then requires no prior communication in order to establish or exchange keys on a session-by-session basis?
A. Internet Security Association and Key Management Protocol (ISAKMP)
B. Simple Key-management for Internet Protocols (SKIP)
C. Diffie-Hellman Key Distribution Protocol
D. IPsec Key exchange (IKE)
Answer: B (LEAVE A REPLY)
RFC 2828 (Internet Security Glossary) defines Simple Key Management for Internet Protocols (SKIP) as:
A key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.
SKIP is an hybrid Key distribution protocol similar to SSL, except that it establishes a long-term key once, and then requires no prior communication in order to establish or exchange keys on a session-by-session basis. Therefore, no connection setup overhead exists and new keys values are not continually generated. SKIP uses the knowledge of its own secret key or private component and the destination's public component to calculate a unique key that can only be used between them.
IKE stand for Internet Key Exchange, it makes use of ISAKMP and OAKLEY internally.
Internet Key Exchange (IKE or IKEv2) is the protocol used to set up a security association (SA) in the IPsec protocol suite. IKE builds upon the Oakley protocol and ISAKMP. IKE uses X.509 certificates for authentication and a Diffie-Hellman key exchange to set up a shared session secret from which cryptographic keys are derived.
The following are incorrect answers:
ISAKMP is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism.
IKE is an Internet, IPsec, key-establishment protocol (partly based on OAKLEY) that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations, such as in AH and ESP.
IPsec Key exchange (IKE) is only a detracto.
Reference(s) used for this question:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
and
http://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol
and
http://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol

NEW QUESTION: 246

Theoretically, quantum computing offers the possibility of factoring the products of large prime numbers and calculating discreet logarithms in polynomial time. These calculations can be accomplished in such a compressed time frame because:

A. A quantum computer takes advantage of quantum tunneling in molecular scale transistors. This mode permits ultra high-speed switching to take place, thus, exponentially increasing the speed of computations.

B. Information can be transformed into quantum light waves that travel through fiber optic channels. Computations can be performed on the associated data by passing the light waves through various types of optical filters and solid-state materials with varying indices of refraction, thus drastically increasing the throughput over conventional computations.

C. A quantum computer exploits the time-space relationship that changes as particles approach the speed of light. At that interface, the resistance of conducting materials effectively is zero and exponential speed computations are possible.

D. A quantum bit in a quantum computer is actually a linear superposition of both the one and zero states and, therefore, can theoretically represent both values in parallel. This phenomenon allows computation that usually takes exponential time to be accomplished in polynomial time since different values of the binary pattern of the solution can be calculated simultaneously.

Answer: D (LEAVE A REPLY)

In digital computers, a bit is in either a one or zero state. In a quantum computer, through linear superposition, a quantum bit can be in both states, essentially simultaneously. Thus, computations consisting of trail evaluations of binary patterns can take place simultaneously in exponential time. The probability of obtaining a correct result is increased through a phenomenon called constructive interference of light while the probability of obtaining an incorrect result is decreased through destructive interference. Answer a describes optical computing that is effective in applying Fourier and other transformations to data to perform high-speed computations. Light representing large volumes of data passing through properly shaped physical objects can be subjected to mathematical transformations and recombined to provide the appropriate results. However, this mode of computation is not defined as quantum computing. Answers c and d are diversionary answers that do not describe quantum computing.

NEW QUESTION: 247

A large bank deploys hardware tokens to all customers that use their online banking system. The token generates and displays a six digit numeric password every 60 seconds. The customers must log into their bank accounts using this numeric password. This is an example of

A. Single Sign-On (SSO) token.

B. asynchronous token.

C. single factor authentication token.
D. synchronous token.
Answer: (SHOW ANSWER)

NEW QUESTION: 248
Which of the following services is NOT provided by the digital signature standard (DSS)?
A. Encryption
B. Integrity
C. Digital signature
D. Authentication
Answer: A (LEAVE A REPLY)
DSS provides Integrity, digital signature and Authentication, but does not provide Encryption.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 160).

NEW QUESTION: 249
Which of the following is true about Kerberos?
A. It utilizes public key cryptography.
B. It encrypts data after a ticket is granted, but passwords are exchanged in plain text.
C. It depends upon symmetric ciphers.
D. It is a second party authentication system.
Answer: C (LEAVE A REPLY)
Kerberos depends on secret keys (symmetric ciphers). Kerberos is a third party authentication protocol. It was designed and developed in the mid 1980's by MIT. It is considered open source but is copyrighted and owned by MIT. It relies on the user's secret keys. The password is used to encrypt and decrypt the keys.
The following answers are incorrect:
It utilizes public key cryptography. Is incorrect because Kerberos depends on secret keys (symmetric ciphers).
It encrypts data after a ticket is granted, but passwords are exchanged in plain text. Is incorrect because the passwords are not exchanged but used for encryption and decryption of the keys.
It is a second party authentication system. Is incorrect because Kerberos is a third party authentication system, you authenticate to the third party (Kerberos) and not the system you are accessing.
References:
MIT http://web.mit.edu/kerberos/
Wikipedi http://en.wikipedia.org/wiki/Kerberos_%28protocol%29
OIG CBK Access Control (pages 181 - 184)
AIOv3 Access Control (pages 151 - 155)

NEW QUESTION: 250
In Operations Security trusted paths provide:

A. trustworthy integration into integrity functions.
B. trusted access to unsecure paths.
C. trustworthy interfaces into priviledged user functions.
D. trustworthy interfaces into priviledged MTBF functions.
Answer: (SHOW ANSWER)
The following answers are incorrect:
Integrity paths has no meaning in the context of this question. Trusted paths brings to mind the word integrity only in the context that the data was not changed and is in it's orginal condition. This question also has less to do with integration and more to do with actual implementation of a concept.
There is less need to create trusted paths to something that is already not secure.
MTBF is Mean Time Between Failure. This is not really related to a trusted path therefore not related to this question.
The following reference(s) were/was used to create this question:
"Trusted paths provide trustworthy interfaces into privledged user functions and are intended to provide a way to ensure that any communications over that path cannot be intercepted or corrupted."
pp. 544 Official Guide to the CISSP CBK, Second Edition, copyright 2010, Edited by Harold F. Tipton, Trusted Paths and Fail Secure Mechanisms;

NEW QUESTION: 251
Which of the following is the FIRST action that a system administrator should take when it is revealed during a penetration test that everyone in an organization has unauthorized access to a server holding sensitive data?
A. Immediately document the finding and report to senior management.
B. Terminate the penetration test and pass the finding to the server management team
C. Continue the testing to its completion and then inform IT management
D. Use system privileges to alter the permissions to secure the server
Answer: A (LEAVE A REPLY)

NEW QUESTION: 252
According to FEMA, which choice below is NOT a recommended way
to purify water after a disaster?
A. Distilling the water for twenty minutes
B. Adding 16 drops per gallon of household liquid bleach to the water
C. Adding water treatment tablets to the water
D. Boiling from 3 to 5 minutes
Answer: (SHOW ANSWER)
FEMArecommends that water treatment products sold in camping or surplus stores should not be used, unless the only active ingredient is 5.25 percent hypochloritE. When adding liquid bleach, it should contain 5.25 percent hypochlorite and no other added cleaners or scents. Distilling the water is the most highly

recommended method, as it also removes other chemicals and heavy metals, as well as most microbes.
Source: Emergency Water and Food Procedures, Federal Emergency Management Agency, April, 1997.

NEW QUESTION: 253
Which of the following is an advantage of a qualitative over a quantitative risk analysis?
A. It prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.
B. It provides specific quantifiable measurements of the magnitude of the impacts.
C. It makes a cost-benefit analysis of recommended controls easier.
D. It can easily be automated.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Qualitative risk assessments quantify the level of risk whereas quantitative risk assessments place a monetary value on the effect of risk. For example, a qualitative risk assessment may use a scale such as low risk, medium risk and high risk or a 1 to 10 scale.
One risk assessment methodology is called FRAP, which stands for Facilitated Risk Analysis Process. The crux of this qualitative methodology is to focus only on the systems that really need assessing to reduce costs and time obligations. It stresses prescreening activities so that the risk assessment steps are only carried out on the item(s) that needs it the most. It is to be used to analyze one system, application, or business process at a time. Data is gathered and threats to business operations are prioritized based upon their criticality. The risk assessment team documents the controls that need to be put into place to reduce the identified risks along with action plans for control implementation efforts.
Incorrect Answers:
B: Quantitative, not qualitative risk assessments provide specific quantifiable measurements of the magnitude of the impacts.
C: Quantitative, not qualitative risk assessments make a cost-benefit analysis of recommended controls easier.
D: Quantitative, not qualitative risk assessments can easily be automated or at least partially automated.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 79

NEW QUESTION: 254
What should be the FIRST action for a security administrator who detects an intrusion on the network based on precursors and other indicators?
A. Notify system and application owners.
B. Isolate and contain the intrusion.
C. Apply patches to the Operating Systems (OS).
D. Document and verify the intrusion.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 255

For maximum security design, what type of fence is most effective and cost-effective method (Foot are being used as measurement unit below)?

A. 3' to 4' high.

B. 6' to 7' high.

C. 8' high and above with strands of barbed wire.

D. Double fencing

Answer: D (LEAVE A REPLY)

The most commonly used fence is the chain linked fence and it is the most affordable. The standard is a six-foot high fence with two-inch mesh square openings. The material should consist of nine-gauge vinyl or galvanized metal. Nine-gauge is a typical fence material installed in residential areas.

Additionally, it is recommended to place barbed wire strands angled out from the top of the fence at a 45(o) angle and away from the protected area with three strands running across the top. This will provide for a seven-foot fence. There are several variations of the use of "top guards" using V-shaped barbed wire or the use of concertina wire as an enhancement, which has been a replacement for more traditional three strand barbed wire "top guards."

The fence should be fastened to ridged metal posts set in concrete every six feet with additional bracing at the corners and gate openings. The bottom of the fence should be stabilized against intruders crawling under by attaching posts along the bottom to keep the fence from being pushed or pulled up from the bottom. If the soil is sandy, the bottom edge of the fence should be installed below ground level.

For maximum security design, the use of double fencing with rolls of concertina wire positioned between the two fences is the most effective deterrent and cost-efficient method. In this design, an intruder is required to use an extensive array of ladders and equipment to breach the fences.

Most fencing is largely a psychological deterrent and a boundary marker rather than a barrier, because in most cases such fences can be rather easily penetrated unless added security measures are taken to enhance the security of the fence. Sensors attached to the fence to provide electronic monitoring of cutting or scaling the fence can be used.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 24416-24431). Auerbach Publications. Kindle Edition.

NEW QUESTION: 256

Which type of risk assessment is the formula ALE = ARO x SLE used for?

A. Quantitative Analysis

B. Qualitative Analysis

C. Objective Analysis

D. Expected Loss Analysis

Answer: A (LEAVE A REPLY)

The formula ALE = ARO x SLE involves numerical values or quantities of a given resource or occurrence so it is thus a quantitative analysis.

ALE = Annual Lose expectancy or how much it might cost per year if you were to lose the asset

ARO = Annual Rate of Occurrence or how often the loss might occur.
SLE = Single Loss Expectancy or how much each incident of loss would cost the organization.
Using these values you can determine how much you should spend to secure the resources against loss.
It is useful to use these costs when we compare them to the value of the asset for which we are responsible.
It wouldn't be sensible to spend $10,000 USD a year for an asset you could replace for
$2,000 USD.
The following answers are incorrect:
- Qualitative Analysis: This is part of the risk analysis process where interviews are conducted with employees to determine risk and where focus should be made for protecting assets. Many analysts combine Quantitative and Qualitative risk assessments to form an effective picture of where dollars should be spent to secure critical resources for the organization. It is not a correct answer because it does not use a mathematical formula to determine a hard value.
- Objective Analysis: This is not a commonly used term to describe an approach to risk analysis but an objective approach could be likened more to a quantitative analysis where specific values are determined in the risk analysis process.
- Expected Loss Analysis: This is also not a common term in risk analysis but it could describe the concept of analysis an expected loss due to a threat for which you must plan.
The following reference(s) was used to create this question:
Gregg, Michael; Haines, Billy (2012-02-16). CASP: CompTIA Advanced Security
Practitioner Study Guide Authorized Courseware: Exam CAS-001 (p. 215). Wiley. Kindle
Edition.

NEW QUESTION: 257
The privacy provisions of the federal law, the Health Insurance Portability and Accountability Act of 1996 (HIPAA),
A. apply to health information created or maintained by some large health care providers who engage in certain electronic transactions, health plans, and health care clearinghouses.
B. apply to health information created or maintained by health care providers who engage in certain electronic transactions, health plans, and health care clearinghouses.
C. apply to health information created or maintained by health care providers regardless of whether they engage in certain electronic transactions, health plans, and health care clearinghouses.
D. apply to certain types of critical health information created or maintained by health care providers who engage in certain electronic transactions, health plans, and health care clearinghouses.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 258
Which of the following encryption methods is known to be unbreakable?
A. Symmetric ciphers.
B. DES codebooks.
C. One-time pads.
D. Elliptic Curve Cryptography.
Answer: C (LEAVE A REPLY)
A One-Time Pad uses a keystream string of bits that is generated completely at random that is used only once. Because it is used only once it is considered unbreakable.
The following answers are incorrect:
Symmetric ciphers. This is incorrect because a Symmetric Cipher is created by substitution and transposition. They can and have been broken
DES codebooks. This is incorrect because Data Encryption Standard (DES) has been broken, it was replaced by Advanced Encryption Standard (AES).
Elliptic Curve Cryptography. This is incorrect because Elliptic Curve Cryptography or ECC is typically used on wireless devices such as cellular phones that have small processors.
Because of the lack of processing power the keys used at often small. The smaller the key, the easier it is considered to be breakable. Also, the technology has not been around long enough or tested thourough enough to be considered truly unbreakable.

NEW QUESTION: 259
Which of the following attributes could be used to describe a protection mechanism of an open design methodology?
A. It can facilitate blackbox penetration testing.
B. It exposes the design to vulnerabilities and malicious attacks.
C. It can facilitate independent confirmation of the design security.
D. It must be tamperproof to protect it from malicious attacks.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 260
Which of the following attack is MOSTLY performed by an attacker to steal the identity information of a user such as credit card number, passwords,etc?
A. Smurf attack
B. Traffic analysis
C. Pharming
D. Interrupt attack
Answer: C (LEAVE A REPLY)
Pharming is a cyber attack intended to redirect a website's traffic to another, bogus site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS

server software. DNS servers are computers responsible for resolving Internet names into their real IP addresses. Compromised DNS servers are sometimes referred to as "poisoned". Pharming requires unprotected access to target a computer, such as altering a customer's home computer, rather than a corporate business server.

The term "pharming" is a neologism based on the words "farming" and "phishing". Phishing is a type of social-engineering attack to obtain access credentials, such as user names and passwords. In recent years, both pharming and phishing have been used to gain information for online identity theft. Pharming has become of major concern to businesses hosting ecommerce and online banking websites. Sophisticated measures known as anti-pharming are required to protect against this serious threat. Antivirus software and spyware removal software cannot protect against pharming.

For your exam you should know the information below: Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. Spear phishing - Phishing attempts directed at specific individuals or companies have been termed spearphishing.Attackers may gather personal information about their target to increase their probability of success.

Link manipulation Most methods of phishing use some form of technical deception designed to make a link in an email (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of subdomains are common tricks used by phishers. In the following example URL, http://www.yourbank.example.com/, it appears as though the URL will take you to the example section of the yourbank website; actually this URL points to the "yourbank" (i.e. phishing) section of the example website. Another common trick is to make the displayed text for a link (the text between the ahref tags) suggest a reliable destination, when the link actually goes to the phishers' site. The following example link, //en.wikipedia.org/wiki/Genuine, appears to direct the user to an article entitled "Genuine"; clicking on it will in fact take the user to the article entitled "Deception". In the lower left hand corner of most browsers users can preview and verify where the link is going to take them. Hovering your cursor over the link for a couple of seconds may do a similar thing, but this can still be set by the phisher through the HTML tooltip tag. Website forgery Once a victim visits the phishing website, the deception is not over. Some phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original bar and opening up a new one with the legitimate URL.

An attacker can even use flaws in a trusted website's own scripts against the victim.These types of attacks (known as cross-site scripting) are particularly problematic, because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears

correct. In reality, the link to the website is crafted to carry out the attack, making it very difficult to spot without specialist knowledge.
The following answers are incorrect: Smurf Attack - Occurs when mis-configured network device allow packet to be sent to all hosts on a particular network via the broadcast address of the network
Traffic analysis - is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence, counter-intelligence, or pattern-of-life analysis, and is a concern in computer security. Interrupt attack - Interrupt attack occurs when a malicious action is performed by invoking the operating system to execute a particular system call.
Following reference(s) were/was used to create this question: CISA review manual 2014 Page number 323 Official ISC2 guide to CISSP CBK 3rd Edition Page number326 http://en.wikipedia.org/wiki/Phishing http://en.wikipedia.org/wiki/Pharming

NEW QUESTION: 261
Clipping levels are used to:
A. Reduce the amount of data to be evaluated in audit logs.
B. Limit errors in callback systems.
C. Limit the number of letters in a password.
D. Set thresholds for voltage variations.
Answer: (SHOW ANSWER)
The correct answer is reducing the amount of data to be evaluated
by definition. Answer "Limit the number of letters in a password" is incorrect because clipping levels do not relate to letters in a password.
Answer "Set thresholds for voltage variations" is incorrect because clipping levels in this context have nothing to do with controlling voltage levels. Answer "Limit errors in callback syste" is incorrect because they are not used to limit callback errors.

NEW QUESTION: 262
Which of the following is often the greatest challenge of distributed computing solutions?
A. scalability
B. security
C. heterogeneity
D. usability
Answer: (SHOW ANSWER)
The correct answer to this "security". It is a major factor in deciding if a centralized or decentralized environment is more appropriate.
Example: In a centralized computing environment, you have a central server and workstations (often "dumb terminals") access applications, data, and everything else from that central servers. Therefore, the vast

majority of your security resides on a centrally managed server. In a decentralized (or distributed) environment, you have a collection of
PC's each with their own operating systems to maintain, their own software to maintain, local data storage requiring protection and backup. You may also have PDA's and "smart phones", data watches, USB devices of all types able to store data... the list gets longer all the time.
It is entirely possible to reach a reasonable and acceptable level of security in a distributed environment. But doing so is significantly more difficult, requiring more effort, more money, and more time.
The other answers are not correct because:
scalability - A distributed computing environment is almost infinitely scalable. Much more so than a centralized environment. This is therefore a bad answer.
heterogeneity - Having products and systems from multiple vendors in a distributed environment is significantly easier than in a centralized environment. This would not be a
"challenge of distributed computing solutions" and so is not a good answer.
usability - This is potentially a challenge in either environment, but whether or not this is a problem has very little to do with whether it is a centralized or distributed environment.
Therefore, this would not be a good answer.
Reference:
Official ISC2 Guide page: 313-314
All in One Third Edition page: (unavailable at this time)

NEW QUESTION: 263
Following the completion of a network security assessment, which of the following can
BEST be demonstrated?
A. The effectiveness of controls can be accurately measured
B. A penetration test of the network will fail
C. The network is compliant to industry standards
D. All unpatched vulnerabilities have been identified
Answer: A (LEAVE A REPLY)

NEW QUESTION: 264
Which of the following is NOT a true statement about Network Address
Translation (NAT)?
A. Private addresses can easily be routed globally.
B. NAT is used when corporations want to use private addressing
ranges for internal networks.
C. NAT is designed to mask the true IP addresses of internal systems.
D. NAT translates private IP addresses to registered real IP addresses.
Answer: A (LEAVE A REPLY)
The correct answer is "Private addresses can easily be routed globally" Private addresses are not easily routable; hence the reason for using NAT.

NEW QUESTION: 265
Which of the following testing method examines internal structure or working of an application?
A. White-box testing
B. Parallel Test
C. Regression Testing
D. Pilot Testing
Answer: A (LEAVE A REPLY)
Explanation/Reference:
White-box testing is a method of testing software that tests internal structures or workings of an application, versus its functionality. White-box testing allows access to program source code, data structures, variables, etc.
Incorrect Answers:
B: Parallel Testing is the process of entering the same inputs in two different versions of the application and reporting the anomalies.
C: Regression Testing is the process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors.
D: Pilot Testing is a preliminary test that focuses on specific and predefined aspect of a system.
References:
Conrad, Eric, Seth Misenar, Joshua Feldman, CISSP Study Guide, 2nd Edition, Syngress, Waltham, 2012, p. 194 Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 1105
https://en.wikipedia.org/wiki/White-box_testing
http://www.tutorialspoint.com/software_testing_dictionary/parallel_testing.htm
http://soft-engineering.blogspot.co.za/2010/12/what-is-difference-between-pilot-and.html

NEW QUESTION: 266
The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system is referred to as?
A. Confidentiality
B. Availability
C. Integrity
D. Reliability
Answer: B (LEAVE A REPLY)
An company security program must:
1) assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability;
2) protect informationcommensurate with the level of risk and magnitude ofharmresulting fromloss, misuse, unauthorized access, or modification.
The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them.
The following are incorrect answers:

Confidentiality - The information requires protection from unauthorized disclosure and only the INTENDED recipient should have access to the meaning of the data either in storage or in transit.
Integrity - The information must be protected from unauthorized, unanticipated, or unintentional modification. This includes, but is not limited to:
Authenticity -A third party must be able to verify that the content of a message has not been changed in transit.
Non-repudiation - The origin or the receipt of a specific message must be verifiable by a third party.
Accountability - A security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
Reference used for this question:
RFC 2828
and
SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (page 5).

NEW QUESTION: 267
A security practitioner has been tasked with establishing organizational asset handling procedures.
What should be considered that would have the GRFATEST impact to the development of these procedures?
A. Acceptable Use Policy (ALP)
B. User roles and responsibilities
C. Media handling procedures
D. Information classification scheme
Answer: (SHOW ANSWER)

NEW QUESTION: 268
When conducting a security assessment of access controls , Which activity is port of the data analysis phase?
A. Present solutions to address audit exceptions.
B. Collect logs and reports.
C. Conduct statiscal sampling of data transactions.
D. Categorize and Identify evidence gathered during the audit
Answer: D (LEAVE A REPLY)

NEW QUESTION: 269
Proxies works by transferring a copy of each accepted data packet from one network to another, thereby masking the:
A. data's payload.
B. data's details.
C. data's owner.
D. data's origin.
Answer: (SHOW ANSWER)

The application firewall (proxy) relays the traffic from a trusted host running a specific application to an untrusted server. It will appear to the untrusted server as if the request originated from the proxy server.
"Data's payload" is incorrect. Only the origin is changed.
"Data's details" is incorrect. Only the origin is changed.
"Data's owner" is incorrect. Only the origin is changed.
References:
CBK, p. 467
AIO3, pp. 486 - 490

NEW QUESTION: 270
What Access Control model was developed to deal mainly with information flow in computer systems?
A. Lattice Based
B. Integrity Based
C. Flow Based
D. Area Based
Answer: A (LEAVE A REPLY)
The Lattice Based Access Control model was developed to deal mainly with information flow in computer systems. Information flow is clearly central to confidentiality but to some extent it also applies to integrity. The basic work in this area was done around 1970 and was driven mostly by the defense sector. Information flow in computer systems is concerned with flow from one security class (also called security label) to another. These controls are applied to objects. An object is a container of information, and an object can be a directory or file.

NEW QUESTION: 271
How is an SLE derived?
A. ARO x EF
B. AV x EF
C. (Cost - benefit) x (% of Asset Value)
D. % of AV - implementation cost
Answer: (SHOW ANSWER)
The correct answer is AV x Ef. A Single Loss Expectancy is derived by multiplying the Asset Value with its Exposure Factor. The other answers do not exist.

NEW QUESTION: 272
Which of the following categories of hackers poses the greatest threat?
A. Disgruntled employees
B. Student hackers
C. Criminal hackers
D. Corporate spies
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Employee sabotage can become an issue if an employee is knowledgeable enough about the IT infrastructure of an organization, has sufficient access.
Incorrect Answers:
B: Student hackers are a lesser threat as a disgruntled employee already has access to the system.
C: A disgruntled employee is a larger threat compared to a criminal hacker as the employee already has access to the system.
D: A disgruntled employee is a larger threat compared to a corporate spy as the employee already has access to the system.
References:
Stewart, James M., Ed Tittel, and Mike Chapple, CISSP: Certified Information Systems Security Professional Study Guide, 5th Edition, Sybex, Indianapolis, 2011, p. 602

NEW QUESTION: 273
Which answer BEST describes information access permissions where, unless the user is specifically given access to certain data they are denied any access by default?
A. Implicit Deny
B. Explicit Deny
C. Implied Permissions
D. Explicit Permit
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Implicit Deny means that a user is denied access by default. To be given access, the user must (explicitly) be permitted access to the resource.
Incorrect Answers:
B: Explicit Deny means the user has been denied access to the data. It does not mean the user is denied by default.
C: Implied Permissions does not describe information access permissions where, unless the user is specifically given access to certain data they are denied any access by default.
D: Explicit Permit means that a user is specifically given access to the data. However, it does not mean that the user is denied by default.
References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 205

NEW QUESTION: 274
In biometric identification systems, at the beginning, it was soon apparent that truly positive identification could only be based on physical attributes of a person. This raised the necessicity of answering 2 questions:
A. What was the sex of a person and his age
B. what was the tone of the voice of a person and his habits
C. what part of body to be used and how to accomplish identification to be viable
D. what was the age of a person and his income level
Answer: C (LEAVE A REPLY)

NEW QUESTION: 275
The primary purpose for using one-way hashing of user passwords within a password file is which of the following?
A. It prevents an unauthorized person from trying multiple passwords in one logon attempt.
B. It prevents an unauthorized person from reading the password.
C. It minimizes the amount of storage required for user passwords.
D. It minimizes the amount of processing time used for encrypting passwords.
Answer: B (LEAVE A REPLY)
The whole idea behind a one-way hash is that it should be just that - one-way. In other words, an attacker should not be able to figure out your password from the hashed version of that password in any mathematically feasible way (or within any reasonable length of time).
Password Hashing and Encryption In most situations , if an attacker sniffs your password from the network wire, she still has some work to do before she actually knows your password value because most systems hash the password with a hashing algorithm, commonly MD4 or MD5, to ensure passwords are not sent in cleartext.
Although some people think the world is run by Microsoft, other types of operating systems are out there, such as Unix and Linux. These systems do not use registries and SAM databases, but contain their user passwords in a file cleverly called "shadow." Now, this shadow file does not contain passwords in cleartext; instead, your password is run through a hashing algorithm, and the resulting value is stored in this file. Unixtype systems zest things up by using salts in this process. Salts are random values added to the encryption process to add more complexity and randomness. The more randomness entered into the encryption process, the harder it is for the bad guy to decrypt and uncover your password. The use of a salt means that the same password can be encrypted into several thousand different formats. This makes it much more difficult for an attacker to uncover the right format for your system.
Password Cracking tools Note that the use of one-way hashes for passwords does not prevent password crackers from guessing passwords. A password cracker runs a plain-text string through the same one-way hash algorithm used by the system to generate a hash, then compares that generated has with the one stored on the system. If they match, the password cracker has guessed your password.

This is very much the same process used to authenticate you to a system via a password. When you type your username and password, the system hashes the password you typed and compares that generated hash against the one stored on the system - if they match, you are authenticated.

Pre-Computed password tables exists today and they allow you to crack passwords on Lan Manager (LM) within a VERY short period of time through the use of Rainbow Tables. A Rainbow Table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a plaintext password up to a certain length consisting of a limited set of characters. It is a practical example of a space/time trade-off

also called a Time-Memory trade off, using more computer processing time at the cost of less storage when calculating a hash on every attempt, or less processing time and more storage when compared to a simple lookup table with one entry per hash. Use of a key derivation function that employs a salt makes this attack unfeasible.

You may want to review "Rainbow Tables" at the links:

http://en.wikipedia.org/wiki/Rainbow_table

http://www.antsight.com/zsl/rainbowcrack/

Today's password crackers:

Meet oclHashcat. They are GPGPU-based multi-hash cracker using a brute-force attack (implemented as mask attack), combinator attack, dictionary attack, hybrid attack, mask attack, and rule-based attack.

This GPU cracker is a fusioned version of oclHashcat-plus and oclHashcat-lite, both very well-known suites at that time, but now deprecated. There also existed a now very old oclHashcat GPU cracker that was replaced w/ plus and lite, which - as said - were then merged into oclHashcat 1.00 again.

This cracker can crack Hashes of NTLM Version 2 up to 8 characters in less than a few hours. It is definitively a game changer. It can try hundreds of billions of tries per seconds on a very large cluster of GPU's. It supports up to 128 Video Cards at once.

I am stuck using Password what can I do to better protect myself?

You could look at safer alternative such as Bcrypt, PBKDF2, and Scrypt.

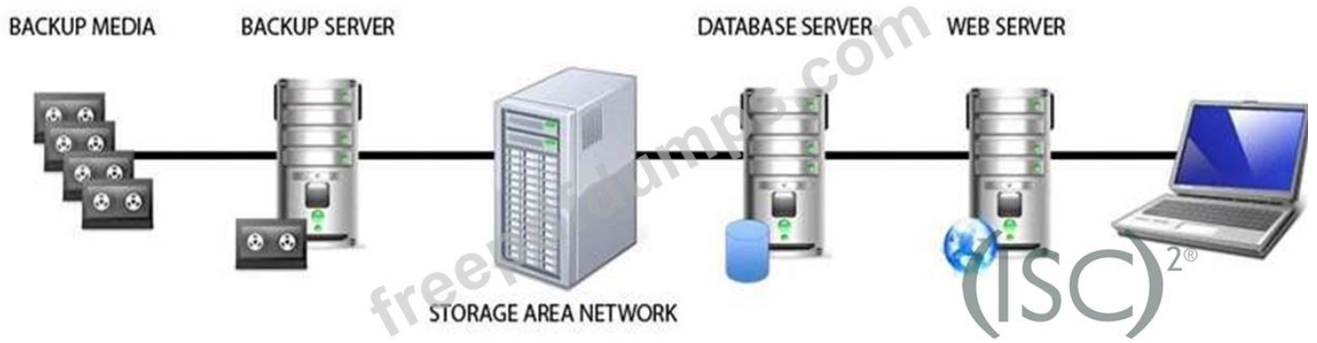
bcrypt is a key derivation function for passwords designed by Niels Provos and David Mazieres, based on the Blowfish cipher, and presented at USENIX in 1999. Besides incorporating a salt to protect against rainbow table attacks, bcrypt is an adaptive function: over time, the iteration count can be increased to make it slower, so it remains resistant to brute-force search attacks even with increasing computation power.

In cryptography, scrypt is a password-based key derivation function created by Colin Percival, originally for the Tarsnap online backup service. The algorithm was specifically designed to make it costly to perform large-scale custom hardware attacks by requiring large amounts of memory. In 2012, the scrypt algorithm was published by the IETF as an Internet Draft, intended to become an informational RFC, which has since expired. A simplified version of scrypt is used as a proof-of-work scheme by a number of cryptocurrencies, such as Litecoin and Dogecoin.

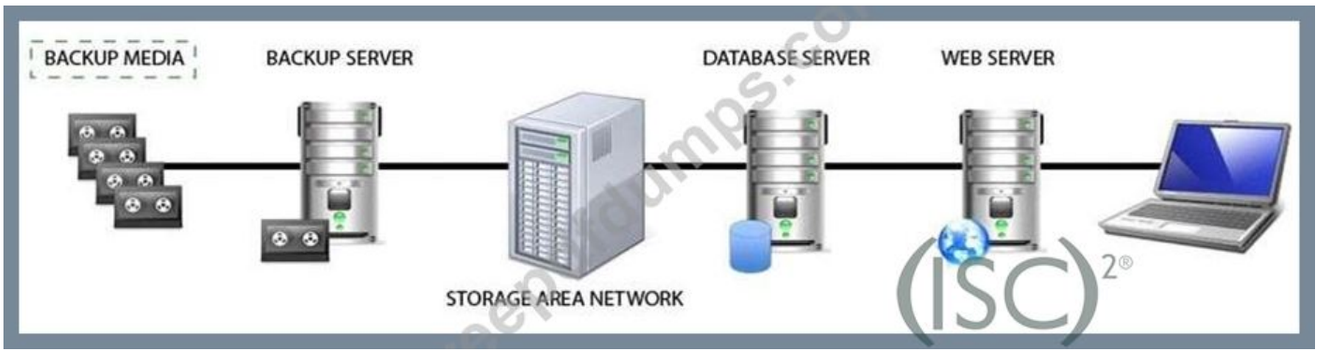
PBKDF2 (Password-Based Key Derivation Function 2) is a key derivation function that is part of RSA Laboratories' Public-Key Cryptography Standards (PKCS) series, specifically PKCS #5 v2.0,

also published as Internet Engineering Task Force's RFC 2898. It replaces an earlier standard, PBKDF1, which could only produce derived keys up to 160 bits long.
PBKDF2 applies a pseudorandom function, such as a cryptographic hash, cipher, or HMAC to the input password or passphrase along with a salt value and repeats the process many times to produce a derived key, which can then be used as a cryptographic key in subsequent operations. The added computational work makes password cracking much more difficult, and is known as key stretching. When the standard was written in 2000, the recommended minimum number of iterations was 1000, but the parameter is intended to be increased over time as CPU speeds increase. Having a salt added to the password reduces the ability to use precomputed hashes (rainbow tables) for attacks, and means that multiple passwords have to be tested individually, not all at once. The standard recommends a salt length of at least 64 bits.
The other answers are incorrect:
"It prevents an unauthorized person from trying multiple passwords in one logon attempt." is incorrect because the fact that a password has been hashed does not prevent this type of brute force password guessing attempt.
"It minimizes the amount of storage required for user passwords" is incorrect because hash algorithms always generate the same number of bits, regardless of the length of the input. Therefore, even short passwords will still result in a longer hash and not minimize storage requirements.
"It minimizes the amount of processing time used for encrypting passwords" is incorrect because the processing time to encrypt a password would be basically the same required to produce a one-way has of the same password.
Reference(s) used for this question:
http://en.wikipedia.org/wiki/PBKDF2
http://en.wikipedia.org/wiki/Scrypt
http://en.wikipedia.org/wiki/Bcrypt
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 195) . McGraw-Hill. Kindle Edition.

NEW QUESTION: 276
Identify the component that MOST likely lacks digital accountability related to information access.
Click on the correct device in the image below.



Answer:



Explanation
Backup Media
Reference: Official (ISC)2 Guide to the CISSP CBK, Third Edition page 1029

NEW QUESTION: 277
Which of the following can best be defined as a cryptanalysis technique in which the analyst tries to determine the key from knowledge of some plaintext-ciphertext pairs?
A. A known-plaintext attack
B. A known-algorithm attack
C. A chosen-ciphertext attack
D. A chosen-plaintext attack
Answer: A (LEAVE A REPLY)
RFC2828 (Internet Security Glossary) defines a known-plaintext attack as a cryptanalysis technique in which the analyst tries to determine the key from knowledge of some plaintext-ciphertext pairs (although the analyst may also have other clues, such as the knowing the cryptographic algorithm). A chosen-ciphertext attack is defined as a cryptanalysis technique in which the analyst tries to determine the key from knowledge of plaintext that corresponds to ciphertext selected (i.e., dictated) by the analyst. A chosen- plaintext attack is a cryptanalysis technique in which the analyst tries to determine the key from knowledge of ciphertext that corresponds to plaintext selected (i.e., dictated) by the analyst. The other choice is a distracter.
The following are incorrect answers:
A chosen-plaintext attacks
The attacker has the plaintext and ciphertext, but can choose the plaintext that gets encrypted to see the corresponding ciphertext. This gives her more power and possibly a deeper understanding of the way the encryption process works so she can gather more information about the key being used. Once the key is discovered, other messages encrypted with that key can be decrypted.
A chosen-ciphertext attack
In chosen-ciphertext attacks, the attacker can choose the ciphertext to be decrypted and has access to the resulting decrypted plaintext. Again, the goal is to figure out the key. This is a harder attack to carry out compared to the previously mentioned attacks, and the attacker may need to have control of the system that contains the cryptosystem.
A known-algorithm attack
Knowing the algorithm does not give you much advantage without knowing the key. This is a bogus detractor. The algorithm should be public, which is the Kerckhoffs's Principle . The only secret should be the key.

Reference(s) used for this question:
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 866). McGraw-Hill. Kindle Edition.
and
Kerckhoffs's Principle

NEW QUESTION: 278
Why are coaxial cables called "coaxial"?
A. it includes two physical channels that carries the signal surrounded (after a layer of insulation) by another concentric physical channel, both running along the same axis.
B. it includes one physical channel that carries the signal surrounded (after a layer of insulation) by another concentric physical channel, both running along the same axis
C. it includes two physical channels that carries the signal surrounded (after a layer of insulation) by another two concentric physical channels, both running along the same axis.
D. it includes one physical channel that carries the signal surrounded (after a layer of insulation) by another concentric physical channel, both running perpendicular and along the different axis
Answer: (SHOW ANSWER)
Coaxial cable is called "coaxial" because it includes one physical channel that carries the signal surrounded (after a layer of insulation) by another concentric physical channel, both running along the same axis.
The outer channel serves as a ground. Many of these cables or pairs of coaxial tubes can be placed in a single outer sheathing and, with repeaters, can carry information for a great distance.
Source: STEINER, Kurt, Telecommunications and Network Security, Version 1, May 2002, CISSP Open Study Group (Domain Leader: skottikus), Page 14.

NEW QUESTION: 279
Which of the following is NOT true of Secure Sockets Layer (SSL)?
A. By convention it uses 's-http://' instead of 'http://'.
B. Is the predecessor to the Transport Layer Security (TLS) protocol.
C. It was developed by Netscape.
D. It is used for transmitting private information, data, and documents over the Internet.
Answer: A (LEAVE A REPLY)
Web pages that use SSL use 'https://' instead of 'http://', whereas documents that use Secure-http start with s-http://.
The following answers are incorrect:
Is the predecessor to Transport Layer Security, It was developed by Netscape, and It is used for transmitting private documents over the Internet.
As these are all TRUE answers, therefore incorrect for this question.
References: TIPTON, Harold F. & HENRY, Kevin, Official (ISC)2 Guide to the CISSP CBK,

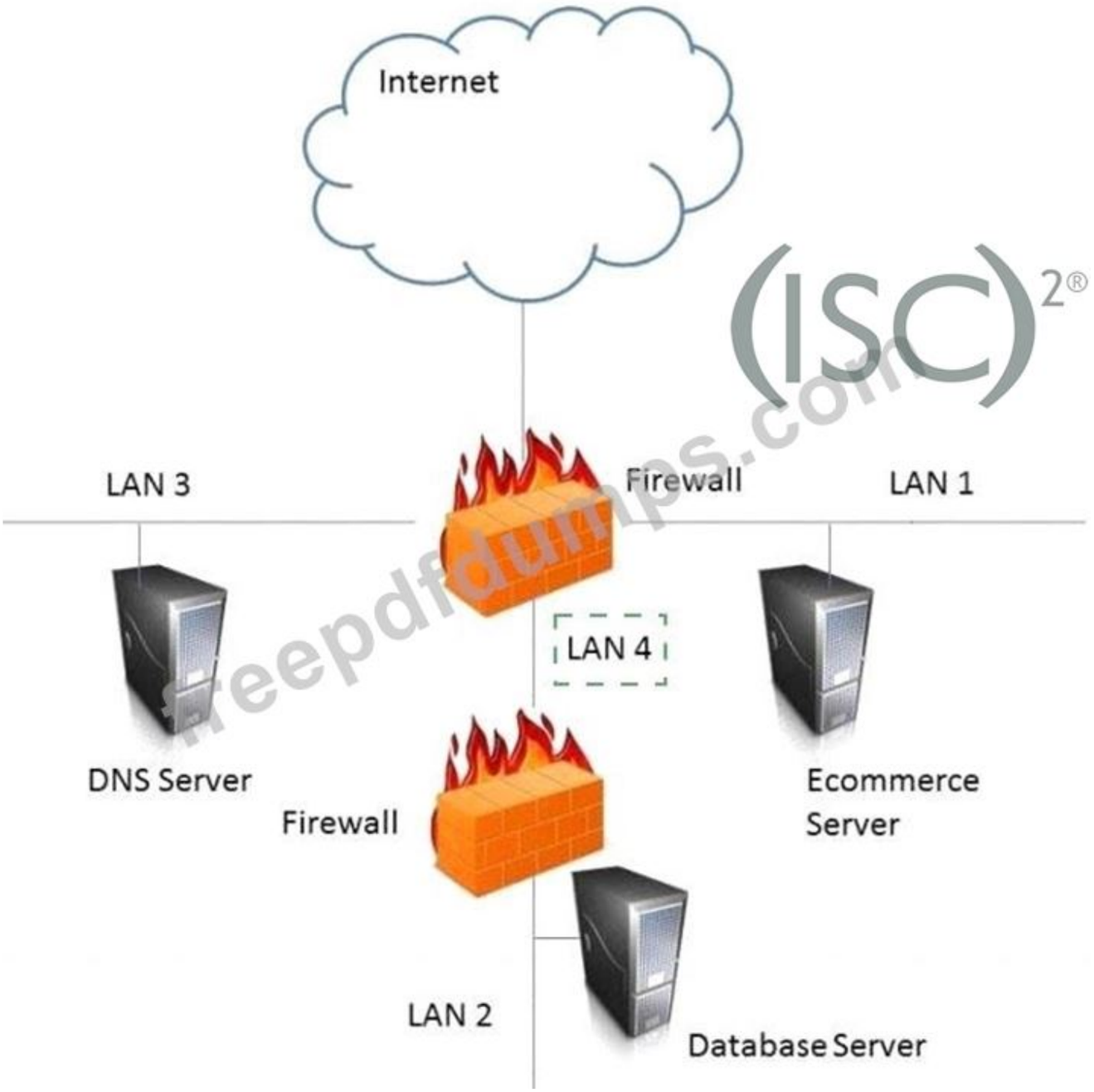
2007, pages 496, 976
KRUTZ, Ronald L. & VINES, Russell Dean, The CISSP Prep Guide, Gold Edition, 2003, page 117

NEW QUESTION: 280
Controlling access to information systems and associated networks is
necessary for the preservation of their confidentiality, integrity, and
availability. Which of the following is NOT a goal of integrity?
A. Preservation of the internal and external consistency of the information
B. Prevention of the modification of information by unauthorized users
C. Prevention of the unauthorized or unintentional modification of information by authorized users
D. Prevention of authorized modifications by unauthorized users
Answer: (SHOW ANSWER)
The other options are the three principles of integrity. Answer "Prevention of authorized modifications by unauthorized users" is a distracter and does not make sensE.
* Internal consistency ensures that internal data correlate. For example, the total number of a particular data item in the database should be the sum of all the individual, non-identical occurrences of that data item in the database. External consistency requires that the database content be consistent with the real world items that it represents.

NEW QUESTION: 281
In the network design below, where is the MOST secure Local Area Network (LAN) segment to deploy a Wireless Access Point (WAP) that provides contractors access to the Internet and authorized enterprise services?


Internet
LAN 3
Firewall
LAN 1
LAN 4
DNS Server
Firewall
Ecommerce Server
LAN 2
Database Server

Answer:



Explanation
LAN 4

NEW QUESTION: 282
Which of the following are the three classifications of RAID identified by the RAID Advisory Board?
A. Failure Resistant Disk Systems (FRDSs), Failure Tolerant Disk Systems, and Disaster Tolerant Disk Systems.
B. Foreign Resistant Disk Systems (FRDSs), Failure Tolerant Disk Systems, and Disaster Tolerant Disk Systems.
C. Failure Resistant Disk Systems (FRDSs), File Transfer Disk Systems, and Disaster Tolerant Disk Systems.

D. Federal Resistant Disk Systems (FRDSs), Fault Tolerant Disk Systems, and Disaster Tolerant Disk Systems.

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

The RAID Advisory Board has defined three classifications of RAID: Failure Resistant Disk Systems (FRDSs), Failure Tolerant Disk Systems, and Disaster Tolerant Disk Systems. As of this writing only the first one, FRDS, is an existing standard, and the others are still pending. We will now discuss the various implementation levels of an FRDS.

Failure Resistant Disk System: The basic function of an FRDS is to protect file servers from data loss and a loss of availability due to disk failure. It provides the ability to reconstruct the contents of a failed disk onto a replacement disk and provides the added protection against data loss due to the failure of many hardware parts of the server. One feature of an FRDS is that it enables the continuous monitoring of these parts and the alerting of their failure.

Failure Resistant Disk System Plus: An update to the FRDS standard is called FRDS+. This update adds the ability to automatically hot swap (swapping while the server is still running) failed disks. It also adds protection against environmental hazards (such as temperature, out-of-range conditions, and external power failure) and includes a series of alarms and warnings of these failures.

Incorrect Answers:

B: Foreign Resistant Disk Systems is not one of the three classifications of RAID identified by the RAID Advisory Board.

C: File Transfer Disk Systems is not one of the three classifications of RAID identified by the RAID Advisory Board.

D: Federal Resistant Disk Systems is not one of the three classifications of RAID identified by the RAID Advisory Board.

References:

Krutz, Ronald L. and Russell Dean Vines, The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 144

NEW QUESTION: 283

Which of the following violates identity and access management best practices?

A. Generic accounts

B. Privileged accounts

C. System accounts

D. User accounts

Answer: A (LEAVE A REPLY)

NEW QUESTION: 284

An internal Service Level Agreement (SLA) covering security is signed by senior managers and is in place. When should compliance to the SLA be reviewed to ensure that a good security posture is being delivered?

A. Immediately after a security breach

B. Prior to a planned security audit
C. As part of the SLA renewal process
D. At regularly scheduled meetings
Answer: D (LEAVE A REPLY)

NEW QUESTION: 285
Which of the following enables the person responsible for contingency planning to focus risk management efforts and resources in a prioritized manner only on the identified risks?
A. Risk assessment
B. Residual risks
C. Security controls
D. Business units
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A risk assessment is a critical part of the disaster recovery planning process. In disaster recovery planning, once you've completed a business impact analysis (BIA), the next step is to perform a risk assessment. Once risks and vulnerabilities have been identified, i.e. after the risk assessment has been completed, four types of defensive responses can be considered:
Protective measures
Mitigation measures
Recovery activities
Contingency plans
Incorrect Answers:
B: Contingency plans depend on risk assessments, not on residual risks. The residual risk is remaining risk after the security controls have been applied.
C: Contingency plans depend on risk assessments, not on Security controls.
D: Contingency plans depend on risk assessments, not on Business units.
References:
http://searchdisasterrecovery.techtarget.com/Risk-assessments-in-disaster-recovery-planning-A-free-IT- risk-assessment-template-and-guide

NEW QUESTION: 286
Domain Name Service is a distributed database system that is used to map:
A. Domain Name to IP addresses.
B. MAC addresses to domain names.
C. MAC Address to IP addresses.
D. IP addresses to MAC Addresses.
E. Explanation:
The Domain Name Service is a distributed database system that is used to map domain names to IP addresses and IP addresses to domain names. The Domain Name System is maintained by a distributed

database system, which uses the client-server model. The nodes of this database are the name servers. Each domain has at least one authoritative DNS server that publishes information about that domain and the name servers of any domains subordinate to it. The top of the hierarchy is served by the root nameservers, the servers to query when looking up (resolving) a TLD.
Reference(s) used for this question: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 100. and https://en.wikipedia.org/wiki/Domain_Name_System
164.
The Domain Name System (DNS) is a global network of:
A. servers that provide these Domain Name Services.
B. clients that provide these Domain Name Services.
C. hosts that provide these Domain Name Services.
D. workstations that provide these Domain Name Services.
Answer: A (LEAVE A REPLY)
The Domain Name System (DNS) is a global network of servers that provide these Domain Name Services.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 100.

NEW QUESTION: 287
Why is it so important to test disaster recovery plans frequently?
A. Natural disasters can change frequently.
B. The businesses that provide subscription services might have changed ownership.
C. Employees might get bored with the planning process.
D. A plan is not considered viable until a test has been performed.
Answer: D (LEAVE A REPLY)
A plan is not considered functioning and viable until a test has been performed. An untested plan sitting on a shelf is useless and might even have the reverse effect of creating a false sense of security. While the other answers are good reasons to test, they are not the primary reason.

NEW QUESTION: 288
The lattice-based model aims at protecting against:
A. Illegal attributes.
B. None of the choices.

C. Illegal information flow among the entities.

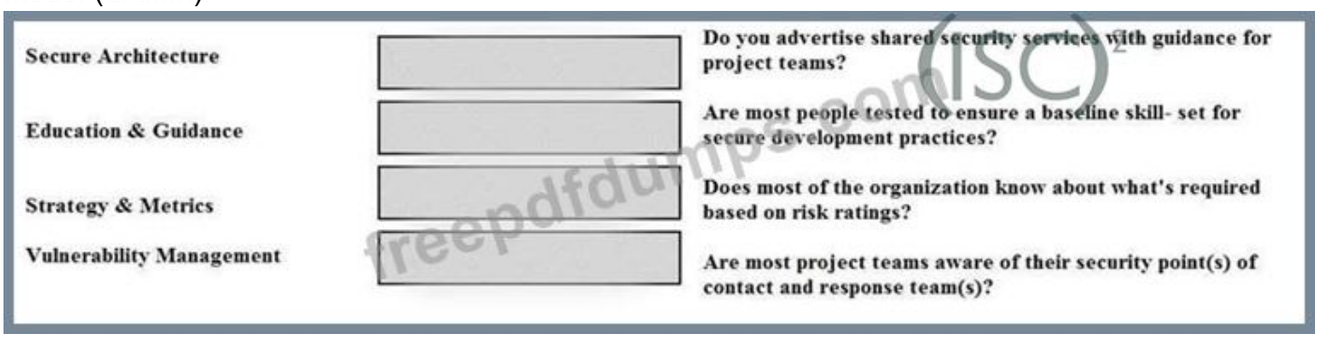
D. Illegal access rights

Answer: C (LEAVE A REPLY)

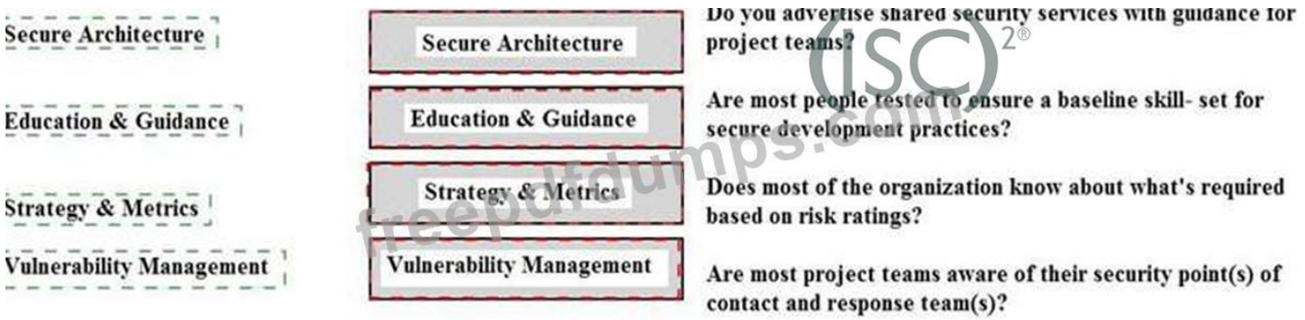
The lattice-based model aims at protecting against illegal information flow among the entities. One security class is given to each entity in the system. A flow relation among the security classes is defined to denote that information in one class can flow into another class.

NEW QUESTION: 289

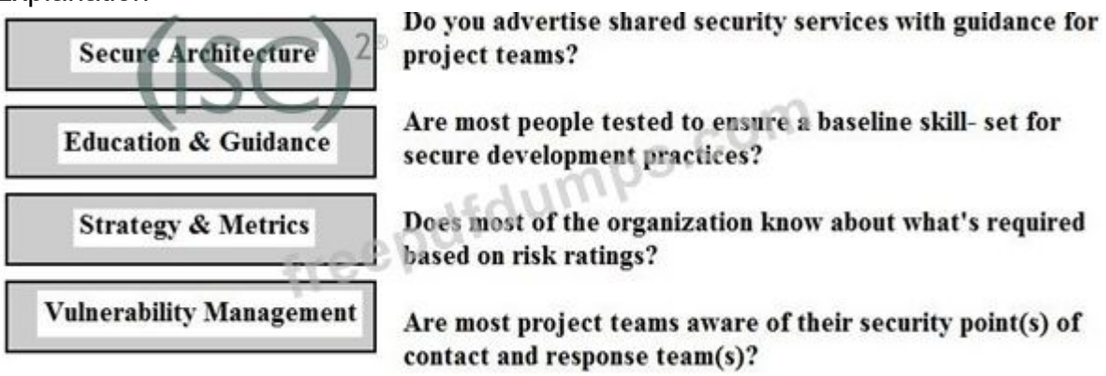
Match the objectives to the assessment questions in the governance domain of Software Assurance Maturity Model (SAMM).



Answer:



Explanation



NEW QUESTION: 290

When companies come together to work in an integrated manner such as extranets, special care must be taken to ensure that each party promises to provide the necessary level of protection, liability and responsibility. These aspects should be defined in the contracts that each party signs. What describes this type of liability?

A. Cascade liabilities
B. Downstream liabilities
C. Down-flow liabilities
D. Down-set liabilities
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
References: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGrawHill/Osborne, 2001, Page 659.

NEW QUESTION: 291
A security practitioner is tasked with securing the organization's Wireless Access Points (WAP). Which of these is the MOST effective way of restricting this environment to authorized users?
A. Enable Wi-Fi Protected Access 2 (WPA2) encryption on the wireless access point
B. Disable the broadcast of the Service Set Identifier (SSID) name
C. Change the name of the Service Set Identifier (SSID) to a random value not associated with the organization
D. Create Access Control Lists (ACL) based on Media Access Control (MAC) addresses
Answer: (SHOW ANSWER)
Section: Communication and Network Security

NEW QUESTION: 292
Which of the following would constitute the best example of a password to use for access to a system by a network administrator?
A. holiday
B. Christmas12
C. Jenny
D. GyN19Za!
Answer: (SHOW ANSWER)
GyN19Za! would be the best answer because it contains a mixture of upper and lower case characters, alphabetic and numeric characters, and a special character making it less vulnerable to password attacks.
All of the other answers are incorrect because they are vulnerable to brute force or dictionary attacks. Passwords should not be common words or names. The addition of a number to the end of a common word only marginally strengthens it because a common password attack would also check combinations of words: Christmas23
Christmas123 etc...

NEW QUESTION: 293
Which of the following specifically addresses cyber attacks against an organization's IT systems?
A. Continuity of support plan
B. Continuity of operations plan

C. Business continuity plan
D. Incident response plan
Answer: (SHOW ANSWER)

NEW QUESTION: 294
Which of the following statements pertaining to block ciphers is incorrect?
A. It operates on fixed-size blocks of plaintext.
B. It is more suitable for software than hardware implementations.
C. Plain text is encrypted with a public key and decrypted with a private key.
D. Some Block ciphers can operate internally as a stream.
Answer: C (LEAVE A REPLY)
Block ciphers do not use public cryptography (private and public keys).
Block ciphers is a type of symmetric-key encryption algorithm that transforms a fixed-size block of plaintext (unencrypted text) data into a block of ciphertext (encrypted text) data of the same length. They are appropriate for software implementations and can operate internally as a stream. See more info below about DES in Output Feedback Mode (OFB), which makes use internally of a stream cipher.
The output feedback (OFB) mode makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext. Just as with other stream ciphers, flipping a bit in the ciphertext produces a flipped bit in the plaintext at the same location. This property allows many error correcting codes to function normally even when applied before encryption.
Reference(s) used for this question: Wikipedia on Block Cipher mode at:
https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation and http://www.itl.nist.gov/fipspubs/fip81.htm

NEW QUESTION: 295
Which of the following is an accurate statement when an assessment results in the discovery of vulnerabilities in a critical network component?
A. There is little likelihood that the entire network is being placed at a significant risk of attack.
B. A second assessment should immediately be performed after all vulnerabilities are corrected.
C. The fact that every other host is sufficiently hardened does not change the fact frat the network is placed at risk of attack.
D. There is a low possibility that any adjacently connected components have been compromised by an attacker
Answer: B (LEAVE A REPLY)

NEW QUESTION: 296
Refer to the information below to answer the question.
A large, multinational organization has decided to outsource a portion of their Information Technology (IT) organization to a third-party provider's facility. This provider will be responsible for the design, development, testing, and support of several critical, customer-based applications used by the organization.
The organization should ensure that the third party's physical security controls are in place so that they
A. are more rigorous than the original controls.

B. allow access by the organization staff at any time.
C. are able to limit access to sensitive information.
D. cannot be accessed by subcontractors of the third party.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 297
The PRIMARY purpose of accreditation is to:
A. allow senior management to make an informed decision regarding whether to accept the risk of operating the system.
B. comply with applicable laws and regulations.
C. verify that all security controls have been implemented properly and are operating in the correct manner.
D. protect an organization's sensitive data.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 298
An organization is found lacking the ability to properly establish performance indicators for its Web hosting solution during an audit. What would be the MOST probable cause?
A. Improper deployment of the Service-Oriented Architecture (SOA)
B. Inadequate cost modeling
C. Insufficient Service Level Agreement (SLA)
D. Absence of a Business Intelligence (BI) solution
Answer: C (LEAVE A REPLY)

NEW QUESTION: 299
During the course of a Business Impact Analysis (BIA) you will less likely:
A. Determine the impact upon the organizations market share and corporate image
B. Determine if functions Recovery Time Objective (RTO)
C. Estimate the financial and operational impact of a disruption
D. Identify regulatory exposure
Answer: (SHOW ANSWER)

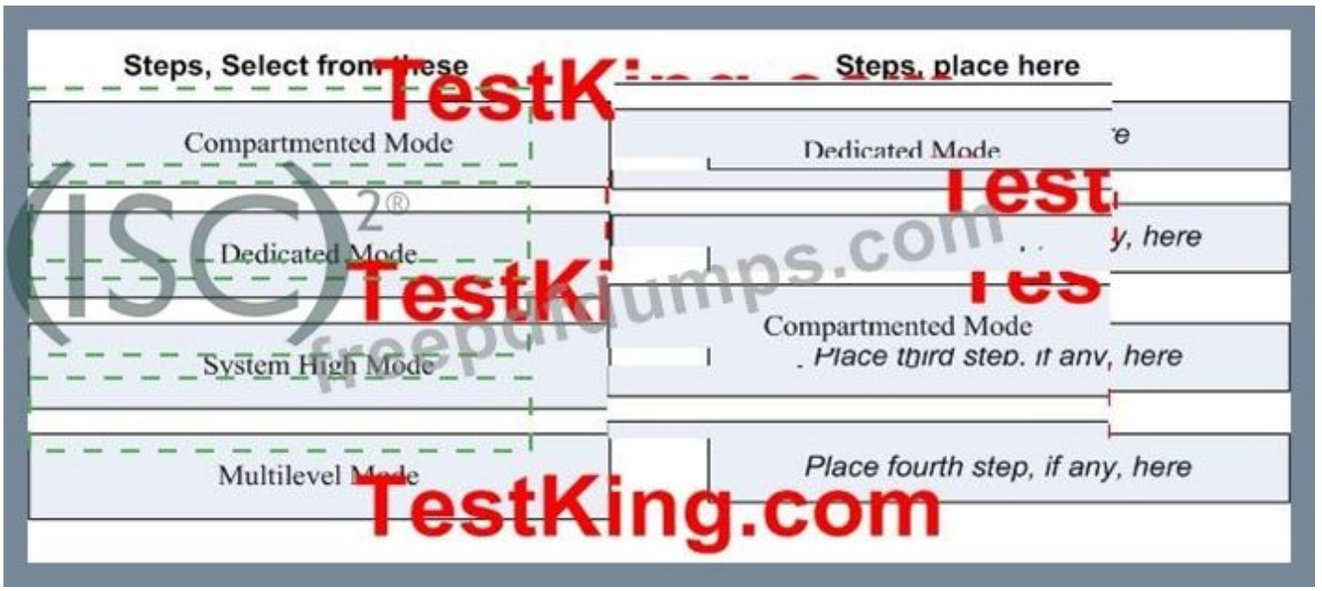
NEW QUESTION: 300
In what way can violation clipping levels assist in violation tracking and analysis?
A. Clipping levels enable the security administrator to customize the audit trail to record only actions for users with access to usercodes with a privileged status
B. Clipping levels set a baseline for normal user errors, and violations exceeding that threshold will be recorded for analysis of why the violations occurred
C. Clipping levels enable a security administrator to view all reductions in security levels which have been made to usercodes which have incurred violations
D. Clipping levels enable a security administrator to customize the audit trail to record only those violations which are deemed to be security relevant

Answer: B (LEAVE A REPLY)

NEW QUESTION: 301
What is the main purpose of undertaking a parallel run of a new system?
A. Resolve any errors in the program and file interfaces
B. Verify that the system provides required business functionality
C. Validate the operation of the new system against its predecessor
D. Provide a backup of the old system
Answer: B (LEAVE A REPLY)

NEW QUESTION: 302
DRAG DROP
Place the four systems security modes of operation in order, from the most secure to the least:

Answer:



Explanation:

65-2

The mode of operation is a description of the conditions under which an AIS functions, based on the sensitivity of data processed and the clearance levels and authorizations of the users. Four modes of operation are defined:

Dedicated ModE. An AIS is operating in the dedicated mode when each user with direct or indirect individual access to the AIS, its peripherals, remote terminals, or remote hosts has all of the following:

A. Avalid personnel clearance for all information on the system

B. Formal access approval for, and has signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments, and/or

special access programs)
C. A valid need-to-know for all information contained within the system
System-High ModE. An AIS is operating in the system-high mode when each user with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts has all of the following:
A. A valid personnel clearance for all information on the AIS
B. Formal access approval for, and has signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs)
C. A valid need-to-know for some of the information contained within the AIS
Compartmented ModE. An AIS is operating in the compartmented mode when each user with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts has all of the following:
A. A valid personnel clearance for the most restricted information processed in the AIS
B. Formal access approval for, and has signed nondisclosure agreements for that information to which he/she is to have access
C. A valid need-to-know for that information to which he/she is to have access
Multilevel ModE. An AIS is operating in the multilevel mode when all the following statements are satisfied concerning the users with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts:
A. Some do not have a valid personnel clearance for all the information processed in the AIS.
B. All have the proper clearance and have the appropriate formal access approval for that information to which he/she is to have access.
C. All have a valid need-to-know for that information to which they are to have access.
Source: DoD 5200.28-STD Department of Defense Trusted Computer System Evaluation Criteria.

NEW QUESTION: 303
Operations Security seeks to primarily protect against which of the following?

A. object reuse
B. facility disaster
C. compromising emanations
D. asset threats
Answer: (SHOW ANSWER)
The most important reason for identifying threats is to know from what do the assets need protection and what is the likelihood that a threat will occur. Threats cannot be eliminated, but can be anticipated, and safeguards put in place to minimize their impact.
Operations Security provides audit and monitoring for mechanisms, tools and facilities which permit the identification of security events and documentation of subsequent corrective actions.
Source: State of Nebraska - Information Security Systems (ISS) Security Officer Instruction Guide.

NEW QUESTION: 304
What sort of attack is described by the following: An attacker has a list of broadcast addresses which it stores into an array, the attacker sends a spoofed icmp echo request to each of those addresses in series and starts again. The spoofed IP address used by the attacker as the source of the packets is the target/victim IP address.
A. Smurf Attack
B. Fraggle Attack
C. LAND Attack
D. Replay Attack
Answer: A (LEAVE A REPLY)
The Smurf Attack is a denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address.
Most devices on a network will, in their default settings, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic.
This can slow down the victim's computer to the point where it becomes impossible to work on.
The name Smurf comes from the file "smurf.c", the source code of the attack program, which was released in 1997 by TFreak.
The author describes the attack as:
The `smurf' attack is quite simple. It has a list of broadcast addresses which it stores into an array, and sends a spoofed icmp echo request to each of those addresses in series and starts again. The result is a devistating attack upon the spoofed ip with, depending on the amount of broadcast addresses used, many, many computers responding to the echo request.
Mitigation:
- Best method for mitigating this threat is to control access to the physical network infrastructure. If the attacker can't send the attack, this attack will obviously not work.
- Currently the preferred method for controlling access to the network is by using 802.1X - Certificate security.

- Also, modern operating systems don't usually permit a PING to a broadcast address and just returns an error message if you try.
The following answers are incorrect:
- Fraggle Attack: Close but not quite right. A Fraggle attack uses UDP rather than the ICMP that Smurf Attack uses.
- LAND Attack: Sorry, not correct. A LAND attack is simply a series of packets sent to the target where the source and destination IP Addresses are the same as the victim.
- Replay Attack: This isn't an attack that takes advantage of a system vulnerability so it isn't the correct answer.
The following reference(s) was used to create this question:
http://en.wikipedia.org/wiki/Smurf_attack
and
http://searchsecurity.techtarget.com/answer/What-is-a-land-attack
and
http://www.phreak.org/archives/exploits/denial/smurf.c

NEW QUESTION: 305
Which of the following command line tools can be used in the reconnaisance phase of a network vulnerability assessment?
A. nbtstat
B. ifconfig
C. dig
D. ipconfig
Answer: C (LEAVE A REPLY)

NEW QUESTION: 306
Which of the following is a type of mandatory access control?
A. Rule-based access control
B. Role-based access control
C. User-directed access control
D. Lattice-based access control
Answer: A (LEAVE A REPLY)
Reference: pg 46 Krutz: CISSP Prep Guide: Gold Edition

NEW QUESTION: 307
Which type of fire detectors sends an alarm when the temperature of the room rises dramatically?
A. Odor-sensing
B. Heat-sensing
C. Smoke-actuated
D. Flame-actuated
Answer: B (LEAVE A REPLY)

A rate-of-rise detector triggers an alarm
when the ambient temperature of a room increases rapidly. Another
type of heat-sensing detector, a fixed temperature device, sends an
alarm when the temperature passes a predetermined level.

NEW QUESTION: 308
Which of the following ensures that security is NOT breached when a system crash or other system failure occurs?
A. Trusted recovery
B. Hot swappable
C. Redundancy
D. Secure boot
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Trusted recovery ensures that security is not breached when a system crash or other system failure (sometimes called a "discontinuity") occurs. It must ensure that the system is restarted without compromising its required protection scheme, and that it can recover and rollback without being compromised after the failure. Trusted recovery is required only for B3 and A1 level systems. A system failure represents a serious security risk because the security controls may be bypassed when the system is not functioning normally. For example, if a system crashes while sensitive data is being written to a disk (where it would normally be protected by controls), the data may be left unprotected in memory and may be accessible by unauthorized personnel.
Trusted recovery has two primary activities - preparing for a system failure and recovering the system.
Incorrect Answers:
B: Hot swappable refers to computer components that can be swapped while the computer is running. This is not what is described in the question.
C: Redundancy refers to multiple instances of computer or network components to ensure that the system can remain online in the event of a component failure. This is not what is described in the question.
D: Secure Boot refers to a security standard that ensures that a computer boots using only software that is trusted. This is not what is described in the question.
References:
Krutz, Ronald L. and Russell Dean Vines, The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 310

NEW QUESTION: 309
They in form of credit card-size memory cards or smart cards, or those resembling small calculators, are used to supply static and dynamic passwords are called?
A. Token Ring
B. Tokens
C. Token passing networks

D. Coupons

Answer: B (LEAVE A REPLY)

Tokens are usually used to provide authentication through "What we have", is most commonly implemented to provide two-factor authentication. For example, SecurID requires two pieces of information, a password and a token. The token is usually generated by the SecurID token - a small electronic device that users keep with them that display a new number every 60 seconds. Combining this number with the users password allows the SecurID server to determine whatever or not the user should be granted access.

NEW QUESTION: 310

Which of the following is NOT a characteristic of a host-based intrusion detection system?

A. A HIDS does not consume large amounts of system resources

B. A HIDS can analyse system logs, processes and resources

C. A HIDS looks for unauthorized changes to the system

D. A HIDS can notify system administrators when unusual events are identified

Answer: A (LEAVE A REPLY)

A HIDS does not consume large amounts of system resources is the correct choice. HIDS can consume inordinate amounts of CPU and system resources in order to function effectively, especially during an event.

All the other answers are characteristics of HIDSes

A HIDS can:

- scrutinize event logs, critical system files, and other auditable system resources;
- look for unauthorized change or suspicious patterns of behavior or activity
- can send alerts when unusual events are discovered

Reference:

Official guide to the CISSP CBK. Pages 197 to 198.

NEW QUESTION: 311

What is the GREATEST challenge to identifying data leaks?

A. Available technical tools that enable user activity monitoring.

B. Senior management cooperation in investigating suspicious behavior.

C. Documented asset classification policy and clear labeling of assets.

D. Law enforcement participation to apprehend and interrogate suspects.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 312

An incremental backup process

A. Backs up all the files that have changed since the last full or incremental backup and sets the archive bit to 0.

B. Backs up the files that been modified since the last full backup. It does not change the archive bit value.

C. Backs up all the data and changes the archive bit to 0.

D. Backs up all the data and changes the archive bit to 1.

Answer: (SHOW ANSWER)

Explanation/Reference:
Explanation:
The incremental backup method backs up all the files that have changed since the last full or incremental backup and resets the archive bit to 0. This is known as "clearing the archive bit". A full backup backs up all files regardless of whether the archive bit is 1 or 0 and sets the archive bit to 0.
The archive bit is used by the backup process to determine whether a file has been changed. When you modify a file or create a new file, the archive bit is set to 1. This tells the backups process that the file has changed (or is a new file) and needs to be backed up. When an incremental backup backs up the file, it sets the archive bit to 0. When the next incremental backup runs and sees that the archive bit is 0, the incremental backup knows that the file has not changed since the last backup and so will not back up the file again.
Incorrect Answers:
B: This answer describes the differential backup process. The differential backup does not change the archive bit value; an incremental backup does change the archive bit value to 0.
C: This answer describes the full backup process. An incremental backup does not back up ALL files; it only backs up changed files.
D: An incremental backup does not back up ALL files; it only backs up changed files. Furthermore, it changes the archive bit value to 0, not 1.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, pp. 801-802

NEW QUESTION: 313
What is the primary goal of setting up a honey pot?
A. To lure hackers into attacking unused systems
B. To entrap and track down possible hackers
C. To set up a sacrificial lamb on the network
D. To know when certain types of attacks are in progress and to learn about attack techniques so the network can be fortified.
Answer: D (LEAVE A REPLY)
The primary purpose of a honeypot is to study the attack methods of an attacker for the purposes of understanding their methods and improving defenses.
"To lure hackers into attacking unused systems" is incorrect. Honeypots can serve as decoys but their primary purpose is to study the behaviors of attackers.
"To entrap and track down possible hackers" is incorrect. There are a host of legal issues around enticement vs entrapment but a good general rule is that entrapment is generally prohibited and evidence gathered in a scenario that could be considered as "entrapping" an attacker would not be admissible in a court of law. "To set up a sacrificial lamb on the network" is incorrect. While a honeypot is a sort of sacrificial lamb and may attract attacks that might have been directed against production systems, its real purpose is to study the methods of attackers with the goals of better understanding and improving network defenses.
References: AIO3, p. 213

NEW QUESTION: 314

Which of the following is a web application control that should be put into place to prevent exploitation of Operating System (OS) bugs?

A. Check arguments in function calls

B. Test for the security patch level of the environment

C. Include logging functions

D. Digitally sign each application module

Answer: B (LEAVE A REPLY)

NEW QUESTION: 315

Which of the following protocol is PRIMARILY used to provide confidentiality in a web based application thus protecting data sent across a client machine and a server?

A. SSL

B. FTP

C. SSH

D. S/MIME

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

SSL is primarily used to protect HTTP traffic. SSL capabilities are already embedded into most web browsers.

Incorrect Answers:

B: FTP is used to transfer files, not to secure data that are transferred.

C: S/MIME is not to protect data sent in web applications. S/MIME, more specifically, is used to secure email messages.

D: SSH is not used in a web based application. SSH allows remote login and other network services to operate securely over an unsecured network.

References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 846

NEW QUESTION: 316

Computer-generated evidence is considered:

A. Best evidence

B. Second hand evidence

C. Demonstrative evidence

D. Direct evidence

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

Computer-generated evidence normally falls under the category of hearsay evidence, or second-hand evidence, because it cannot be proven accurate and reliable. Under the U.S. Federal Rules of Evidence, hearsay evidence is generally not admissible in court. Best evidence is original or primary evidence rather

than a copy or duplicate of the evidence. It does not apply to computer-generated evidence. Direct evidence is oral testimony by witness. Demonstrative evidence is used to aid the jury (models, illustrations, charts). References: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 9: Law, Investigation, and Ethics (page 310). ROTHKE, Ben, CISSP CBK Review presentation on domain 9.

NEW QUESTION: 317
Electronic signatures can prevent messages from being:
A. Repudiated
B. Erased
C. Disclosed
D. Forwarded
Answer: A (LEAVE A REPLY)

NEW QUESTION: 318
Which of the following is an effective control in preventing electronic cloning of Radio Frequency Identification (RFID) based access cards?
A. Physical Access Control System (PACS) repeated attempt detection
B. Personal Identity Verification (PIV)
C. Cardholder Unique Identifier (CHUID) authentication
D. Asymmetric Card Authentication Key (CAK) challenge-response
Answer: (SHOW ANSWER)

NEW QUESTION: 319
Which statement below MOST accurately describes configuration
control?
A. Assuring that only the proposed and approved system changes are implemented
B. Tracking the status of current changes as they move through the configuration control process
C. Verifying that all configuration management policies are being followed
D. The decomposition process of a verification system into CIs
Answer: (SHOW ANSWER)
Configuration control is a means of assuring that system changes are approved before being implemented, only the proposed and approved changes are implemented, and the implementation is complete and

accuratE. This involves strict procedures for proposing, monitoring, and approving system changes and their implementation. Configuration control entails central direction of the change process by personnel who coordinate analytical tasks, approve system changes, review the implementation of changes, and supervise other tasks such as documentation. *Answer "The decomposition process of a verification system into CIs" is configuration identification. The decomposition process of a verification system into Configuration Items (CIs) is called configuration identification. A CI is a uniquely identifiable subset of the system that represents the smallest portion to be subject to independent configuration control procedures. Answer "Tracking the status of current changes as they move through the configuration control process" is configuration accounting. Configuration accounting documents the status of configuration control activities and, in general, provides the information needed to manage a configuration effectively. It allows managers to trace system changes and establish the history of any developmental problems and associated fixes. Configuration accounting also tracks the status of current changes as they move through the configuration control process. Configuration accounting establishes the granularity of recorded information and thus shapes the accuracy and usefulness of the audit function. *Answer "Verifying that all configuration management policies are being follow" is configuration audit. Configuration audit is the quality assurance component of configuration management. It involves periodic checks to determine the consistency and completeness of accounting information and to verify that all configuration management policies are being followeD. A vendors configuration management program must be able to sustain a complete configuration audit
by an NCSC review team.
Source: NCSC-TG-014, Guidelines for Formal Verification Systems.

NEW QUESTION: 320
What technique used for spoofing the origin of an email can successfully conceal the sender s Internet Protocol (IP) address?
A. Virtual Private Network (VPN)
B. Web crawling
C. Change In-Reply-To data
D. Onion routing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 321
Which of the following is NOT true of the Kerberos protocol?
A. Only a single login is required per session.
B. The initial authentication steps are done using public key algorithm.
C. The KDC is aware of all systems in the network and is trusted by all of them
D. It performs mutual authentication
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Kerberos uses shared secret keys and tickets for the initial authentication, not a public key algorithm.
Incorrect Answers:

A: Kerberos is an example of a single sign-on system for distributed environments, and therefore only requires a single login per session.
C: the foundation of Kerberos security is trust that clients and services have in the integrity of the KDC.
D: Kerberos provides mutual authentication in that both the user and the server verify each other's identity.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, pp. 209-213
https://en.wikipedia.org/wiki/Kerberos_(protocol)

NEW QUESTION: 322
The type of authorized interactions a subject can have with an object is
A. procedure.
B. protocol.
C. permission.
D. control.
Answer: (SHOW ANSWER)

NEW QUESTION: 323
A database view is the results of which of the following operations?
A. Join and Select.
B. Join, Insert, and Project.
C. Join, Project, and Create.
D. Join, Project, and Select.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
SQL offers three classes of operators for creating views: select, project, and join.
The select operator serves to shrink the table vertically by eliminating unwanted rows (tuples).
- The project operator serves to shrink the table horizontally by removing unwanted columns (attributes).
- Most commercial implementations of SQL do not support a project operation, instead projections are achieved by specifying the columns desired in the output.
The join operator allows the dynamic linking of two tables that share a common column value.
- Incorrect Answers:
A: SQL offers three classes of operators for creating views: select, project, and join. However, modern implementations of SQL do not support a project operation, instead projections are achieved by specifying the columns desired in the output. Nevertheless, project is a SQL operator.
B: Insert is a SQL command used to insert data into a table. It is not used to output a view.
C: Create is a SQL command used to create a new database, table, view, or index. However, the data or output of the view requires a select statement to shrink the table vertically by not showing unwanted rows, a project operation that shrinks the table horizontally by not showing unwanted columns, and a join statement when data from more than one table is required.

References:
http://db.grussell.org/section010.html
http://databasemanagement.wikia.com/wiki/Relational_Database_Model

NEW QUESTION: 324
This type of backup management provides a continuous on-line backup by using optical or tape "jukeboxes", similar to WORMs, (Write Once, Read Many)
A. Hierarchical Storage Management (HSM).
B. Hierarchical Resource Management (HRM).
C. Hierarchical Access Management (HAM).
D. Hierarchical Instance Management (HIM).
Answer: (SHOW ANSWER)
Hierarchical Storage Management originated in the mainframe world where it was used to minimize storage costs. The HSM name signifies that the software has the intelligence to move files along a hierarchy of storage devices that are ranked in terms of cost per megabyte of storage, speed of storage and retrieval, and overall capacity limits. Files are migrated along the hierarchy to less expensive forms of storage based on rules tied to the frequency of data access. File migration and retrieval is transparent to users. Two major factors, data access response time and storage costs determine the appropriate combination of storage devices used in HSM. A typical three tier strategy may be composed of hard drives as primary storage on the file servers, rewritable optical as the secondary storage type, and tape as the final tertiary storage location. If faster access is required, a hard drive can be considered as an alternative to optical for secondary storage, and WORM (Write Once, Read Many) optical can also be implemented, in place of tape, as the final storage destination.

NEW QUESTION: 325
What is a characteristic of using the Electronic Code Book mode of DES encryption?
A. A given block of plaintext and a given key will always produce the same ciphertext.
B. Repetitive encryption obscures any repeated patterns that may have been present in the plaintext.
C. Individual characters are encoded by combining output from earlier encryption routines with plaintext.
D. The previous DES output is used as input.
Answer: A (LEAVE A REPLY)
A given message and key always produce the same ciphertext.
The following answers are incorrect:
Repetitive encryption obscures any repeated patterns that may have been present in the plaintext. Is incorrect because with Electronic Code Book a given 64 bit block of plaintext always produces the same ciphertext
Individual characters are encoded by combining output from earlier encryption routines with plaintext. This is incorrect because with Electronic Code Book processing 64 bits at a time until the end of the file was reached. This is a characteristic of Cipher Feedback. Cipher
Feedback the ciphertext is run through a key-generating device to create the key for the next block of plaintext.

The previous DES output is used as input. Is incorrect because This is incorrect because with Electronic Code Book processing 64 bits at a time until the end of the file was reached
. This is a characteristic of Cipher Block Chaining. Cipher Block Chaining uses the output from the previous block to encrypt the next block.

NEW QUESTION: 326
Government data classifications include which of the following:(Choose four)
A. Open
B. Unclassified
C. Confidential
D. Private
E. Secret
F. Top Secret
Answer: B,C,E,F (LEAVE A REPLY)
One of the most common systems used to classify information is the one developed within the US Department of Defense. These include: unclassified, sensitive, confidential, secret, and top secret.

NEW QUESTION: 327
Which of the following disaster recovery test plans will be MOST effective while providing minimal risk?
A. Parallel
B. Simulation
C. Read-through
D. Full interruption
Answer: A (LEAVE A REPLY)

NEW QUESTION: 328
Which answer below is true about the difference between FTP and TFTP?
A. FTP enables print job spooling, whereas TFTP does not.
B. FTP does not have a directory-browsing capability, whereas TFTP
does.
C. FTP is less secure because session authentication does not occur.
D. TFTP is less secure because session authentication does not occur.
Answer: (SHOW ANSWER)
The correct answer is "TFTP is less secure because session authentication does not occur". The Trivial File Transfer Protocol (TFTP) is considered less secure than the File
Transfer Protocol (FTP) because authentication does not occur during session establishment (although FTP is very insecure in its own right).

NEW QUESTION: 329
Which of the following is needed for System Accountability?
A. Audit mechanisms.

B. Documented design as laid out in the Common Criteria.
C. Authorization.
D. Formal verification of system design.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Accountability is the ability to identify users and to be able to track user actions. Through the use of audit logs and other tools the user actions are recorded and can be used at a later date to verify what actions were performed.
Incorrect Answers:
B: Common Criteria is an international standard to evaluate trust and would not be a factor in System Accountability.
C: Authorization is granting access to subjects, just because you have authorization does not hold the subject accountable for their actions.
D: Formal verification involves Validating and testing highly trusted systems. It does not, however, involve System Accountability.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, pp. 203, 248-250, 402.

NEW QUESTION: 330
An organization publishes and periodically updates its employee policies in a file on their intranet.
Which of the following is a PRIMARY security concern?
A. Availability
B. Integrity
C. Confidentiality
D. Ownership
Answer: A (LEAVE A REPLY)

NEW QUESTION: 331
Which of the following best describes the purpose of debugging programs?
A. To generate random data that can be used to test programs before implementing them.
B. To ensure that program coding flaws are detected and corrected.
C. To protect, during the programming phase, valid changes from being overwritten by other changes.
D. To compare source code versions before transferring to the test environment
Answer: (SHOW ANSWER)
Debugging provides the basis for the programmer to correct the logic errors in a program under development before it goes into production.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 298).

NEW QUESTION: 332
Which of the following is a MAJOR consideration in implementing a Voice over IP (VoIP) network?
A. Use of separation for the voice network.
B. Use of a unified messaging.
C. Use of Network Access Control (NAC) on switches.
D. Use of Request for Comments (RFC) 1918 addressing.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 333
Which is NOT a suitable method for distributing certificate revocation information?
A. CA revocation mailing list
B. Delta CRL
C. OCSP (online certificate status protocol)
D. Distribution point CRL
Answer: A (LEAVE A REPLY)
The following are incorrect answers because they are all suitable methods.
A Delta CRL is a CRL that only provides information about certificates whose statuses have changed since the issuance of a specific, previously issued CRL.
The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.
A Distribution point CRL or CRL Distribution Point, a location specified in the CRL Distribution Point (CRL DP) X.509, version 3, certificate extension when the certificate is issued.
References: RFC 2459: Internet X.509 Public Key Infrastru
http://csrc.nist.gov/groups/ST/crypto_apps_infra/documents/sliding_window.pdf
http://www.ipswitch.eu/online_certificate_status_protocol_en.html
Computer Security Handbook By Seymour Bosworth, Arthur E. Hutt, Michel E. Kabay
http://books.google.com/books?id=rCx5OfSFUPkC&printsec=frontcover&dq=Computer+Security+Handbook#PRA6-PA4,M1

NEW QUESTION: 334
Which of the following is the MOST challenging issue in apprehending cyber criminals?
A. They often use sophisticated method to commit a crime.
B. It is often hard to collect and maintain integrity of digital evidence.

C. The crime is often committed from a different jurisdiction.
D. There is often no physical evidence involved.
Answer: C (LEAVE A REPLY)
Section: Security Operations

NEW QUESTION: 335
In a stateful inspection firewall, data packets are captured by an inspection engine that is operating at the:
A. Network or Transport Layer.
B. Application Layer.
C. Inspection Layer.
D. Data Link Layer.
Answer: A (LEAVE A REPLY)
Most stateful packet inspection firewalls work at the network or transport layers. For
the TCP/IP protcol, this allows the firewall to make decisions both on IP addresses, protocols and
TCP/UDP port numbers
Application layer is incorrect. This is too high in the OSI stack for this type of firewall.
Inspection layer is incorrect. There is no such layer in the OSI stack.
"Data link layer" is incorrect. This is too low in the OSI stack for this type of firewall.
References:
CBK, p. 466
AIO3, pp. 485 - 486

NEW QUESTION: 336
Which one of the following is an asymmetric algorithm?
A. Data Encryption Algorithm.
B. Data Encryption Standard
C. Enigma
D. Knapsack
Answer: D (LEAVE A REPLY)
Merkle-Hellman Knapsack is a Public Key Algorithm Pg 206 Krutz: CISSP Prep Guide: Gold Edition.
Not A:
"DES describes the Data Encryption Algorithm (DEA) and is the name of the Federal Information Processing Standard (FIPS) 46-1 that was adopted in 1977..." pg 195 Krutz: CISSP Prep Guide: Gold Edition.
Not B:
"The best-known symmetric key system is probably the Data Encryption Standard (DES)." pg 195 Krutz: CISSP Prep Guide: Gold Edition.
Not C:
"The German military used a polyalphabetic substitution cipher machine called the Enigma as its principal encipherment system during World War II." Pg 185 Krutz: CISSP Prep Guide: Gold Edition.

NEW QUESTION: 337

Risk reduction in a system development life-cycle should be applied:
A. Mostly to the initiation phase.
B. Mostly to the development phase.
C. Mostly to the disposal phase.
D. Equally to all phases.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Risk reduction should be applied equally to the initiation phase, the development phase, and to the disposal phase.
Within the initiation phase a preliminary risk assessment should be carried out to develop an initial description of the confidentiality, integrity, and availability requirements of the system.
The development phase include formal risk assessment which identifies vulnerabilities and threats in the proposed system and the potential risk levels as they pertain to confidentiality, integrity, and availability.
This builds upon the initial risk assessment carried out in the previous phase (the initiation phase). The results of this assessment help the team build the system's security plan.
Disposal activities need to ensure that an orderly termination of the system takes place and that all necessary data are preserved. The storage medium of the system may need to be degaussed, put through a zeroization process, or physically destroyed.
Incorrect Answers:
A: Risk reduction should be applied to all phases equally, not mostly to the initiation phase.
B: Risk reduction should be applied to all phases equally, not mostly to the development phase.
C: Risk reduction should be applied to all phases equally, not mostly to the disposal phase.
References:
Conrad, Eric, Seth Misenar and Joshua Feldman, CISSP Study Guide, 2nd Edition, Syngress, Waltham, 2012, pp. 1091-1093

NEW QUESTION: 338
Which of the following would BEST describe a Concealment cipher?
A. Permutation is used, meaning that letters are scrambled.
B. Every X number of words within a text, is a part of the real message.
C. Replaces bits, characters, or blocks of characters with different bits, characters or blocks.
D. Hiding data in another message so that the very existence of the data is concealed.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The concealment cipher is a symmetric key, transposition cipher where the words or characters of the plaintext message are embedded in a page of words or characters at a consistent interval.
Incorrect Answers:
A: Transposition cyphers moves the original values around.
C: The substitution cipher substitutes bits, characters, or blocks of characters with different bits, characters, or blocks.

D: Steganography is a technique used to hide data in another media type so that the presence of the data is masked.
Reference:
Miller, David R, Microsoft CISSP Training Kit, O'Reilly Media, 2013, California, p. 156 Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, pp. 774, 777

NEW QUESTION: 339
Which of the following should not be performed by an operator?
A. Mounting disk or tape
B. Backup and recovery
C. Data entry
D. Handling hardware
Answer: C (LEAVE A REPLY)
This is very obvious, the operators are responsible of making operative tasks that deals with the hardware and software implementations, they can handle the hardware and put t in condition for the user, be in charge of the backup and restore procedures and
Mounting the disk or tapes for the backup. Those are all common tasks. When we talk about the data entry, is the user who has to make does, If the operator do that too, what is the user going to do?

NEW QUESTION: 340
Which of the following is required in order to provide accountability?
A. Authentication
B. Integrity
C. Confidentiality
D. Audit trails
Answer: A (LEAVE A REPLY)
Reference: pg 5 Tittel: CISSP Study Guide

NEW QUESTION: 341
Which of the following would be an example of the best password?
A. golf001
B. Elizabeth
C. T1me4g0lF
D. password
Answer: C (LEAVE A REPLY)
The best passwords are those that are both easy to remember and hard to crack using a dictionary attack. The best way to create passwords that fulfil both criteria is to use two small unrelated words or phonemes, ideally with upper and lower case characters, a special character, and/or a number. Shouldn't be used: common names, DOB, spouse, phone numbers, words found in dictionaries or system defaults.
Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 1

NEW QUESTION: 342
What is the maximum length of cable that can be used for a twisted-pair, Category 5
10Base-T cable?
A. 80 meters
B. 100 meters
C. 185 meters
D. 500 meters
Answer: B (LEAVE A REPLY)
As a signal travels though a medium, it attenuates (loses strength) and at some point will become indistinguishable from noise. To assure trouble-free communication, maximum cable lengths are set between nodes to assure that attenuation will not cause a problem. The maximum CAT-5 UTP cable length between two nodes for
10BASE-T is 100M.
The following answers are incorrect:
8 0 meters. It is only a distracter.
1 85 meters. Is incorrect because it is the maximum length for 10Base-2
5 00 meters. Is incorrect because it is the maximum length for 10Base-5

NEW QUESTION: 343
A chain of custody shows who _____ _____ and _____.(Choose three)
A. Who controlled the evidence
B. Who transcribed the evidence
C. Who validated the evidence
D. Who presented the evidence
E. Secured the evidence
F. Obtained the evidence
Answer: A,E,F (LEAVE A REPLY)
The chain of evidence shows who obtained the evidence, who secured the evidence, and who controlled the evidence.

NEW QUESTION: 344
Which of the following NAT firewall translation modes allows a large group of internal clients to share a single or small group of ROUTABLE IP addresses for the purpose of hiding their identities when communicating with external hosts?
A. Static translation
B. Load balancing translation
C. Network redundancy translation
D. Dynamic translation
Answer: D (LEAVE A REPLY)
With dynamic translation (also called Automatic, Hide Mode, or IP Masquerade), a large group of internal clients to share a single or small group of ROUTABLE IP addresses for the purpose of hiding their identities

when communicating with external hosts or expanding the internal network address space. Static translation (also called port forwarding), assigns a fixed address to a specific internal network resource (usually a server). Static NAT is required to make internal hosts available for connection from external hosts.
Load Balancing Translation is used to translate a single IP address and port to a pool of identically configured servers so that a single public address can be served by a number of servers. In Network Redundancy Translation, multiple Internet connections are attached to a single NAT firewall that it chooses and uses based on load and availability.
Reference used for this question:
STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 7: Network Address Translation.

NEW QUESTION: 345
Degaussing is used to clear data from all of the following media except:
A. Floppy Disks
B. Read-Only Media
C. Video Tapes
D. Magnetic Hard Disks
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Atoms and Data
Shon Harris says: "A device that performs degaussing generates a coercive magnetic force that reduces the magnetic flux density of the storage media to zero. This magnetic force is what properly erases data from media. Data are stored on magnetic media by the representation of the polarization of the atoms. Degaussing changes this polarization (magnetic alignment) by using a type of large magnet to bring it back to its original flux (magnetic alignment). "
Degaussing is achieved by passing the magnetic media through a powerful magnet field to rearrange the metallic particles, completely removing any resemblance of the previously recorded signal. Therefore, degaussing will work on any electronic based media such as floppy disks, or hard disks - all of these are examples of electronic storage. However, "read-only media" includes items such as paper printouts and CD-ROM which do not store data in an electronic form or is not magnetic storage. Passing them through a magnet field has no effect on them.
Not all clearing/ purging methods are applicable to all media- for example, optical media is not susceptible to degaussing, and overwriting may not be effective against Flash devices. The degree to which information may be recoverable by a sufficiently motivated and capable adversary must not be underestimated or guessed at in ignorance. For the highest-value commercial data, and for all data regulated by government or military classification rules, read and follow the rules and standards.
Incorrect Answers:
A: Floppy Disks can be erased by degaussing.
C: Video Tapes can be erased by degaussing.
D: Magnetic Hard Disks can be erased by degaussing.

References:
http://www.degausser.co.uk/degauss/degabout.htm
http://www.degaussing.net/
http://www.cerberussystems.com/INFOSEC/stds/ncsctg25.htm

NEW QUESTION: 346
Which of the following is TRUE of two-factor authentication?
A. It uses the RSA public-key signature based on integers with large prime factors.
B. It requires two measurements of hand geometry.
C. It does not use single sign-on technology.
D. It relies on two independent proofs of identity.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
There are three general factors that are used for authentication:
Something a person knows.
▪
Something a person has.
▪
Something a person is.
▪
Two-factor authentication requires two of the three factors to be part of authentication process.
Incorrect Answers:
A: RSA encryption uses integers with exactly two prime factors, but the term "two-factor authentication" is not used in that context.
B: Measuring hand geometry twice only provides one factor.
C: Single sign-on (SSO) technology allows a user to enter their credentials once to gain access to multiple systems. Two-factor authentication could be used for SSO, not the other way around.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, pp. 162, 163, 207, 815

NEW QUESTION: 347
What is necessary for a subject to have write access to an object in a Multi-Level Security Policy?
A. The subject's sensitivity label must dominate the object's sensitivity label.
B. The subject's sensitivity label subordinates the object's sensitivity label.

C. The subject's sensitivity label is subordinated by the object's sensitivity label.
D. The subject's sensitivity label is dominated by the object's sensitivity label.
Answer: A (LEAVE A REPLY)
The correct answer is: The subject's sensitivity label must dominate the object's sensitivity label.
With a Multi-level security policy you have information that has different sensitivity labels. In order to read an object the subject's sensitivity label must be equal to or greater than that of the object. So it would be considered to dominate it, no read up.
The following answers are incorrect: The subject's sensitivity label subordinates the object's sensitivity label. Is incorrect because if the subject's sensitivity label subordinates the object's sensitivity label that would mean it is lower and the subject should not have read access to the object.
The subject's sensitivity label is subordinated by the object's sensitivity label. Is incorrect because the this would not allow for read access if the sensitivity lables were equal. So the subject's sensitivity label is not subordinated by the object's sensitivity label, the subject's label must dominate the object's label. Remember dominate means equal to or greater than where subordinate means less than.
The subject's sensitivity label is dominated by the object's sensitivity label. Is incorrect because if the object's sensitivity label dominates the subject's sensitivity label then the subject should not have access, it is the subject that must dominate the object and not the other way around. Remember dominate means equal to or greater than so this would mean that the object's sensitivity label is equal to or greater than the subject.
According to the OIG, Multi-level security is defined as a class of system-containing information with different sensitivities that simultaneously permits access by users with different security clearances and need-to-know, but prevents users from obtaining access to information for which they lack authorization. The Subject's sensitivity label must be equal to or greater than the object's sensitivity label in order for the subject to have read access to it, no read up.

NEW QUESTION: 348
Which of the following is the preferred way to suppress an electrical fire in an information center?
A. CO2
B. CO2, soda acid, or Halon
C. water or soda acid
D. ABC Rated Dry Chemical
Answer: A (LEAVE A REPLY)
It must be noted that Halon is now banned in most countries or cities.
The reason CO2 is preferred in an information center is the agent is considered a clean agent, as well as non-conductive. The agent evaporates and does not leave a residue on the equipment. CO2 can be hazardous to people so special care must be taken when implemented.
Water may be a sound solution for large physical areas such as warehouses, but it is entirely inappropriate for computer equipment. A water spray can irreparably damage hardware more quickly than encroaching smoke or heat. Gas suppression systems operate to starve the fire of oxygen. In the past, Halon was the choice for gas suppression systems; however, Halon leaves residue, depletes the ozone layer, and can injure nearby personnel.
NOTE FROM CLEMENT:

For the purpose of the exam do not go outside of the 4 choices presented. YES, it is true that there are many other choices that would be more adequate for a Data Centre. An agent such as IG-55 from Ardent would probably be a better choice than CO2, however it is
NOT in the list of choices.
You will also notice that Shon Harris and Krutz and Vines disagree on which one is the best. This is why you must do your own research to supplement the books, sometimes books could be opiniated as well. When in doubt refer to the official book and look at what is ISC2 view of the topic and which one ISC2 considers to be the best for the exam.
ISC2 recommends also the following:
Aero-K - uses an aerosol of microscopic potassium compounds in a carrier gas released from small canisters mounted on walls near the ceiling. The Aero-K generators are not pressurized until fire is detected. The Aero-K system uses multiple fire detectors and will not release until a fire is "confirmed" by two or more detectors (limiting accidental discharge). The gas is non-corrosive, so it does not damage metals or other materials. It does not harm electronic devices or media such as tape or discs. More important, Aero-K is nontoxic and does not injure personnel.
FM-200 - is a colorless, liquefied compressed gas. It is stored as a liquid and dispensed into the hazard as a colorless, electrically non-conductive vapor that is clear and does not obscure vision. It leaves no residue and has acceptable toxicity for use in occupied spaces at design concentration. FM-200 does not displace oxygen and, therefore, is safe for use in occupied spaces without fear of oxygen deprivation.
The following are incorrect choices:
Water or Soda/Acid & Halon: (old water extinguishers) will damage sensitive equipment as well as conduct electricity which could endanger the life of the person using such a fire extinghisher. Halon has been banned due to the Montreal Protocol.
ABC rated Dry chemical extinguishers: They are suitable for electrically energized fires, but they are not acceptable on sensitive equipment. It is like throwing a couple kilograms of flour in around in a room. It is extremely hard to clean off of equipment and some of the chemicals are corrosive in nature.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third
Edition ((ISC)2 Press) (Kindle Locations 25609-25612). Auerbach Publications. Kindle
Edition.
and
http://www.ehs.ucf.edu/labsafe/safemgequip.html
or
http://www.osha.gov/doc/outreachtraining/htmlfiles/extmark.html

NEW QUESTION: 349
Which is a benefit of a guard over an automated control?
A. Guards are cheaper.
B. Guards do not need pre-employment screening.
C. Guards do not need training.
D. Guards can use discriminating judgment.

Answer: D (LEAVE A REPLY)
Guards can use discriminating judgment.
Guards are typically more expensive than automated controls, need
training as to the protection requirements of the specific site, and need to be screened and bonded.

NEW QUESTION: 350
The act of validating a user with a unique and specific identifier is called what?
A. Validation
B. Registration
C. Authentication
D. Authorization
E. Identification
Answer: (SHOW ANSWER)
Authentication is the act of validating a user with a unique and specific identifier.
..

NEW QUESTION: 351
Which of the following is an effective control in preventing electronic cloning of Radio Frequency Identification (RFID) based access cards?
A. Personal Identity Verification (PIV)
B. Cardholder Unique Identifier (CHUID) authentication
C. Physical Access Control System (PACS) repeated attempt detection
D. Asymmetric Card Authentication Key (CAK) challenge-response
Answer: D (LEAVE A REPLY)
Section: Asset Security

NEW QUESTION: 352
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
The effectiveness of the security program can PRIMARILY be measured through
A. audit requirements.
B. risk elimination.
C. audit findings.
D. customer satisfaction.
Answer: (SHOW ANSWER)

NEW QUESTION: 353
During a review of system logs of the enterprise, a security manager discovers that a colleague working on an exercise ran a job to collect confidential information on the company's clients. The

colleague who ran the job has since left the company to work for a competitor. Based on the (ISC) Code of Ethics, which one of the following statements is MOST correct?
-The manager should call the colleague and explain what has been discovered.
The manager should then ask for the return of the information in exchange for silence.
A. The manager should warn the competitor that a potential crime has been committed that could put their company at risk.
B. The manager should inform his or her appropriate company management, and secure the results of the recover exercise for future review.
C. The manager should call the colleague and ask the purpose of running the job prior to informing his or her company management of the situation.
Answer: C (LEAVE A REPLY)
In the references I have not found out anything that directly relates to this but It would be logical to assume the answer of going to necessary management. "ISC2 Code of Ethics.... Not commit or be party to any unlawful or unethical act that may negatively affect their professional reputation or the reputation of their profession. Appropriately report activity related to the profession that they believe to be unlawful and shall cooperate with the resulting investigations." -Ronald Krutz The CISSP PREP Guide (gold edition) pg 440

NEW QUESTION: 354
Which of the following testing method examines the functionality of an application without peering into its internal structure or knowing the details of it's internals?
A. Black-box testing
B. Parallel Test
C. Regression Testing
D. Pilot Testing
Answer: (SHOW ANSWER)
Black-box testing is a method of software testing that examines the functionality of an application (e.g. what the software does) without peering into its internal structures or workings (see white-box testing). This method of test can be applied to virtually every level of software testing: unit, integration, system and acceptance. It typically comprises most if not all higher level testing, but can also dominate unit testing as well.
For your exam you should know the information below:
Alpha and Beta Testing - An alpha version is early version is an early version of the application system submitted to the internal user for testing. The alpha version may not contain all the features planned for the final version. Typically software goes to two stages testing before it consider finished.The first stage is called alpha testing is often performed only by the user within the organization developing the software. The second stage is called beta testing, a form of user acceptance testing, generally involves a limited number of external users. Beta testing is the last stage of testing, and normally involves real world exposure, sending the beta version of the product to independent beta test sites or offering it free to interested user.
Pilot Testing - A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests - usually over interim platform and with only basic functionalities.

White box testing - Assess the effectiveness of a software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's specific logic path. However testing all possible logical path in large information system is not feasible and would be cost prohibitive, and therefore is used on selective basis only.
Black Box Testing - An integrity based form of testing associated with testing components of an information system's "functional" operating effectiveness without regards to any specific internal program structure. Applicable to integration and user acceptance testing.
Function/validation testing - It is similar to system testing but it is often used to test the functionality of the system against the detailed requirements to ensure that the software that has been built is traceable to customer requirements.
Regression Testing - The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.
Parallel Testing - This is the process of feeding test data into two systems - the modified system and an alternative system and comparing the result.
Sociability Testing - The purpose of these tests is to confirm that new or modified system can operate in its target environment without adversely impacting existing system. This should cover not only platform that will perform primary application processing and interface with other system but , in a client server and web development, changes to the desktop environment. Multiple application may run on the users desktop, potentially simultaneously , so it is important to test the impact of installing new dynamic link libraries (DLLs), making operating system registry or configuration file modification, and possibly extra memory utilization.
The following answers are incorrect:
Parallel Testing - This is the process of feeding test data into two systems - the modified system and an alternative system and comparing the result.
Regression Testing - The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.
Pilot Testing - A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests - usually over interim platform and with only basic functionalities
The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 167
Official ISC2 guide to CISSP CBK 3rd Edition Page number 176

NEW QUESTION: 355
Which is NOT a layer in the TCP/IP architecture model?
A. Internet
B. Host-to-host
C. Application
D. Session

Answer: D (LEAVE A REPLY)
The correct answer is Session. The Session Layer is an OSI model layer.

NEW QUESTION: 356
Which of the following is the BEST statement for a professional to include as port of businees continuity (BC) procedure?
A. In incremental data backup must be done after each system change.
B. A full data backup must be done based on the needs of the business.
C. An incremental data backup must be done upon management request.
D. A full data backup must be done upon management request.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 357
What is called the type of access control where there are pairs of elements that have the least upper bound of values and greatest lower bound of values?
A. Mandatory model
B. Discretionary model
C. Lattice model
D. Rule model
Answer: (SHOW ANSWER)
In a lattice model, there are pairs of elements that have the least upper bound of
values and greatest lower bound of values.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION: 358
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 (LEAVE A REPLY)
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

NEW QUESTION: 359
Which one of the following access control models associates every resource and every user of a resource with one of an ordered set of classes?
A. Take-Grant model

B. Biba model
C. Lattice model
D. Clark-Wilson model
Answer: (SHOW ANSWER)
With a lattice model you first have to define a set of security classes that can be assigned to users or objects...After you have defined set of security classes, you define a set flow operations showing when information can flow from one class to another - Roberta Bragg Cissp Certification Training Guide (que) pg 23

NEW QUESTION: 360
Which of the following is defined as a key establishment protocol based on the Diffie-
Hellman algorithm proposed for IPsec but superseded by IKE?
A. Diffie-Hellman Key Exchange Protocol
B. Internet Security Association and Key Management Protocol (ISAKMP)
C. Simple Key-management for Internet Protocols (SKIP)
D. OAKLEY
Answer: D (LEAVE A REPLY)
RFC 2828 (Internet Security Glossary) defines OAKLEY as a key establishment protocol (proposed for IPsec but superseded by IKE) based on the Diffie-
Hellman algorithm and designed to be a compatible component of ISAKMP.
ISAKMP is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism.
SKIP is a key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.
ISAKMP provides a framework for authentication and key exchange but does not define them. ISAKMP is designed to be key exchange independant; that is, it is designed to support many different key exchanges.
Oakley and SKEME each define a method to establish an authenticated key exchange.
This includes payloads construction, the information payloads carry, the order in which they are processed and how they are used.
Oakley describes a series of key exchanges-- called modes and details the services provided by each (e.g. perfect forward secrecy for keys, identity protection, and authentication).
SKEME describes a versatile key exchange technique which provides anonymity, repudiability, and quick key refreshment.
RFC 2049 describes the IKE protocol using part of Oakley and part of SKEME in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for other security associations such as AH and ESP for the IETF IPsec DOI.
While Oakley defines "modes", ISAKMP defines "phases". The relationship between the two is very straightforward and IKE presents different exchanges as modes which operate in one of two phases.
Phase 1 is where the two ISAKMP peers establish a secure, authenticated channel with which to communicate. This is called the ISAKMP Security Association (SA). "Main Mode" and "Aggressive Mode" each accomplish a phase 1 exchange. "Main Mode" and

"Aggressive Mode" MUST ONLY be used in phase 1.
Phase 2 is where Security Associations are negotiated on behalf of services such as IPsec or any other service which needs key material and/or parameter negotiation. "Quick Mode" accomplishes a phase 2 exchange. "Quick Mode" MUST ONLY be used in phase 2.
References:
CISSP: Certified Information Systems Security Professional Study Guide By James
Michael Stewart, Ed Tittel, Mike Chappl, page 397
RFC 2049 at: http://www.ietf.org/rfc/rfc2409
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
The All-in-one CISSP Exam Guide, 3rd Edition, by Shon Harris, page 674
The CISSP and CAP Prep Guide, Platinum Edition, by Krutz and Vines

NEW QUESTION: 361
In non-discretionary access control, a central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on:
A. the society's role in the organization
B. the individual's role in the organization
C. the group-dynamics as they relate to the individual's role in the organization
D. the group-dynamics as they relate to the master-slave role in the organization
Answer: B (LEAVE A REPLY)
Non-Discretionary Access Control. A central authority determines what subjects can have access to certain objects based on organizational security policy. The access controls may be based on the individual's role in the organization (role-based) or the subject's responsibilities and duties (task-based). Pg. 33 Krutz: The CISSP Prep Guide.

NEW QUESTION: 362
In Mandatory Access Control, sensitivity labels attached to object contain what information?
A. The item's classification
B. The item's classification and category set
C. The item's category
D. The items's need to know
Answer: (SHOW ANSWER)
A Sensitivity label must contain at least one classification and one category set.

Category set and Compartment set are synonyms, they mean the same thing. The sensitivity label must contain at least one Classification and at least one Category. It is common in some environments for a single item to belong to multiple categories. The list of all the categories to which an item belongs is called a compartment set or category set.
The following answers are incorrect:
the item's classification. Is incorrect because you need a category set as well.
the item's category. Is incorrect because category set and classification would be both be required.
The item's need to know. Is incorrect because there is no such thing. The need to know is indicated by the catergories the object belongs to. This is NOT the best answer.
Reference(s) used for this question:
OIG CBK, Access Control (pages 186 - 188)
AIO, 3rd Edition, Access Control (pages 162 - 163)
AIO, 4th Edittion, Access Control, pp 212-214.
Wikipedia - http://en.wikipedia.org/wiki/Mandatory_Access_Control

NEW QUESTION: 363
Which of the following is NOT an assumption of the basic Kerberos paradigm?
A. Specific servers and locations cannot be secured.
B. Messages are not secure from interception.
C. Cabling is not secure.
D. Client computers are not secured and are easily accessible.
Answer: (SHOW ANSWER)
The correct answer is "Specific servers and locations cannot be secured". Kerberos requires that centralized servers implementing the trusted authentication mechanism must be secured.

NEW QUESTION: 364
Which of the following should be allowed through a firewall to easy communication and usage by users?
A. RIP
B. IGRP
C. DNS
D. OSPF
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
DNS translates domain names into IP addresses, which enables us to use domain names instead of IP addresses.
Incorrect Answers:
A: RIP is a routing protocol. A routing protocol forwards routing information between routers, but does make it easier for users to communicate.

B: IGRP is a routing protocol. A routing protocol forwards routing information between routers, but does make it easier for users to communicate.
D: OSPF is a routing protocol. A routing protocol forwards routing information between routers, but does make it easier for users to communicate.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 599

NEW QUESTION: 365
IF an operating system permits executable objects to be used simultaneously by multiple users without a refresh of the objects, what security problem is most likely to exist?
A. Disclosure of residual data.
B. Unauthorized obtaining of a privileged execution state.
C. Data leakage through covert channels.
D. Denial of service through a deadly embrace.
Answer: A (LEAVE A REPLY)
This is a well known issue knew by many programmers, since the operating system is allowing the executables to be used by many users in different sessions at the same time, and there is not refreshing every certain time, there will be a disclosure of residual data. To fix this we need to get sure that objects are refreshed frequently, for added security its better an OS that does not allow the use of an executable object by many users at the same time.

NEW QUESTION: 366
Which of the following is an IP address that is private (i.e. reserved for internal networks, and not a valid address to use on the Internet)?
A. 192.168.42.5
B. 192.166.42.5
C. 192.175.42.5
D. 192.1.42.5
Answer: A (LEAVE A REPLY)
This is a valid Class C reserved address. For Class C, the reserved addresses are
192.168.0.0 - 192.168.255.255.
The private IP address ranges are defined within RFC 1918:
RFC 1918 private ip address range
The following answers are incorrect:
192.166.42.5 Is incorrect because it is not a Class C reserved address.
192.175.42.5 Is incorrect because it is not a Class C reserved address.
192.1.42.5 Is incorrect because it is not a Class C reserved address.

NEW QUESTION: 367
A manufacturing organization wants to establish a Federated Identity Management (FIM) system with its 20 different supplier companies. Which of the following is the BEST solution for the manufacturing organization?

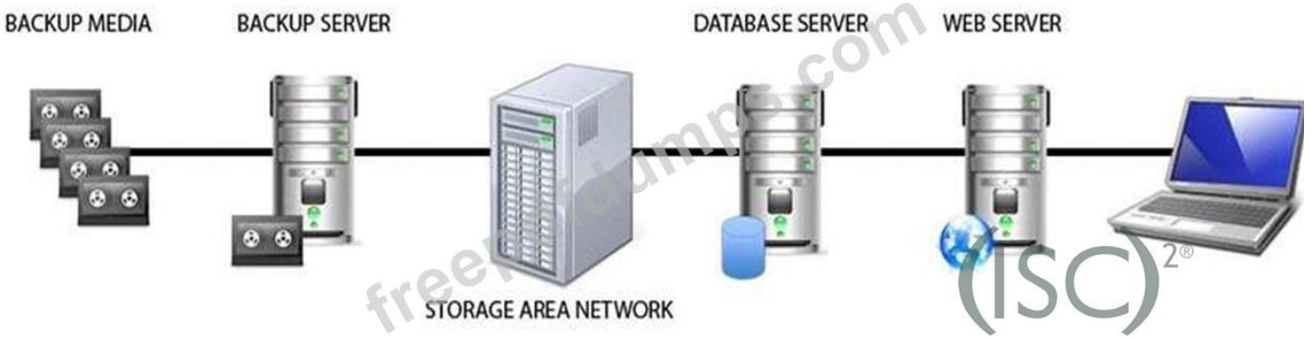
A. Trusted third-party certification
B. Lightweight Directory Access Protocol (LDAP)
C. Security Assertion Markup language (SAML)
D. Cross-certification
Answer: C (LEAVE A REPLY)
Section: Identity and Access Management (IAM)
Explanation/Reference: https://www.netiq.com/documentation/access-manager-43/applications-configuration-guide/ data/b1ka6lkd.html

NEW QUESTION: 368
Which of the following questions will be addressed through the use of a Privacy Impact Assessment (PIA)?
A. How the information is to be maintained
B. Why the information is to be collected
C. What information is to be destroyed
D. Where the information is to be stored
Answer: (SHOW ANSWER)
Section: Mixed questions

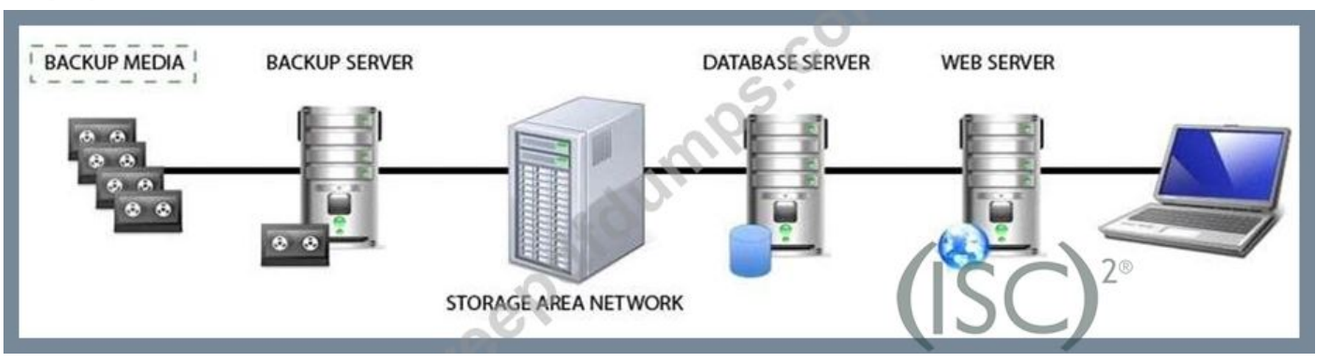
NEW QUESTION: 369
Which Orange book security rating is the FIRST to be concerned with covert channels?
A. A1
B. B3
C. B2
D. B1
Answer: C (LEAVE A REPLY)
This class ("Structured Protection") requires more stringent authentication mechanisms and well-defined interfaces between layers. Subjects and devices require labels and the system must not allow covert channels.
A1 is incorrect. A1 is also called "Verified Design" and requires formal verification of the design and specifications.
B3 is incorrect. B3 is also called "Security Domains" and imposes more granularity in each protection mechanism.
B1 is incorrect. B1 is also called "Labeled Security" and each data object must have a classification label and each subject a clearance label. On each access attempt, the classification and clearance are checked to verify that the access is permissible.
EXAM TIP:
The CBK only discusses the TCSEC in a very minimal fashion and the details are presented in a much more completely in the Shon Harris, All In One book. Folk wisdom has it that this reflects the CBK/security industry migration away from the TCSEC to the CC but the wise candidate will develop at least some familiarity with the TCSEC. There are still questions on TCSEC showing up randomly on the exam.

NOTE FROM CLEMENT:
As of today (April 2014) subjects such as the TCSEC are still proclaimed to be on the exam. Do make sure that you take some time to review the TCSEC ratings.
You can download a nice one page resume of the TCSEC rating at the following link:
https://www.freepracticetests.org/documents/tcsec.pdf
Do study this one page document and get familiar with what is being introduced at each of the TCSEC levels. Good questions might be for example:
1.At what level are labels introduced?
2.At what level is the Security Administrator role defined?
3.At what level are covert channel first introduced?
4.At what level do you use formal methods?
References:
The Official ISC2 CBK study guide, pages 329 - 330.
AIO3, pp. 302 - 306
AIOv4 Security Architecture and Design (pages 357 - 361)
AIOv5 Security Architecture and Design (pages 358 - 362)

NEW QUESTION: 370
Identify the component that MOST likely lacks digital accountability related to information access.
Click on the correct device in the image below.



Answer:



Explanation
Backup Media
Reference: Official (ISC)2 Guide to the CISSP CBK, Third Edition page 1029

NEW QUESTION: 371
Which of the following statements pertaining to biometrics is false?
A. Increased system sensitivity can cause a higher false rejection rate
B. The crossover error rate is the point at which false rejection rate equals the false acceptance rate.
C. False acceptance rate is also known as Type II error.
D. Biometrics are based on the Type 2 authentication mechanism.
Answer: D (LEAVE A REPLY)
Authentication is based on three factor types: type 1 is something you know, type 2 is something you have and type 3 is something you are. Biometrics are based on the
Type 3 authentication mechanism.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the
Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 37).

NEW QUESTION: 372
Out of the steps listed below, which one is not one of the steps conducted during the Business Impact Analysis (BIA)?
A. Alternate site selection
B. Create data-gathering techniques
C. Identify the company's critical business functions
D. Select individuals to interview for data gathering
Answer: A (LEAVE A REPLY)
Selecting and Alternate Site would not be done within the initial BIA. It would be done at a later stage of the BCP and DRP recovery effort. All of the other choices were steps that would be conducted during the BIA. See below the list of steps that would be done during the BIA.
A BIA (business impact analysis) is considered a functional analysis, in which a team collects data through interviews and documentary sources; documents business functions, activities, and transactions ; develops a hierarchy of business functions; and finally applies a classification scheme to indicate each individual function's criticality level.
BIA Steps
1.Select individuals to interview for data gathering.
2.Create data-gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).
3.Identify the company's critical business functions.
4.Identify the resources these functions depend upon.
5.Calculate how long these functions can survive without these resources.
6.Identify vulnerabilities and threats to these functions.
7.Calculate the risk for each different business function.
8.Document findings and report them to management.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 905-909). McGraw-Hill.
Kindle Edition.

NEW QUESTION: 373
In the Software Development Life Cycle (SDLC), maintaining accurate hardware and software inventories is a critical part of
A. systems integration.
B. risk management.
C. quality assurance.
D. change management.
Answer: D (LEAVE A REPLY)
Section: Software Development Security

NEW QUESTION: 374
In addition to accuracy, a biometric system has additional factors that determine its effectiveness. Which one of the following listed items is
NOT one of these additional factors?
A. Corpus
B. Throughput rate
C. Enrollment time
D. Acceptability
Answer: A (LEAVE A REPLY)
A corpus is a biometric term that refers to collected biometric images. The corpus is stored in a database of images. Potential sources of error are the corruption of images during collection and mislabeling or other transcription problems associated with the database. Therefore, the image collection, process and storage must be performed carefully with constant checking. These images are collected during the enrollment process and thus, are critical to the correct operation of the biometric device. In enrollment, images are collected and features are extracted, but no comparison occurs. The information is stored for use in future comparison steps. Answer a, the throughput rate, refers to the rate at which individuals, once enrolled, can be processed by a biometric system. If an individual is being authenticated, the biometric system will take a sample of the individual's characteristic to be evaluated and compare it to a template. A metric called distance is used to determine if the sample matches the template. Distance is the difference between the quantitative measure of the sample and the template. If the distance falls within a threshold value, a match is declared. If not, there is no match.
* Answer "acceptability" is determined by privacy issues, invasiveness, and psychological and physical comfort when using the biometric system.
*"Enrollment time" is the time it takes to initially register with a system by providing samples of the biometric characteristic to be evaluated.

NEW QUESTION: 375
The Clark-Wilson Integrity Model (d. Clark, d. Wilson, A Comparison
of Commercial and Military Computer Security Policies, Proceedings of
the 1987 IEEE Computer Society Symposium on Research in Security and
Privacy, Los Alamitos, CA, IEEE Computer Society Press, 1987) focuses on what two concepts?
A. Capability lists and domains
B. Least privilege and well-formed transactions
C. Separation of duty and well-formed transactions
D. Well-formed transactions and denial of service
Answer: (SHOW ANSWER)
The Clark-Wilson Model is a model focused on the needs of the commercial world and is based on the theory that integrity is more important than confidentiality for commercial organizations. Further, the model incorporates the commercial concepts of separation of duty and wellformed transactions. The well-formed transaction of the model is implemented by the transformation procedure (TP.)ATP is defined in the model as the mechanism for transforming the set of constrained data items (CDIs) from one valid state of integrity to another valid state of integrity. The
Clark-Wilson Model defines rules for separation of duty that denote the relations between a user, TPs, and the CDIs that can be operated upon by those TPs. The model talks about the access triple that is the user, the program that is permitted to operate on the data, and the data. The other answers are distracters.

NEW QUESTION: 376
In addition to the Legal Department, with what company function must the collection of physical evidence be coordinated if an employee is suspected?
A. Human Resources
B. Industrial Security
C. Public Relations
D. External Audit Group
Answer: A (LEAVE A REPLY)
If an employee is suspected of causing an incident, the human resources department may be involved-for example, in assisting with disciplinary proceedings.
Legal Department. The legal experts should review incident response plans, policies, and procedures to ensure their compliance with law and Federal guidance, including the right to privacy. In addition, the guidance of the general counsel or legal department should be sought if there is reason to believe that an incident may have legal ramifications, including evidence collection, prosecution of a suspect, or a lawsuit, or if there may be a need for a memorandum of understanding (MOU) or other binding agreements involving liability limitations for information sharing.
Public Affairs, Public Relations, and Media Relations. Depending on the nature and impact of an incident, a need may exist to inform the media and, by extension, the public.
The Incident response team members could include:
Management Information Security Legal / Human Resources Public Relations Communications

Physical Security
Network Security
Network and System Administrators
Network and System Security Administrators
Internal Audit
Events versus Incidents
An event is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data. This guide addresses only adverse events that are computer security- related, not those caused by natural disasters, power failures, etc.
A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
Examples of incidents are:
An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
Users are tricked into opening a "quarterly report" sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
A user provides or exposes sensitive information to others through peer-to-peer file sharing services.
The following answers are incorrect:
Industrial Security. Is incorrect because it is not the best answer, the human resource department must be involved with the collection of physical evidence if an employee is suspected.
public relations. Is incorrect because it is not the best answer. It would be an important element to minimize public image damage but not the best choice for this question.
External Audit Group. Is incorrect because it is not the best answer, the human resource department must be involved with the collection of physical evidence if an employee is suspected.
Reference(s) used for this question: NIST Special Publication 800-61

NEW QUESTION: 377
What uses a key of the same length as the message where each bit or character from the plaintext is encrypted by a modular addition?
A. Running key cipher
B. One-time pad
C. Steganography
D. Cipher block chaining
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
In cryptography, the one-time pad (OTP) is an encryption technique that cannot be cracked if used correctly. In this technique, a plaintext is paired with a random secret key (also referred to as a one-time pad). Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition. If the key is truly random, is at least as long as the plaintext, is never reused in whole or in part, and is kept completely secret, then the resulting ciphertext will be impossible to decrypt or break. However, practical problems have prevented one-time pads from being widely used.
The "pad" part of the name comes from early implementations where the key material was distributed as a pad of paper, so that the top sheet could be easily torn off and destroyed after use.
The one-time pad has serious drawbacks in practice because it requires:
Truly random (as opposed to pseudorandom) one-time pad values, which is a non-trivial requirement.
▪
Secure generation and exchange of the one-time pad values, which must be at least as long as the
▪
message. (The security of the one-time pad is only as secure as the security of the one-time pad exchange).
Careful treatment to make sure that it continues to remain secret, and is disposed of correctly
▪
preventing any reuse in whole or part-hence "one time".
Because the pad, like all shared secrets, must be passed and kept secure, and the pad has to be at least as long as the message, there is often no point in using one-time padding, as one can simply send the plain text instead of the pad (as both can be the same size and have to be sent securely).
Distributing very long one-time pad keys is inconvenient and usually poses a significant security risk. The pad is essentially the encryption key, but unlike keys for modern ciphers, it must be extremely long and is much too difficult for humans to remember. Storage media such as thumb drives, DVD-Rs or personal digital audio players can be used to carry a very large one-time-pad from place to place in a non- suspicious way, but even so the need to transport the pad physically is a burden compared to the key negotiation protocols of a modern public-key cryptosystem, and such media cannot reliably be erased securely by any means short of physical destruction (e.g., incineration).
The key material must be securely disposed of after use, to ensure the key material is never reused and to protect the messages sent. Because the key material must be transported from one endpoint to another, and persist until the message is sent or received, it can be more vulnerable to forensic recovery than the transient plaintext it protects.
Incorrect Answers:
A: Running key cipher does not use a key of the same length as the message.

C: Steganography is a method of hiding data in another media type so the very existence of the data is concealed. This is not what is described in the question.
D: Cipher block chaining is an encryption method where each block of text, the key, and the value based on the previous block are processed in the algorithm and applied to the next block of text. This is not what is described in the question.
References:
https://en.wikipedia.org/wiki/One-time_pad

NEW QUESTION: 378
Which of the following technologies has been developed to support TCP/IP networking over low-speed serial interfaces?
A. ISDN
B. SLIP
C. xDSL
D. T1
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Serial Line Internet Protocol (SLIP) is an older technology developed to support TCP/IP communications over asynchronous serial connections, such as serial cables or modem dial - up.
Incorrect Answers:
A: ISDN can be considered a suite of digital services existing on layers 1, 2, and 3 of the OSI model. ISDN is digital, not serial.
C: xDSL is a digital technology. xDSL is the term for the Broadband Access technologies based on Digital Subscriber Line (DSL) technology D: The T1 carrier is the most commonly used digital, not serial, transmission service.
References:
Stewart, James M., Ed Tittel, and Mike Chapple, CISSP: Certified Information Systems Security Professional Study Guide, 5th Edition, Sybex, Indianapolis, 2011, p. 138

NEW QUESTION: 379
Refer to the information below to answer the question.
A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns.
What MUST the plan include in order to reduce client-side exploitation?
A. Employee education
B. Approved web browsers
C. Network firewall procedures
D. Proxy configuration
Answer: (SHOW ANSWER)

NEW QUESTION: 380
What is the maximum allowable key size of the Rijndael encryption algorithm?
A. 128 bits
B. 192 bits
C. 256 bits
D. 512 bits
Answer: C (LEAVE A REPLY)
The Rijndael algorithm, chosen as the Advanced Encryption Standard (AES) to
replace DES, can be categorized as an iterated block cipher with a variable block length and key length that can be independently chosen as 128, 192 or 256 bits.
Below you have a summary of the differences between AES and Rijndael.
AES is the advanced encryption standard defined by FIPS 197. It is implemented differently than Rijndael:
FIPS-197 specifies that the block size must always be 128 bits in AES, and that the key size may be either 128, 192, or 256 bits. Therefore AES-128, AES-192, and AES-256 are actually:
Key Size (bits) Number of rounds
Block Size (bits)
AES-128
128 10 Rounds
128
AES-192
192 12 Rounds
128
AES-256
256 14 Rounds
128
Some book will say "up to 9 rounds will be done with a 128 bits keys". Really it is 10 rounds because you must include round zero which is the first round.
By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.
Reference(s) used for this question: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 153). and FIPS 197 and https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

NEW QUESTION: 381
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.

Following best practice, where should the permitted access for each department and job classification combination be specified?
A. Human resource policy
B. Human resource standards
C. Security standards
D. Security procedures
Answer: C (LEAVE A REPLY)

NEW QUESTION: 382
Related to information security, the guarantee that the message sent is the message received with the assurance that the message was not intentionally or unintentionally altered is an example of which of the following?
A. Integrity
B. Confidentiality
C. Availability
D. Identity
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Information must be accurate, complete, and protected from unauthorized modification. When a security mechanism provides integrity, it protects data, or a resource, from being altered in an unauthorized fashion. If any type of illegitimate modification does occur, the security mechanism must alert the user or administrator in some manner.
Hashing can be used in emails to guarantee that the message sent is the message received with the assurance that the message was not intentionally or unintentionally altered.
Incorrect Answers:
B: Confidentiality is the assurance that information is not disclosed to unauthorized individuals, programs, or processes. This is not what is described in the question.
C: Availability ensures reliability and timely access to data and resources to authorized individuals. This is not what is described in the question.
D: Identity would be the sender or recipient of the email message. It does not guarantee that the message sent is the message received with the assurance that the message was not intentionally or unintentionally altered.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, pp. 23, 159

NEW QUESTION: 383
Which of the following biometric devices has the lowest user acceptance level?
A. Retina Scan
B. Fingerprint scan
C. Hand geometry

D. Signature recognition

Answer: A (LEAVE A REPLY)

According to the cited reference, of the given options, the Retina scan has the lowest user acceptance level as it is needed for the user to get his eye close to a device and it is not user friendly and very intrusive. However, retina scan is the most precise with about one error per 10 millions usage.

Look at the 2 tables below. If necessary right click on the image and save it on your desktop for a larger view or visit the web site directly at

https://sites.google.com/site/biometricsecuritysolutions/crossover-accuracy .

Biometric Comparison Chart

Biometric Aspect Descriptions

Reference(s) used for this question:

RHODES, Keith A., Chief Technologist, United States General Accounting Office, National Preparedness, Technologies to Secure Federal Buildings, April 2002 (page 10).

and

https://sites.google.com/site/biometricsecuritysolutions/crossover-accuracy

NEW QUESTION: 384

Which of the following is NOT a media viability control used to protect the viability of data storage media?

A. clearing

B. marking

C. handling

D. storage

Answer: A (LEAVE A REPLY)

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, pages 231, 348. Marking, handling and storage are all media viability controls used to protect the viability of data storage media.

NEW QUESTION: 385

Which of the following is not a form of passive attack?

A. Scavenging

B. Data diddling

C. Shoulder surfing

D. Sniffing

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Explanation:

Details: Data diddling involves alteration of existing data and is extremely common. It is one of the easiest types of crimes to prevent by using access and accounting controls, supervision, auditing, separation of duties, and authorization limits. It is a form of active attack. All other choices are examples of passive attacks, only affecting confidentiality.

References: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGrawHill/Osborne, 2002, Chapter 10: Law, Investigation, and Ethics (page 645).

NEW QUESTION: 386
Which of the following media is MOST resistant to tapping?
A. microwave.
B. twisted pair.
C. coaxial cable.
D. fiber optic.
Answer: D (LEAVE A REPLY)
Fiber Optic is the most resistant to tapping because Fiber Optic uses a light to transmit the signal. While there are some technologies that will allow to monitor the line passively, it is very difficult to tap into without detection sot this technology would be the MOST resistent to tapping.
The following answers are in correct:
microwave. Is incorrect because microwave transmissions can be intercepted if in the path of the broadcast without detection.
twisted pair. Is incorrect because it is easy to tap into a twisted pair line.
coaxial cable. Is incorrect because it is easy to tap into a coaxial cable line.

NEW QUESTION: 387
Which one of these is a basic firewall?
A. Packet Filtering Firewalls
B. Proxy Firewalls
C. All of the above
D. None of the above
Answer: A (LEAVE A REPLY)
Packet Filtering Firewall - only examines an IP packet based on Source IP (SIP), Destination IP (DIP), Source Port and Destination Port for both UDP and TCP by subjecting each IP packet to an Access Control List.

NEW QUESTION: 388
Which of the following refers to the number of columns in a relation?
A. degree
B. depth
C. breadth
D. cardinality
Answer: A (LEAVE A REPLY)

NEW QUESTION: 389
The theft of a laptop poses a threat to which tenet of the C.I.A. triad?
A. All of the above

B. Availability
C. Integrity
D. Confidentiality
Answer: A (LEAVE A REPLY)
The correct answer is confidentiality, because the data can now
be read by someone outside of a monitored environment; availability,
because the user has lost the computing ability provided by the unit;
and integrity, because the data residing on and any telecommunications
from the portable are now suspect.

NEW QUESTION: 390
Which of the following is NOT a precaution you can take to reduce static electricity?
A. anti-static flooding
B. maintain proper humidity levels
C. power line conditioning
D. anti-static sprays
Answer: C (LEAVE A REPLY)

NEW QUESTION: 391
A business continuity plan is an example of which of the following?
A. Corrective control
B. Detective control
C. Preventive control
D. Compensating control
Answer: A (LEAVE A REPLY)
Business Continuity Plans are designed to minimize the damage done by the event,
and facilitate rapid restoration of the organization to its full operational capacity. They are for use
"after the fact", thus are examples of corrective controls.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of
Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and
Disaster Recovery Planning (page 273).
and
Conrad, Eric; Misenar, Seth; Feldman, Joshua (2012-09-01). CISSP Study Guide (Kindle Location
8069). Elsevier Science (reference). Kindle Edition.
and

NEW QUESTION: 392
Which of the following is the BIGGEST concern with firewall security?
A. Internal hackers
B. Complex configuration rules leading to misconfiguration
C. Buffer overflows
D. Distributed denial of service (DDoS) attacks
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Firewalls filter traffic based on a defined set of rules. The rules must be configured correctly for the firewall to provide the intended security.
Incorrect Answers:
A: Firewalls main duty is to defend against external, not internal, threats.
C: Firewalls do not product from buffer overflows attacks.
D: Firewalls can help in defending from DDoS attacks, but the main concern with firewall is to configure them correctly.
References:
Stewart, James M., Ed Tittel, and Mike Chapple, CISSP: Certified Information Systems Security Professional Study Guide, 5th Edition, Sybex, Indianapolis, 2011, p. 25

NEW QUESTION: 393
Biometrics is used for identification in the physical controls and for
authentication in the:
A. Detective controls.
B. Corrective controls.
C. Logical controls.
D. Preventive controls.
Answer: C (LEAVE A REPLY)
The correct answer is "Logical controls". The other answers are different categories of controls where preventive controls attempt to eliminate or reduce vulnerabilities before an attack occurs; detective controls attempt to determine that an attack is taking place or has taken place; and corrective controls involve taking action to restore the system to normal operation after a successful attack.

NEW QUESTION: 394
Which of the following is a communication mechanism that enables direct conversation between two applications?
A. DDE

B. OLE
C. ODBC
D. DCOM
Answer: A (LEAVE A REPLY)
"Dynamic Data Exchange (DDE) enables applications to share data by providing IPC. It is based on the client/server model and enables two programs to send commands to each other directly. DDE is a communication mechanism that enables direct conversation between two applications. The source of the data is called the server, and the receiver of the data is the client." Pg. 718 Shon Harris: All-In-One CISSP Certification Exam Guide

NEW QUESTION: 395
Non-Discretionary Access Control. A central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on?
A. The societies role in the organization.
B. The individual's role in the organization.
C. The group-dynamics as they relate to the individual's role in the organization.
D. The group-dynamics as they relate to the master-slave role in the organization.
Answer: B (LEAVE A REPLY)
An access control model defines a computer and/or network system's rules for user access to information resources. Access control models provide confidentiality, integrity and also provide accountability through audit trails. An audit trail documents the access of an object by a subject with a record of what operations were performed. Operations include: read, write, execute and own. Non-Discretionary Access Control is usually role-based, centrally administered with authorization decisions based on the roles individuals have within an organization (e.g. bank teller, loan officer, etc. in a banking model). A system's security administrator grants and/or revokes system privileges based on a user's role. This model works well for corporations with a large turnover of personnel.

NEW QUESTION: 396
Phreakers are hackers who specialize in telephone fraud. What type of telephone fraud manipulates the line voltage to receive a toll-free call?
A. Blue boxes
B. White boxes
C. Black boxes
D. Red boxes
Answer: (SHOW ANSWER)

NEW QUESTION: 397
What is RAD?
A. A development methodology
B. A project management technique
C. A measure of system complexity

D. Risk-assessment diagramming

Answer: A (LEAVE A REPLY)

RAD stands for Rapid Application Development.

RAD is a methodology that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality.

RAD is a programming system that enables programmers to quickly build working programs.

In general, RAD systems provide a number of tools to help build graphical user interfaces that would normally take a large development effort.

Two of the most popular RAD systems for Windows are Visual Basic and Delphi. Historically, RAD systems have tended to emphasize reducing development time, sometimes at the expense of generating in-efficient executable code. Nowadays, though, many RAD systems produce extremely faster code that is optimized.

Conversely, many traditional programming environments now come with a number of visual tools to aid development. Therefore, the line between RAD systems and other development environments has become blurred.

Reference:

Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 307)

http://www.webopedia.com

NEW QUESTION: 398

A periodic review of user account management should NOT determine:

A. conformity with the concept of least privilege.

B. whether active accounts are still being used.

C. strength of user-chosen passwords.

D. whether management authorizations are up-to-date.

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation:

Organizations should have a process for (1) requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.

Reviews should examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth. These reviews can be conducted on at least two levels: (1) on an application-by-application basis, or (2) on a system wide basis.

The strength of user passwords is beyond the scope of a simple user account management review, since it requires specific tools to try and crack the password file/database through either a dictionary or brute-force attack in order to check the strength of passwords.

Incorrect Answers:

A: A periodic review of user account management should determine conformity with the concept of least privilege.
B: A periodic review of user account management should determine whether active accounts are still being used.
D: A periodic review of user account management should determine whether management authorizations are up-to-date.

NEW QUESTION: 399
Which of the following test makes sure the modified or new system includes appropriate access controls and does not introduce any security holes that might compromise other systems?
A. Recovery testing
B. Security testing
C. Stress/volume testing
D. Interface testing
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Security testing tests all security mechanisms and features within a system to determine the level of protection they provide. Security testing can include authorization testing, penetration testing, formal design and implementation verification, and functional testing.
Authorization testing is the process of determining that a requester is allowed to receive a service or perform an operation. Access control is an example of authorization.
Incorrect Answers:
A: Recovery testing is the activity of testing how well an application is able to recover from crashes, hardware failures and other similar problems. Recovery testing does not test access control and does not find any security holes.
C: Stress testing is a form of deliberately intense or thorough testing used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results. Stress testing does not test access control and does not find any security holes.
D: Interface testing can be used to check the handling of data passed between various units, or subsystem components, beyond full integration testing between those units. Interface testing does not test access control and does not find any security holes.
References:
Conrad, Eric, Seth Misenar and Joshua Feldman, CISSP Study Guide, 2nd Edition, Syngress, Waltham, 2012, p. 14

NEW QUESTION: 400
What is used to protect programs from all unauthorized modification or executional interference?
A. A protection domain
B. A security perimeter
C. Security labels

D. Abstraction

Answer: A (LEAVE A REPLY)

A protection domain consists of the execution and memory space assigned to each process. The purpose of establishing a protection domain is to protect programs from all unauthorized modification or executional interference. The security perimeter is the boundary that separates the Trusted Computing Base (TCB) from the remainder of the system. Security labels are assigned to resources to denote a type of classification. Abstraction is a way to protect resources in the fact that it involves viewing system components at a high level and ignoring its specific details, thus performing information hiding.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architecture and Models (page 193).

NEW QUESTION: 401

Within the OSI model, at what layer are some of the SLIP, CSLIP, PPP control functions provided?

A. Data Link

B. Transport

C. Presentation

D. Application

Answer: (SHOW ANSWER)

RFC 1661 - The Point-to-Point Protocol (PPP) specifies that the Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP is comprised of three main components:

1 A method for encapsulating multi-protocol datagrams.

2 A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection.

3 A family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols.

NEW QUESTION: 402

Which of the following is responsible for MOST of the security issues?

A. Outside espionage

B. Hackers

C. Personnel

D. Equipment failure

Answer: (SHOW ANSWER)

Personnel cause more security issues than hacker attacks, outside espionage, or equipment failure.

The following answers are incorrect because:

Outside espionage is incorrect as it is not the best answer.

Hackers is also incorrect as it is not the best answer.

Equipment failure is also incorrect as it is not the best answer.

Reference : Shon Harris AIO v3 , Chapter-3: Security Management Practices , Page : 56

NEW QUESTION: 403
What is an important characteristic of Role Based Access Control (RBAC)?
A. Requires two factor authentication
B. Relies on rotation of duties
C. Supports Mandatory Access Control (MAC)
D. Simplifies the management of access rights
Answer: D (LEAVE A REPLY)

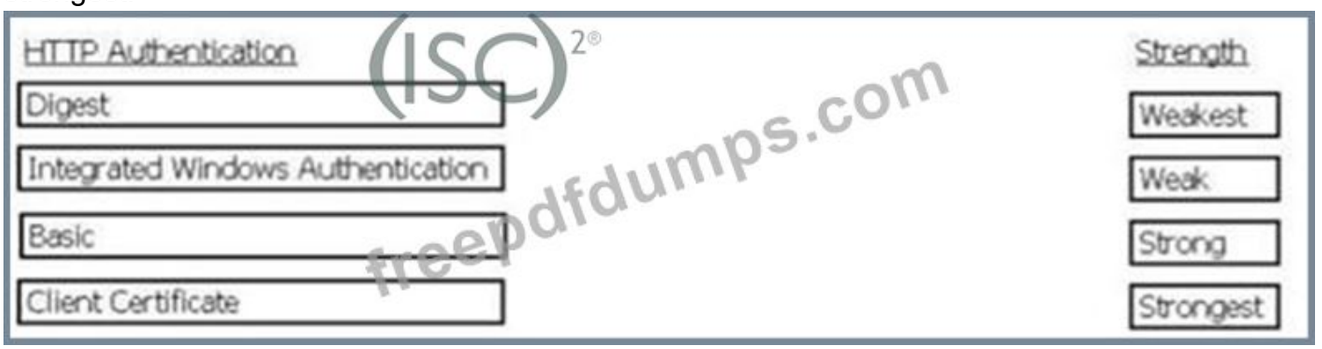
NEW QUESTION: 404
When implementing controls in a heterogeneous end-point network for an organization, it is critical that
A. firewalls running on each host are fully customizable by the user.
B. users can make modifications to their security software configurations.
C. hosts are able to establish network communications.
D. common software security components be implemented across all hosts.
Answer: (SHOW ANSWER)

NEW QUESTION: 405
Which of the following refers to the number of columns in a table?
A. Cardinality
B. Schema
C. Degree
D. Relation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 406
An organization regularly conducts its own penetration tests. Which of the following scenarios MUST be covered for the test to be effective?
A. Internal user accidentally accessing data
B. Third-party vendor with access to the system
C. Internal attacker with access to the system
D. System administrator access compromised
Answer: D (LEAVE A REPLY)

NEW QUESTION: 407
In order for a security policy to be effective within an organization, it MUST include
A. owner information and date of last revision.
B. a list of all standards that apply to the policy.
C. strong statements that clearly define the problem.
D. disciplinary measures for non compliance.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 408
Drag and Drop Question
Rank the Hypertext Transfer protocol (HTTP) authentication types shows below in order of relative strength.
Drag the authentication type on the correct positions on the right according to strength from weakest to strongest.



Answer:

NEW QUESTION: 409
What is NOT an authentication method within IKE and IPsec?
A. CHAP
B. Pre shared key
C. certificate based authentication
D. Public key authentication
Answer: A (LEAVE A REPLY)
CHAP is not used within IPSEC or IKE. CHAP is an authentication scheme used by
Point to Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake. This happens at the time of establishing the initial link (LCP), and may happen again at any time afterwards. The verification is based on a shared secret (such as the client user's password).
After the completion of the link establishment phase, the authenticator sends a "challenge"

message to the peer.
The peer responds with a value calculated using a one-way hash function on the challenge and the secret combined.
The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authenticator acknowledges the authentication; otherwise it should terminate the connection.
At random intervals the authenticator sends a new challenge to the peer and repeats steps 1 through 3.
The following were incorrect answers:
Pre Shared Keys
In cryptography, a pre-shared key or PSK is a shared secret which was previously shared between the two parties using some secure channel before it needs to be used. To build a key from shared secret, the key derivation function should be used. Such systems almost always use symmetric key cryptographic algorithms. The term PSK is used in WiFi encryption such as WEP or WPA, where both the wireless access points (AP) and all clients share the same key.
The characteristics of this secret or key are determined by the system which uses it; some system designs require that such keys be in a particular format. It can be a password like 'bret13i', a passphrase like 'Idaho hung gear id gene', or a hexadecimal string like '65E4 E556 8622 EEE1'. The secret is used by all systems involved in the cryptographic processes used to secure the traffic between the systems. Certificat Based Authentication
The most common form of trusted authentication between parties in the wide world of Web commerce is the exchange of certificates. A certificate is a digital document that at a minimum includes a Distinguished Name (DN) and an associated public key.
The certificate is digitally signed by a trusted third party known as the Certificate Authority (CA). The CA vouches for the authenticity of the certificate holder. Each principal in the transaction presents certificate as its credentials. The recipient then validates the certificate's signature against its cache of known and trusted CA certificates. A "personal certificate" identifies an end user in a transaction; a "server certificate" identifies the service provider.
Generally, certificate formats follow the X.509 Version 3 standard. X.509 is part of the Open Systems Interconnect (OSI) X.500 specification.
Public Key Authentication Public key authentication is an alternative means of identifying yourself to a login server, instead of typing a password. It is more secure and more flexible, but more difficult to set up.
In conventional password authentication, you prove you are who you claim to be by proving that you know the correct password. The only way to prove you know the password is to tell the server what you think the password is. This means that if the server has been hacked, or spoofed an attacker can learn your password.
Public key authentication solves this problem. You generate a key pair, consisting of a public key (which everybody is allowed to know) and a private key (which you keep secret and do not give to anybody). The private key is able to generate signatures. A signature created using your private key cannot be forged by anybody who does not have a copy of that private key; but anybody who has your public key can verify that a particular signature is genuine.

So you generate a key pair on your own computer, and you copy the public key to the server. Then, when the server asks you to prove who you are, you can generate a signature using your private key. The server can verify that signature (since it has your public key) and allow you to log in. Now if the server is hacked or spoofed, the attacker does not gain your private key or password; they only gain one signature. And signatures cannot be re-used, so they have gained nothing.
There is a problem with this: if your private key is stored unprotected on your own computer, then anybody who gains access to your computer will be able to generate signatures as if they were you. So they will be able to log in to your server under your account. For this reason, your private key is usually encrypted when it is stored on your local machine, using a passphrase of your choice. In order to generate a signature, you must decrypt the key, so you have to type your passphrase. References:
RFC 2409: The Internet Key Exchange (IKE); DORASWAMY, Naganand & HARKINS, Dan Ipsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, 1999, Prentice Hall PTR; SMITH, Richard E. Internet Cryptography, 1997, Addison-Wesley Pub Co.; HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 467. http://en.wikipedia.org/wiki/Pre-shared_key
http://www.home.umk.pl/~mgw/LDAP/RS.C4.JUN.97.pdf
http://the.earth.li/~sgtatham/putty/0.55/htmldoc/Chapter8.html#S8.1

NEW QUESTION: 410
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
What MUST the access control logs contain in addition to the identifier?
A. Security classification
B. Denied access attempts
C. Associated clearance
D. Time of the access
Answer: D (LEAVE A REPLY)

NEW QUESTION: 411
What does the protocol RARP do?
A. Sends messages to the devices regarding the health of the network
B. Facilitates file transfers
C. Takes an IP address and finds out the MAC address to which it belongs
D. Takes a MAC address and finds an IP address to match
Answer: (SHOW ANSWER)
The correct answer is "Takes a MAC address and finds an IP address to match", the reverse of ARP. The Reverse Address Resolution Protocol knows a MAC (Media Access Control) address and asks the RARP server to match it with an IP address.

NEW QUESTION: 412
Unshielded Twisted Pair cabling is a:
A. four-pair wire medium that is used in a variety of networks.
B. three-pair wire medium that is used in a variety of networks.
C. two-pair wire medium that is used in a variety of networks.
D. one-pair wire medium that is used in a variety of networks.
Answer: A (LEAVE A REPLY)
Unshielded Twisted Pair cabling is a four-pair wire medium that is used in a variety of networks Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 101.

NEW QUESTION: 413
Computer-generated evidence is considered:
A. Best evidence
B. Second hand evidence
C. Demonstrative evidence
D. Direct evidence
Answer: (SHOW ANSWER)
Computer-generated evidence normally falls under the category of hearsay evidence, or second-hand evidence, because it cannot be proven accurate and reliable. Under the
U.S. Federal Rules of Evidence, hearsay evidence is generally not admissible in court. Best evidence is original or primary evidence rather than a copy or duplicate of the evidence. It does not apply to computer-generated evidence. Direct evidence is oral testimony by witness. Demonstrative evidence are used to aid the jury (models, illustrations, charts).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 9: Law, Investigation, and
Ethics (page 310).
And: ROTHKE, Ben, CISSP CBK Review presentation on domain 9.

NEW QUESTION: 414
Which authentication technique BEST protects against hijacking?
A. Static authentication
B. Continuous authentication
C. Robust authentication
D. Strong authentication
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
There are three major types of authentication available: static, robust, and continuous. Static authentication includes passwords and other techniques that can be compromised through replay attacks. They are often

called reusable passwords. Robust authentication involves the use of cryptography or other techniques to create one-time passwords that are used to create sessions. These can be compromised by session hijacking. Continuous authentication prevents session hijacking.
Continuous Authentication provides protection against impostors who can see, alter, and insert information passed between the claimant and verifier even after the claimant/verifier authentication is complete. These are typically referred to as active attacks, since they assume that the imposter can actively influence the connection between claimant and verifier. One way to provide this form of authentication is to apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier. There are other combinations of cryptography that can provide this form of authentication but current strategies rely on applying some type of cryptography to every bit of data sent. Otherwise, any unprotected bit would be suspect.
Incorrect Answers:
A: Static authentication only provides protection against attacks in which an imposter cannot see, insert or alter the information passed between the claimant and the verifier during an authentication exchange and subsequent session. Static authentication does not protect against hijacking.
C: Robust Authentication relies on dynamic authentication data that changes with each authenticated session between a claimant and verifier. Robust or dynamic authentication does not protect against hijacking.
D: Strong authentication is not a specific authentication type; it is another term for multi-factor authentication.
References:
http://www.windowsecurity.com/whitepapers/policy_and_standards/Internet_Security_Policy/Internet_Security_Policy__Sample_Policy_Areas.html

NEW QUESTION: 415
What is the second phase of Public Key Infrastructure (PKI) key/certificate life-cycle management?
A. Implementation Phase
B. Issued Phase
C. Cancellation Phase
D. Initialization Phase
Answer: (SHOW ANSWER)

NEW QUESTION: 416
The principle of accountability is a principle by which specific action can be traced back to:
A. A policy
B. An individual
C. A group
D. A manager
Answer: (SHOW ANSWER)
The principle of accountability has been described in many references; it is a principle by which specific action can be traced back to an individual. As mentioned by Idrach, any significant action should be traceable to a specific user. The definition of "Significant" is entirely dependant on your business circumstances and

risk management model. It was also mentioned by Rino that tracing the actions of a specific user is fine but we must also be able to ascertain that this specific user was responsible for the uninitiated action.

NEW QUESTION: 417
An organization has hired a security services firm to conduct a penetration test. Which of the following will the organization provide to the tester?
A. Limits and scope of the testing.
B. Employee directory and organizational chart.
C. Logical location of filters and concentrators.
D. Physical location of server room and wiring closet.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 418
Which of the following is not a responsibility of a database administrator?
A. Implementing access rules to databases
B. Maintaining databases
C. Reorganizing databases
D. Providing access authorization to databases
Answer: D (LEAVE A REPLY)

NEW QUESTION: 419
Which of the following is a trusted, third party authentication protocol that was developed under Project Athena at MIT?
A. Kerberos
B. SESAME
C. KryptoKnight
D. NetSP
Answer: A (LEAVE A REPLY)
"Kerberos is an authentication protocol and was designed in the mid-1980s as part of MIT's Project Athena." Pg 129 Shon Harris: All-in-One CISSP Certification

NEW QUESTION: 420
Which of the following ensures that security is not breached when a system crash or other system failure occurs?
A. trusted recovery
B. hot swappable
C. redundancy
D. secure boot
Answer: A (LEAVE A REPLY)
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide:
Mastering the Ten Domains of Computer Security, page 222.

"System crash" and "system failure" are the key words. One "recovers" from a crash or failure.

NEW QUESTION: 421
Which of the following is the BIGGEST weakness when using native Lightweight Directory Access Protocol (LDAP) for authentication?
A. Passwords are passed in cleartext
B. Unsalted hashes are passed over the network
C. The authentication session can be replayed
D. Authorizations are not included in the server response
Answer: (SHOW ANSWER)

NEW QUESTION: 422
A demilitarized zone is:
A. a part of a network perfectly safe from hackers
B. a militarized network segment
C. a firewall
D. the network segment between the Internet and a private network
Answer: D (LEAVE A REPLY)
The DMZ is a buffer between the protected and unprotected network.
"A part of a network perfectly safe from hackers" is incorrect. There is no such thing.
"A militarized network segment" is incorrect. While the term DMZ originated in the Korean War, it has nothing to do with the military.
"A firewall" is incorrect. Firewalls can play an important part in building a DMZ but a DMZ is much more than a firewall.
References:
CBK, p. 850
AIO, p. 483

NEW QUESTION: 423
Good security is built on which of the following concept?
A. The concept of a pass-through device that only allows certain traffic in and out
B. The Concept of defense in depth
C. The Concept of Preventative controls

D. The Concept of Defensive Controls
Answer: (SHOW ANSWER)
This the best of the four answers as a defense that depends on multiple layers is superior to one where all protection is embedded in a single layer (e.g., a firewall).
Defense in depth would include all categories of controls.
The Following answers are incorrect:
"Concept of a pass through device that only allows certain traffic in and out" is incorrect.
This is one definition of a firewall which can be a component of a defense in depth strategy in combination with other measures.
"Concept of preventative controls" is incorrect. This is a component of a defense in depth strategy but the core concept is that there must be multiple layers of defenses.
"Concept of defensive controls" is incorrect. This is a component of a defense in depth strategy but the core concept is that there must be multiple layers of defenses.
References:
http://en.wikipedia.org/wiki/Defense_in_depth_(computing)
http://www.nsa.gov/snac/support/defenseindepth.pdf

NEW QUESTION: 424
Which of the following is considered the last line defense in regard to a Governance, Risk managements, and compliance (GRC) program?
A. Internal audit
B. Board review
C. Internal controls
D. Risk management
Answer: (SHOW ANSWER)

NEW QUESTION: 425
Which choice is the BEST description of authentication as opposed to
authorization?
A. A system's capability to determine the actions and behavior of a single individual within a system
B. The testing or reconciliation of evidence of a user's identity
C. The means by which a user provides a claim of his or her identity to a system
D. The rights and permissions granted to an individual to access a computer resource
Answer: B (LEAVE A REPLY)
The correct answer is "The testing or reconciliation of evidence of a user's identity". Answer
"The means by which a user provides a claim of his or her identity to a system" is identification, "A system's capability to determine the actions and behavior of a single individual within a system" is accountability, and "The rights and permissions granted to an individual to access a computer resource" is authorization.

NEW QUESTION: 426
What is a sequence of characters that is usually longer than the allotted number for a password called?

A. passphrase
B. cognitive phrase
C. anticipated phrase
D. Real phrase
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
A passphrase is a sequence of characters that is longer than a password and, in some cases, takes the place of a password during an authentication process. Passphrases are long static passwords, which is made up of words in a phrase or sentence.
Incorrect Answers:
B: A sequence of characters that is usually longer than the allotted number for a password is called a passphrase, not a cognitive phrase.
C: A sequence of characters that is usually longer than the allotted number for a password is called a passphrase, not an anticipated phrase.
D: A sequence of characters that is usually longer than the allotted number for a password is called a passphrase, not a real phrase.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 199 Conrad, Eric, Seth Misenar, Joshua Feldman, CISSP Study Guide, 2nd Edition, Syngress, Waltham, 2012, p. 30

NEW QUESTION: 427
ICMP and IGMP belong to which layer of the OSI model?
A. Datagram Layer.
B. Network Layer.
C. Transport Layer.
D. Data Link Layer.
Answer: B (LEAVE A REPLY)
The network layer contains the Internet Protocol (IP), the Internet Control
Message Protocol (ICMP), and the Internet Group Management Protocol (IGMP)
The following answers are incorrect:
Datagram Layer. Is incorrect as a distractor as there is no Datagram Layer.
Transport Layer. Is incorrect because it is used to data between applications and uses the
TCP and UDP protocols.
Data Link Layer. Is incorrect because this layer deals with addressing hardware.

NEW QUESTION: 428
Which of the following is the BEST reason for the use of security metrics?
A. They ensure that the organization meets its security objectives.
B. They provide an appropriate framework for Information Technology (IT) governance.
C. They speed up the process of quantitative risk assessment.

D. They quantify the effectiveness of security processes.
Answer: B (LEAVE A REPLY)
Section: Software Development Security

NEW QUESTION: 429
The Bell-LaPadula model addresses which one of the following items?
A. Covert channels
B. Definition of a secure state transition
C. Information flow from high to low
D. The creation and destruction of subjects and objects
Answer: C (LEAVE A REPLY)
Information flow from high to low is addressed by the * -property
of the Bell0LaPadula model, which states that a subject cannot write
data from a higher level of classification to a lower level of
classification. This property is also known as the confinement property or the no write down property.
* In answer "Covert channels", covert channels are not addressed by the model. The Bell-LaPadula model deals with information flow through normal channels and does not address the covert passing of information through unintended paths.
The creation and destruction of subjects and objects, answer "The creation and destruction of subjects and objects", is not addressed by the model.
* Answer "Definition of a secure state transition" refers to the fact that the model discusses a secure transition from one secure state to another, but it never provides a definition of a secure transition.

NEW QUESTION: 430
Retaining system logs for six months or longer can be valuable for what activities?
A. Physical and logical access control
B. Forensics and incident response
C. Identity and authorization management
D. Disaster recovery and business continuity
Answer: (SHOW ANSWER)

NEW QUESTION: 431
Which of the following could cause a Denial of Service (DoS) against an authentication system?
A. Hashing of audit logs
B. Encryption of audit logs
C. No archiving of audit logs
D. Remote access audit logs
Answer: (SHOW ANSWER)

NEW QUESTION: 432
In the public sector, as opposed to the private sector, due care is usually determined by

A. Potential for litigation.
B. Insurance rates.
C. Legislative requirements.
D. Minimum standard requirements.
Answer: (SHOW ANSWER)

NEW QUESTION: 433
In an object-oriented system, polymorphism denotes:
A. Objects of many different classes that are unrelated but respond to some common set of operations in the same way.
B. Objects of many different classes that are related by some common superclass; thus, all objects denoted by this name can respond to some common set of operations in identical fashion.
C. Objects of many different classes that are related by some common superclass; thus, any object denoted by this name can respond to some common set of operations in a different way.
D. Objects of the same class; thus, any object denoted by this name can respond to some common set of operations in the same way.
Answer: C (LEAVE A REPLY)
Objects of many different classes that are related by some common superclass that are able to respond to some common set of operations in a different way.
The other answers are incorrect by the definition of polymorphism.

NEW QUESTION: 434
Which action is MOST effective for controlling risk and minimizing maintenance costs in the software supply chain?
A. Selecting redundant suppliers
B. Selecting suppliers based on business requirements
C. Selecting fewer, more reliable suppliers
D. Selecting software suppliers with the fewest known vulnerabilities
Answer: D (LEAVE A REPLY)
Section: Mixed questions

NEW QUESTION: 435
Which general TCSEC security class category describes that mandatory access policies be enforced in the TCB?
Exhibit:

A. A
B. B
C. C
D. D
Answer: B (LEAVE A REPLY)
The Trusted Computer System Evaluation Criteria [Orange Book] defines major hierarchical classes of security by the letters D (least secure) through A (most secure):
D. Minimal protection
C. Discretionary protection (C1&C2)
B. Mandatory protection (B1, B2, B3)
A. Verified protection; formal methods (A1)
Source: DoD 5200.28-STD Department of Defense Trusted Computer
System Evaluation Criteria.

NEW QUESTION: 436
In order for application developers to detect potential vulnerabilities earlier during the Software Development Life Cycle (SDLC), which of the following safeguards should be implemented FIRST as part of a comprehensive testing framework?
A. Source code review
B. Acceptance testing
C. Threat modeling
D. Automated testing
Answer: A (LEAVE A REPLY)
Section: Mixed questions

NEW QUESTION: 437

A contingency plan should address:

A. Potential risks.

B. Residual risks.

C. Identified risks.

D. All answers are correct.

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

Contingency plans are developed as a result of a risk being identified. Contingency plans are pre-defined actions plans that can be implemented if identified risks actually occur. One type of identified risk is a residual risk. Residual risks are those risks that are expected to remain after implementing the planned risk response, as well as those that have been deliberately accepted.

A contingency plan should address the risks found during risk assessment. Risk assessment includes both the identification of potential risk and the evaluation of the potential impact of the risk.

Incorrect Answers:

A: Contingency plans should not just address potential risks. It should address identified risks and residual risks as well.

B: Contingency plans should not just address residual risks. It should address identified risks and potential risks as well.

C: Contingency plans should not just address identified risks. It should address potential risks and residual risks as well.

NEW QUESTION: 438

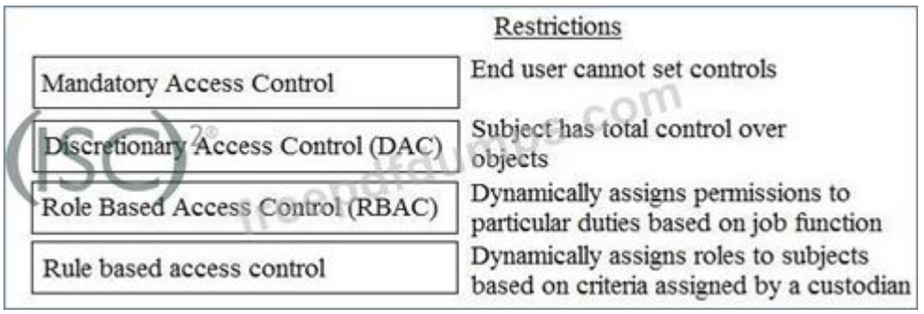
Match the name of access control model with its associated restriction.

Drag each access control model to its appropriate restriction access on the right.

Access Control Model		Restrictions
Mandatory Access Control		End user cannot set controls
Discretionary Access Control (DAC)		Subject has total control over objects
Role Based Access Control (RBAC)		Dynamically assigns permissions to particular duties based on job function
Rule based access control		Dynamically assigns roles to subjects based on criteria assigned by a custodian

Answer:

Explanation



NEW QUESTION: 439

Which of the following is NOT a component of IPSec?

A. Authentication Header

B. Encapsulating Security Payload

C. Key Distribution Center

D. Internet Key Exchange

Answer: C (LEAVE A REPLY)

AH, ESP and IKE are the three main components of IPSec. A KDC (Key Distribution Center) is a component of Kerberos, not IPSec.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 4: Protection of Information Assets (page 217).

NEW QUESTION: 440

A code, as is pertains to cryptography:

A. Is a generic term for encryption.

B. Is specific to substitution ciphers.

C. Deals with linguistic units.

D. Is specific to transposition ciphers.

Answer: C (LEAVE A REPLY)

Historically, a code refers to a cryptosystem that deals with linguistic units: words, phrases, sentences, and so forth. Codes are only useful for specialized circumstances where the message to transmit has an already defined equivalent ciphertext word.

Source: DUPUIS, Cl?ment, CISSP Open Study Guide on domain 5, cryptography, April 1999.

NEW QUESTION: 441

In a Public Key Infrastructure (PKI) context, which of the following is a primary concern with LDAP servers?

A. Confidentiality

B. Accountability

C. Flexibility

D. Availability

Answer: (SHOW ANSWER)

NEW QUESTION: 442

What is the MOST significant benefit of an application upgrade that replaces randomly generated session keys with certificate based encryption for communications with backend servers?
A. Non-repudiation
B. Efficiency
C. Confidentially
D. Privacy
Answer: A (LEAVE A REPLY)
Section: Asset Security

NEW QUESTION: 443
What is the RESULT of a hash algorithm being applied to a message?
A. A digital signature
B. A ciphertext
C. A message digest
D. A plaintext
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A cryptographic hash function is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone.
The input data is often called the message, and the hash value is often called the message digest or simply the digest.
Incorrect Answers:
A: To create a digital signature, a message digest is calculated (by the hash algorithm being applied to the message) then it is encrypted with the sender's private key. However, the digital signature is not the direct output of the hash algorithm being applied to the message.
B: A ciphertext is the output of an encryption algorithm, not a hash algorithm being applied to data.
D: A plaintext is the message 'before' the hash algorithm is applied to the message; it is the input to the hash algorithm, not the output.
References:
https://en.wikipedia.org/wiki/Cryptographic_hash_function
Krutz, Ronald L. and Russel Dean Vines, The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, New York, 2001, p. 151

NEW QUESTION: 444
The DMZ does not normally contain:
A. encryption server
B. web server
C. external DNS server
D. mail relay
Answer: A (LEAVE A REPLY)

Only servers providing public access to required services should be located in the DMZ.
"Web server" is incorrect. An organization's public web site is a very common DMZ scenario.
"External DNS server" is incorrect. An organization's external DNS servers is a very common DMZ scenario.
"Mail relay" is incorrect. An organization's mail relay is a very common DMZ scenario.
References:
CBK, p. 434
AIO3, p. 483

NEW QUESTION: 445
What does normalizing data in a data warehouse mean?
A. Data is restricted to a range of values.
B. Numerical data is divided by a common factor.
C. Data is converted to a symbolic representation.
D. Redundant data is removed.
Answer: D (LEAVE A REPLY)
The correct answer is removing redundant data.

NEW QUESTION: 446
A message can be encrypted and digitally signed, which provides _____
A. Confidentiality, Authentication, Non-repudiation, and Integrity.
B. Confidentiality and Authentication
C. Confidentiality and Non-repudiation
D. Confidentiality and Integrity.
Answer: A (LEAVE A REPLY)
For the purpose of the exam, one needs to be very clear on all the available choices
within cryptography,
because different steps and algorithms provide different types of security services:
A message can be encrypted, which provides confidentiality.
A message can be digitally signed, which provides authentication, nonrepudiation, and integrity.
A message can be hashed, which provides integrity.
A message can be encrypted and digitally signed, which provides confidentiality, authentication,
nonrepudiation, and integrity.
The following answers are incorrect:
Confidentiality and Authentication
Confidentiality and Non-repudiation
Confidentiality and Integrity
The following reference(s) were/was used to create this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (pp. 829-830). McGraw-Hill
. Kindle Edition.

NEW QUESTION: 447

Which choice below most accurately describes a business continuity program?

A. A standard that allows for rapid recovery during system interruption and data loss

B. A determination of the effects of a disaster on human, physical, economic, and natural resources

C. A program that implements the mission, vision, and strategic goals of the organization

D. Ongoing process to ensure that the necessary steps are taken to identify the impact of potential losses and maintain viable recovery

Answer: D (LEAVE A REPLY)

A business continuity program is an ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and recovery plans, and ensure continuity of services through personnel training, plan testing, and maintenance. Answer "A program that implements the mission, vision, and strategic goals of the organization" describes a disaster/emergency management program. A disaster/ emergency management program, like a disaster recovery program, is a program that implements the mission, vision, and strategic goals and objectives as well as the management framework of the program and organization. *Answer "A determination of the effects of a disaster on human, physical, economic, and natural resources" describes a damage assessment. A damage assessment is an appraisal or determination of the effects of a disaster on human, physical, economic, and natural resources. *Answer "A standard that allows for rapid recovery during system interruption and data loss" is a distracter. Source: NFPA1600 Standard on Disaster/Emergency Management and Business Continuity, National Fire Protection Association, 2000 edition.

NEW QUESTION: 448

As per the Orange Book, what are two types of system assurance?

A. Operational Assurance and Architectural Assurance.

B. Design Assurance and Implementation Assurance.

C. Architectural Assurance and Implementation Assurance.

D. Operational Assurance and Life-Cycle Assurance.

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation:

When products are evaluated for the level of trust and assurance they provide, many times operational assurance and life-cycle assurance are part of the evaluation process.

Operational assurance concentrates on the product's architecture, embedded features, and functionality that enable a customer to continually obtain the necessary level of protection when using the product.

Examples of operational assurances examined in the evaluation process are access control mechanisms, the separation of privileged and user program code, auditing and monitoring capabilities, covert channel analysis, and trusted recovery when the product experiences unexpected circumstances.

Life-cycle assurance pertains to how the product was developed and maintained. Each stage of the product's life cycle has standards and expectations it must fulfill before it can be deemed a highly trusted product.

Examples of life-cycle assurance standards are design specifications, clipping-level configurations, unit and

integration testing, configuration management, and trusted distribution. Vendors looking to achieve one of the higher security ratings for their products will have each of these issues evaluated and tested.
Incorrect Answers:
A: Architectural Assurance is not one of the two types of system assurance defined in the Orange Book.
B: Design Assurance and Implementation Assurance are not the two types of system assurance defined in the Orange Book.
C: Architectural Assurance and Implementation Assurance are not the two types of system assurance defined in the Orange Book.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 1240

NEW QUESTION: 449
Which of the following should be used as a replacement for Telnet for secure remote login over an insecure network?
A. S-Telnet
B. SSL
C. Rlogin
D. SSH
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Secure Shell (SSH) works as a type of tunneling mechanism that delivers terminal like access to remote computers. SSH should be used instead of Telnet, FTP, rlogin, rexec, or rsh, because it is more secure.
Incorrect Answers:
A: S-Telnet is only used for IBM 5250 data streams.
B: SSL is supported for Telnet implementations.
C: Rlogin is a software utility for Unix-like computer operating systems that enables users to log in on another host via a network. It is, however, less secure that SSH.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 860
https://en.wikipedia.org/wiki/Telnet
https://en.wikipedia.org/wiki/Rlogin

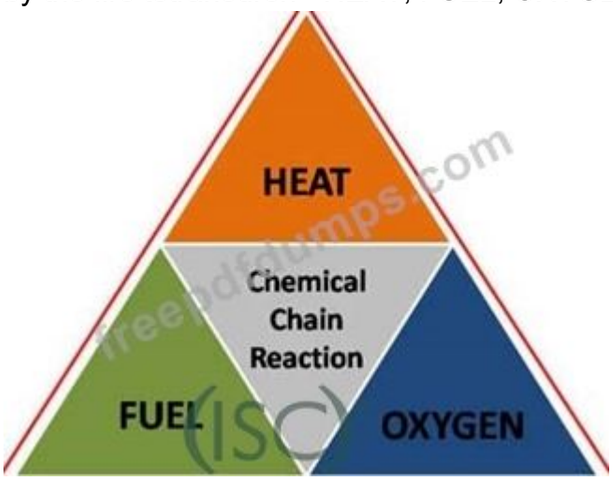
NEW QUESTION: 450
What are the four basic elements of Fire?
A. Heat, Fuel, Oxygen, and Chain Reaction
B. Heat, Fuel, CO2, and Chain Reaction
C. Heat, Wood, Oxygen, and Chain Reaction
D. Flame, Fuel, Oxygen, and Chain Reaction
Answer: A (LEAVE A REPLY)
Four elements must be presentin order for fire to exist. These elements are HEAT,

FUEL, OXYGENand CHAIN REACTION.

While not everything is known about the combustion process, it is generally accepted that fire is a chemical reaction. This reaction is dependent upon a material rapidly oxidizing, or uniting with oxygen so rapidly that it produces heat and flame.

Until the advent of newer fire extinguishing agents, fire was thought of as a triangle with the three sides represented by heat, fuel, and oxygen. If any one of the three sides were to be taken away, the fire would cease to exist.

Studies of modern fire extinguishing agents have revealed a fourth element - a self propagating chain reaction in the combustion process. As a result, the basic elements of fire are represented by the fire tetrahedron - HEAT, FUEL, OXYGEN and CHAIN REACTION.



Fire Tetrahedron

The theory of fire extinguishment is based on removing any one or more of the four elements in the fire tetrahedron to suppress the fire.

REMOVING THE HEAT In order to remove the heat, something must be applied to the fire to absorb the heat or act as a heat exchanger. Water is not the only agent used to accomplish this, but it is the most common.

REMOVING THE FUEL Under many circumstances, it is not practical to attempt to remove the fuel from the fire. When dealing with flammable liquid fires, valves can be shut off and storage vessels pumped to safe areas to help eliminate the supply of fuel to the fire. Flammable gas fires are completely extinguished by shutting off the fuel supply.

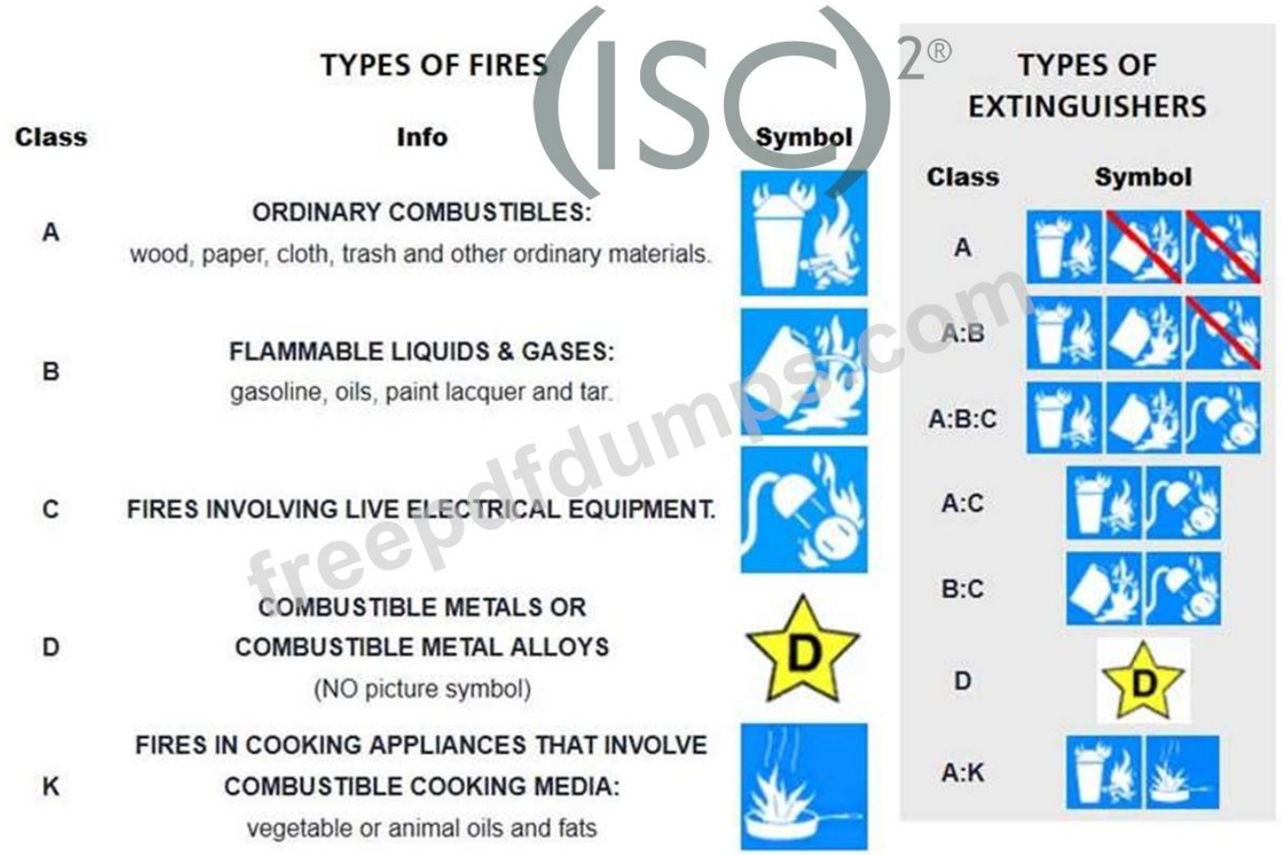
REMOVE THE OXYGEN Oxygen as it exists in our atmosphere (21%) is sufficient to support combustion in most fire situations. Removal of the air or oxygen can be accomplished by separating it from the fuel source or by displacing it with an inert gas. Examples of separation would be foam on a flammable liquid fire, a wet blanket on a trash fire, or a tight fitting lid on a skillet fire. Agents such as CO2, nitrogen, and steam are used to displace the oxygen.

INTERRUPT THE CHAIN REACTION

Modern extinguishing agents, such as dry chemical and halons, have proven to be effective on various fires even though these agents do not remove heat, fuel, or oxygen. Dry chemical and halogenated agents are thought to suspend or bond with "free radicals" that are created in the combustion process and thus prevent them from continuing the chain reaction.

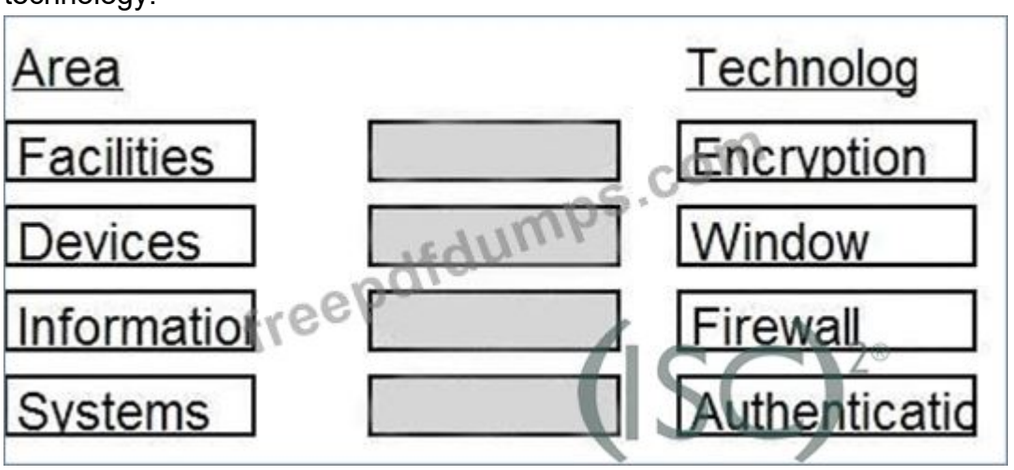
It must be noted that Halon is now banned in most country or cities. The agreement banning Halon

Production is called The Montreal Protocol.
Click on the following link to see a nice video on fire fighting and extinguishing agents, it cover key information you need to know for the exam.
Resume of the class of Fires:

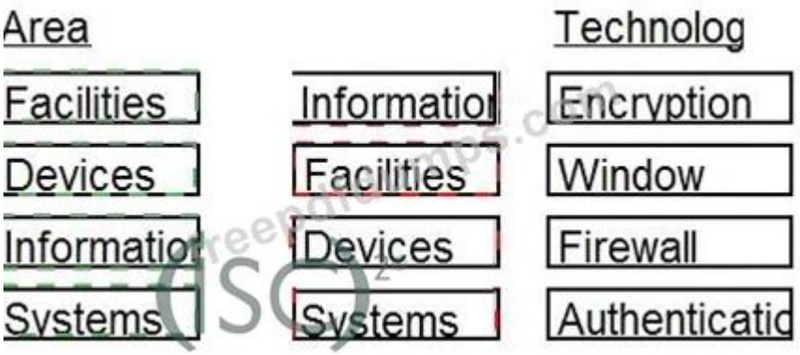


Class of Fires
All of the other answers are incorrect:
References: Fire and Fire Extinguishment and http://code7700.com/fire.html

NEW QUESTION: 451
Given the various means to protect physical and logical assets, match the access management area to the technology.



Answer:



Explanation

NEW QUESTION: 452

One of these statements about the key elements of a good configuration process is NOT true

A. Accommodate the reuse of proven standards and best practices

B. Ensure that all requirements remain clear, concise, and valid

C. Control modifications to system hardware in order to prevent resource changes

D. Ensure changes, standards, and requirements are communicated promptly and precisely

Answer: (SHOW ANSWER)

Configuration management isn't about preventing change but ensuring the integrity of IT resources by preventing unauthorised or improper changes.

According to the Official ISC2 guide to the CISSP exam, a good CM process is one that can:

(1)

accommodate change;

(2)

accommodate the reuse of proven standards and best practices;
(3)
ensure that all requirements remain clear, concise, and valid;
(4)
ensure changes, standards, and requirements are communicated promptly and precisely; and
(5)
ensure that the results conform to each instance of the product.
Configuration management Configuration management (CM) is the detailed recording and updating of information that describes an enterprise's computer systems and networks, including all hardware and software components. Such information typically includes the versions and updates that have been applied to installed software packages and the locations and network addresses of hardware devices. Special configuration management software is available. When a system needs a hardware or software upgrade, a computer technician can accesses the configuration management program and database to see what is currently installed. The technician can then make a more informed decision about the upgrade needed. An advantage of a configuration management application is that the entire collection of systems can be reviewed to make sure any changes made to one system do not adversely affect any of the other systems Configuration management is also used in software development, where it is called Unified Configuration Management (UCM). Using UCM, developers can keep track of the source code, documentation, problems, changes requested, and changes made. Change management In a computer system environment, change management refers to a systematic approach to keeping track of the details of the system (for example, what operating system release is running on each computer and which fixes have been applied).

NEW QUESTION: 453
HIPAA preempts state laws
A. except to the extent that the state law more stringent
B. regardless of the extent that the state law is more stringent
C. except to the extent that the state law is less stringent
D. except to the extent that the state law is legislated later than HIPAA
Answer: (SHOW ANSWER)

NEW QUESTION: 454
Which of the following usually provides reliable, real-time information without consuming network or host resources?
A. network-based IDS
B. host-based IDS
C. application-based IDS
D. firewall-based IDS
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:

On-line network-based IDS monitors network traffic in real time and it analyses the Ethernet packet and applies it on the same rules to decide if it is an attack or not.
Incorrect Answers:
B: A host-based intrusion detection system (HIDS) monitors and analyzes the internals of a computing system, as well as the network packets on its network interfaces in certain instances.
C: An application-based IDS is designed to monitor a specific application.
D: Firewalls are different to IDS because it looks outwardly for intrusions in order to stop them from happening.
References:
https://en.wikipedia.org/wiki/Intrusion_detection_system
https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system

NEW QUESTION: 455
How are memory cards and smart cards different?
A. Memory cards normally hold more memory than smart cards
B. Smart cards provide a two-factor authentication whereas memory cards don't
C. Memory cards have no processing power
D. Only smart cards can be used for ATM cards
Answer: C (LEAVE A REPLY)
"The main difference between memory cards and smart cards is the processing power. A memory card holds information, but does not process information. A smart card has the necessary hardware and logic to actually process information." Pg 121 Shon Harris CISSP All-In-One Exam Guide

NEW QUESTION: 456
Which of the following would MOST likely ensure that a system development project meets business objectives?
A. Development and tests are run by different individuals
B. User involvement in system specification and acceptance
C. Development of a project plan identifying all development activities
D. Strict deadlines and budgets
Answer: B (LEAVE A REPLY)
Effective user involvement is the most critical factor in ensuring that the application meets business objectives.
A great way of getting early input from the user community is by using Prototyping. The prototyping method was formally introduced in the early 1980s to combat the perceived weaknesses of the waterfall model with regard to the speed of development. The objective is to build a simplified version (prototype) of the application, release it for review, and use the feedback from the users' review to build a second, better version.
This is repeated until the users are satisfied with the product. t is a four-step process:
initial concept,
design and implement initial prototype,

refine prototype until acceptable, and
complete and release final version.
There is also the Modified Prototype Model (MPM. This is a form of prototyping that is ideal for Web application development. It allows for the basic functionality of a desired system or component to be formally deployed in a quick time frame. The maintenance phase is set to begin after the deployment. The goal is to have the process be flexible enough so the application is not based on the state of the organization at any given time. As the organization grows and the environment changes, the application evolves with it, rather than being frozen in time.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 12101-12108 and 12099-12101). Auerbach Publications. Kindle Edition.
and
Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 296).

NEW QUESTION: 457
When an organization takes reasonable measures to ensure that it took precautions to protect its network and resources is called:
A. Reasonable Action
B. Security Mandate
C. Due Care
D. Prudent Countermeasures
Answer: C (LEAVE A REPLY)
Due care are the steps taken to show it has taken responsibility for its actions.

NEW QUESTION: 458
Which of the following provides coordinated procedures for minimizing loss of life, injury, and property damage in response to a physical threat?
A. Business continuity plan
B. Incident response plan
C. Disaster recovery plan
D. Occupant emergency plan
Answer: D (LEAVE A REPLY)
The Occupant Emergency Plan (OEP) provides the response procedures for occupants of a facility in the event of a situation posing a potential threat to the health and safety of personnel, the environment, or property.
Such events would include a fire, hurricane, criminal attack, or a medical emergency. OEPs are developed at the facility level, specific to the geographic location and structural design of the building.

The following are incorrect answers:
The business continuity plan addresses business processes and provides procedures for sustaining essential business operations while recovering from a significant disruption.
The incident response plan focuses on information security responses to incidents affecting systems and/or networks. It establishes procedures to address cyber attacks against an organization's IT systems.
The disaster recovery plan (DRP) applies to major, usually catastrophic events that deny access to the normal facility for an extended period.
Reference(s) used for this question:
SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

NEW QUESTION: 459
Phreakers are hackers who specialize in telephone fraud. What type of telephone fraud simulates the tones of coins being deposited into a payphone?
A. Red Boxes
B. Blue Boxes
C. White Boxes
D. Black Boxes
Answer: A (LEAVE A REPLY)
The Red box basically simulates the sounds of coins being dropped into the coin slot of a payphone. The traditional Red Box consisting of a pair of Wien-bridge oscillators with the timing controlled by 555 timer chips. The Blue Box, The mother of all boxes, The first box in history, which started the whole phreaking scene. Invented by John Draper (aka "Captain Crunch") in the early 60s, who discovered that by sending a tone of 2600Hz over the telephone lines of AT&T, it was possible to make free calls. A Black Box is a device that is hooked up to your phone that fixes your phone so that when you get a call, the caller doesn't get charged for the call. This is good for calls up to 1/2 hour, after 1/2 hour the Phone Co. gets suspicious, and then you can guess what happens. The White Box turns a normal touch tone keypad into a portable unit. This kind of box can be commonly found in a phone shop.

NEW QUESTION: 460
You are using an open source packet analyzer called Wireshark and are sifting through the various conversations to see if anything appears to be out of order.
You are observing a UDP conversation between a host and a router. It was a file transfer between the two on port 69. What protocol was used here to conduct the file transfer?
A. TFTP
B. SFTP
C. FTP
D. SCP
Answer: A (LEAVE A REPLY)

Discussion: TFTP is a curious protocol that doesn't use authentication and is often used to transfer configuration files between an administrator's computer and switch or router.
The admin's computer would have the TFTP server software installed on it and he would
SSH into the router and run a command that instructs the router to get its configuration from a TFTP server like this:
#copy running-config tftp
The router would request the IP or name of the host from where to get the config and the name of the config file. It would then be copied down into the running-config (RAM) on the router.
This is how wireshark could have seen the file transfer.
It is advisable that you use a more secure means to transfer router configuration files because of their sensitive nature. SCP or Secure Copy can be used on most mainstream routing and switching devices.
The following answers are incorrect:
- SFTP: This isn't correct because SFTP uses TCP and is on port 22.
- FTP: This is not the right answer because FTP uses TCP and ordinarily uses ports 20/21.
- SCP: Good guess but SCP doesn't use UDP or port 69 and even if you did 'see' a file transfer between SCP hosts you wouldn't see the contents of the packets because they're encrypted. Sorry. Here's more about SCP.
The following reference(s) was used to create this question:
2013. Official Security+ Curriculum.
TFTP

NEW QUESTION: 461
Which of the following is not a one-way hashing algorithm?
A. MD2
B. RC4
C. SHA-1
D. HAVAL
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
RC4 is a Symmetric Key Algorithm.
Incorrect Answers:
A: MD2 is a one-way hashing algorithm.
C: SHA-1 is a one-way hashing algorithm.
D: HAVAL is a one-way hashing algorithm.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 831

NEW QUESTION: 462
Why might a network administrator choose distributed virtual switches instead of stand-alone switches for network segmentation?

A. To standardize on a single vendor
B. To ensure isolation of management traffic
C. To maximize data plane efficiency
D. To reduce the risk of configuration errors
Answer: (SHOW ANSWER)
Section: Mixed questions

NEW QUESTION: 463
Which of the following describes a computer processing architecture in which a language compiler or pre-processor breaks program instructions down into basic operations that can be performed by the processor at the same time?
A. Very-Long Instruction-Word Processor (VLIW)
B. Complex-Instruction-Set-Computer (CISC)
C. Reduced-Instruction-Set-Computer (RISC)
D. Super Scalar Processor Architecture (SCPA)
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Very long instruction word (VLIW) describes a computer processing architecture in which a language compiler or pre-processor breaks program instruction down into basic operations that can be performed by the processor in parallel (that is, at the same time).
These operations are put into a very long instruction word which the processor can then take apart without further analysis, handing each operation to an appropriate functional unit. The following answer are incorrect:
The term "CISC" (complex instruction set computer or computing) refers to computers designed with a full set of computer instructions that were intended to provide needed capabilities in the most efficient way.
Later, it was discovered that, by reducing the full set to only the most frequently used instructions, the computer would get more work done in a shorter amount of time for most applications. Intel's Pentium microprocessors are CISC microprocessors. The PowerPC microprocessor, used in IBM's RISC System/6000 workstation and Macintosh computers, is a RISC microprocessor. RISC takes each of the longer, more complex instructions from a CISC design and reduces it to multiple instructions that are shorter and faster to process.
RISC technology has been a staple of mobile devices for decades, but it is now finally poised to take on a serious role in data center servers and server virtualization. The latest RISC processors support virtualization and will change the way computing resources scale to meet workload demands. A superscalar CPU architecture implements a form of parallelism called instruction level parallelism within a single processor. It therefore allows faster CPU throughput than would otherwise be possible at a given clock rate. A superscalar processor executes more than one instruction during a clock cycle by simultaneously dispatching multiple instructions to redundant functional units on the processor. Each functional unit is not a separate CPU core but an execution resource within a single CPU such as an arithmetic logic unit, a bit shifter, or a multiplier.
References:
http://whatis.techtarget.com/definition/0,,sid9_gci214395,00.html

http://searchcio-midmarket.techtarget.com/definition/CISC
http://en.wikipedia.org/wiki/Superscalar

NEW QUESTION: 464
According to the Orange Book, which security level is the first to require a system to protect against covert timing channels?
A. A1
B. B3
C. B2
D. B1
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The TCSEC defines two kinds of covert channels:
Storage channels - Communicate by modifying a "storage location"
▪
Timing channels - Perform operations that affect the "real response time observed" by the receiver
▪
The TCSEC, also known as the Orange Book, requires analysis of covert storage channels to be classified as a B2 system and analysis of covert timing channels is a requirement for class B3.
Incorrect Answers:
A: Level A1 requires a system to protect against covert timing channels. However, the lower level B3 also requires it.
C: Level B2 does not require a system to protect against covert timing channels.
D: Level B1 does not require a system to protect against covert timing channels.
References:
https://en.wikipedia.org/wiki/Covert_channel

NEW QUESTION: 465
If a token and 4-digit personal identification number (PIN) are used to access a computer system and the token performs off-line checking for the correct PIN, what type of attack is possible?
A. Birthday
B. Brute force
C. Man-in-the-middle
D. Smurf
Answer: B (LEAVE A REPLY)
Brute force attacks are performed with tools that cycle through many possible character, number, and symbol combinations to guess a password. Pg 134 Shon Harris CISSP All-In-One Certification Exam Guide. Since the token allows offline checking of PIN, the cracker can keep trying PINS until it is cracked.

NEW QUESTION: 466
What should happen when an emergency change to a system must be performed?

A. The change is performed and a notation is made in the system log.
B. Testing and approvals must be performed quickly.
C. The change must be given priority at the next meeting of the change control board.
D. The change must be performed immediately and then submitted to the change board.
Answer: (SHOW ANSWER)

NEW QUESTION: 467
Which of the following attack includes social engineering, link manipulation or web site forgery techniques?
A. Smurf attack
B. Traffic analysis
C. Phishing
D. Interrupt attack
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Phishing is the attempt to get information such as usernames, passwords, and credit card details commonly through email spoofing and instant messaging that contain links directing the unsuspecting user to enter details at a fake website whose look and feel are almost identical to the legitimate website.
Attempts to deal with phishing include legislation, user training, public awareness, and technical security measures.
Incorrect Answers:
A: A smurf attack is a distributed denial of service (DDoS) attack in which an ICMP ECHO REQUEST packet with the victims spoofed source address is sent to the victim's network broadcast address. Each system on the victim's subnet receives an ICMP ECHO REQUEST packet and replies with an ICMP ECHO REPLY packet to the spoof address in the ICMP ECHO REQUEST packet. This floods the victims system, causing it to slow down, freeze, crash, or reboot. This attack does not make use of social engineering, link manipulation or web site forgery techniques.
B: A traffic analysis attack is carried out to uncover information by analyzing traffic patterns on a network. Traffic padding can be used to counter this kind of attack, in which decoy traffic is sent out over the network to disguise patterns and make it more difficult to uncover them. This attack does not make use of social engineering, link manipulation or web site forgery techniques.
D: An interrupt or denial of service (DoS) attack occurs when an attacker sends multiple service requests to the victim's computer until they eventually overwhelm the system, causing it to freeze, reboot, and ultimately

not be able to carry out regular tasks. This attack does not make use of social engineering, link manipulation or web site forgery techniques.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, pp. 271-273, 587, 1293, 1294
http://en.wikipedia.org/wiki/Phishing

NEW QUESTION: 468
In a multilevel security system (MLS), the Pump is:
A. A one-way information flow device
B. A two-way information flow device
C. A device that implements role-based access control
D. Compartmented Mode Workstation (CMW)
Answer: (SHOW ANSWER)
The Pump (M.h. Kang, I.S. Moskowitz, APump for Rapid, Reliable, Secure Communications, The 1st ACM Conference on Computer and Communications Security, Fairfax, VA, 1993) was developed at the US Naval Research Laboratory (NRL). It permits information flow in one direction only, from a lower level of security classification or sensitivity to a higher level. It is a convenient approach to multilevel security in that it can be used to put together systems with different security levels.
*Answer "A two-way information flow device" is a distracter.
*Answer "Compartmented Mode Workstation (CMW)", the CMW, refers to windows-based workstations that require users to work with information at different classification levels. Thus, users may work with multiple windows with
different classification levels on their workstations. When data is
attempted to be moved from one window to another, mandatory access
control policies are enforced. This prevents information of a higher classification
from being deposited to a location of lower classification.
*Answer "A device that implements role-based access control", role-based access control, is an access control mechanism and is
now being considered for mandatory access control based on users'
roles in their organizations.

NEW QUESTION: 469
Which of the following describes a computer processing architecture in which a language compiler or pre-processor breaks program instructions down into basic operations that can be performed by the processor at the same time?
A. Very-Long Instruction-Word Processor (VLIW)
B. Complex-Instruction-Set-Computer (CISC)
C. Reduced-Instruction-Set-Computer (RISC)
D. Super Scalar Processor Architecture (SCPA)
Answer: A (LEAVE A REPLY)

Very long instruction word (VLIW) describes a computer processing architecture in which a language compiler or pre-processor breaks program instruction down into basic operations that can be performed by the processor in parallel (that is, at the same time). These operations are put into a very long instruction word which the processor can then take apart without further analysis, handing each operation to an appropriate functional unit.
The following answer are incorrect: The term "CISC" (complex instruction set computer or computing) refers to computers designed with a full set of computer instructions that were intended to provide needed capabilities in the most efficient way. Later, it was discovered that, by reducing the full set to only the most frequently used instructions, the computer would get more work done in a shorter amount of time for most applications. Intel's Pentium microprocessors are CISC microprocessors.
The PowerPC microprocessor, used in IBM's RISC System/6000 workstation and Macintosh computers, is a RISC microprocessor. RISC takes each of the longer, more complex instructions from a CISC design and reduces it to multiple instructions that are shorter and faster to process. RISC technology has been a staple of mobile devices for decades, but it is now finally poised to take on a serious role in data center servers and server virtualization. The latest RISC processors support virtualization and will change the way computing resources scale to meet workload demands.
A superscalar CPU architecture implements a form of parallelism called instruction level parallelism within a single processor. It therefore allows faster CPU throughput than would otherwise be possible at a given clock rate. A superscalar processor executes more than one instruction during a clock cycle by simultaneously dispatching multiple instructions to redundant functional units on the processor. Each functional unit is not a separate CPU core but an execution resource within a single CPU such as an arithmetic logic unit, a bit shifter, or a multiplier.
Reference(s) Used for this question: http://whatis.techtarget.com/definition/0,,sid9_gci214395,00.html and http://searchcio-midmarket.techtarget.com/definition/CISC
and http://en.wikipedia.org/wiki/Superscalar

NEW QUESTION: 470
Which of the following activities BEST identifies operational problems, security misconfigurations, and malicious attacks?
A. Policy documentation review
B. Interface testing
C. Authentication validation
D. Periodic log reviews
Answer: D (LEAVE A REPLY)

NEW QUESTION: 471
What control is based on a specific profile for each user?
A. Lattice based access control.
B. Directory based access control.
C. Rule based access control.
D. ID based access control.

Answer: D (LEAVE A REPLY)
The correct answer should be ID based access control. Rule based isn't necessarily identity based.

NEW QUESTION: 472
A circuit level proxy is _____ when compared to an application level proxy.
A. lower in processing overhead.
B. more difficult to maintain.
C. more secure.
D. slower.
Answer: (SHOW ANSWER)
Since the circuit level proxy does not anayze the application content of the packet in making its decisions, it has lower overhead than an application level proxy.
"More difficult to maintain" is incorrect. Circuit level proxies are typicall easier to configure and simpler to maintain that an application level proxy.
"More secure" is incorrect. A circuit level proxy is not necessarily more secure than an application layer proxy.
"Slower" is incorrect. Because it is lower in overhead, a circuit level proxy is typically faster than an application level proxy.
References: CBK,pp. 466 - 467 AIO3, pp.488 - 490

NEW QUESTION: 473
Which of the following division is defined in the TCSEC (Orange Book) as minimal protection?
A. Division D
B. Division C
C. Division B
D. Division A
Answer: A (LEAVE A REPLY)
The criteria are divided into four divisions: D, C, B, and A ordered in a hierarchical manner with the highest division (A) being reserved for systems providing the most comprehensive security.
Each division represents a major improvement in the overall confidence one can place in the system for the protection of sensitive information.
Within divisions C and B there are a number of subdivisions known as classes. The classes are also ordered in a hierarchical manner with systems representative of division C and lower classes of division B being characterized by the set of computer security mechanisms that they possess.
Assurance of correct and complete design and implementation for these systems is gained mostly through testing of the security- relevant portions of the system. The security-relevant portions of a system are referred to throughout this document as the Trusted Computing Base (TCB).
Systems representative of higher classes in division B and division A derive their security attributes more from their design and implementation structure. Increased assurance that the required features are operative, correct, and tamperproof under all circumstances is gained through progressively more rigorous analysis during the design process.

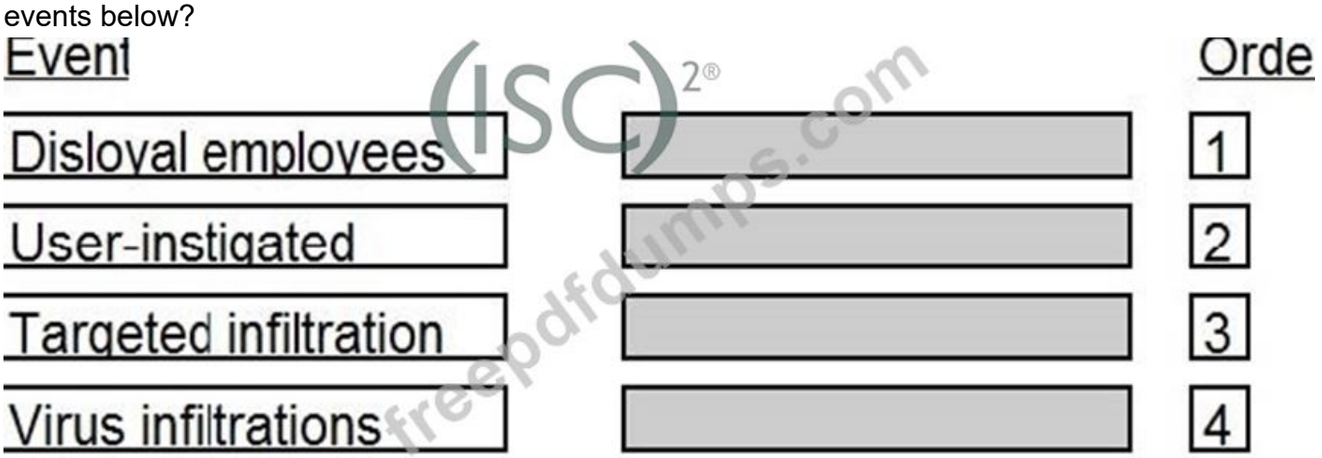
TCSEC provides a classification system that is divided into hierarchical divisions of assurance levels: Division D - minimal security Division C - discretionary protection Division B - mandatory protection Division A - verified protection Reference: page 358 AIO V.5 Shon Harris
also
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, page 197.
Also:
THE source for all TCSEC "level" questions: http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt

NEW QUESTION: 474
The Federal Intelligence Surveillance Act (FISA) of 1978, the Electronic Communications Privacy Act (ECPA) of 1986, and the Communications Assistance for Law Enforcement Act (CALEA) of 1994 are legislative acts passed by the United States Congress. These acts all address what major information security issue?
A. Computer fraud
B. Wiretapping
C. Unlawful use of and access to government computers and networks
D. Malicious code
Answer: (SHOW ANSWER)
These laws reflected different views concerning wiretapping as technology progresseD. The Federal Intelligence Surveillance Act (FISA) of 1978 limited wiretapping for national security purposes as a result of the record of the Nixon Administration in using illegal wiretaps. The Electronic Communications Privacy Act (ECPA) of 1986 prohibited eavesdropping or the interception of message contents without distinguishing between private or public systems. The Communications Assistance for Law Enforcement Act (CALEA) of 1994 required all communications carriers to make wiretaps possible in ways approved by the FBI.

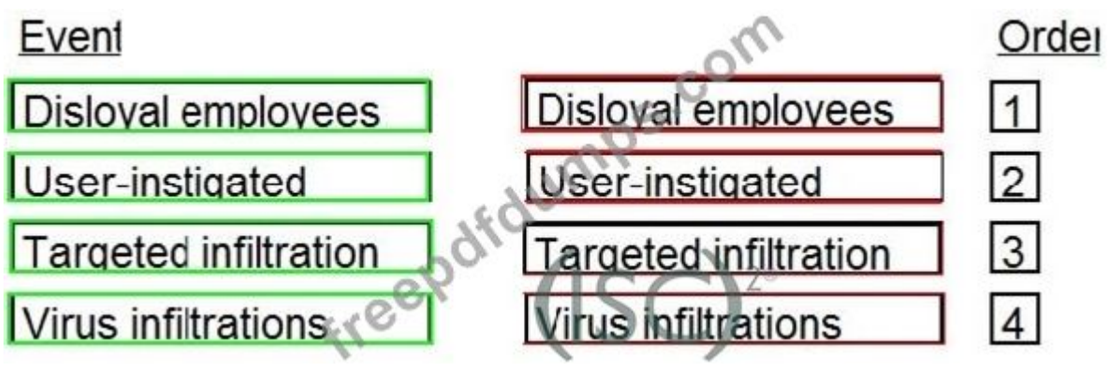
NEW QUESTION: 475
A form of digital signature where the signer is not privy to the content of the message is called a:
A. Encrypted signature
B. Zero knowledge proof
C. Masked signature
D. Blind signature
Answer: D (LEAVE A REPLY)
A blind signature algorithm for the message M uses a blinding factor, f; a modulus m; the private key, s, of the signer and the public key, q, of the signer. The sender, who generates f and knows q, presents the message to the signer in the form:

Mf q (mod m)
Thus, the message is not in a form readable by the signer since the signer does not know f. The signer signs Mf q (mod m) with his/her private key, returning
(Mf q)s (mod m)
This factor can be reduced to fMs (mod m) since s and q are inverses of each other. The sender then divides fMs (mod m) by the blinding factor, f, to obtain
Ms (mod m)
Ms (mod m) is, therefore, the message, M, signed with the private key, s, of the signer.
Answer Zero knowledge proof refers to a zero knowledge proof. In general, a zero knowledge proof involves a person, A, trying to prove that he/she knows something, S, to another person, B, without revealing S or anything about S. Answers Masked signature and Encrypted signature are distracters.

NEW QUESTION: 476
DRAG DROP
In which order, from MOST to LEAST impacted, does user awareness training reduce the occurrence of the events below?



Answer:



NEW QUESTION: 477
Who should direct short-term recovery actions immediately following a disaster?

A. Chief Information Officer.
B. Chief Operating Officer.
C. Disaster Recovery Manager.
D. Chief Executive Officer.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The disaster recovery manager should direct short-term recovery actions immediately following a disaster.
Incorrect Answers:
A: The Chief Information Officer (CIO) does not handle disaster recovery.
As a CIO must make executive decisions regarding things such as the purchase of IT equipment from suppliers or the creation of new systems, they are therefore responsible to lead and direct the workforce of their specific organization. In addition, the CIO is 'required to have strong organizational skills'. This is particularly relevant for a Chief Information Officer of an organization, who must balance roles in order to gain a competitive advantage and keep the best interests of the organization's employees. CIOs also have the responsibility of recruiting, so it is important that they take on the best employees to complete the jobs the company needs fulfilling.
B: The Chief Operating Officer does Direct recovery actions following a disaster. The Chief Operating Officer is responsible for the daily operation of the company, and routinely reports to the highest ranking executive.
D: The Chief Executive Officer (CEO) does not handle disaster recovery. The CEO has responsibilities as a director, decision maker, leader, manager and executor.
References:
Stewart, James M., Ed Tittel, and Mike Chapple, CISSP: Certified Information Systems Security Professional Study Guide, 5th Edition, Sybex, Indianapolis, 2011, p. 657

NEW QUESTION: 478
Under MAC, who can change the category of a resource?
A. All users.
B. Administrators only.
C. All managers.
D. None of the choices.
Answer: (SHOW ANSWER)
MAC is defined as follows in the Handbook of Information Security Management: With mandatory controls, only administrators and not owners of resources may make decisions that bear on or derive from policy. Only an administrator may change the category of a resource, and no one may grant a right of access that is explicitly forbidden in the access control policy.

NEW QUESTION: 479
In terms of the order of effectiveness, which of the following technologies is the least effective?
A. Voice pattern
B. Signature

C. Keystroke pattern
D. Hand geometry
Answer: B (LEAVE A REPLY)
The order of effectiveness has not changed for a few years. It is still the same today as it was three years ago. The list below present them from most effective to list effective: Iris scan Retina scan Fingerprint Hand geometry Voice pattern Keystroke pattern Signature

NEW QUESTION: 480
Which of the following methods provides the MOST protection for user credentials?
A. Digest authentication
B. Forms-based authentication
C. Self-registration
D. Basic authentication
Answer: A (LEAVE A REPLY)

NEW QUESTION: 481
The PRIMARY purpose of accreditation is to:
A. comply with applicable laws and regulations.
B. allow senior management to make an informed decision regarding whether to accept the risk of operating the system.
C. protect an organization's sensitive data.
D. verify that all security controls have been implemented properly and are operating in the correct manner.
Answer: (SHOW ANSWER)
Section: Software Development Security
Explanation/Reference:

NEW QUESTION: 482
In SSL/TLS protocol, what kind of authentication is supported when you establish a secure session between a client and a server?
A. Peer-to-peer authentication
B. Only server authentication (optional)
C. Server authentication (mandatory) and client authentication (optional)
D. Role based authentication scheme

Answer: (SHOW ANSWER)
Reference:
RESCORLA, Eric, SSL and TLS: Designing and Building Secure Systems, 2000, Addison Wesley Professional; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

NEW QUESTION: 483
Which of the following is NOT a property of a one-way hash function?
A. It converts a message of a fixed length into a message digest of arbitrary length.
B. It is computationally infeasible to construct two different messages with the same digest.
C. It converts a message of arbitrary length into a message digest of a fixed length.
D. Given a digest value, it is computationally infeasible to find the corresponding message.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Cryptographic hash functions are designed to take a string of any length as input and produce a fixed- length message digest, not a message digest of arbitrary length.
A cryptographic hash function is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. These one-way hash functions have been called "the workhorses of modern cryptography". The input data is often called the message, and the hash value is often called the message digest or simply the digest.
The ideal cryptographic hash function has four main properties:
it is easy to compute the hash value for any given message
- it is infeasible to generate a message from its hash
- it is infeasible to modify a message without changing the hash
- it is infeasible to find two different messages with the same hash.

Incorrect Answers:
B: It is true that it is computationally infeasible to construct two different messages with the same digest.
C: It is true that it converts a message of arbitrary length into a message digest of a fixed length.
D: It is true that given a digest value, it is computationally infeasible to find the corresponding message.
References:
https://en.wikipedia.org/wiki/Cryptographic_hash_function