ISC.CISSP.v2022-03-15.q465

Exam Code:	CISSP
Exam Name:	Certified Information Systems Security Professional (CISSP)
Certification Provider:	ISC
Free Question Number:	465
Version:	v2022-03-15
# of views:	6438
# of Questions views:	4650
https://www.dumpsdb.com/dumps/ISC/CISSP/ISC.CISSP.v2022-03-15.q465	

NEW QUESTION: 1
An organization is selecting a service provider to assist in the consolidation of multiple computing sites including development, implementation and ongoing support of various computer systems. Which of the following MUST be verified by the Information Security
Department?
A. The service provider will segregate the data within its systems and ensure that each region's policies are met.
B. The service provider's policies are consistent with ISO/IEC27001 and there is evidence that the service provider is following those policies.
C. The service provider will impose controls and protections that meet or exceed the current systems controls and produce audit logs as verification.
D. The service provider's policies can meet the requirements imposed by the new environment even if they differ from the organization's current policies.
Answer: (SHOW ANSWER)

NEW QUESTION: 2
What would be the PRIMARY concern when designing and coordinating a security assessment for an Automatic Teller Machine (ATM) system?
A. Processing delays
B. Regularly scheduled maintenance process
C. Physical access to the electronic hardware
D. Availability of the network connection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 3
A potential problem related to the physical installation of the Iris Scanner in regards to the usage of the iris pattern within a biometric system is:
A. Concern that the laser beam may cause eye damage.
B. The iris pattern changes as a person grows older.
C. There is a relatively high rate of false accepts.
D. The optical unit must be positioned so that the sun does not shine into the aperture.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The optical unit of the iris pattern biometric system must be positioned so that the sun does not shine into the aperture.
Incorrect Answers:
A: Iris recognition systems do not use laser like beams.
B: With iris scans, the kind of errors that can occur during the authentication process is reduced because the iris remains constant through adulthood.
C: Extreme resistance to false matching is an advantage of iris recognition.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 191
https://en.wikipedia.org/wiki/Iris_recognition

NEW QUESTION: 4
Which of the following MUST system and database administrators be aware of and apply when configuring systems used for storing personal employee data?
A. Secondary use of the data by business users
B. The business purpose for which the data is to be used
C. The overall protection of corporate resources and data
D. The organization's security policies and standards
Answer: D (LEAVE A REPLY)

NEW QUESTION: 5
What would be considered the biggest drawback of Host-based Intrusion Detection systems (HIDS)?
A. It can be very invasive to the host operating system
B. Monitors all processes and activities on the host system only
C. Virtually eliminates limits associated with encryption
D. They have an increased level of visibility and control compared to NIDS
Answer: A (LEAVE A REPLY)
The biggest drawback of HIDS, and the reason many organizations resist its use, is that it can be very invasive to the host operating system. HIDS must have the capability to monitor all

processes and activities on the host system and this can sometimes interfere with normal system processing.

HIDS versus NIDS

A host-based IDS (HIDS) can be installed on individual workstations and/ or servers to watch for inappropriate or anomalous activity. HIDSs are usually used to make sure users do not delete system files, reconfigure important settings, or put the system at risk in any other way.

So, whereas the NIDS understands and monitors the network traffic, a HIDS's universe is limited to the computer itself. A HIDS does not understand or review network traffic, and a NIDS does not "look in" and monitor a system's activity. Each has its own job and stays out of the other's way.

The ISC2 official study book defines an IDS as:

An intrusion detection system (IDS) is a technology that alerts organizations to adverse or unwanted activity. An IDS can be implemented as part of a network device, such as a router, switch, or firewall, or it can be a dedicated IDS device monitoring traffic as it traverses the network.

When used in this way, it is referred to as a network IDS, or NIDS. IDS can also be used on individual host systems to monitor and report on file, disk, and process activity on that host. When used in this way it is referred to as a host-based IDS, or HIDS.

An IDS is informative by nature and provides real-time information when suspicious activities are identified. It is primarily a detective device and, acting in this traditional role, is not used to directly prevent the suspected attack.

What about IPS?

In contrast, an intrusion prevention system (IPS), is a technology that monitors activity like an IDS but will automatically take proactive preventative action if it detects unacceptable activity. An IPS permits a predetermined set of functions and actions to occur on a network or system; anything that is not permitted is considered unwanted activity and blocked. IPS is engineered specifically to respond in real time to an event at the system or network layer. By proactively enforcing policy, IPS can thwart not only attackers, but also authorized users attempting to perform an action that is

not within policy. Fundamentally, IPS is considered an access control and policy enforcement technology, whereas IDS is considered network monitoring and audit technology.

The following answers were incorrect:

All of the other answer were advantages and not drawback of using HIDS

TIP FOR THE EXAM:

Be familiar with the differences that exists between an HIDS, NIDS, and IPS. Know that IDS's are mostly detective but IPS are preventive. IPS's are considered an access control and policy enforcement technology, whereas IDS's are considered network monitoring and audit technology.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 5817-5822). McGraw-Hill. Kindle Edition.

and

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Access

Control ((ISC)2 Press), Domain1, Page 180-188 or on the kindle version look for Kindle Locations 3199-3203 Auerbach Publications.

NEW QUESTION: 6
Security measures that protect message traffic independently on each communication path are called:
A. Link oriented
B. Procedure oriented
C. Pass-through oriented
D. End-to-end oriented
Answer: A (LEAVE A REPLY)
Link encryption encrypts all the data along a specific communication path like a satellite link, T3 line, or telephone circuit. Not only is the user information encrypted, but the header, trailers, addresses, and routing data hat are part of the packets are also encrypted. This provides extra protection against packet sniffers and eavesdroppers. - Shon Harris All-in-one CISSP Certification Guide pg 560

NEW QUESTION: 7
The ISO/IEC 27001:2005 is a standard for:
A. Information Security Management System
B. Implementation and certification of basic security measures
C. Evaluation criteria for the validation of cryptographic algorithms
D. Certification of public key infrastructures
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The ISO 27000 Directory at: http://www.27000.org/index.htm has great coverage of the ISO 27000 series.
The text below was extracted from their website.
As mention by Belinda the ISO 27001 standard is the certification controls criteria while ISO 27002 is the actual standard. ISO 27002 used to be called ISO 17799 before being renamed.
The ISO 27001 standard was published in October 2005, essentially replacing the old BS7799-2 standard.
It is the specification for an ISMS, an Information Security Management System. BS7799 itself was a long standing standard, first published in the nineties as a code of practice. As this matured, a second part emerged to cover management systems. It is this against which certification is granted. Today in excess of a thousand certificates are in place, across the world.
ISO 27001 enhanced the content of BS7799-2 and harmonized it with other standards. A scheme has been introduced by various certification bodies for conversion from BS7799 certification to ISO27001 certification.

The objective of the standard itself is to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System".
Regarding its adoption, this should be a strategic decision. Further, "The design and implementation of an organization's ISMS is influenced by their needs and objectives, security requirements, the process employed and the size and structure of the organization".
The standard defines its 'process approach' as "The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management". It employs the PDCA, Plan-Do-Act model to structure the processes, and reflects the principles set out in the OECG guidelines (see oecd.org).
THE CONTENTS OF ISO 27001
The content sections of the standard are:
Context Of The Organization
- Information Security Leadership
- Planning An ISMS
- Support
- Operation
- Performance Evaluation
- Improvement
- Annex A - List of controls and their objectives

The ISO 27002 standard is the rename of the ISO 17799 standard, and is a code of practice for information security. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided within ISO 27001.
The standard "established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization". The actual controls listed in the standard are intended to address the specific requirements identified via a formal risk assessment. The standard is also intended to provide a guide for the development of "organizational security standards and effective security management practices and to help build confidence in inter-organizational activities".
The basis of the standard was originally a document published by the UK government, which became a standard 'proper' in 1995, when it was re-published by BSI as BS7799. In 2000 it was again re-published, this time by ISO, as ISO 17799. A new version of this appeared in 2005, along with a new publication, ISO
27001. These two documents are intended to be used together, with one complimenting the other.
ISO's future plans for this standard are focused largely around the development and publication of industry specific versions (for example: health sector, manufacturing, and so on). Note that this is a lengthy process, so the new standards will take some time to appear
THE CONTENTS OF ISO 17799 / 27002

The content sections are:
Structure
- Risk Assessment and Treatment
- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical Security
- Communications and Ops Management
- Access Control
- Information Systems Acquisition, Development, Maintenance
- Information Security Incident management
- Business Continuity
- Compliance
- References:

http://www.iso.org/iso/catalogue_detail?csnumber=42103
http://www.27000.org/index.htm

NEW QUESTION: 8
Which of the following is addressed by Kerberos?
A. Confidentiality and Integrity
B. Authentication and Availability
C. Validation and Integrity
D. Auditability and Integrity
Answer: A (LEAVE A REPLY)
Kerberos addresses the confidentiality and integrity of information.
It also addresses primarily authentication but does not directly address availability.
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 42 and https://www.ietf.org/rfc/rfc4120txt and http://learn-networking.com/network-security/how-kerberos-authentication-works

NEW QUESTION: 9
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: 10
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: 11
Between which pair of Open System Interconnection (OSI) Reference Model layers are routers used as a communications device?
A. Data-Link and Transport
B. Network and Session

C. Physical and Data-Link
D. Transport and Session
Answer: (SHOW ANSWER)

NEW QUESTION: 12
Java follows which security model:
A. least privilege
B. Sand box
C. CIA
D. OSI
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
When a Java applet is executed, the JVM (Java Virtual Machine) will create a virtual machine, which provides an environment called a sandbox. This virtual machine is an enclosed environment in which the applet carries out its activities.
Incorrect Answers:
A: The principle of least privilege (POLP) is the practice of limiting access to the minimal level that will allow normal functioning. Java uses the sandbox model, not the POLP model.
C: A simple but widely-applicable security model is the CIA triad; standing for Confidentiality, Integrity and Availability; three key principles which should be guaranteed in any kind of secure system. Java does not use the CIA security model.
D: OSI (Open Systems Interconnection) is reference model for how applications can communicate over a network. OSI is not related to Java.
References:
Conrad, Eric, Seth Misenar and Joshua Feldman, CISSP Study Guide, 2nd Edition, Syngress, Waltham,
2012, p. 1154

NEW QUESTION: 13
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: (SHOW ANSWER)
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: 14
Related to information security, confidentiality is the opposite of which of the following?
A. closure
B. disclosure
C. disposal
D. disaster
Answer: B (LEAVE A REPLY)
Confidentiality is the opposite of disclosure.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

NEW QUESTION: 15
Which of the following is true regarding a secure access model?
A. Secure information cannot flow to a more secure user.
B. Secure information cannot flow to a less secure user.
C. Secure information can flow to a less secure user.
D. None of the choices.
Answer: B (LEAVE A REPLY)
Access restrictions such as access control lists and capabilities sometimes are not enough. In some cases, information needs to be tightened further, sometimes by an authority higher than the owner of the information. For example, the owner of a top-secret document in a government office might deem the information available to many users, but his manager might know the information should be restricted further than that. In this case, the flow of information needs to be controlled -- secure information cannot flow to a less secure user.

NEW QUESTION: 16
Which of the following are the two commonly defined types of covert channels?
A. Storage and Timing
B. Software and Timing
C. Storage and Kernel
D. Kernel and Timing
Answer: A (LEAVE A REPLY)
Explanation/Reference:

Explanation:
A covert channel is a way for an entity to receive information in an unauthorized manner. It is an information flow that is not controlled by a security mechanism.
Covert channels are of two types: storage and timing.
A covert storage channel involves direct or indirect reading of a storage location by another process. A covert timing channel depends upon being able to influence the rate that some other process is able to acquire resources, such as the CPU.
A covert storage channel is a "covert channel that involves the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process.
Covert storage channels typically involve a finite resource (e.g. sectors on a disk) that is shared by two subjects at different security levels.
A covert timing channel is a "covert channel in which one process signals information to another by modulating its own use of system resources (e.g. CPU time) in such a way that this manipulation affects the real response time observed by the second process
Incorrect Answers:
B: Software and Timing are not defined types of covert channels.
C: Kernel is not a defined type of covert channel.
D: Kernel is not a defined type of covert channel.
References:
http://www.isg.rhul.ac.uk/~prai175/ISGStudentSem07/CovertChannels.ppt
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, pp. 378-379

NEW QUESTION: 17
Which of the following statements regarding trade secrets is FALSE?
A. For a company to have a resource qualify as a trade secret, it must provide the company with some type of competitive value or advantage.
B. The Trade Secret Law normally protects the expression of the idea of the resource.
C. Many companies require their employees to sign nondisclosure agreements regarding the protection of their trade secrets.
D. A resource can be protected by law if it is not generally known and if it requires special skill, ingenuity, and/or expenditure of money and effort to develop it.
Answer: B (LEAVE A REPLY)

Explanation/Reference:
Explanation:
It does not protect the expression of the idea of the resource, but specific resources. The other answers are incorrect because: For a company to have a resource qualify as a trade secret, it must provide the company with some type of competitive value or advantage is incorrect as it is a feature of a trade secret.
Many companies require their employees to sign nondisclosure agreements regarding the protection of their trade secrets is also incorrect as it is one of the ways to protect the trade secrets of a company. A resource can be protected by law if it is not generally known and if it requires special skill, ingenuity, and/or expenditure of money and effort to develop it is also incorrect as it is also a feature of a trade secret.
References: Shon Harris AIO v3, Chapter 10: Law, Investigation, and Ethics, Page: 720- 721

NEW QUESTION: 18
Assessing a third party's risk by counting bugs in the code may not be the best measure of an attack surface within the supply chain.
Which of the following is LEAST associated with the attack surface?
A. Input protocols
B. Target processes
C. Error messages
D. Access rights
Answer: (SHOW ANSWER)
Section: Security Assessment and Testing

NEW QUESTION: 19
Which of the following is the marriage of object-oriented and relational technologies combining the attributes of both?
A. object-relational database
B. object-oriented database
C. object-linking database
D. object-management database
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
An object-relational database is described as is the marriage of object-oriented and relational technologies combining the attributes of both.
An object-relational database (ORD) or object-relational database management system (ORDBMS) is a relational database with a software front end that is written in an object-oriented programming language. A relational database just holds data in static two-dimensional tables. When the data are accessed, some type of processing needs to be carried out on it-otherwise, there is really no reason to obtain the data. If we have a front end that provides the procedures

(methods) that can be carried out on the data, then each and every application that accesses this database does not need to have the necessary procedures. This means that each and every application does not need to contain the procedures necessary to gain what it really wants from this database.
Incorrect Answers:
B: An object-oriented database is a database designed to handle a variety of data types (images, audio, documents, video). This is not what is described in the question.
C: An object-linking database is not a valid database type.
D: An object-management database is not a valid database type.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 1175

NEW QUESTION: 20
How many times should a diskette be formatted to comply with TCSEC
Orange Book object reuse recommendations?
A. Five
B. Nine
C. Three
D. Seven
Answer: D (LEAVE A REPLY)
The correct answer is 7. Most computer certification and accreditation
standards recommend that diskettes be formatted seven times to
prevent any possibility of data remanence .

NEW QUESTION: 21
A copyright protects _____.
A. The trade secrets of a company
B. A persons private papers
C. An invention
D. An expression or an idea
E. Distinguishing or unique characters, colors, or words
Answer: (SHOW ANSWER)
A copyright protects the expression of a resource, not the resource directly.

NEW QUESTION: 22
What is NOT included in a data dictionary?
A. Data Element Definitions
B. Schema Objects
C. Reference Keys
D. Structured Query Language
Answer: D (LEAVE A REPLY)

Structured Query Language (SQL) is a standard programming language used to
allow clients to interact with a database. Although SQL can be used to access the data dictionary, it is NOT a part of the data dictionary.
A data dictionary, or metadata repository, as defined in the IBM Dictionary of Computing, is a "centralized repository of information about data such as meaning, relationships to other data, origin, usage, and format." The term may have one of several closely related meanings pertaining to databases and database management systems (DBMS):
a document describing a database or collection of databases
an integral component of a DBMS that is required to determine its structure
a piece of middleware that extends or supplants the native data dictionary of a DBMS
METADATA & DATA DICTIONARY
In addition to facilitating the effective retrieving of information, metadata can also manage restricted access to information. Metadata can serve as a gatekeeper function to filter access and thus provide security controls. One specialized form of metadata is the data dictionary, a central repository of information regarding the various databases that may be used within an enterprise. The data dictionary does not provide direct control of the databases, or access control functions, but does give the administrator a full picture of the various bodies of information around the company, potentially including the sensitivity and classification of material held in different objects.
Therefore, the data dictionary can be used in risk management and direction of protective resources.
A data dictionary is a central collection of data element definitions, schema objects, and reference keys. The schema objects can contain tables, views, indexes, procedures, functions, and triggers. A data dictionary can contain the default values for columns, integrity information, the names of users, the privileges and roles for users, and auditing information. It is a tool used to centrally manage parts of a database by controlling data about the data (referred to as metadata) within the
database. It provides a cross-reference between groups of data elements and the databases. The database management software creates and reads the data dictionary to ascertain what schema objects exist and checks to see if specific users have the proper access rights to view them
The following answers were incorrect:
All of the other options were included within the data dictionary, only SQL is NOT part of the Data Dictionary.
The following reference(s) were/was used to create this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition , Software Development, Page 1178. For kindle users see Kindle Locations 23951-23957.
Corporate; (Isc)2 (2010-04-20). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press), Software Development Security, Page 667. For Kindle users see Kindle Locations 5950-5954.
http://en.wikipedia.org/wiki/Data_dictionary

NEW QUESTION: 23
Which of the following can be defined as an attribute in one relation that has values matching the primary key in another relation?
A. foreign key
B. candidate key
C. primary key
D. secondary key
Answer: A (LEAVE A REPLY)
If an attribute in one relation has values matching the primary key in another relation, this attribute is called a foreign key. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 45.

NEW QUESTION: 24
Which of the following is a CHARACTERISTIC of a decision support system (DSS) in regards to Threats and Risks Analysis?
A. DSS is aimed at solving highly structured problems.
B. DSS emphasizes flexibility in the decision making approach of users.
C. DSS supports only structured decision-making tasks.
D. DSS combines the use of models with non-traditional data access and retrieval functions.
Answer: B (LEAVE A REPLY)
DSS emphasizes flexibility in the decision-making approach of users. It is aimed at solving less structured problems, combines the use of models and analytic techniques with
traditional data access and retrieval functions and supports semi-structured decision-making tasks.
DSS is sometimes referred to as the Delphi Method or Delphi Technique:
The Delphi technique is a group decision method used to ensure that each member gives an honest opinion of what he or she thinks the result of a particular threat will be. This avoids a group of individuals feeling pressured to go along with others' thought processes and enables them to participate in an independent and anonymous way. Each member of the group provides his or her opinion of a certain threat and turns it in to the team that is performing the analysis. The results are compiled and distributed to the group members, who then write down their comments anonymously and return them to the analysis group. The comments are compiled and redistributed for more comments until a consensus is formed. This method is used to obtain an agreement on cost, loss values, and probabilities of occurrence without individuals having to agree
verbally.
Here is the ISC2 book coverage of the subject:
One of the methods that uses consensus relative to valuation of information is the consensus/modified Delphi method. Participants in the valuation exercise are asked to comment anonymously on the task being discussed. This information is collected and disseminated to a participant other than the original author. This participant comments upon the observations of the

original author. The information gathered is discussed in a public forum and the best course is agreed upon by the group (consensus).
EXAM TIP:
The DSS is what some of the books are referring to as the Delphi Method or Delphi Technique. Be
familiar with both terms for the purpose of the exam.
The other answers are incorrect:
'DSS is aimed at solving highly structured problems' is incorrect because it is aimed at solving less
structured problems.
'DSS supports only structured decision-making tasks' is also incorrect as it supports semi-structured decision-making tasks.
'DSS combines the use of models with non-traditional data access and retrieval functions' is also incorrect as it combines the use of models and analytic techniques with traditional data access and retrieval functions.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 91). McGraw-Hill. Kindle
Edition.
and
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Information Security Governance and Risk Management ((ISC)2 Press) (Kindle Locations 1424-1426). Auerbach Publications. Kindle Edition.

NEW QUESTION: 25
In a refinement of the Bell?LaPadula model, the strong tranquility
property states that:
A. Objects never change their security level.
B. Objects can change their security level in an unconstrained fashion.
C. Objects never change their security level in a way that would violate the system security policy.
D. Subjects can read up.
Answer: A (LEAVE A REPLY)
Answer "Objects never change their security level in a way that would violate the system security policy" is known as the weak tranquility property. The two other answers are distracters.

NEW QUESTION: 26
Which access control model provides upper and lower bounds of access capabilities for a subject?
A. Role-based access control
B. Lattice-based access control
C. Biba access control

D. Content-dependent access control

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Explanation:

Lattice-based access control is a mathematical model that allows a system to easily represent the different security levels and control access attempts based on those levels. Every pair of elements has a highest lower bound and a lowest upper bound of access rights.

Incorrect Answers:

A: Role-based access control (RBAC) provides access to resources according to the role the user holds within the company or the tasks that the user has been assigned.

C: Biba is a security model, rather than an access control model. It centers on preventing information from flowing from a low integrity level to a high integrity level D: Content-dependent access control is when the access decisions depend upon the value of an attribute of the object itself.

References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, pp. 224, 377, G-9

http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.41.5365

NEW QUESTION: 27

Phreakers are hackers who specialize in telephone fraud. What type of telephone fraud manipulates the line voltage to receive a tool-free call?

A. Red Boxes

B. Blue Boxes

C. White Boxes

D. Black Boxes

Answer: (SHOW ANSWER)

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 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.

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: 28

Which Orange Book evaluation level is described as "Structured Protection"?

A. A1

B. B3
C. B2
D. B1
Answer: C (LEAVE A REPLY)
Class B2 corresponds to Structured Protection.
Division B - Mandatory Protection
Mandatory access is enforced by the use of security labels. The architecture is based on the Bell-LaPadula security model and evidence of the reference monitor enforcement must be available.
B1: Labeled Security Each data object must contain a classification label and each subject must have a clearance label. When a subject attempts to access an object, the system must compare the subject and the object's security labels to ensure the requested actions are acceptable. Data leaving the system must also contain an accurate security label. The security policy is based on an informal statement and the design specifications are reviewed and verified. It is intended for environments that handle classified data.
B2: Structured Protection The security policy is clearly defined and documented and the system design and implementation is subjected to more thorough review and testing procedures. This class requires more stringent authentication mechanisms and well- defined interfaces between layers. Subject 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 there are no trapdoors. There is a separation of operator and administration functions within the system to provide more trusted and protected operational functionality. Distinct address spaces must be provided to isolated processes, and a covert channel analysis is conducted. This class adds assurance by adding requirements to the design of the system. The environment that would require B2 systems could process sensitive data that requires a higher degree of security. This environment would require systems that are relatively resistant to penetration and compromise.
B3 Security Domains In this class, more granularity is provided in each protects mechanism and the programming code that is not necessary to support the security is excluded. The design and implementation should not provide too much complexity because as the complexity of a system increases, the ability of the individuals who need to test, maintain, and configure it reduces; thus, the overall security can be threatened. The reference monitor components must be small enough to test properly and be tamperproof.
The security administrator role is clearly defined and the system must be able to recover from failures without its security level being compromised. When the system starts up and loads its operating system and components, it must be done in an initial secure state to ensure any weakness of the system cannon be taken advantage of in this slice of time. An environment that requires B3 systems is a highly secured environment that processes very sensitive information. It requires systems that are highly resistant to penetration.
Note: In class (B2) systems, the TCB is based on a clearly defined and documented formal security policy model that requires the discretionary and mandatory access control enforcement found in class (B1) systems be extended to all subjects and objects in the

ADP system. In addition, covert channels are addressed. The TCB must be carefully structured into protection-critical and non-protection-critical elements. Class B corresponds to "Structured Protection" inside the Orange Book.

NEW QUESTION: 29
What does CSMA stand for?
A. Common Systems Methodology Applications
B. Carrier Sense Multiple Access
C. Carrier Sense Multiple Attenuation
D. Carrier Station Multi-port Actuator
Answer: B (LEAVE A REPLY)
The correct answer is "Carrier Sense Multiple Access". The other acronyms do not exist.

NEW QUESTION: 30
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: A (LEAVE A REPLY)
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: 31
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: 32
Which of the following statements pertaining to ethical hacking is incorrect?
A. An organization should use ethical hackers who do not sell auditing, hardware, software, firewall, hosting, and/or networking services.
B. Testing should be done remotely to simulate external threats.
C. Ethical hacking should not involve writing to or modifying the target systems negatively.
D. Ethical hackers never use tools that have the potential of affecting servers or services.
Answer: D (LEAVE A REPLY)
This means that many of the tools used for ethical hacking have the potential of exploiting vulnerabilities and causing disruption to IT system. It is up to the individuals performing the tests to be familiar with their use and to make sure that no such disruption can happen or at least shoudl be avoided.
The first step before sending even one single packet to the target would be to have a signed agreement with clear rules of engagement and a signed contract. The signed contract explains to the client the associated risks and the client must agree to them before you even send one packet to the target range. This way the client understand that some of the test could lead to interruption of service or even crash a server. The client signs that he is aware of such risks and willing to accept them.
The following are incorrect answers:
An organization should use ethical hackers who do not sell auditing, hardware, software, firewall, hosting, and/or networking services. An ethical hacking firm's independence can be questioned if they sell security solutions at the same time as doing testing for the same client. There has to be independance between the judge (the tester) and the accuse (the client).
Testing should be done remotely to simulate external threats Testing simulating a cracker from the

Internet is often time one of the first test being done, this is to validate perimeter security. By performing tests remotely, the ethical hacking firm emulates the hacker's approach more realistically.
Ethical hacking should not involve writing to or modifying the target systems negatively. Even though ethical hacking should not involve negligence in writing to or modifying the target systems or reducing its response time, comprehensive penetration testing has to be performed using the most complete tools available just like a real cracker would.
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, Appendix F: The Case for Ethical Hacking (page 520).

NEW QUESTION: 33
Which backup method only copies files that have been recently added or changed and also leaves the archive bit unchanged?
A. Full backup method
B. Incremental backup method
C. Fast backup method
D. Differential backup method
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The Differential backup method backs up the files that have been modified since the last full backup. The differential process does not change the archive bit value.
Incorrect Answers:
A: During a full backup all data are backed up and saved to some type of storage media, and the archive bit is cleared.
B: The Incremental backup method backs up all the files that have changed since the last full or incremental backup and sets the archive bit to 0.
C: There is no backup method named fast backup method.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 936

NEW QUESTION: 34
Which of the following security-focused protocols operates at a layer different from the others?
A. Simple Key Management for Internet Protocols (SKIP)
B. Secure shell (SSH-2)
C. Secure HTTP
D. Secure socket layer (SSL)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 35
Which of the following elements MUST a compliant EU-US Safe Harbor Privacy Policy contain?
A. An explanation of how long the data subject's collected information will be retained for and how it will be eventually disposed.
B. An explanation of the regulatory frameworks and compliance standards the information collecting organization adheres to.
C. An explanation of all the technologies employed by the collecting organization in gathering information on the data subject.
D. An explanation of who can be contacted at the organization collecting the information if corrections are required by the data subject.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 36
The MULTICS operating system is a classic example of:
A. Ring protection system.
B. Object orientation.
C. An open system.
D. Database security.
Answer: (SHOW ANSWER)
The correct answer is "Ring protection system". Multics is based on the ring protection architecture.

NEW QUESTION: 37
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. Remove all non-essential client-side web services from the network.
B. Screen for harmful exploits of client-side services before implementation.
C. Block all client side web exploits at the perimeter.
D. Harden the client image before deployment.
Answer: (SHOW ANSWER)

NEW QUESTION: 38
Which of the following processes establish the minimum national standards for certifying and accrediting national security systems?
A. DITSCAP
B. NIACAP
C. CIAP
D. Defense audit
Answer: B (LEAVE A REPLY)

The NIACAP provides a standard set of activities, general tasks, and
a management structure to certify and accredit systems that will maintain the information assurance and security posture of a system or site.
The NIACAP is designed to certify that the information system meets
documented accreditation requirements and will continue to maintain
the accredited security posture throughout the system life cycle.
* Answer CIAP is being developed for the evaluation of critical commercial systems and uses the NIACAP methodology.
* DITSCAP establishes for the defense entities a standard process, set of activities, general task descriptions, and a management structure to certify and accredit IT systems that will maintain the required security posture. The process is designed to certify that the IT system meets the accreditation requirements and that the system will maintain the accredited security posture throughout the system life cycle. The four phases to the DITSCAP are Definition, Verification, Validation, and
Post Accreditation.
* Answer "Defense audit" is a distracter.

NEW QUESTION: 39
The end result of implementing the principle of least privilege means which of the following?
A. Users would get access to only the info for which they have a need to know
B. Users can access all systems.
C. Users get new privileges added when they change positions.
D. Authorization creep.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Least privilege means an individual should have just enough permissions and rights to fulfill his role in the company and no more.
Incorrect Answers:
B Least privilege means an individual should have just enough permissions and rights to fulfill his role in the company and no more. Not all users in an organization requires access to all systems.
C: The principle of least privilege would require that the rights required for the position be closely evaluated and where possible rights revoked.
D: Authorization creep occurs when users are given additional rights with new positions and responsibilities. The principle of least privilege should actually prevent authorization creep.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, pp. 281, 1236
https://en.wikipedia.org/wiki/Principle_of_least_privilege

NEW QUESTION: 40

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. Scalar processors

Answer: C (LEAVE A REPLY)

Complex Instruction Set Computer (CISC) uses instructions that perform many operations per instruction. It was based on the fact that in earlier technologies, the instruction fetch was the longest part of the cycle. Therefore, by packing more operations into an instruction, the number of fetches could be reduced. Pipelining involves overlapping the steps of different instructions to increase the performance in a computer. Reduced Instruction Set Computers (RISC) involve simpler instructions that require fewer clock cycles to execute. Scalar processors are processors that execute one instruction at a time. 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 Architectures and Models (page 188).

NEW QUESTION: 41

Which of the following can be defined as THE unique attribute used as a unique identifier within a given table to identify a tuple?

A. primary key

B. candidate key

C. foreign key

D. secondary key

Answer: A (LEAVE A REPLY)

The following answers were NOT correct:

Candidate Key: A candidate key is a combination of attributes that can be uniquely used to identify a database record without any extraneous data. Each table may have one or more candidate keys. One of these candidate keys is selected as the table primary key.

Foreign Key: A foreign key is a field in a relational table that matches the primary key column of another table. The foreign key can be used to cross-reference tables.

Secondary key: The term secondary key is a key that is used strictly for data-retrieval purposes. A secondary key is sometimes defined as a "data item value that identifies a set of records." It is important to note that a secondary key does not need to have unique values in a table; in this respect, secondary keys differ from primary keys (and candidate keys and superkeys).

References:

A candidate key is an attribute that is a unique identifier within a given table.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 45.

Candidate Key Ref: http://databases.about.com/cs/specificproducts/g/candidate.htm

Feedback from Jerry: A candidate key is one of several alternative columns in a table that may be chosen as a primary key. The PRIMARY KEY IS the unique identifier. The foundation of a relational database is the establishiment and reliance on a unique primary key, not candidate keys. Primary key is a more correct answer to this question than candidate key.
Secondary key ref: http://www.gslis.utexas.edu/~wyllys/DMPAMaterials/keys.html

NEW QUESTION: 42
In the US, HIPAA addresses which of the following?
A. Availability and Accountability
B. Security and Availability
C. Security and Privacy
D. Accuracy and Privacy
Answer: C (LEAVE A REPLY)

NEW QUESTION: 43
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: 44
Which of the following would BEST support effective testing of patch compatibility when patches are applied to an organization's systems?
A. Management support for patching
B. Automated system patching
C. Standardized patch testing equipment
D. Standardized configurations for devices
Answer: D (LEAVE A REPLY)

NEW QUESTION: 45
Which protocol makes USE of an electronic wallet on a customer's PC and sends encrypted credit card information to merchant's Web server, which digitally signs it and sends it on to its processing bank?
A. SSH (Secure Shell)
B. S/MIME (Secure MIME)
C. SET (Secure Electronic Transaction)
D. SSL (Secure Sockets Layer)
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Secure Electronic Transaction (SET) is a security technology proposed by Visa and MasterCard to allow for more secure credit card transaction possibilities than what is currently available. SET has been waiting in the wings for full implementation and acceptance as a standard for quite some time. Although SET provides an effective way of transmitting credit card information,

businesses and users do not see it as efficient because it requires more parties to coordinate their efforts, more software installation and configuration for each entity involved, and more effort and cost than the widely used SSL method.
SET is a cryptographic protocol and infrastructure developed to send encrypted credit card numbers over the Internet. The following entities would be involved with a SET transaction, which would require each of them to upgrade their software, and possibly their hardware:
Issuer (cardholder's bank) The financial institution that provides a credit card to the individual.
Cardholder The individual authorized to use a credit card.
Merchant The entity providing goods.
Acquirer (merchant's bank) The financial institution that processes payment cards.
Payment gateway This processes the merchant payment. It may be an acquirer.
Incorrect Answers:
A: SSH is a network protocol that allows for a secure connection to a remote system. Developed to replace Telnet and other insecure remote shell methods. This is not what is described in the question.
B: S/MIME stands for Secure/Multipurpose Internet Mail Extensions, which outlines how public key cryptography can be used to secure MIME data types. This is not what is described in the question.
D: SSL (Secure Sockets Layer) is most commonly used to Internet connections and e-commerce transactions. It is used instead of SET but is not what is described in the question.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 856

NEW QUESTION: 46
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. allow access by the organization staff at any time.
B. are more rigorous than the original controls.
C. cannot be accessed by subcontractors of the third party.
D. are able to limit access to sensitive information.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 47
Which of the following is often implemented by a one-for-one disk to disk ratio?
A. RAID Level 1
B. RAID Level 0
C. RAID Level 2
D. RAID Level 5
Answer: A (LEAVE A REPLY)
This is often implemented by a one-for-one disk-to-disk ratio.
RAID Level 2 provides redundancy by writing all data to two or more drives set. The performance of a level 1 array tends to be faster on reads and slower on writes compared to a single drive, but if either of the drive sets fails, no data is lost. This is a good entry-level redundant system, since only two drives are required as a minimum; however, since one drive is used to store a duplicate of the data, the cost per megabyte is high. This level is commonly referred to as mirroring.
Please visit http://www.sohoconsult.ch/raid/raid1.html for a nice overview of RAID Levels.
For the purpose of the exam you must be familiar with RAID 0 to 5, 10, and 50.
References:
http://www.sohoconsult.ch/raid/raid1.html
and
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: 48
What is it called when a system has apparent flaws that were deliberately available for penetration and exploitation?
A. A jail
B. Investigation
C. Enticement
D. Data manipulation
E. Trapping
Answer: C (LEAVE A REPLY)
Administrators that leave systems with apparent flaws are performing an act of enticement. This is sometimes called a honeypot.

NEW QUESTION: 49

Which of the following is the MOST important output from a mobile application threat modeling exercise according to Open Web Application Security Project (OWASP)?

A. Countermeasures and mitigations for vulnerabilities

B. The likelihood and impact of a vulnerability

C. Application interface entry and endpoints

D. A data flow diagram for the application and attack surface analysis

Answer: (SHOW ANSWER)

NEW QUESTION: 50

Which one of the following is NOT one of the outcomes of a vulnerability assessment?

A. Quantative loss assessment

B. Qualitative loss assessment

C. Formal approval of BCP scope and initiation document

D. Defining critical support areas

Answer: C (LEAVE A REPLY)

When seeking to determine the security position of an organization, the security professional will eventually turn to a vulnerability assessment to help identify specific areas of weakness that need to be addressed. A vulnerability assessment is the use of various tools and analysis methodologies to determine where a particular system or process may be susceptible to attack or misuse. Most vulnerability assessments concentrate on technical vulnerabilities in systems or applications, but the assessment process is equally as effective when examining physical or administrative business processes.

The vulnerability assessment is often part of a BIA. It is similar to a Risk Assessment in that there is a quantitative (financial) section and a qualitative (operational) section. It differs in that i t is smaller than a full risk assessment and is focused on providing information that is used solely for the business continuity plan or disaster recovery plan.

A function of a vulnerability assessment is to conduct a loss impact analysis. Because there will be two parts to the assessment, a financial assessment and an operational assessment, it will be necessary to define loss criteria both quantitatively and qualitatively.

Quantitative loss criteria may be defined as follows:

-Incurring financial losses from loss of revenue, capital expenditure, or personal liability resolution

-The additional operational expenses incurred due to the disruptive event

-

Incurring financial loss from resolution of violation of contract agreements

-

Incurring financial loss from resolution of violation of regulatory or compliance requirements

Qualitative loss criteria may consist of the following:

-

The loss of competitive advantage or market share

-

The loss of public confidence or credibility, or incurring public mbarrassment

During the vulnerability assessment, critical support areas must be defined in order to assess the impact of a disruptive event. A critical support area is defined as a business unit or function that must be present to sustain continuity of the business processes, maintain life safety, or avoid public relations embarrassment.
Critical support areas could include the following:
-Telecommunications, data communications, or information technology areas
-Physical infrastructure or plant facilities, transportation services
-Accounting, payroll, transaction processing, customer service, purchasing
The granular elements of these critical support areas will also need to be identified. By granular elements we mean the personnel, resources, and services the critical support areas need to maintain business continuity
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 4628-4632). Auerbach Publications. Kindle Edition.
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 277.

NEW QUESTION: 51
Which of the following is the MOST important element of change management documentation?
A. Number of changes being made
B. Business case justification
C. A stakeholder communication
D. List of components involved
Answer: (SHOW ANSWER)

NEW QUESTION: 52
By requiring the user to use more than one finger to authenticate, you can:
A. Provide statistical improvements in EAR.
B. Provide statistical improvements in MTBF.
C. Provide statistical improvements in FRR.
D. Provide statistical improvements in ERR.
Answer: (SHOW ANSWER)
Statistical improvements in false rejection rates can also be achieved by requiring the user to use more than one finger to authenticate. Such techniques are referred to as flexible verification.

NEW QUESTION: 53
Which of the following choices is a valid Public Key Cryptography Standard (PKCS) addressing RSA?
A. PKCS #17799
B. PKCS-RSA
C. PKCS#1

D. PKCS#11

Answer: C (LEAVE A REPLY)

This document provides recommendations for the implementation of public-key cryptography based on the RSA algorithm, covering the following aspects: cryptographic primitives; encryption schemes; signature schemes with appendix; ASN.1 syntax for representing keys and for identifying the schemes.

Reference(s) used for this question: RSA Laboratories at http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs-rsacryptography-standard.htm

NEW QUESTION: 54

What is the main purpose of Corporate Security Policy?

A. To transfer the responsibility for the information security to all users of the organization

B. To communicate management's intentions in regards to information security

C. To provide detailed steps for performing specific actions

D. To provide a common framework for all development activities

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Explanation:

A security policy is an overall general statement produced by senior management (or a selected policy board or committee) that dictates what role security plays within the organization.

Incorrect Answers:

A: It is not the main purpose of Corporate Security Policy to transfer the responsibility for the information security to all users of the organization.

C: It is not the main purpose of Corporate Security Policy to provide detailed steps for performing specific actions.

D: It is not the main purpose of Corporate Security Policy to provide a common framework for all development activities.

References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 102

NEW QUESTION: 55

When block chaining cryptography is used, what type of code is calculated and appended to the data to ensure authenticity?

A. Message authentication code.

B. Ciphertext authentication code

C. Cyclic redundancy check

D. Electronic digital signature

Answer: A (LEAVE A REPLY)

The original Answer was B.

This is incorrect as cipthertext is the result not an

authentication code.

"If meaningful plaintext is not automatically recognizable, a message authentication code (MAC) can be computed and appended to the message. The computation is a function of the entire message and a secret key; it is practically impossible to find another message with the same authenticator. The receiver checks the authenticity of the message by computing the MAC using the same secret key and then verifying that the computed value is the same as the one transmitted with the message. A MAC can be used to provide authenticity for unencrypted messages as well as for encrypted ones. The National Institute of Standards and Technology (NIST) has adopted a standard for computing a MAC. (It is found in Computer Data Authentication, Federal Information Processing Standards Publication (FIPS PUB) 113.)" http://www.cccure.org/Documents/HISM/637-639.html from the Handbook of Information Security Management by Micki Krause

NEW QUESTION: 56
At which OSI layer does SSL reside in?
A. Application
B. Session
C. Transport
D. Network
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
SSL encryption takes place at the transport layer.
Incorrect Answers:
A: SSL resides at transport layer, not at the application layer.
B: SSL resides at transport layer, not at the session layer.
D: SSL resides at transport layer, not at the network layer.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 846

NEW QUESTION: 57
As a security manger which of the following is the MOST effective practice for providing value to an organization?
A. Assess business risk and apply security resources accordingly
B. Coordinate security implementations with internal audit
C. Achieve compliance regardless of related technical issues
D. Identify confidential information and protect it
Answer: D (LEAVE A REPLY)

NEW QUESTION: 58
What is another name for a VPN?
A. Firewall

B. Tunnel
C. Packet switching
D. Pipeline
E. Circuit switching
Answer: B (LEAVE A REPLY)
A VPN creates a secure tunnel through an insecure network.

NEW QUESTION: 59
Which factors MUST be considered when classifying information and supporting assets for risk management, legal discovery, and compliance?
A. Data stewardship roles, data handling and storage standards, data lifecycle requirements
B. Compliance office roles and responsibilities, classified material handling standards, storage system lifecycle requirements
C. System owner roles and responsibilities, data handling standards, storage and secure development lifecycle requirements
D. System authorization roles and responsibilities, cloud computing standards, lifecycle requirements
Answer: A (LEAVE A REPLY)

NEW QUESTION: 60
This type of supporting evidence is used to help prove an idea or a point, however it cannot stand on its own, it is used as a supplementary tool to help prove a primary piece of evidence. What is the name of this type of evidence?
A. Circumstantial evidence
B. Corroborative evidence
C. Opinion evidence
D. Secondary evidence
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Corroborative evidence is supporting evidence used to help prove an idea or point. It cannot stand its own.
Incorrect Answers:
A: Circumstantial evidence can prove an intermediate fact, but not a direct fact by itself. The intermediate fact can then be used to deduce or assume the existence of another fact. This type of fact is used so the judge or jury will logically assume the existence of a primary fact.
C: Opinion evidence would be the opinion of a witness, but the opinion rule dictates that the witness must testify to only the facts of the issue and not her opinion of the facts.
D: Secondary evidence is not viewed as reliable and strong in proving innocence or guilt (or liability in civil cases) when compared to best evidence. Oral evidence, such as a witness's testimony, and copies of original documents are placed in the secondary evidence category.

References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 1055

NEW QUESTION: 61
A packet filtering firewall looks at the data packet to get information about the source and destination addresses of an incoming packet, the session's communications protocol (TCP, UDP or ICMP), and the source destination application port for the?
A. Desired service
B. Dedicated service
C. Delayed service
D. Distributed service.
Answer: A (LEAVE A REPLY)
This is true, the packets filters show the desired service port (Remember that they are layer 3 devices), this is because you can have many different referenced port number in the destination port field of the different packets. You have to look for the well-known port numbers of the service desired. For example, look in port 80 for HTTP and port 21 for FTP. This is the correct terminology, see the features of Packet Filters in your CISSP documentation.

NEW QUESTION: 62
A chemical plan wants to upgrade the Industrial Control System (ICS) to transmit data using Ethernet instead of RS422. The project manager wants to simplify administration and maintenance by utilizing the office network infrastructure and staff to implement this upgrade. Which of the following is the GREATEST
A. The ICS does not support the office password policy
B. The network administrators have no knowledge of ICS
C. RS422 is more reliable than Ethernet
D. The ICS is now accessible from the office network
Answer: (SHOW ANSWER)

NEW QUESTION: 63
Which of the following is not a weakness of symmetric cryptography?
A. Limited security
B. Key distribution

C. Speed
D. Scalability
Answer: (SHOW ANSWER)
In secret key cryptography, a single key is used for both encryption and decryption. The sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key (or rule set) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key. Symmetric encryption is around 1000 times faster than Asymmetric encryption, the second is commonly used just to encrypt the keys for Symmetric Cryptography.

NEW QUESTION: 64
Which of the following embodies all the detailed actions that personnel are required to follow?
A. Standards
B. Guidelines
C. Procedures
D. Baselines
Answer: C (LEAVE A REPLY)
Procedures are step-by-step instructions in support of of the policies, standards, guidelines and baselines. The procedure indicates how the policy will be implemented and who does what to accomplish the tasks."
Standards is incorrect. Standards are a "Mandatory statement of minimum requirements that support some part of a policy, the standards in this case is your own company standards and not standards such as the ISO standards"
Guidelines is incorrect. "Guidelines are discretionary or optional controls used to enable individuals to make judgments with respect to security actions."
Baselines is incorrect. Baselines "are a minimum acceptable level of security. This minimum is implemented using specific rules necessary to implement the security controls in support of the policy and standards." For example, requiring a password of at leat 8 character would be an example. Requiring all users to have a minimun of an antivirus, a personal firewall, and an anti spyware tool could be another example.
References:
CBK, pp. 12 - 16. Note especially the discussion of the "hammer policy" on pp. 16-17 for the differences between policy, standard, guideline and procedure.
AIO3, pp. 88-93.

NEW QUESTION: 65
Which of the following is most relevant to determining the maximum effective cost of access control?

A. the value of information that is protected.
B. management's perceptions regarding data importance.
C. budget planning related to base versus incremental spending.
D. the cost to replace lost data.
Answer: A (LEAVE A REPLY)
The cost of access control must be commensurate with the value of the information that is being protected. 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: 66
Which expert system operating mode allows determining if a given hypothesis is valid?
A. Blackboard
B. Lateral chaining
C. Forward chaining
D. Backward chaining
Answer: D (LEAVE A REPLY)
Backward-chaining mode - the expert system backtracks to determine if a given hypothesis is valid. Backward-chaining is generally used when there are a large number of possible solutions relative to the number of inputs.
Incorrect answers are:
In a forward-chaining mode, the expert system acquires information and comes to a conclusion based on that information. Forward-chaining is the reasoning approach that can be used when there is a small number of solutions relative to the number of inputs.
Blackboard is an expert system-reasoning methodology in which a solution is generated by the use of a virtual blackboard, wherein information or potential solutions are placed on the blackboard
by a plurality of individuals or expert knowledge sources. As more information is placed on the blackboard in an iterative process, a solution is generated.
Lateral-chaining mode - No such expert system mode.
Sources:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 259).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Expert Systems (page 354).

NEW QUESTION: 67
At which of the Orange Book evaluation levels is configuration management required?
A. C1 and above.
B. C2 and above.
C. B1 and above.

D. B2 and above.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Configuration management consists of identifying, controlling, accounting for, and auditing all changes made to a particular system or equipment during its life cycle. In particular, as related to equipment used to process classified information, equipment can be identified in categories of COMSEC, TEMPEST, or as a Trusted Computer Base (TCB).
The Trusted Computer System Evaluation Criteria (TCSEC) requires all changes to the TCB for classes B2 through A1 be controlled by configuration management.
Incorrect Answers:
A: Configuration management is not required at level C1.
B: Configuration management is not required at level C2.
C: Configuration management is not required at level B1.
References:
http://surflibrary.org/ses/TEMPBOOK/CH6CONFGMGT.pdf

NEW QUESTION: 68
Which of the following is not a problem regarding computer investigation issues?
A. In many instances, an expert or specialist is required
B. Evidence is difficult to gather
C. Information is intangible
D. Computer-generated records are only considered secondary evidence, thus are no as reliable as best evidence
Answer: A (LEAVE A REPLY)

NEW QUESTION: 69
During a fingerprint verification process, which of the following is used to verify identity and authentication?
A. A hash table is matched to a database of stored value
B. A pressure value is compared with a stored template
C. Sets of digits are matched with stored values
D. A template of minutiae is compared with a stored template
Answer: D (LEAVE A REPLY)

NEW QUESTION: 70
A group of independent servers, which are managed as a single system, that provides higher availability, easier manageability, and greater scalability is:
A. server cluster.
B. client cluster.
C. guest cluster.

D. host cluster.

Answer: A (LEAVE A REPLY)

A server cluster is a group of independent servers, which are managed as a single system, that provides higher availability, easier manageability, and greater scalability. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 67.

NEW QUESTION: 71

Secure Sockets Layer (SSL) is very heavily used for protecting which of the following?

A. Web transactions.

B. EDI transactions.

C. Telnet transactions.

D. Electronic Payment transactions.

Answer: A (LEAVE A REPLY)

SSL was developed Netscape Communications Corporation to improve security and privacy of HTTP transactions.

SSL is one of the most common protocols used to protect Internet traffic.

It encrypts the messages using symmetric algorithms, such as IDEA, DES, 3DES, and Fortezza, and also calculates the MAC for the message using MD5 or SHA-1. The MAC is appended to the message and encrypted along with the message data.

The exchange of the symmetric keys is accomplished through various versions of Diffie-Hellmann or RSA. TLS is the Internet standard based on SSLv3. TLSv1 is backward compatible with SSLv3. It uses the same algorithms as SSLv3; however, it computes an HMAC instead of a MAC along with other enhancements to improve security.

The following are incorrect answers:

"EDI transactions" is incorrect. Electronic Data Interchange (EDI) is not the best answer to this question though SSL could play a part in some EDI transactions.

"Telnet transactions" is incorrect. Telnet is a character mode protocol and is more likely to be secured by Secure Telnet or replaced by the Secure Shell (SSH) protocols.

"Eletronic payment transactions" is incorrect. Electronic payment is not the best answer to this question though SSL could play a part in some electronic payment transactions.

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 16615-16619). Auerbach Publications. Kindle Edition.

and

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

NEW QUESTION: 72

An organization regularly conducts its own penetration tests. Which of the following scenarios MUST be covered for the test to be effective?

A. Third-party vendor with access to the system
B. System administrator access compromised
C. Internal attacker with access to the system
D. Internal user accidentally accessing data
Answer: C (LEAVE A REPLY)
Section: Software Development Security

NEW QUESTION: 73
Which of the following is the MOST secure form of triple-DES encryption?
A. DES-EDE3
B. DES-EDE1
C. DES-EEE4
D. DES-EDE2
Answer: A (LEAVE A REPLY)
Explanation/Reference:
DES-EDE3 is the most secure form of triple-DES encryption as it uses three different keys for encryption.
3DES can work in different modes, and the mode chosen dictates the number of keys used and what functions are carried out:
DES-EEE3: Uses three different keys for encryption, and the data are encrypted, encrypted, encrypted.
- DES-EDE3: Uses three different keys for encryption, and the data are encrypted, decrypted, encrypted.
- DES-EEE2: The same as DES-EEE3, but uses only two keys, and the first and third encryption processes use the same key.
- DES-EDE2: The same as DES-EDE3, but uses only two keys, and the first and third encryption processes use the same key.

Incorrect Answers:
B: DES-EDE1 uses one encryption key and returns the algorithm (and strength) as DES. It is only provided for backwards compatibility. This is not the most secure form of triple-DES encryption.
C: DES-EEE4 is not a valid form of 3DES encryption.
D: DES-EDE2 uses only two keys and is not the most secure form of triple-DES encryption.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 808

NEW QUESTION: 74
Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished:
A. through access control mechanisms that do not require identification and authentication and do not operate through the audit function.

B. through logical or technical controls involving the restriction of access to systems and the protection of information
C. through access control mechanisms that require identification and authentication and through the audit function.
D. through logical or technical controls but not involving the restriction of access to systems and the protection of information.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 75
The Secure Hash Algorithm (SHA) is specified in?
A. Digital Encryption Standard
B. Digital Signature Standard
C. Digital Encryption Standard
D. Advanced Encryption Standard
E. NSA 1403
Answer: (SHOW ANSWER)
The Secure Hash Algorithm (SHA) is specified in the Digital Encryption
Standard. This is the most widely used encryption to date. It is used to encrypt millions of files ranging from matters of national security, to bank accounts, and electronic funds transfers.

NEW QUESTION: 76
The design phase in a system development life cycle includes all of the following EXCEPT
A. Determining sufficient security controls.
B. Conducting a detailed design review.
C. Developing an operations and maintenance manual.
D. Developing a validation, verification, and testing plan.
Answer: C (LEAVE A REPLY)
Systems Development Life Cycle Conceptual Defintion Functional Requirements Determination Protection Specifications Development Design Review Code Review Walk-Through System Test Review Certification and Accreditation Maintenance
Pg 224-228 Tittel: CISSP Study Guide.

NEW QUESTION: 77

In order to enable users to perform tasks and duties without having to go through extra steps it is important that the security controls and mechanisms that are in place have a degree of?

A. Complexity

B. Non-transparency

C. Transparency

D. Simplicity

Answer: C (LEAVE A REPLY)

The security controls and mechanisms that are in place must have a degree of transparency. This enables the user to perform tasks and duties without having to go through extra steps because of the presence of the security controls. Transparency also does not let the user know too much about the controls, which helps prevent him from figuring out how to circumvent them. If the controls are too obvious, an attacker can figure out how to compromise them more easily.

Security (more specifically, the implementation of most security controls) has long been a sore point with users who are subject to security controls. Historically, security controls have been very intrusive to users, forcing them to interrupt their work flow and remember arcane codes or processes (like long passwords or access codes), and have generally been seen as an obstacle to

getting work done. In recent years, much work has been done to remove that stigma of security controls as a detractor from the work process adding nothing but time and money. When developing access control, the system must be as transparent as possible to the end user. The users should be required to interact with the system as little as possible, and the process around using the control should be engineered so as to involve little effort on the part of the user.

For example, requiring a user to swipe an access card through a reader is an effective way to ensure a person is authorized to enter a room. However, implementing a technology (such as RFID) that will automatically scan the badge as the user approaches the door is more transparent to the user and will do less to impede the movement of personnel in a busy area.

In another example, asking a user to understand what applications and data sets will be required when requesting a system ID and then specifically requesting access to those resources may allow for a great deal of granularity when provisioning access, but it can hardly be seen as transparent. A more transparent process would be for the access provisioning system to have a role-based structure, where the user would simply specify the role he or she has in the organization and the system would know the specific resources that user needs to access based on that role. This requires less work and interaction on the part of the user and will lead to more accurate and secure access control decisions because access will be based on predefined need, not user preference.

When developing and implementing an access control system special care should be taken to ensure that the control is as transparent to the end user as possible and interrupts his work flow as

little as possible.

The following answers were incorrect:

All of the other detractors were incorrect.

Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 6th edition. Operations Security, Page 1239-1240
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 25278-25281). McGraw-Hill. Kindle Edition.
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Access Control ((ISC)2 Press) (Kindle Locations 713-729). Auerbach Publications. Kindle Edition.

NEW QUESTION: 78
Which of the following would an internal technical security audit BEST validate?
A. Whether managerial controls are in place
B. Support for security programs by executive management
C. Appropriate third-party system hardening
D. Implementation of changes to a system
Answer: D (LEAVE A REPLY)
Section: Mixed questions

NEW QUESTION: 79
Individual accountability does not include which of the following?
A. access rules
B. unique identifiers
C. policies & procedures
D. audit trails
Answer: C (LEAVE A REPLY)

NEW QUESTION: 80
Which of the following is addressed by Kerberos?
A. Authorization and authentication.
B. Validation and integrity.
C. Confidentiality and integrity.
Answer: (SHOW ANSWER)
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: 81

Which of the following is a class C fire?
A. electrical
B. liquid
C. common combustibles
D. soda acid
Answer: A (LEAVE A REPLY)
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide:
Mastering the Ten Domains of Computer Security, page 335.

NEW QUESTION: 82
The Information Technology Security Evaluation Criteria (ITSEC) was written to address which of the following that the Orange Book did not address?
A. integrity and confidentiality
B. confidentiality and availability
C. integrity and availability
D. none of the above
Answer: C (LEAVE A REPLY)
"ITSECTCSEC (Orange Book) E0D F1+E1C1 F2+E2C2 F3+E3B1 F4+E4B2 F5+E5B3 F5+E6A1 F6=Systems that provide high integrity F7=Systems that provide high availability F8=Systems that provide data integrity during communication F9=Systems that provide high confidentiality F10=Networks with high demands on confidentiality and integrity"
Pg. 230 Shon Harris: All-in-One CISSP Certification

NEW QUESTION: 83
The number of times a password should be changed is NOT a function of:
A. The responsibilities and clearance of the user.
B. The criticality of the information to be protected.
C. The type of workstation used.
D. The frequency of the password's use.
Answer: (SHOW ANSWER)
The correct answer is "The type of workstation used.". The type of workstation used as the platform is not the determining factor. The other options are determining factors.

NEW QUESTION: 84
Which of the following item would best help an organization to gain a common understanding of functions that are critical to its survival?
A. A risk assessment
B. A business assessment
C. A disaster recovery plan
D. A business impact analysis
Answer: D (LEAVE A REPLY)

Explanation/Reference:
Explanation:
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.
Incorrect Answers:
A: A risk assessment includes the identification of potential risk and the evaluation of the potential impact of the risk. A risk assessment is a functional analysis of critical business functions.
B: A Business Assessment is a functional analysis of critical business functions. The Business Assessment is an analysis that identifies the resources that are critical to an organization's ongoing viability and the threats posed to those resources.
C: A disaster recovery plan focuses on how to recover various IT mechanisms after a disaster. A disaster recovery plan is a functional analysis of critical business functions.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 905

NEW QUESTION: 85
What is the most correct choice below when talking about the steps to resume normal operation at the primary site after the green light has been given by the salvage team?
A. The most critical operations are moved from alternate site to primary site before others
B. Operation may be carried by a completely different team than disaster recovery team
C. The least critical functions should be moved back first
D. You move items back in the same order as the categories document in your plan or exactly in the same order as you did on your way to the alternate site
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The salvage team must ensure the reliability of primary site. This is done by returning the least-mission- critical processes to the restored original site to stress - test the rebuilt network. As the restored site shows resiliency, more important processes are transferred.
Incorrect Answers:
A: The most critical operations should be to the primary site after, Before, the other less critical operations have been moved.
B: As many operations that the salvage team handles are the same as the operations carried out by the disaster recovery team, there can be very well be an overlap between the team members. A person can be a member of both teams.
D: The order in which the operations are restored should Be exactly the same order in which the operations where moved to the alternative site. You should transfer the least critical operations first.
References:

Stewart, James M., Ed Tittel, and Mike Chapple, CISSP: Certified Information Systems Security Professional Study Guide, 5th Edition, Sybex, Indianapolis, 2011, p. 669

NEW QUESTION: 86
In the area of disaster planning and recovery, what strategy entails the presentation of information about the plan?
A. Recovery
B. Planning
C. Escalation
D. Communication
Answer: D (LEAVE A REPLY)

NEW QUESTION: 87
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)
Explanation/Reference:
Explanation:
Port address translation (PAT) is an implementation of Network Address Translation. PAT is a mechanism for converting the internal private IP addresses found in packet headers into public IP addresses and port numbers for transmission over the Internet. PAT supports a many-to-one mapping of internal to external IP addresses by using ports.
Incorrect Answers:
A: IP Spoofing does not involve mapping of IP addresses. IP spoofing is the creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system B: IP subnetting is the practice of dividing a network into two or more networks.
D: The distribution of IP addresses does not involve mapping of IP addresses.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 606

NEW QUESTION: 88
Which of the following control is intended to discourage a potential attacker?
A. Deterrent
B. Preventive
C. Corrective

D. Recovery

Answer: A (LEAVE A REPLY)

Deterrent Control are intended to discourage a potential attacker

For your exam you should know below information about different security controls

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions. The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events.

When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed.

Deterrent controls work on the theory that it is easier to obey the control rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other

technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal

operations. There are several situations that may affect access controls, their applicability, status, or management.
Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.
Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.
The following answers are incorrect:
Preventive - Preventive controls are intended to avoid an incident from occurring
Corrective - Corrective control fixes components or systems after an incident has occurred
Recovery - Recovery controls are intended to bring the environment back to regular operations
The following reference(s) were/was used to create this question:
CISA Review Manual 2014 Page number 44
and
Official ISC2 CISSP guide 3rd edition Page number 50 and 51

NEW QUESTION: 89
Which one of the following is NOT a typical bus designation in a digital computer?
A. Control
B. Address
C. Data
D. Secondary
Answer: D (LEAVE A REPLY)
The correct answer is Secondary, a distracter.

NEW QUESTION: 90
Which of the following tasks is NOT usually part of a Business Impact Analysis (BIA)?
A. Calculate the risk for each different business function.
B. Identify the company's critical business functions.
C. Calculate how long these functions can survive without these resources.
D. Develop a mission statement.
Answer: D (LEAVE A REPLY)
The Business Impact Analysis is critical for the development of a business continuity plan (BCP). It identifies risks, critical processes and resources needed in case of recovery and quantifies the impact a disaster will have upon the organization. The development of a mission statement is normally performed before 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
The more detailed and granular steps of a BIA are outlined here:
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:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Location 21076). Auerbach Publications. Kindle Edition.
and
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 905-910). McGraw-Hill. Kindle Edition.

NEW QUESTION: 91
Which tape format type is mostly used for home/small office backups?
A. Quarter Inch Cartridge drives (QIC)
B. Digital Linear Tapes (DLT)
C. 8mm tape
D. Digital Audio Tape (DAT)
Answer: A (LEAVE A REPLY)
QIC technology utilizates belt-driven dual-hub cartridges containing integral tape motion and guidance mechanisms, providing a rich spectrum of compatible solutions across a wide range of PC system platforms. QIC reliability is unsurpassed by any other removable storage technology. Reliability can be measured both in mean-time-between failure (MTBF) and, more practically, as a function of drive duty cycles. QIC has a worldwide installed base in excess of 15 million drives -- more than twice that of any alternate removable storage technology
-- a level of acceptance that would have been unachievable without rock-solid reliability. QIC is the most common tape solution for SOHO.

NEW QUESTION: 92
What does "residual risk" mean?
A. The security risk that remains after controls have been implemented
B. Weakness of an assets which can be exploited by a threat
C. Risk that remains after risk assessment has has been performed
D. A security risk intrinsic to an asset being audited, where no mitigation has taken place.
Answer: (SHOW ANSWER)
Residual risk is "The security risk that remains after controls have been implemented" ISO/IEC TR 13335-1 Guidelines for the Management of IT Security (GMITS),
Part 1: Concepts and Models for IT Security, 1996. "Weakness of an assets which can be exploited by a threat" is vulnerability. "The result of unwanted incident" is impact. Risk that remains after risk analysis has been performed is a distracter.
Risk can never be eliminated nor avoided, but it can be mitigated, transferred or accpeted.
Even after applying a countermeasure like for example putiing up an Antivirus. But still it is not 100% that systems will be protected by antivirus.

NEW QUESTION: 93
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: 94
which of the following example is NOT an asymmetric key algorithms?
A. Elliptic curve cryptosystem(ECC)
B. Diffie-Hellman
C. Advanced Encryption Standard(AES)
D. Merkle-Hellman Knapsack
Answer: C (LEAVE A REPLY)
AES is an example of Symmetric Key algorithm. After DES was used as an encryption standard for over 20 years and it was cracked in a relatively short time once the necessary technology was available, NIST decided a new standard, the Advanced
Encryption Standard (AES), needed to be put into place .
In January 1997 , NIST announced its request for AES candidates and outlined the requirements in FIPS PUB 197. AES was to be a symmetric block cipher supporting key sizes of 128, 192, and 256 bits.
The following five algorithms were the finalists:
* MARS Developed by the IBM team that created Lucifer
* RC6 Developed by RSA Laboratories
* Serpent Developed by Ross Anderson, Eli Biham, and Lars Knudsen
* Twofish Developed by Counterpane Systems
* Rijndael Developed by Joan Daemen and Vincent Rijmen
Out of these contestants, Rijndael was chosen.
The block sizes that Rijndael supports are 128, 192 , and 256 bits.
The number of rounds depends upon the size of the block and the key length:
* If both the key and block size are 128 bits, there are 10 rounds.
* If both the key and block size are 192 bits, there are 12 rounds.
* If both the key and block size are 256 bits, there are 14 rounds.
When preparing for my CISSP exam, i came across this post by Laurel Marotta at the URL below:
http://cissp-study.3965.n7.nabble.com/CCCure-CISSP-Study-Plan-to-crack-CISSP- clarification-td401.html
This tips was originally contributed by Doug Landoll
Here is an easy way to remember the types of crypto cipher:
The sentence to remember is: DEER MRS H CARBIDS
Asymmetric: encrypt with 1 key, decrypt with other Key exchange. A key pair: Public and Private.
Services: Confidentiality, Nonrepudiation, Integrity, Digital Signature

D - Diffie-Hellman
E - El Gamal: DH +nonrepudiation
E - ECC
R - RSA
Hash- one-way algorithm, no key
M - MD5
R - RIPEMD (160)
S - SHA (3)
H - Haval (v)
Symmetric: Encryption, one key
C - CAST
A - AES: 128k, 10r; 192k, 12 r; 256k, 14r
R - RC4, RC5, RC6
B - BLOWFISH:23-448k, 64bit block
I - IDEA : 128k, 64bit block
D - DES-64-bit block, 16r
S - SERPENT
The following answers are all incorrect because they are all Asymmetric Crypto ciphers:
Elliptic curve cryptosystem(ECC)
Diffie-Hellman
Merkle-Hellman Knapsack
The following reference(s) were/was used to create this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 809). McGraw-Hill . Kindle Edition.

NEW QUESTION: 95
Which of the following answers is the BEST example of Risk Transference?
A. Insurance
B. Results of Cost Benefit Analysis
C. Acceptance
D. Not hosting the services at all
Answer: A (LEAVE A REPLY)
When we operate an organizational information system we are accepting a tolerable level of risk to allow the business functions to operate.
There may be risks you are not qualified to accept or risks you would be better off having undertaken by an outside entity.
A classic example is having your popular web server hosted by a web hosting agency which completely relieves you of the risks associated with that.
Another example is insurance where you offload the risk to an insurance agency and pay them to accept the risk.

When we transfer risk we are giving the risk to someone else to accept and it could be for a number of reasons. Expense primarily but it could also be performance, offers of better service elsewhere, legal reasons and other reasons.
The following answers are incorrect:
- Results of Cost Benefit Analysis: This might be involved in the process of Risk Mitigation but it isn't part of Risk Transference. Sorry, wrong answer.
- Acceptance: This isn't correct because accepting the risk is the opposite of transferring the risk to someone else.
- Not hosting the services at all: Sorry, this defines Risk Avoidance.
The following reference(s) was used to create this question:
2 013. Official Security+ Curriculum.

NEW QUESTION: 96
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)
Explanation/Reference:
Explanation:
The U.S. Department of Defense developed the Trusted Computer System Evaluation Criteria (TCSEC), which was used to evaluate operating systems, applications, and different products. These evaluation criteria are published in a book known as the Orange Book.
TCSEC provides a classification system that is divided into hierarchical divisions of assurance levels:
A. Verified protection
B. Mandatory protection
C. Discretionary protection
D. Minimal security
C1: Discretionary Security Protection: Discretionary access control is based on individuals and/or groups.
It requires a separation of users and information, and identification and authentication of individual entities.
Some type of access control is necessary so users can ensure their data will not be accessed and corrupted by others. The system architecture must supply a protected execution domain so privileged system processes are not adversely affected by lower-privileged processes. There must be specific ways of validating the system's operational integrity. The documentation requirements include design documentation, which shows that the system was built to include protection mechanisms, test documentation (test plan and results), a facility manual (so companies know how to install and configure the system correctly), and user manuals.

Incorrect Answers:
A: Division C, not D deals with discretionary protection.
C: Division C, not B deals with discretionary protection.
D: Division C, not A deals with discretionary protection.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, pp. 392-394

NEW QUESTION: 97
What is the BEST first step for determining if the appropriate security controls are in place for protecting data at rest?
A. Identify regulatory requirements
B. Review the security baseline configuration
C. Conduct a risk assessment
D. Determine business drivers
Answer: C (LEAVE A REPLY)

NEW QUESTION: 98
The scope and focus of the Business continuity plan development depends most on:
A. Directives of Senior Management
B. Business Impact Analysis (BIA)
C. Scope and Plan Initiation
D. Skills of BCP committee
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
A BIA is performed at the beginning of business continuity planning to identify the areas that would suffer the greatest financial or operational loss in the event of a disaster or disruption. It identifies the company's critical systems needed for survival and estimates the outage time that can be tolerated by the company as a result of a disaster or disruption.
Incorrect Answers:
A: The Business continuity plan depends on the BIA, not on directives from Senior Management.
C: The Business continuity plan depends on the BIA, not on Scope and Plan Initiation.
D: The Business continuity plan depends on the BIA, not on Skills of BCP committee.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 909

NEW QUESTION: 99
After following the processes defined within the change management plan, a super user has upgraded a device within an Information system.

What step would be taken to ensure that the upgrade did NOT affect the network security posture?

A. Review the results of the most recent vulnerability scan

B. Conduct a gap analysis with the baseline configuration

C. Conduct a security impact analysis

D. Conduct an Assessment and Authorization (A&A)

Answer: (SHOW ANSWER)

NEW QUESTION: 100

What is NOT true with pre shared key authentication within IKE / IPsec protocol?

A. Pre shared key authentication is normally based on simple passwords

B. Needs a Public Key Infrastructure (PKI) to work

C. IKE is used to setup Security Associations

D. IKE builds upon the Oakley protocol and the ISAKMP protocol.

Answer: (SHOW ANSWER)

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 which are either pre-shared or distributed using DNS
(preferably with DNSSEC) and a Diffie-Hellman key exchange to set up a shared session secret from which cryptographic keys are derived.

Internet Key Exchange (IKE) Internet key exchange allows communicating partners to prove their identity to each other and establish a secure communication channel, and is applied as an authentication component of IPSec.

IKE uses two phases:

Phase 1: In this phase, the partners authenticate with each other, using one of the following:

Shared Secret: A key that is exchanged by humans via telephone, fax, encrypted e-mail, etc.

Public Key Encryption: Digital certificates are exchanged.

Revised mode of Public Key Encryption: To reduce the overhead of public key encryption, a nonce
(a Cryptographic function that refers to a number or bit string used only once, in security engineering) is encrypted with the communicating partner's public key, and the peer's identity is encrypted with symmetric encryption using the nonce as the key. Next, IKE establishes a temporary security association and secure tunnel to protect the rest of the key exchange. Phase 2: The peers' security associations are established, using the secure tunnel and temporary SA created at the end of phase 1.

The following reference(s) were 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 7032-7048). Auerbach Publications. Kindle Edition. and RFC 2409 at http://tools.ietf.org/html/rfc2409 and http://en.wikipedia.org/wiki/Internet_Key_Exchange

NEW QUESTION: 101
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: 102
Which choice below is an incorrect description of a control?
A. Controls are the countermeasures for vulnerabilities.
B. Corrective controls reduce the likelihood of a deliberate attack.
C. Detective controls discover attacks and trigger preventative or
corrective controls.
D. Corrective controls reduce the effect of an attack.
Answer: B (LEAVE A REPLY)
Controls are the countermeasures for vulnerabilities. There are
many kinds, but generally they are categorized into four types:
Deterrent controls reduce the likelihood of a deliberate attack.
Preventative controls protect vulnerabilities and make an attack
unsuccessful or reduce its impact. Preventative controls inhibit
attempts to violate security policy.
Corrective controls reduce the effect of an attack.
Detective controls discover attacks and trigger preventative or

corrective controls. Detective controls warn of violations or
attempted violations of security policy and include such controls
as audit trails, intrusion detection methods, and checksums.
Source: Introduction to Risk Analysis, "Corrective controls reduce the effect of an attack" &
"Detective controls discover attacks and trigger preventative or
corrective controls" Security Risk Analysis
Group and NIST Special Publication 800-30, Risk Management Guide for
Information Technology Systems.

NEW QUESTION: 103
Which port does the Post Office Protocol Version 3 (POP3) make use of?
A. 110
B. 109
C. 139
D. 119
Answer: A (LEAVE A REPLY)
The other answers are not correct because of the following protocol/port numbers matrix:
Post Office Protocol (POP2) 109 Network News Transfer Protocol 119 NetBIOS 139

NEW QUESTION: 104
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)
Explanation/Reference:
Explanation:
DES is a symmetric block encryption algorithm. When 64-bit blocks of plaintext go in, 64-bit blocks of ciphertext come out. It is also a symmetric algorithm, meaning the same key is used for encryption and decryption. It uses a 64-bit key: 56 bits make up the true key, and 8 bits are used for parity.
When the DES algorithm is applied to data, it divides the message into blocks and operates on them one at a time. The blocks are put through 16 rounds of transposition and substitution functions. The order and type of transposition and substitution functions depend on the value of the key used with the algorithm. The result is 64-bit blocks of ciphertext
Incorrect Answers:
A: When 64-bit blocks of plaintext go in, 64-bit blocks of encrypted data come out.
B: DES uses a 64-bit key (not 128-bit): 56 bits make up the true key, and 8 bits are used for parity.

D: DES uses 64-bit blocks, not 56-bit.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 801

NEW QUESTION: 105
Users require access rights that allow them to view the average salary of groups of employees. Which control would prevent the users from obtaining an individual employee's salary?
A. Limit access to predefined queries
B. Segregate the database into a small number of partitions each with a separate security level
C. Implement Role Based Access Control (RBAC)
D. Reduce the number of people who have access to the system for statistical purposes
Answer: C (LEAVE A REPLY)
Section: Identity and Access Management (IAM)

NEW QUESTION: 106
What Service Organization Controls (SOC) report can be freely distributed and used by customers to gain confidence in a service organization's systems?
A. SOC 3
B. SOC 1 Type 2
C. SOC 1 Type 1
D. SOC 2
Answer: (SHOW ANSWER)

NEW QUESTION: 107
Due is not related to:
A. Good faith
B. Prudent man
C. Profit
D. Best interest
Answer: C (LEAVE A REPLY)
This is obviously a term not related to Profit, a "due" is not going to give us profit, its going to give us the opposite. Its always a good practice to pay your due. This can be learned in the real life. A

Prudent man always pays its due, also a Good faith men pays them. This term is not related to profit.

NEW QUESTION: 108
Under DAC, a subjects rights must be _____ when it leaves an organization altogether.
A. recycled
B. terminated
C. suspended
D. resumed
Answer: B (LEAVE A REPLY)
Discretionary access controls can extend beyond limiting which subjects can gain what type of access to which objects. Administrators can limit access to certain times of day or days of the week. Typically, the period during which access would be permitted is 9 a.m. to 5 p.m. Monday through Friday. Such a limitation is designed to ensure that access takes place only when supervisory personnel are present, to discourage unauthorized use of data. Further, subjects' rights to access might be suspended when they are on vacation or leave of absence. When subjects leave an organization altogether, their rights must be terminated rather than merely suspended.

NEW QUESTION: 109
Which of the following is related to physical security and is not considered a technical control?
A. Access control Mechanisms
B. Intrusion Detection Systems
C. Firewalls
D. Locks
Answer: D (LEAVE A REPLY)
All of the above are considered technical controls except for locks, which are physical controls.
Administrative, Technical, and Physical Security Controls
Administrative security controls are primarily policies and procedures put into place to define and guide employee actions in dealing with the organization's sensitive information. For example, policy might dictate (and procedures indicate how) that human resources conduct background checks on employees with access to sensitive information. Requiring that information be classified and the process to classify and review information classifications is another example of an administrative control. The organization security awareness program is an administrative control used to make employees cognizant of their security roles and responsibilities. Note that administrative security controls in the form of a policy can be enforced or verified with technical or physical security controls. For instance, security policy may state that computers without antivirus software cannot connect to the network, but a technical control, such as network access control software, will check for antivirus software when a computer tries to attach to the network.
Technical security controls (also called logical controls) are devices, processes, protocols, and other measures used to protect the C.I.A. of sensitive information. Examples include logical

access systems, encryptions systems, antivirus systems, firewalls, and intrusion detection systems.
Physical security controls are devices and means to control physical access to sensitive information and to protect the availability of the information. Examples are physical access systems (fences, mantraps, guards), physical intrusion detection systems (motion detector, alarm system), and physical protection systems (sprinklers, backup generator). Administrative and technical controls depend on proper physical security controls being in place. An administrative policy allowing only authorized employees access to the data center do little good without some kind of physical access control.
From the GIAC.ORG website

NEW QUESTION: 110
Discovery, recording, collection, and preservation are part of what process related to the gathering of evidence?
A. The chain of evidence
B. Admissibility of evidence
C. Relevance of evidence
D. The evidence life cycle
Answer: (SHOW ANSWER)
The correct answer is The evidence life cycle. The evidence life cycle covers the evidence gathering and application process.
* Answer "Admissibility of evidence" refers to certain requirements
that evidence must meet to be admissible in court.
* Answer "The chain of evidence" the chain of evidence, is comprised of steps that must be followed to protect the evidence.
* Relevance of evidence is one of the requirements of evidence admissibility.

NEW QUESTION: 111
For an organization considering two-factor authentication for secure network access, which of the following is MOST secure?
A. Tokens and passphrase
B. Digital certificates and Single Sign-On (SSO)
C. Challenge response and private key
D. Smart card and biometrics
Answer: D (LEAVE A REPLY)

NEW QUESTION: 112
What is the name of a one way transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string? Such a transformation cannot be reversed?
A. One-way hash

B. DES
C. Transposition
D. Substitution
Answer: A (LEAVE A REPLY)
A cryptographic hash function is a transformation that takes an input (or 'message') and returns a fixed-size string, which is called the hash value (sometimes termed a message digest, a digital fingerprint, a digest or a checksum).
The ideal hash function has three main properties - it is extremely easy to calculate a hash for any given data, it is extremely difficult or almost impossible in a practical sense to calculate a text that has a given hash, and it is extremely unlikely that two different messages, however close, will have the same hash.
Functions with these properties are used as hash functions for a variety of purposes, both within and outside cryptography. Practical applications include message integrity checks, digital signatures, authentication, and various information security applications. A hash can also act as a concise representation of the message or document from which it was computed, and allows easy indexing of duplicate or unique data files.
In various standards and applications, the two most commonly used hash functions are MD5 and SHA-1. In 2005, security flaws were identified in both of these, namely that a possible mathematical weakness might exist, indicating that a stronger hash function would be desirable. In 2007 the National Institute of Standards and Technology announced a contest to design a hash function which will be given the name SHA-3 and be the subject of a FIPS standard.
A hash function takes a string of any length as input and produces a fixed length string which acts as a kind of "signature" for the data provided. In this way, a person knowing the hash is unable to work out the original message, but someone knowing the original message can prove the hash is created from that message, and none other. A cryptographic hash function should behave as much as possible like a random function while still being deterministic and efficiently computable.
A cryptographic hash function is considered "insecure" from a cryptographic point of view, if either of the following is computationally feasible:
finding a (previously unseen) message that matches a given digest
finding "collisions", wherein two different messages have the same message digest.
An attacker who can do either of these things might, for example, use them to substitute an authorized message with an unauthorized one.
Ideally, it should not even be feasible to find two messages whose digests are substantially similar; nor would one want an attacker to be able to learn anything useful about a message given only its digest. Of course the attacker learns at least one piece of information, the digest itself, which for instance gives the attacker the ability to recognise the same message should it occur again.
REFERENCES:

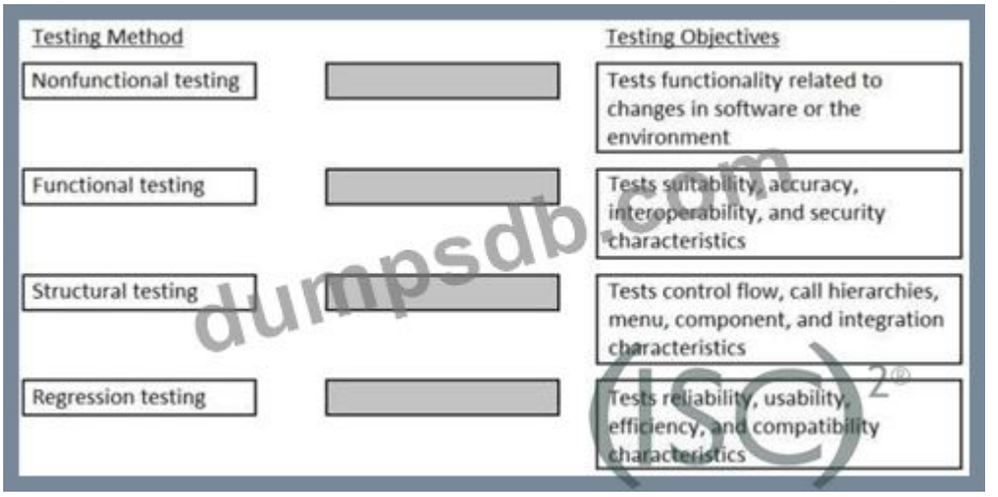
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 40-41.
also see:
http://en.wikipedia.org/wiki/Cryptographic_hash_function

NEW QUESTION: 113
In the context of access control, locks, gates, guards are examples of which of the following?
A. Administrative controls
B. Technical controls
C. Physical controls
D. Logical controls
Answer: C (LEAVE A REPLY)
Administrative, technical and physical controls are categories of access control mechanisms.
Logical and Technical controls are synonymous. So both of them could be eliminated as possible choices.
Physical Controls: These are controls to protect the organization's people and physical environment, such as locks, gates, and guards. Physical controls may be called "operational controls" in some contexts.
Physical security covers a broad spectrum of controls to protect the physical assets (primarily the people) in an organization. Physical Controls are sometimes referred to as "operational" controls in
some risk management frameworks. These controls range from doors, locks, and windows to environment controls, construction standards, and guards. Typically, physical security is based on the notion of establishing security zones or concentric areas within a facility that require increased security as you get closer to the valuable assets inside the facility. Security zones are the physical representation of the defense-in-depth principle discussed earlier in this chapter. Typically, security zones are associated with rooms, offices, floors, or smaller elements, such as a cabinet or
storage locker. The design of the physical security controls within the facility must take into account the protection of the asset as well as the individuals working in that area.
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 1301-1303). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1312-1318). Auerbach Publications. Kindle Edition.

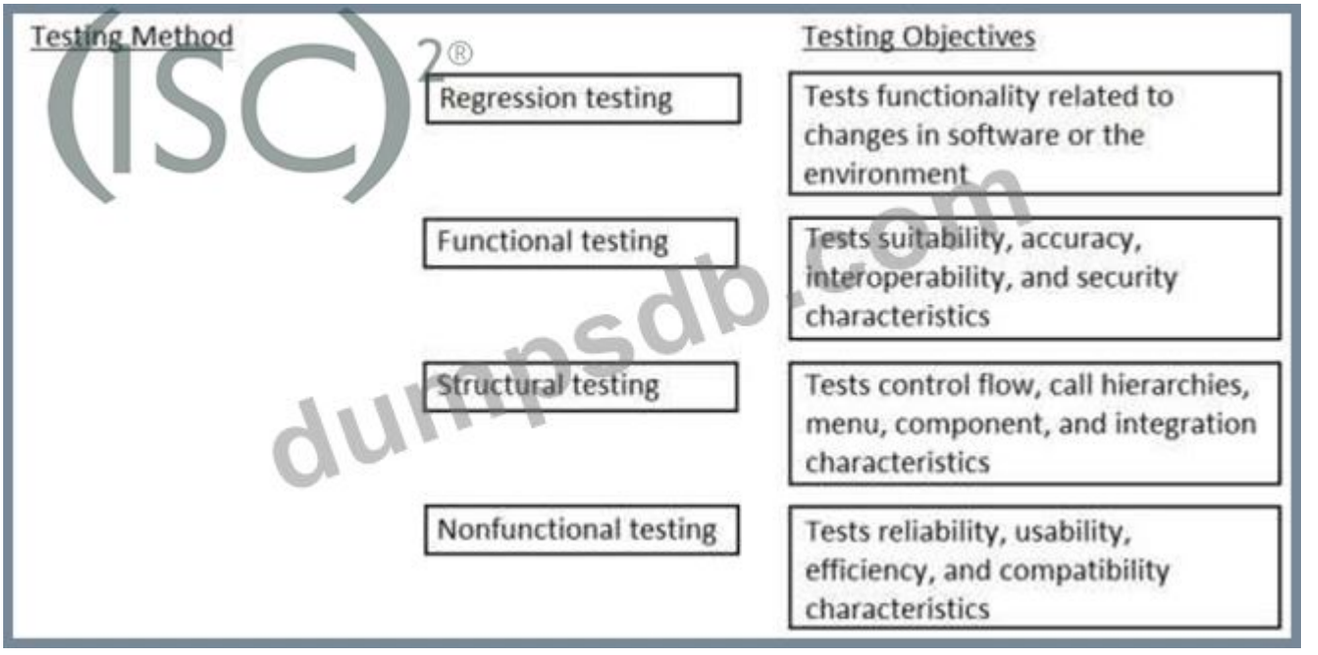
NEW QUESTION: 114
Which of the following is the PRIMARY mechanism used to limit the range of objects available to a given subject within different execution domains?

A. Process isolation
B. Data hiding and abstraction
C. Use of discrete layering and Application Programming Interfaces (API)
D. Virtual Private Network (VPN)
Answer: C (LEAVE A REPLY)
Reference:
https://books.google.com.pk/books?id=LnjxBwAAQBAJ&pg=PT504&lpg=PT504&dq=CISSP+mechanism+use

NEW QUESTION: 115
Drag and Drop Question
Match the following generic software testing methods with their major focus and objective.
Drag each testing method next to its corresponding set of testing objectives.



Answer:



NEW QUESTION: 116

In which of the following programs is it MOST important to include the collection of security process data?

A. Quarterly access reviews

B. Annual security training

C. Business continuity testing

D. Security continuous monitoring

Answer: (SHOW ANSWER)

NEW QUESTION: 117

Which of the following is NOT a major element of Business Continuity Planning?

A. Scope plan initiation

B. Creation of a BCP committee

C. Business Continuity Plan Development

D. Business Impact Assessment (BIA)

Answer: (SHOW ANSWER)

NEW QUESTION: 118

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 analyze 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: (SHOW ANSWER)

Explanation/Reference:

Explanation:

HIDS constantly monitors the system. This can consume quite a few resources.

Incorrect Answers:

B: A HIDS might look at the state of a system, its stored information, whether in RAM, in the file system, log files or elsewhere; and check that the contents of these appear as expected, e.g. have not been changed by intruders.

C: HIDS detects unauthorized changes to the system.

D: When a HIDS detect an anomaly it typically alerts the system administrator of the intrusion.

References:

https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system

NEW QUESTION: 119

In the world of keystroke dynamics, what represents the amount of time it takes a person to switch between keys?

A. Dynamic time

B. Flight time

C. Dwell time

D. Systems time.

Answer: (SHOW ANSWER)

Keystroke dynamics looks at the way a person types at a keyboard. Specifically, keyboard dynamics measures two distinct variables: "dwell time" which is the amount of time you hold down a particular key and "flight time" which is the amount of time it takes a person to switch between keys. Keyboard dynamics systems can measure one's keyboard input up to 1000 times per second.

NEW QUESTION: 120

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

A. Biba

B. Bell LaPadulaLattice

C. Lattice

D. Info Flow

Answer: A (LEAVE A REPLY)

The Handbook of Information System Management, 1999 Edition, ISBN: 0849399742 presents the following definition: In studying the two properties of the Bell-LaPadula model, Biba discovered a plausible notion of integrity, which he defined as prevention of unauthorized modification. The resulting Biba integrity model states that maintenance of integrity requires that data not flow from a receptacle of given integrity to a receptacle of higher integrity. For example, if a process can write above its security level, trustworthy data could be contaminated by the addition of less trustworthy data. SANS glossary at http://www.sans.org/newlook/resources/glossary.htm define it as: Formal security model for the integrity of subjects and objects in a system.

NEW QUESTION: 121

Which of the following is an advantage of prototyping?

A. Prototype systems can provide significant time and cost savings.

B. Change control is often less complicated with prototype systems.

C. It ensures that functions or extras are not added to the intended system.

D. Strong internal controls are easier to implement.

Answer: A (LEAVE A REPLY)

The Prototype Phase is also called the "Proof of Concept" Phase.

Whether it's called one or the other depends on what the creator is trying to "prove."

If the main deliverable of the Phase includes a working version of the product's technical features, it's a "prototype." If the main deliverable just looks like it has the product's technical features, then it's a "proof of concept."

Prototypes can save time and money because you can test some functionality earlier in the process. You don't have to make the whole final product to begin testing it.

NEW QUESTION: 122
When an outgoing request is made on a port number greater than 1023, this type of firewall creates an ACL to allow the incoming reply on that port to pass:
A. packet filtering
B. CIrcuit level proxy
C. Dynamic packet filtering
D. Application level proxy
Answer: C (LEAVE A REPLY)
The dynamic packet filtering firewall is able to create ACL's on the fly to allow replies on dynamic ports (higher than 1023). Packet filtering is incorrect. The packet filtering firewall usually requires that the dynamic ports be left open as a group in order to handle this situiation. Circuit level proxy is incorrect. The circuit level proxy builds a conduit between the trusted and untrusted hosts and does not work by dynamically creating ACL's. Application level proxy is incorrect. The application level proxy "proxies" for the trusted host in its communications with the untrusted host. It does not dynamically create ACL's to control traffic.

NEW QUESTION: 123
The definition A mark used in the sale or advertising of services to identify the services of one person and distinguish them from the services of others refers to a:
A. Trade name
B. Trademark
C. Service mark
D. Copyright
Answer: (SHOW ANSWER)
For answer "a trademark" is a distinctive mark of authenticity, through which the products of particular manufacturers or the vendible commodities of particular merchants may be distinguished from those of others.
Answer "a trade name" is any designation
which is adopted and used by a person to denominate goods which he markets, or services which he renders or business which he conducts. A trade name is descriptive of a manufacturer or dealer

and applies to business and goodwill. A trademark is applicable
only to vendible commodities.
In answer "a copyright "is an
intangible, incorporeal right granted by statute to the author or
originator of certain literary or artistic productions, whereby he is
invested, for a statutorily prescribed period, with the sole and
exclusive privilege of multiplying copies of the same and publishing
and selling them. (These definitions were also taken from Blacks
Law Dictionary, Abridged Fifth Edition, West Publishing Company,
St. Paul Minnesota , 1983.)

NEW QUESTION: 124
Who is essential for developing effective test scenarios for disaster recovery (DR) test plans?
A. Chief Information Officer (CIO) and DR manager
B. DR manager end IT staff members
C. IT staff members and project managers
D. Business line management and IT staff members
Answer: A (LEAVE A REPLY)

NEW QUESTION: 125
The top speed of ISDN BRI is 256 KBS.(True/False)
A. True
B. False
Answer: B (LEAVE A REPLY)
The top speed of ISDN BRI is 128 KBS. Its two primary channels are each capable
of carrying 64 KBS so the combined top speed is 128 KBS.

NEW QUESTION: 126
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: 127
Cryptography does NOT help in:
A. Detecting fraudulent insertion.

B. Detecting fraudulent deletion.
C. Detecting fraudulent modification.
D. Detecting fraudulent disclosure.
Answer: (SHOW ANSWER)
Cryptography is a detective control in the fact that it allows the detection of fraudulent insertion, deletion or modification. It also is a preventive control is the fact that it prevents disclosure, but it usually does not offers any means of detecting disclosure.
Source: DUPUIS, Clement, CISSP Open Study Guide on domain 5, cryptography, April 1999.

NEW QUESTION: 128
Which of the following categories of hackers poses the greatest threat?
A. Disgruntled employees
B. Student hackers
C. Criminal hackers
D. Corporate spies
Answer: (SHOW ANSWER)
According to the authors, hackers fall in these categories, in increasing threat order: security experts, students, underemployed adults, criminal hackers, corporate spies and disgruntled employees.
Disgruntled employees are the most dangerous security problem of all because they are most likely to have a good knowledge of the organization's IT systems and security measures.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 2: Hackers.

NEW QUESTION: 129
Which of the following provides the MOST comprehensive filtering of Peer-to-Peer (P2P) traffic?
A. Application proxy
B. Network boundary router
C. Port filter
D. Access layer switch
Answer: A (LEAVE A REPLY)

NEW QUESTION: 130
A minimal implementation of endpoint security includes which of the following?
A. Trusted platforms
B. Host-based firewalls
C. Token-based authentication
D. Wireless Access Points (AP)
Answer: A (LEAVE A REPLY)
Section: Security Architecture and Engineering

NEW QUESTION: 131
When logging on to a workstation, the log-on process should:
A. Provide a Help mechanism that provides log-on assistance.
B. Not provide information on the previous successful log-on and on previous unsuccessful log-on attempts.
C. Place no limits on the time allotted for log-on or on the number of unsuccessful log-on attempts.
D. Validate the log-on only after all input data has been supplied.
Answer: D (LEAVE A REPLY)
This approach is necessary to ensure that all the information required for a log-on has been submitted and to avoid providing information that would aid a cracker in trying to gain unauthorized access to the workstation or network. If a log-on attempt fails, information as to which part of the requested log-on information was incorrect should not be supplied to the user.
Answer "Provide a Help mechanism that provides log-on assistance" is incorrect since a Help utility would provide help to a cracker trying to gain unauthorized access to the network.
For answer "Place no limits on the time allotted for log-on or on the number of unsuccessful log-on attempts", maximum and minimum time limits should be placed on the log-on process. Also, the log-on process should limit the number of unsuccessful log-on attempts and temporarily suspend the log-on capability if that number is exceeded. One approach is to progressively increase the time interval allowed between unsuccessful log-on attempts.
Answer "Not provide information on the previous successful log-on and on previous unsuccessful log-on attempts" is incorrect since providing such information will alert an authorized user if someone has been attempting to
gain unauthorized access to the network from the user's workstation.

NEW QUESTION: 132
Which type of security control is also known as "Logical" control?
A. Physical
B. Technical
C. Administrative
D. Risk
Answer: (SHOW ANSWER)
The following answers are incorrect:
Physcial: This is a type of security control, but does not have an alternate name.
Administrative: This is a type of security control, but doe not have an alternate name.
Risk:This is not a type of security control.
The following reference(s) were/was used to create this question:
Shon Harris AIO 4th Edition, Chapter 3, Page 57

NEW QUESTION: 133

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

NEW QUESTION: 134
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)
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: 135
Which of the following tools is less likely to be used by a hacker?
A. l0phtcrack
B. Tripwire
C. OphCrack
D. John the Ripper
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:

Tripwire is a tool that detects when files have been altered by regularly recalculating hashes of them and storing the hashes in a secure location. The product triggers when changes to the files have been detected. By using cryptographic hashes, tripwire is often able to detect subtle changes. Contrast: The simplistic form of tripwire is to check file size and last modification time. l0phtcrack, OphCrack and John the Ripper are password cracking tools and are therefore more likely to be used by hackers than Tripwire.
Incorrect Answers:
A: l0phtcrack is used to test password strength and sometimes to recover lost Microsoft Windows passwords, by using dictionary, brute-force, hybrid attacks, and rainbow tables. It is more likely to be used by a hacker than Tripwire.
C: Ophcrack is a free Windows password cracker based on rainbow tables. It is more likely to be used by a hacker than Tripwire.
D: John the Ripper is a fast password cracker, currently available for many flavors of Unix, Windows, DOS, BeOS, and OpenVMS. It is more likely to be used by a hacker than Tripwire.
References:
http://linux.about.com/cs/linux101/g/tripwire.htm

NEW QUESTION: 136
The Wired Equivalency Privacy algorithm (WEP) of the 802.11 Wireless
LAN Standard uses which of the following to protect the confidentiality
of information being transmitted on the LAN?
A. A digital signature that is sent between a mobile station (e.g., a laptop with a wireless Ethernet card) and a base station access point
B. A public/private key pair that is shared between a mobile station (e.g., a laptop with a wireless Ethernet card) and a base station access point
C. A secret key that is shared between a mobile station (e.g., a laptop with a wireless Ethernet card) and a base station access point
D. Frequency shift keying (FSK) of the message that is sent between a mobile station (e.g., a laptop with a wireless Ethernet card) and a base station access point
Answer: (SHOW ANSWER)
The transmitted packets are encrypted with a secret key and an Integrity Check (IC) field comprised of a CRC-32 check sum that is attached to the message. WEP uses the RC4 variable key-size stream cipher encryption algorithm. RC4 was developed in 1987 by Ron Rivest and operates in output feedback mode. Researchers at the University of California at Berkely (wep@isaac.cs.berkeley.edu) have found that the security of the WEP algorithm can be compromised, particularly with the following attacks: Passive attacks to decrypt traffic based on statistical analysis Active attack to inject new traffic from unauthorized mobile stations, based on known plaintext Active attacks to decrypt traffic, based on tricking the access point Dictionary-building attack that, after analysis of about a day's worth of traffic, allows real-time automated decryption of all traffic The Berkeley researchers have found that these attacks are effective against both the 40-bit and the so-called 128-bit versions of WEP using inexpensive off-the-shelf

equipment. These attacks can also be used against networks that use the 802.11b Standard, which is the extension to 802.11 to support higher data rates, but does not change the WEP algorithm. The weaknesses in WEP and 802.11 are being addressed by the IEEE 802.11i Working Group. WEP will be upgraded to WEP2 with the following proposed changes: Modifying the method of creating the initialization vector (IV) Modifying the method of creating the encryption key Protection against replays Protection against IV collision attacks Protection against forged packets In the longer term, it is expected that the Advanced Encryption Standard (AES) will replace the RC4 encryption algorithm currently used in WEP.

NEW QUESTION: 137
This OSI layer has a service that negotiates transfer syntax and translates data to and from the transfer syntax for users, which may represent data using different syntaxes. At which of the following layers would you find such service?
A. Session
B. Transport
C. Presentation
D. Application
Answer: (SHOW ANSWER)
It is responsible for taking information from the "Application layer protocols" and putting it in a form suitable for the application to process.
The presentation-layer implementation of the OSI protocol suite consists of a presentation protocol and a presentation service. The presentation protocol allows presentation-service users (PSusers) to communicate with the presentation service.
A PS-user is an entity that requests the services of the presentation layer. Such requests are made at Presentation-Service Access Points (PSAPs). PS-users are uniquely identified by using PSAP addresses.
Presentation service negotiates transfer syntax and translates data to and from the transfer syntax
for PS-users, which represent data using different syntaxes. The presentation service is used by two PS-users to agree upon the transfer syntax that will be used. When a transfer syntax is agreed
upon, presentation-service entities must translate the data from the PS-user to the correct transfer

syntax.
The OSI presentation-layer service is defined in the ISO 8822 standard and in the ITU-T X.216 recommendation. The OSI presentation protocol is defined in the ISO 8823 standard and in the ITU-T X.226 recommendation. A connectionless version of the presentation protocol is specified in
the ISO 9576 standard.
To remember the OSI layers you can use the following Mnemonics:
The first one is from the bottom (Physical Layer - Layer 1) up (Application - Layer 7):
Please Do Not Throw Sausage Pizza Away
There is another mnemonic from the top down:
All People Seem To Need Data Processing
Both maps to:
1. Physical - 2. Data link - 3. Network - 4. Transport - 5. Session - 6. Presentation - 7. Application
The following answers are incorrect: Transport: Responsible for providing end to end data transport services and establish the logical connection between COMPUTERS for example TCP and UDP
Session: Responsible for maintaing the connection between two APPLICATIONS during the data transfer for example NFS , RPC protocol Application : Works closest to the application , it does not itself contain applications but rather the protocols that support the applications. for example HTTP work at this layer but the application it support is IE , Mozilla , opera , chrome ...
The following reference(s) were/was used to create this question:
http://www.cisco.com/cpress/cc/td/cpress/fund/ith2nd/it2432.htm and
http://en.wikipedia.org/wiki/List_of_network_protocols_%28OSI_model%29

NEW QUESTION: 138
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 is dominated by 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 must dominate the object's sensitivity label.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 139
Which Orange book security rating introduces security labels?
A. C2
B. B1
C. B2
D. B3
Answer: (SHOW ANSWER)
Explanation/Reference:

Explanation:
B1: Labeled Security: Each data object must contain a classification label and each subject must have a clearance label. When a subject attempts to access an object, the system must compare the subject's and object's security labels to ensure the requested actions are acceptable. Data leaving the system must also contain an accurate security label. The security policy is based on an informal statement, and the design specifications are reviewed and verified.
This security rating is intended for environments that require systems to handle classified data.
Incorrect Answers:
A: Security labels are not required at level C2.
C: Security labels are required at level B2; however, they were introduced at level B1.
D: Security labels are required at level B3; however, they were introduced at level B1.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 395

NEW QUESTION: 140
Fault tolerance countermeasures are designed to combat threats to
A. data integrity
B. an uninterruptible power supply
C. design reliability
D. backup and retention capability
Answer: C (LEAVE A REPLY)

NEW QUESTION: 141
According to Requirement 3 of the Payment Card Industry's Data Security Standard (PCI DSS) there is a requirement to "protect stored cardholder data." Which of the following items cannot be stored by the merchant?
A. Primary Account Number
B. Cardholder Name
C. Expiration Date
D. The Card Validation Code (CVV2)
Answer: (SHOW ANSWER)
Requirement 3 of the Payment Card Industry's Data Security Standard (PCI DSS) is to "protect stored cardholder data." The public assumes merchants and financial institutions will protect data on payment cards to thwart theft and prevent unauthorized use.
But merchants should take note: Requirement 3 applies only if cardholder data is stored. Merchants who do not store any cardholder data automatically provide stronger protection by having eliminated a key target for data thieves.
For merchants who have a legitimate business reason to store cardholder data, it is important to understand what data elements PCI DSS allows them to store and what measures they must take to protect those data. To prevent unauthorized storage, only council certified PIN entry devices and payment applications may be used.

PCI DSS compliance is enforced by the major payment card brands who established the PCI DSS and the PCI Security Standards Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.
PCI DSS Requirement 3 It details technical guidelines for protecting stored cardholder data. Merchants should develop a data retention and storage policy that strictly limits storage amount and retention time to that which is required for business, legal, and/or regulatory purposes. Sensitive authentication data must never be stored after authorization - even if this data is encrypted.
Never store full contents of any track from the card's magnetic stripe or chip (referred to as full track, track, track 1, track 2, or magnetic stripe data). If required for business purposes, the cardholder's name, PAN, expiration date, and service code may be stored as long as they are rotected in accordance with PCI DSS requirements.
Never store the card-validation code (CVV) or value (three- or four-digit number printed on the front or back of a payment card used to validate card-not-present transactions).
Never store the personal identification number (PIN) or PIN Block. Be sure to mask PAN whenever it is displayed. The first six and last four digits are the maximum number of digits that may be displayed. This requirement does not apply to those authorized with a specific need to see the full PAN, nor does it supersede stricter requirements in place for displays of cardholder data such as in a point-of-sale receipt.
PCI Data Storage
[1] These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder data environment. Additionally, other legislation (e.g., related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.
[2] Sensitive authentication data must not be stored after authorization (even if encrypted).
[3] Full track data from the magnetic stripe, magnetic stripe image on the chip, or elsewhere.
Technical Guidelines for Protecting Stored Payment Card Data At a minimum, PCI DSS requires PAN to be rendered unreadable anywhere it is stored - including portable digital media, backup media, and in logs. Software solutions for this requirement may include one of the following:
One-way hash functions based on strong cryptography - also called hashed index, which displays only index data that point to records in the database where sensitive data actually reside.
Truncation - removing a data segment, such as showing only the last four digits.
Index tokens and securely stored pads - encryption algorithm that combines sensitive plain text data with a random key or "pad" that works only once.
Strong cryptography - with associated key management processes and procedures. Refer to the PCI DSS and PA-DSS Glossary of Terms, Abbreviations and Acronyms for the definition of "strong cryptography."
Some cryptography solutions encrypt specific fields of information stored in a database; others encrypt a singular file or even the entire disk where data is stored. If full-disk encryption is used,

logical access must be managed independently of native operating system access control mechanisms. Decryption keys must not be tied to user accounts. Encryption keys used for encryption of cardholder data must be protected against both disclosure and misuse. All key management processes and procedures for keys used for encryption of cardholder data must be fully documented and implemented. Strong Cryptography is define in the glossary of PCI DSS as: Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key-management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible, or "one way"). Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher), and ElGamal (1024 bits and higher).
See NIST Special Publication 800-57 (www.csrc.nist.gov/publications/) for more information on strong crypto.
The following answers are all incorrect: Primary Account Number Cardholder Name Expiration Date All of the items above can be stored according to the PCI Data Storage Guidelines. See graphic above.
The following reference(s) were/was used to create this question:
https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf

NEW QUESTION: 142
A Java program is being developed to read a file from computer A and write it to computer B, using a third computer C.
The program is not working as expected. What is the MOST probable security feature of Java preventing the program from operating as intended?
A. Privilege bracketing
B. Least privilege
C. Defense in depth
D. Privilege escalation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 143
Which of the following does not address Database Management Systems (DBMS) Security?
A. Perturbation
B. Cell suppression
C. Padded cells
D. Partitioning
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
A padded cell system is used in Intrusion Detection Systems (IDSs) and is similar to a honeypot. When an IDS detects an intruder, that intruder is automatically transferred to a padded cell. The

padded cell has the look and layout of the actual network, but within the padded cell the intruder can neither perform malicious activities nor access any confidential data.
Incorrect Answers:
A: Noise and perturbation is a database security technique of inserting fake information in the database to misdirect an attacker or cause confusion on the part of the attacker that the actual attack will not be fruitful.
B: Cell suppression is a database security technique used to hide specific cells in a database that contain information that could be used in inference attacks.
D: Partitioning is a database security technique that involves dividing the database into different parts, which makes it much harder for an unauthorized individual to find connecting pieces of data that can be brought together and other information that can be deduced or uncovered.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 1185
Stewart, James, Ed Tittel and Mike Chapple, CISSP: Certified Information Systems security Professional Study Guide, 5th Edition, Wiley Publishing, Indianapolis, 2011, p. 58

NEW QUESTION: 144
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: A (LEAVE A REPLY)
The Secure Socket Layer (SSL) Protocol is primarily used to provide confidentiality
to the information sent across clients and servers.
For your exam you should know the information below:
The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmitted over a public network such as the Internet.
SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL.
SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers.
SSL is included as part of both the Microsoft and Netscape browsers and most Web server products.
Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security.
The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. Later on SSL uses a Session Key along a Symmetric Cipher for the bulk of the data.

TLS and SSL are an integral part of most Web browsers (clients) and Web servers. If a Web site is
on a server that supports SSL, SSL can be enabled and specific Web pages can be identified as requiring SSL access. Any Web server can be enabled by using Netscape's SSLRef program library which can be downloaded for noncommercial use or licensed for commercial use.
TLS and SSL are not interoperable. However, a message sent with TLS can be handled by a client that handles SSL but not TLS.
The SSL handshake
A HTTP-based SSL connection is always initiated by the client using a URL starting with https:// instead of with http://. At the beginning of an SSL session, an SSL handshake is performed. This handshake produces the cryptographic parameters of the session. A simplified overview of how the SSL handshake is processed is shown in the diagram below.
SSL Handshake
Image Reference - http://publib.boulder.ibm.com/tividd/td/ITAME/SC32-1363-00/en_US/HTML/handshak.gif
The client sends a client "hello" message that lists the cryptographic capabilities of the client (sorted in client preference order), such as the version of SSL, the cipher suites supported by the client, and the data compression methods supported by the client. The message also contains a 28-byte random number.
The server responds with a server "hello" message that contains the cryptographic method (cipher
suite) and the data compression method selected by the server, the session ID, and another random number.
Note:
The client and the server must support at least one common cipher suite, or else the handshake fails. The server generally chooses the strongest common cipher suite.
The server sends its digital certificate. (In this example, the server uses X.509 V3 digital certificates with SSL.)
If the server uses SSL V3, and if the server application (for example, the Web server) requires a digital certificate for client authentication, the server sends a "digital certificate request" message. In the "digital certificate request" message, the server sends a list of the types of digital certificates
supported and the distinguished names of acceptable certificate authorities.
The server sends a server "hello done" message and waits for a client response. Upon receipt of the server "hello done" message, the client (the Web browser) verifies the validity of the server's digital certificate and checks that the server's "hello" parameters are acceptable.
If the server requested a client digital certificate, the client sends a digital certificate, or if no suitable digital certificate is available, the client sends a "no digital certificate" alert. This alert is only a warning, but the server application can fail the session if client authentication is mandatory.
The client sends a "client key exchange" message. This message contains the pre-master secret, a 46-byte random number used in the generation of the symmetric encryption keys and the

message authentication code (MAC) keys, encrypted with the public key of the server.
If the client sent a digital certificate to the server, the client sends a "digital certificate verify" message signed with the client's private key. By verifying the signature of this message, the server
can explicitly verify the ownership of the client digital certificate.
Note:
An additional process to verify the server digital certificate is not necessary. If the server does not have the private key that belongs to the digital certificate, it cannot decrypt the pre-master secret and create the correct keys for the symmetric encryption algorithm, and the handshake fails.
The client uses a series of cryptographic operations to convert the pre-master secret into a master
secret, from which all key material required for encryption and message authentication is derived. Then the client sends a "change cipher spec" message to make the server switch to the newly negotiated cipher suite. The next message sent by the client (the "finished" message) is the first message encrypted with this cipher method and keys.
The server responds with a "change cipher spec" and a "finished" message of its own. The SSL handshake ends, and encrypted application data can be sent.
The following answers are incorrect: FTP - File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet. Like the Hypertext Transfer Protocol (HTTP), which transfers displayable Web pages and related files, and the Simple Mail Transfer Protocol (SMTP), which transfers e-mail, FTP is an application protocol that uses the Internet's TCP/IP protocols. FTP is commonly used to transfer Web page files from their creator to the computer that acts as their server for everyone on the Internet. It's also commonly used to download programs and other files to your computer from other servers.
SSH - Secure Shell (SSH) is a cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked computers. It connects, via a secure channel over an insecure network, a server and a client running SSH server and SSH client programs, respectively.
S/MIME - S/MIME (Secure Multi-Purpose Internet Mail Extensions) is a secure method of sending e-mail that uses the Rivest-Shamir-Adleman encryption system. S/MIME is included in the latest versions of the Web browsers from Microsoft and Netscape and has also been endorsed by other vendors that make messaging products. RSA has proposed S/MIME as a standard to the Internet Engineering Task Force (IETF).
Following reference(s) were/was used to create this question: CISA review manual 2014 Page number 352 Official ISC2 guide to CISSP CBK 3rd Edition Page number 256
http://publib.boulder.ibm.com/tividd/td/ITAME/SC32-1363-00/en_US/HTML/ss7aumst18.htm
Topic 3, Information Security Governence and Risk Management

NEW QUESTION: 145
In access control terms, the word "dominate" refers to which of the following?
A. Higher or equal to access class

B. Rights are superceded
C. Valid need-to-know with read privileges
D. A higher clearance level than other users
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Higher or equal to access class. The reason is the term dominates refers to a subject being authorized to perform an operation if the access class of the subject is higher or dominates the access class of the object requested. This is the best answer for the term "dominates" in access control. If a subject wishes to access an object, his security clearance must be equal or higher than the object he's accessing.
Incorrect Answers:
B: Rights are superceded is incorrect as it is not actually a valid condition.
C: Valid need-to-know with read privileges is too specific to be dominates, and is usually what a user's label indicates.
D: A higher clearance level than others. Although having a higher clearance level might be important to obtain access to the higher levels of data, it is not what the definition of "dominates" refers to in access control.
References: Shon Harris latest "All in One CISSP Exam Prep" page 280.

NEW QUESTION: 146
The BEST method to mitigate the risk of a dictionary attack on a system is to
A. encrypt the access control list (ACL).
B. implement password history.
C. use complex passphrases.
D. use a hardware token.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 147
According to best practice, which of the following is required when implementing third party software in a production environment?
A. Negotiate end user application training
B. Scan the application for vulnerabilities
C. Escrow a copy of the software
D. Contract the vendor for patching
Answer: B (LEAVE A REPLY)

NEW QUESTION: 148
Which of the following restricts the ability of an individual to carry out all the steps of a particular process?
A. Job rotation

B. Separation of duties
C. Least privilege
D. Mandatory vacations
Answer: (SHOW ANSWER)
Section: Software Development Security

NEW QUESTION: 149
Which type of control recognizes that a transaction amount is excessive in accordance with corporate policy?
A. Investigation
B. Correction
C. Detection
D. Prevention
Answer: C (LEAVE A REPLY)

NEW QUESTION: 150
Which is NOT a packet-switched technology?
A. Frame Relay
B. SMDS
C. X.25
D. T1
Answer: D (LEAVE A REPLY)
The correct answer is T1. A T1 line is a type of leased line, which uses a dedicated, point-to-point technology.

NEW QUESTION: 151
What is the key length of the Rijndael Block Cipher?
A. 512 or 1024 bits
B. 512 bits
C. 56 or 64 bits
D. 128, 192, or 256 bits
Answer: D (LEAVE A REPLY)

NEW QUESTION: 152
With SQL Relational databases where is the actual data stored?
A. Views
B. Tables
C. Schemas and sub-schemas
D. Index-sequential tables
Answer: B (LEAVE A REPLY)
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: 153
Controls are implemented to?
A. Eliminate risk and reduce the potential for loss.
B. Mitigate risk and eliminate the potential for loss.
C. Mitigate risk and reduce the potential for loss.
D. Eliminate risk and eliminate the potential for loss.
Answer: C (LEAVE A REPLY)
That's the essence of Controls, you put them in your environment to minimize the impact of a potential loss, with them you can also mitigate the risk and obtain the first through this. Controls are a very good practice to secure an environment, they should be considered by any security professional, CISSP or not, the risk should be minimized as much as you can.

NEW QUESTION: 154
Which of the following is the MOST relevant risk indicator after a penetration test?
A. Lists of hosts vulnerable to remote exploitation attacks
B. Details of vulnerabilities and recommended remediation
C. Lists of target systems on the network identified and scanned for vulnerabilities
D. Details of successful vulnerability exploitations
Answer: D (LEAVE A REPLY)
Section: Mixed questions

NEW QUESTION: 155
Which of following is NOT a service provided by AAA servers (Radius, TACACS and DIAMETER)?
A. Authentication
B. Administration

C. Accounting
D. Authorization
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The AAA term refers to authentication, authorization, and accounting/audit. Administration is not one of the options, therefore, the correct answer.
Incorrect Answers:
A, C, D: Authentication, Accounting, and Authorization are what the AAA term refers to.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 236

NEW QUESTION: 156
Which action is MOST effective for controlling risk and minimizing maintenance costs in the software supply chain?
A. Selecting software suppliers with the fewest known vulnerabilities
B. Selecting redundant suppliers
C. Selecting fewer, more reliable suppliers
D. Selecting suppliers based on business requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 157
An effective information security policy should not have which of the following characteristic?
A. Include separation of duties
B. Be designed with a short- to mid-term focus
C. Be understandable and supported by all stakeholders
D. Specify areas of responsibility and authority
Answer: (SHOW ANSWER)
An effective information security policy should be designed with a long-term focus. All other characteristics apply.
Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Appendix B, Practice-Level Policy Considerations (page 397).

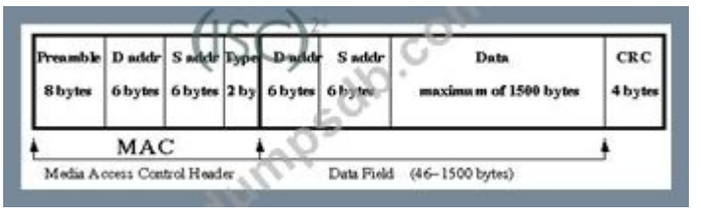
NEW QUESTION: 158
What can be described as a measure of the magnitude of loss or impact on the value of an asset?
A. Probability
B. Exposure factor
C. Vulnerability
D. Threat
Answer: B (LEAVE A REPLY)

The exposure factor is a measure of the magnitude of loss or impact on the value of an asset.
The probability is the chance or likelihood, in a finite sample, that an event will occur or that a specific loss value may be attained should the event occur.
A vulnerability is the absence or weakness of a risk-reducing safeguard.
A threat is event, the occurrence of which could have an undesired impact.
Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 3, August 1999.

NEW QUESTION: 159
Which of the following Disaster Recovery (DR) sites is the MOST difficult to test?
A. Warm site
B. Mobile site
C. Hot site
D. Cold site
Answer: (SHOW ANSWER)

NEW QUESTION: 160
Which of the following are functions that are compatible in a properly segregated environment?
A. Application programming and computer operation
B. Systems programming and job control analysis
C. Access authorization and database administration
D. System development and systems maintenance
Answer: (SHOW ANSWER)
If you think about it, System development and system maintenance are perfectly compatible, you can develop in the systems for certain time, and when it time for a maintenance, you stop the development process an make the maintenance. It's a pretty straight forward process. The other answer do not provide the simplicity and freedom of this option.
Incorrect answer:
Access authorization and database administration are NEVER compatible.

NEW QUESTION: 161
What is the proper term to refer to a single unit of Ethernet data?
A. Ethernet segment
B. Ethernet datagram
C. Ethernet frame
D. Ethernet packet
Answer: (SHOW ANSWER)
Ethernet traffic is transported in units of a frame, where each frame has a definite beginning and end. Here is an Ethernet frame:



sysadm-326-image-22
In this picture we define:
*
Preamble Field used for synchronization, 64-bits
*
Destination Address Ethernet address of the destination host, 48-bits
*
Source Address Ethernet address of the source host, 48-bits
*
Type of data encapsulated, e.g. IP, ARP, RARP, etc, 16-bits.
*
Data Field Data area, 46-1500 bytes, which hasDestination Address Internet address of destination hostSource Address Internet address of source host
*
CRC Cyclical Redundancy Check, used for error detection

NEW QUESTION: 162
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: 163
Although code using a specific program language may not be susceptible to a buffer overflow attack,
A. most calls to plug-in programs are susceptible.
B. most supporting application code is susceptible.
C. the graphical images used by the application could be susceptible.
D. the supporting virtual machine could be susceptible.
Answer: C (LEAVE A REPLY)
Section: Software Development Security

NEW QUESTION: 164
The following concerns usually apply to what type of architecture?
Desktop systems can contain sensitive information that may be at risk of being exposed.
Users may generally lack security awareness.
Modems present a vulnerability to dial-in attacks.
Lack of proper backup may exist.

A. Centralized
B. Open system
C. Distributed
D. Symmetric
Answer: C (LEAVE A REPLY)
Additional concerns associated with distributed systems include:
A desktop PC or workstation can provide an avenue of access into critical information systems of an organization.
Downloading data from the Internet increases the risk of infecting corporate systems with a malicious code or an unintentional modification of the databases.
A desktop system and its associated disks may not be protected from physical intrusion or theft.
*For answer centralized system all the characteristics cited do not apply to a central host with no PCs or workstations with large amounts of memory attached. Also, the vulnerability presented by a modem attached to a PC or workstation would not exist.
*An open system or architecture is comprised of vendorindependent subsystems that have published specifications and interfaces in order to permit operations with the products of other suppliers. One advantage of an open system is that it is subject to review and evaluation by independent parties.
*Answer Symmetric is a distracter.

NEW QUESTION: 165
What is an error called that causes a system to be vulnerable because of the environment in which it is installed?
A. Exceptional condition handling error
B. Configuration error
C. Environmental error
D. Access validation error
Answer: C (LEAVE A REPLY)

NEW QUESTION: 166
Which of the following global privacy legislation principles ensures that data handling policies and the name of the data controller are easily accessible to the public?
A. Openness
B. Individual participation
C. Purpose specification
D. Use limitation
Answer: (SHOW ANSWER)

NEW QUESTION: 167
What is the most effective means of determining that controls are functioning properly within an operating system?
A. Interview with computer operator
B. Review of software control features and/or parameters
C. Review of operating system manual
D. Interview with product vendor
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Various operating system software products provide parameters and options for the tailoring of the system and activation of features such as activity logging. Parameters are important in determining how a system runs because they allow a standard piece of software to be customized to diverse environments. The reviewing of software control features and/or parameters is the most effective means of determining how controls are functioning within an operating system and of assessing and operating system's integrity.
The review of software control features and/or parameters would be part of your security audit. A security audit is typically performed by an independent third party to the management of the system. The audit determines the degree with which the required controls are implemented.
A security review is conducted by the system maintenance or security personnel to discover vulnerabilities within the system. A vulnerability occurs when policies are not followed, misconfigurations are present, or flaws exist in the hardware or software of the system. System reviews are sometimes referred to as a vulnerability assessment.
Incorrect Answers:
A: An interview with the computer operator is not an effective means of determining that controls are functioning properly within an operating system because the computer operator will not necessarily be aware of the detailed settings of the parameters.
C: The operating system manual should provide information as to what settings can be used but will not give any hint as to how parameters are actually set.
D: An interview with the product vendor is not an effective means of determining that controls are functioning properly within an operating system because the product vendor will not be aware of the detailed settings of the parameters.

NEW QUESTION: 168

Which of the following is the lowest TCSEC class wherein the systems must support separate operator and system administrator roles?

A. B2

B. B1

C. A1

D. A2

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

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:

B: Separate operator and system administrator roles are not required at level B1.

C: Separate operator and system administrator roles are required at level A1. However, they are also required at the lower level of B2.

D: Separate operator and system administrator roles are required at level A2. However, they are also required at the lower level of B2.

References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 396

http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt

NEW QUESTION: 169

Normalizing data within a database could includes all or some of the following except which one?

A. Eliminate duplicative columns from the same table.

B. Eliminates functional dependencies on a partial key by putting the fields in a separate table from those that are dependent on the whole key

C. Eliminated Functional dependencies on non-key fields by putting them in a separate table. At this level, all non-key fields are dependent on the primary key.

D. Eliminating duplicate key fields by putting them into separate tables.

Answer: D (LEAVE A REPLY)

1. Eliminate duplicative columns from the same table.

2 . Eliminates functional dependencies on a partial key by putting the fields in a separate table from those that are dependent on the whole key.

3 . Eliminated Functional dependencies on non-key fields by putting them in a separate table. At this level, all non-key fields are dependent on the primary key.

In creating a database, normalization is the process of organizing it into tables in such a way that the results of using the database are always unambiguous and as intended.

Normalization may have the effect of duplicating data within the database and often results in the creation of additional tables. (While normalization tends to increase the duplication of data, it does not introduce redundancy, which is unnecessary duplication.) Normalization is typically a refinement process after the initial exercise of identifying the data objects that should be in the database, identifying their relationships, and defining the tables required and the columns within each table.

A simple example of normalizing data might consist of a table showing:

Customer Item purchased Purchase price

Thomas Shirt $40

Maria Tennis shoes $35

Evelyn Shirt $40

Pajaro Trousers $25

If this table is used for the purpose of keeping track of the price of items and you want to delete one of the customers, you will also delete a price. Normalizing the data would mean understanding this and solving the problem by dividing this table into two tables, one with information about each customer and a product they bought and the second about each product and its price. Making additions or deletions to either table would not affect the other.

Normalization degrees of relational database tables have been defined and include:

First normal form (1NF). This is the "basic" level of normalization and generally corresponds to the definition of any database, namely:

It contains two-dimensional tables with rows and columns.

Each column corresponds to a sub-object or an attribute of the object represented by the entire table.

Each row represents a unique instance of that sub-object or attribute and must be different in some way from any other row (that is, no duplicate rows are possible).

All entries in any column must be of the same kind. For example, in the column labeled "Customer," only customer names or numbers are permitted.

An entity is in First Normal Form (1NF) when all tables are two-dimensional with no repeating groups.

A row is in first normal form (1NF) if all underlying domains contain atomic values only. 1NF eliminates repeating groups by putting each into a separate table and connecting them with a one-to-many relationship. Make a separate table for each set of related attributes and uniquely identify each record with a primary key.

Eliminate duplicative columns from the same table.
Create separate tables for each group of related data and identify each row with a unique column or set of columns (the primary key).
Second normal form (2NF). At this level of normalization, each column in a table that is not a determiner of the contents of another column must itself be a function of the other columns in the table. For example, in a table with three columns containing customer ID, product sold, and price of the product when sold, the price would be a function of the customer ID (entitled to a discount) and the specific product.
An entity is in Second Normal Form (2NF) when it meets the requirement of being in First Normal Form (1NF) and additionally:
Does not have a composite primary key. Meaning that the primary key can not be subdivided into separate logical entities.
All the non-key columns are functionally dependent on the entire primary key.
A row is in second normal form if, and only if, it is in first normal form and every non-key attribute is fully dependent on the key.
2NF eliminates functional dependencies on a partial key by putting the fields in a separate table from those that are dependent on the whole key. An example is resolving many:many relationships using an intersecting entity
Third normal form (3NF). At the second normal form, modifications are still possible because a change to one row in a table may affect data that refers to this information from another table. For example, using the customer table just cited, removing a row describing a customer purchase (because of a return perhaps) will also remove the fact that the product has a certain price. In the third normal form, these tables would be divided into two tables so that product pricing would be tracked separately.
An entity is in Third Normal Form (3NF) when it meets the requirement of being in Second Normal Form (2NF) and additionally:
Functional dependencies on non-key fields are eliminated by putting them in a separate table. At this level, all non-key fields are dependent on the primary key.
A row is in third normal form if and only if it is in second normal form and if attributes that do not contribute to a description of the primary key are move into a separate table. An example is creating look-up tables.
Domain/key normal form (DKNF). A key uniquely identifies each row in a table. A domain is the set of permissible values for an attribute. By enforcing key and domain restrictions, the database is assured of being freed from modification anomalies. DKNF is the normalization level that most designers aim to achieve.
References:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 47.
and
http://psoug.org/reference/normalization.html
and

Tech Target SearcSQLServer at:
http://searchsqlserver.techtarget.com/definition/normalization?vgnextfmt=print

NEW QUESTION: 170
Which of the following devices enables more than one signal to be sent out simultaneously over one physical circuit?
A. Router
B. Multiplexer
C. Channel service unit/Data service unit (CSU/DSU)
D. Wan switch
Answer: (SHOW ANSWER)
Multiplexers are devices that enable enables more than one signal to be sent out simultaneously over one physical circuit. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 118).

NEW QUESTION: 171
Which choice below MOST accurately describes the organization's responsibilities during an unfriendly termination?
A. The employee should be given time to remove whatever files he needs from the network.
B. Cryptographic keys can remain the employee's property.
C. System access should be removed as quickly as possible after termination.
D. Physical removal from the offices would never be necessary.
Answer: C (LEAVE A REPLY)
Friendly terminations should be accomplished by implementing a standard set of procedures for outgoing or transferring employees. This normally includes:
Removal of access privileges, computer accounts, authentication tokens.
The control of keys.
The briefing on the continuing responsibilities for confidentiality and privacy.
Return of property.
Continued availability of data. In both the manual and the electronic worlds this may involve documenting procedures or filing schemes, such as how documents are stored on the hard disk, and how they are backed up. Employees should be instructed whether or not to clean up their PC before leaving.

If cryptography is used to protect data, the availability of cryptographic keys to management personnel must be ensured.
Given the potential for adverse consequences during an unfriendly termination, organizations should do the following:
System access should be terminated as quickly as possible when an employee is leaving a position under less-than-friendly terms.
If employees are to be fired, system access should be removed at the same time (or just before) the employees are notified of their dismissal.
When an employee notifies an organization of the resignation and it can be reasonably expected that it is on unfriendly terms, system access should be immediately terminated.
During the notice of termination period, it may be necessary to assign the individual to a restricted area and function. This may be particularly true for employees capable of changing programs or modifying the system or applications.
In some cases, physical removal from the offices may be necessary.
Source: NIST Special Publication 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems.

NEW QUESTION: 172
What is the best description for CHAP Challenge Handshake Authentication Protocol?
A. Passwords are sent in clear text
B. Passwords are not sent in clear text
C. Passwords are not used, a digital signature is sent
D. It is substandard to PAP
E. It was used with PS2's and has been discontinued
Answer: B (LEAVE A REPLY)
Passwords are not sent in clear text. The server performing the authentication sends a challenge value and the user types in the password. The password is used to encrypt the challenge value then is sent back to the authentication server.

NEW QUESTION: 173
Which of the following mobile code security models relies only on trust?
A. Type safety
B. Code signing
C. Class authentication
D. Sandboxing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 174
Similar to Secure Shell (SSH-2), Secure Sockets Layer (SSL) uses symmetric encryption for encrypting the bulk of the data being sent over the session and it uses asymmetric or public key cryptography for:
A. Peer Authentication
B. Peer Identification
C. Server Authentication
D. Name Resolution
Answer: A (LEAVE A REPLY)
SSL provides for Peer Authentication. Though peer authentication is possible, authentication of the client is seldom used in practice when connecting to public e-commerce web sites. Once authentication is complete, confidentiality is assured over the session by the use of symmetric encryption in the interests of better performance.
The following answers were all incorrect:
"Peer identification" is incorrect. The desired attribute is assurance of the identity of the communicating parties provided by authentication and NOT identification. Identification is only who you claim to be. Authentication is proving who you claim to be.
"Server authentication" is incorrect. While server authentication only is common practice, the protocol provides for peer authentication (i.e., authentication of both client and server).
This answer was not complete.
"Name resolution" is incorrect. Name resolution is commonly provided by the Domain Name System (DNS) not SSL.
Reference(s) used for this question:
CBK, pp. 496 - 497.

NEW QUESTION: 175
Which of the following biometric devices offers the LOWEST CER?
A. Keystroke dynamics
B. Voice verification
C. Iris scan
D. Fingerprint
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
According to the SANS Institute, an Iris scan has a lower CER than keystroke dynamics, voice verification, and fingerprint.
Incorrect Answers:
A, B, D: According to the SANS Institute, keystroke dynamics, voice verification, and fingerprint has a higher CER than iris scan.
References:

https://www.sans.org/reading-room/whitepapers/authentication/biometric-selection-body-parts-online-139

NEW QUESTION: 176
Which of the following is a PRIMARY advantage of using a third-party identity service?
A. Consolidation of multiple providers
B. Directory synchronization
C. Web based logon
D. Automated account management
Answer: D (LEAVE A REPLY)
Section: Security Operations

NEW QUESTION: 177
What would be considered the biggest drawback of Host-based Intrusion Detection systems (HIDS)?
A. It can be very invasive to the host operating system
B. Monitors all processes and activities on the host system only
C. Virtually eliminates limits associated with encryption
D. They have an increased level of visibility and control compared to NIDS
Answer: A (LEAVE A REPLY)
The biggest drawback of HIDS, and the reason many organizations resist its use, is that it can be very invasive to the host operating system. HIDS must have the capability to monitor all processes and activities on the host system and this can sometimes interfere with normal system processing.
HIDS versus NIDS
A host-based IDS (HIDS) can be installed on individual workstations and/ or servers to watch for inappropriate or anomalous activity. HIDSs are usually used to make sure users do not delete system files, reconfigure important settings, or put the system at risk in any other way.
So, whereas the NIDS understands and monitors the network traffic, a HIDS's universe is limited to the computer itself. A HIDS does not understand or review network traffic, and a
NIDS does not "look in" and monitor a system's activity. Each has its own job and stays out of the other's way.
The ISC2 official study book defines an IDS as:
An intrusion detection system (IDS) is a technology that alerts organizations to adverse or unwanted activity. An IDS can be implemented as part of a network device, such as a router, switch, or firewall, or it can be a dedicated IDS device monitoring traffic as it traverses the network. When used in this way, it is referred to as a network IDS, or NIDS.
IDS can also be used on individual host systems to monitor and report on file, disk, and process activity on that host. When used in this way it is referred to as a host-based IDS, or
HIDS.

An IDS is informative by nature and provides real-time information when suspicious activities are identified. It is primarily a detective device and, acting in this traditional role, is not used to directly prevent the suspected attack.
What about IPS?
In contrast, an intrusion prevention system (IPS), is a technology that monitors activity like an IDS but will automatically take proactive preventative action if it detects unacceptable activity. An IPS permits a predetermined set of functions and actions to occur on a network or system; anything that is not permitted is considered unwanted activity and blocked. IPS is engineered specifically to respond in real time to an event at the system or network layer.
By proactively enforcing policy, IPS can thwart not only attackers, but also authorized users attempting to perform an action that is not within policy. Fundamentally, IPS is considered an access control and policy enforcement technology, whereas IDS is considered network monitoring and audit technology.
The following answers were incorrect:
All of the other answer were advantages and not drawback of using HIDS
TIP FOR THE EXAM:
Be familiar with the differences that exists between an HIDS, NIDS, and IPS. Know that IDS's are mostly detective but IPS are preventive. IPS's are considered an access control and policy enforcement technology, whereas IDS's are considered network monitoring and audit technology.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 5817-5822). McGraw-Hill. Kindle Edition.
and
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Access Control ((ISC)2 Press), Domain1, Page 180-188 or on the kindle version look for Kindle Locations 3199-3203 Auerbach Publications.

NEW QUESTION: 178
What is the main focus of the Bell-LaPadula security model?
A. Accountability
B. Integrity
C. Confidentiality
D. Availability
Answer: C (LEAVE A REPLY)
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: 179
When writing security assessment procedures, what is the MAIN purpose of the test outputs and reports?
A. To identify malware or hidden code within the test results

B. To allow for objective pass or fail decisions
C. To find areas of compromise in confidentiality and integrity
D. To force the software to fail and document the process
Answer: B (LEAVE A REPLY)

NEW QUESTION: 180
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 security program can be considered effective when
A. risk is lowered to an acceptable level.
B. vulnerabilities are proactively identified.
C. backups are regularly performed and validated.
D. audits are regularly performed and reviewed.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 181
Which of the following is true of network security?
A. A firewall is a not a necessity in today's connected world.
B. A firewall is a necessity in today's connected world.
C. A whitewall is a necessity in today's connected world.
D. A black firewall is a necessity in today's connected world.
Answer: (SHOW ANSWER)
Commercial firewalls are a dime-a-dozen in todays world. Black firewall and whitewall are just distracters.

NEW QUESTION: 182
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 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 an 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: (SHOW ANSWER)

NEW QUESTION: 183
This backup method makes a complete backup of every file on the server every time it is run by:
A. full backup method
B. tape backup method
C. incremental backup method
D. differential backup method
Answer: A (LEAVE A REPLY)

NEW QUESTION: 184
Which of the following would be defined as an absence of safeguard that could be exploited?
A. A threat
B. A vulnerability
C. A risk
D. An exposure
Answer: (SHOW ANSWER)
In IT, a vulnerability is the weakness of a System to be exploited and corrupted by a security hole. There is always a risk that our systems been vulnerable, with security we cannot make the risk to be 0%, but we can decrease the possibility of a threat becoming in a successful attack through one of those vulnerabilities. There is no system without vulnerabilities, we need to patch our systems frequently to reduce the risk of a threat through a vulnerability of one of our systems.

NEW QUESTION: 185
Which of the following can be defined as an attribute in one relation that has values matching the primary key in another relation?
A. foreign key
B. candidate key
C. primary key
D. secondary key
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A foreign key is an attribute in one table that matches the primary key of another table and is used to cross-reference tables.
Incorrect Answers:
B: Candidate keys are a subset of attributes that from which the database developer can choose the primary key to uniquely identify any tuple or record in a table.
C: The primary key is the attribute that is used to make each row or tuple in a table unique.

D: Secondary keys are candidate keys that have not been chosen as the primary key. The primary key is the attribute that is used to make each row or tuple in a table unique. Candidate keys are a subset of attributes that from which the database developer can choose the primary key.

References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, pp. 1174, 1179-
1180

Stewart, James, Ed Tittel and Mike Chapple, CISSP: Certified Information Systems security Professional Study Guide, 5th Edition, Wiley Publishing, Indianapolis, 2011, pp. 276, 312

http://databases.about.com/cs/specificproducts/g/candidate.htm

http://rdbms.opengrass.net/2_Database Design/2.1_TermsOfReference/2.1.2_Keys.html

NEW QUESTION: 186

Which of the following Common Data Network Services is used to print documents to a shared printer or a print queue/spooler?

A. Mail services.

B. Print services.

C. Client/Server services.

D. Domain Name Service.

E. Explanation:

Print services are used to print documents to a shared printer or a print queue/spooler.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 100.

Which of the following Common Data Network Services allocates computing power resources among workstations with some shared resources centralized on a server?

A. Print services

B. File services

C. Client/Server services

D. Domain Name Service

Answer: (SHOW ANSWER)

Client/Server services allocate computing power resources among workstations with some shared resources centralized in servers. For example, if you are using a product that is working in a client/ server model, in reality you have a small piece of the product on your computer (client portion) and the larger piece of the software product is running on a different computer (server portion). The communication between these two pieces of the same software product needs to be controlled, which is why session layer protocols even exist. Session layer protocols take on the functionality of middleware, which allows software on two different computers to communicate. Distributed systems are the opposite of centralized systems like mainframes and thin client implementations. Traditional client/server architectures are the most common example of a distributed system. In a traditional client/server architecture, responsibilities for processing have

been balanced between centralized servers providing services to multiple clients and client machines that focus on user interaction and standalone processing where appropriate. For the most part, servers are responsible for serving, meaning that they provide services that will be leveraged by the clients in the environment. Clients are the primary consumers of server services, while also hosting services of their own primarily for their own individual use.
Reference used for this question: Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 524). 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 18741-18745). Auerbach Publications. Kindle Edition. and 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: 187
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 of the corresponding vulnerability. Therefore, a legal liability may exists when:
A. (C < L) or C is less than L
B. (C < L - (residual risk)) or C is less than L minus residual risk
C. (C > L) or C is greather than L
D. (C > L - (residual risk)) or C is greather than L minus residual risk
Answer: A (LEAVE A REPLY)
If the cost is lower than the estimated loss (C < L), then legal liability may exists if you fail to implement the proper safeguards.
Government laws and regulations require companies to employ reasonable security measures to reduce private harms such as identity theft due to unauthorized access. The U.S. Gramm-LeachBliley Act (GLBA) Safeguards Rule and the broader European Directive 95/46/EC, Article 17, both require that companies employ reasonable or appropriate administrative and technical security measures to protect consumer information.
The GLBA is a U.S. Federal law enacted by U.S. Congress in 1998 to allow consolidation among commercial banks. The GLBA Safeguards Rule is U.S. Federal regulation created in reaction to the GLBA and enforced by the U.S. Federal Trade Commission (FTC). The Safeguards Rule requires companies to implement a security plan to protect the confidentiality and integrity of consumer personal information and requires the designation of an individual responsible for compliance.
Because these laws and regulations govern consumer personal information, they can lead to new requirements for information systems for which companies are responsible to comply.
The act of compliance includes demonstrating due diligence, which is defined as "reasonable efforts that persons make to satisfy legal requirements or discharge their legal obligations". Reasonableness in software systems includes industries standards and may allow for imperfection. Lawyers representing firms and other organizations, regulators, system

administrators and engineers all face considerable challenge in determining what constitutes "reasonable" security measures for several reasons, including:
1.Compliance changes with the emergence of new security vulnerabilities due to innovations in information technology;
2.Compliance requires knowledge of specific security measures, however publicly available best practices typically include general goals and only address broad categories of vulnerability; and
3.Compliance is a best-effort practice, because improving security is costly and companies must prioritize security spending commensurate with risk of non-compliance. In general, the costs of improved security are certain, but the improvement in security depends on unknown variables and probabilities outside the control of companies.
The following reference(s) were 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 315. and http://www.cs.cmu.edu/~breaux/publications/tdbreaux-cose10.pdf

NEW QUESTION: 188
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.
Given the number of priorities, which of the following will MOST likely influence the selection of top initiatives?
A. Complexity of strategy
B. Severity of risk
C. Ongoing awareness
D. Frequency of incidents
Answer: (SHOW ANSWER)

NEW QUESTION: 189
Which general TCSEC security class category describes that mandatory access policies be enforced in the TCB?
Exhibit:

CLASS	DESCRIPTION
D:	minimal protection
C:	discretionary protection
C1:	discretionary security protection
C2:	controlled access protection
B:	mandatory protection
B1:	labeled security protection
B2:	structured protection
B3:	security domains
A1:	verified protection

A. A

B. B
C. C
D. D
Answer: (SHOW ANSWER)
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: 190
An organization adopts a new firewall hardening standard. How can the security professional verify that the technical staff correct implemented the new standard?
A. Perform a compliance review
B. Perform a penetration test
C. Train the technical staff
D. Survey the technical staff
Answer: B (LEAVE A REPLY)
Explanation
Section: Security Operations

NEW QUESTION: 191
Which of the following type of lock uses a numeric keypad or dial to gain entry?
A. Bolting door locks
B. Cipher lock
C. Electronic door lock
D. Biometric door lock
Answer: B (LEAVE A REPLY)
The combination door lock or cipher lock uses a numeric key pad, push button, or dial to gain entry, it is often seen at airport gate entry doors and smaller server rooms. The combination should be changed at regular interval or whenever an employee with access is transferred, fired or subject to disciplinary action. This reduces risk of the combination being known by unauthorized people.
A cipher lock, is controlled by a mechanical key pad, typically 5 to 10 digits that when pushed in the right combination the lock will releases and allows entry. The drawback is someone looking over a shoulder can see the combination. However, an electric version of the cipher lock is in production in which a display screen will automatically move the numbers around, so if someone

is trying to watch the movement on the screen they will not be able to identify the number indicated unless they are standing directly behind the victim.
Remember locking devices are only as good as the wall or door that they are mounted in and if the frame of the door or the door itself can be easily destroyed then the lock will not be effective. A lock will eventually be defeated and its primary purpose is to delay the attacker.
For your exam you should know below types of lock
Bolting door lock - These locks required the traditional metal key to gain entry. The key should be stamped "do not duplicate" and should be stored and issued under strict management control.
Biometric door lock - An individual's unique physical attribute such as voice, retina, fingerprint, hand geometry or signature, activate these locks. This system is used in instances when sensitive facilities must be protected such as in the military.
Electronic door lock - This system uses a magnetic or embedded chip based plastic card key or token entered into a sensor reader to gain access. A special code internally stored in the card or token is read by sensor device that then activates the door locking mechanism.
The following were incorrect answers:
Bolting door lock - These locks required the traditional metal key to gain entry. The key should be stamped "do not duplicate" and should be stored and issued under strict management control.
Biometric door lock - An individual's unique body features such as voice, retina, fingerprint,, hand geometry or signature, activate these locks. This system is used in instances when extremely sensitive facilities must be protected such as in the military.
Electronic door lock - This system uses a magnetic or embedded chip based plastic card key or token entered into a sensor reader to gain access. A special code internally stored in the card or token is read by sensor device that then activates the door locking mechanism.
Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 376
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 25144-25150). Auerbach Publications. Kindle Edition.

NEW QUESTION: 192
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: 193
How often should an independent review of the security controls be performed, according to OMB Circular A-130?
A. Never
B. Every five years
C. Every three years
D. Every year
Answer: C (LEAVE A REPLY)
The correct answer is "Every three years". OMB Circular A-130 requires that a review of the security controls for each major government application be performed at least every three years. For general support systems, OMB Circular A-130 requires that the security controls be reviewed either by an independent audit or self review. Audits can be selfadministered or independent (either internal or external). The essential difference between a self-audit and an independent audit is objectivity; however, some systems may require a fully independent review. Source: Office of Management and Budget Circular A-130, revised November 30, 2000 .

NEW QUESTION: 194
Which of the following is a Key Performance Indicator (KPI) for a security training and awareness program?
A. The number of attendees at security training events
B. The number of security training materials created
C. The number of security audits performed
D. The number of security controls implemented
Answer: A (LEAVE A REPLY)

NEW QUESTION: 195
The term failover refers to:
A. A fail-soft system.
B. Terminating processing in a controlled fashion.
C. Resiliency.
D. Switching to a duplicate, hot backup component.
Answer: (SHOW ANSWER)
The correct answer is "Switching to a duplicate, hot backup component". Failover means switching to a hot backup system that maintains duplicate states with the primary system. Answer "Terminating processing in a controlled fashion" refers to fail safe, and answers

Resiliency and A fail-soft system refer to fail soft.

NEW QUESTION: 196
Proxies work 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: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Proxy servers act as an intermediary between the clients that want access to certain services and the servers that provide those services. The proxy server sends an independent request to the destination on behalf of the user, thereby masking the origin of the data.
Incorrect Answers:
A: The proxy server transfer they payload data to the destination.
B: The proxy server transfer they payload data (the details of the data) to the destination.
C: The origin of the data, not the owner of the data, is masked by the proxy server.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 653

NEW QUESTION: 197
Which of the following is the GREATEST security risk associated with the use of identity as a service (IDaaS) when an organization is developing its own software?
A. Denial of access due to reduced availability
B. Incompatibility with Federated Identity Management (FIM)
C. Increased likelihood of confidentiality breach
D. Security Assertion Markup Language (SAML) integration
Answer: (SHOW ANSWER)

NEW QUESTION: 198

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: (SHOW ANSWER)

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

AIOv3 Telecommunications and Networking Security (page 438)

NEW QUESTION: 199

Software generated passwords have what drawbacks?

A. Passwords are not easy to remember.
B. Password are too secure.
C. None of the choices.
D. Passwords are unbreakable.
Answer: A (LEAVE A REPLY)
Passwords generated by a software package or some operating systems. These password generators are good at producing unique and hard to guess passwords, however you must ensure that they are not so hard that people can't remember them. If you force your users to write their passwords down then you are defeating the purpose of having strong password management.

NEW QUESTION: 200
The primary goal of the TLS Protocol is to provide:
A. Privacy and data integrity between two communicating applications
B. Authentication and data integrity between two communicating applications
C. Privacy and authentication between two communicating applications
D. Privacy, authentication and data integrity between two communicating applications
Answer: A (LEAVE A REPLY)
The TLS Protocol is comprised of the TLS Record and Handshake Protocols. The TLS Record Protocol is layered on top of a transport protocol such as TCP and provides privacy and reliability to the communications. The privacy is implemented by encryption using symmetric key cryptography such as DES or RC4. The secret key is generated anew for each connection; however, the Record Protocol can be used without encryption. Integrity is provided through the use of a keyed Message Authentication Code (MAC) using hash algorithms such as SHA or MD5. The TLS Record Protocol is also used to encapsulate a higher-level protocol such as the TLS Handshake Protocol. This Handshake Protocol is used by the server and client to authenticate each other. The authentication can be accomplished using asymmetric key cryptography such as RSA or DSS. The Handshake Protocol also sets up the encryption algorithm and cryptographic keys to enable the application protocol to transmit and receive information.

NEW QUESTION: 201
Communications devices must operate:
A. at different speeds to communicate.
B. at the same speed to communicate.
C. at varying speeds to interact.
D. at high speed to interact.
Answer: B (LEAVE A REPLY)
Communications devices must operate at the same speed to communicate.
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: 202
If compromised, which of the following would lead to the exploitation of multiple virtual machines?
A. Virtual machine instance
B. Virtual device drivers
C. Virtual machine monitor
D. Virtual machine file system
Answer: C (LEAVE A REPLY)

NEW QUESTION: 203
A trade secret:
A. Provides the owner with a legally enforceable right to exclude others from practicing the art covered for a specified time period.
B. Is a word, name, symbol, color, sound, product shape, or device used to identify goods and to distinguish them from those made or sold by others.
C. Protects original works of authorship.
D. Secures and maintains the confidentiality of proprietary technical or business-related information that is adequately protected from disclosure by the owner.
Answer: D (LEAVE A REPLY)
This defines a trade secret.
*Answer "Provides the owner with a legally enforceable right to exclude others from practicing the art covered for a specified time period" refers to a patent.
*Answer "Protects original works of authorship" refers to a copyright.
*Answer "Is a word, name, symbol, color, sound, product shape, or device used to identify goods and to distinguish them from those made or sold by others" refers to a trademark.

NEW QUESTION: 204
Which of the following characteristics does a one-time pad have if used properly?
A. The key has to be of greater length than the message to be encrypted.
B. The key does not have to be random.
C. It can be used more than once.
D. It is unbreakable.
Answer: D (LEAVE A REPLY)
The correct answer is "It is unbreakable". If the one-time-pad is used only once and its corresponding key is truly random and does not have repeating characters, it is unbreakable.
Answer "It can be used more than once" is incorrect because if used
properly, the one-time-pad should be used only once.
Answer "The key does not have to be random" is incorrect because the key should be random.
Answer "The key has to be of greater length than the message to be encrypted" is incorrect because the key has to be of the same length as the message.

NEW QUESTION: 205

Which of the following is biggest factor that makes Computer Crimes possible?
A. The fraudster obtaining advanced training & special knowledge.
B. Victim carelessness.
C. Collusion with others in information processing.
D. System design flaws.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Human-unintentional threats represent the most common source of disasters. Examples of human unintentional threats are primarily those that involve inadvertent errors and omissions, in which the person, through lack of knowledge, laziness, or carelessness, serves as a source of disruption.
Incorrect Answers:
A: A more knowledgeable fraudster would increase the risk of Computer Crimes, but it is less of a factor compared to human carelessness.
C: Collusion makes computer crimes possible, but human carelessness is the main factor.
D: System design flaws makes computer crimes possible, but human carelessness is the main factor.
References:
Conrad, Eric, Seth Misenar and Joshua Feldman, CISSP Study Guide, 2nd Edition, Syngress, Waltham,
2012, p. 347

NEW QUESTION: 206
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)
Explanation/Reference:
Explanation:
Historically, a code refers to a cryptosystem that deals with linguistic units: words, phrases, sentences, and so forth. For example, the word "OCELOT" might be the ciphertext for the entire phrase "TURN LEFT 90 DEGREES," the word "LOLLIPOP" might be the ciphertext for "TURN RIGHT 90 DEGREES".
Codes are only useful for specialized circumstances where the message to transmit has an already defined equivalent ciphertext word.
Incorrect Answers:
A: A code is not a generic term for encryption.
B: A code is not specific to substitution ciphers.

D: A code is not a specific to transposition ciphers.
References:
https://www.cs.duke.edu/courses/fall02/cps182s/readings/APPLYC1.pdf

NEW QUESTION: 207
What is a method in an object-oriented system?
A. The code defining the actions that the object performs in response to a message
B. A guide to the programming of objects
C. The means of communication among objects
D. The situation where a class inherits the behavioral characteristics of more that one parent class
Answer: (SHOW ANSWER)
method in an object-oriented system is
the code that defines the actions that the object performs in response
to a message.
Answer "The means of communication among objects" is incorrect because it defines a message.
Answer "A guide to the programming of objects" is a distracter.
Answer "The situation where a class inherits the behavioral characteristics of more that one parent
class" refers to multiple inheritance.

NEW QUESTION: 208
Which of the following protection devices is used for spot protection within a few inches of the object, rather than for overall room security monitoring?
A. Wave pattern motion detectors
B. Capacitance detectors
C. Field-powered devices
D. Audio detectors
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
A capacitance detector, emits a measurable magnetic field. The detector monitors this magnetic field, and an alarm sounds if the field is disrupted. These devices are usually used to protect specific objects (artwork, cabinets, or a safe) versus protecting a whole room or area.
An electrostatic IDS creates an electrostatic magnetic field, which is just an electric field associated with static electric charges. All objects have a static electric charge. They are all made up of many subatomic particles, and when everything is stable and static, these particles constitute one holistic electric charge.
This means there is a balance between the electric capacitance and inductance. Now, if an intruder enters the area, his subatomic particles will mess up this balance in the electrostatic field, causing a capacitance change, and an alarm will sound.

Incorrect Answers:
A: Wave pattern motion detectors are used overall room security monitoring. Therefore, this answer is incorrect.
C: Field-powered devices are not intrusion detection devices. Field-powered device refers to a type of system-sensing proximity card. Therefore, this answer is incorrect.
D: Audio detectors are used overall room security monitoring. Therefore, this answer is incorrect.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 496 Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 850

NEW QUESTION: 209
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: C (LEAVE A REPLY)
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: 210
An organization has discovered that users are visiting unauthorized websites using anonymous proxies.
Which of the following is the BEST way to prevent future occurrences?
A. Remove the anonymity from the proxy
B. Disable the proxy server on the firewall
C. Analyze Internet Protocol (IP) traffic for proxy requests
D. Block the Internet Protocol (IP) address of known anonymous proxies
Answer: D (LEAVE A REPLY)

NEW QUESTION: 211
Which of the following algorithms does NOT provide hashing?
A. SHA-1
B. MD2
C. RC4
D. MD5
Answer: C (LEAVE A REPLY)
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: 212
When developing solutions for mobile devices, in which phase of the Software Development Life Cycle (SDLC) should technical limitations related to devices be specified?
A. Implementation
B. Initiation
C. Review
D. Development
Answer: A (LEAVE A REPLY)
Section: Software Development Security

NEW QUESTION: 213
The IS security analyst's participation in which of the following system development life cycle phases provides maximum benefit to the organization?
A. Program testing.
B. Program development.
C. System requirements definition.
D. System design.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 214

Which ISO/OSI layer establishes the communications link between individual devices over a physical link or channel?

A. Transport layer

B. Network layer

C. Data link layer

D. Physical layer

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation:

The data link layer is responsible for proper communication within the network devices and for changing the data into the necessary format (electrical voltage) for the physical link or channel.

Incorrect Answers:

A: The protocols at the transport layer handle end-to-end transmission and segmentation of a data stream.

B: The responsibilities of the network layer protocols include internetworking service, addressing, and routing.

D: The physical layer include network interface cards and drivers that convert bits into electrical signals and control the physical aspects of data transmission References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 531

NEW QUESTION: 215

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: C (LEAVE A REPLY)

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: 216
What is an error called that causes a system to be vulnerable because of the environment in which it is installed?
A. Configuration error
B. Environmental error
C. Access validation error
D. Exceptional condition handling error
Answer: (SHOW ANSWER)
In an environmental error, the environment in which a system is installed somehow causes the system to be vulnerable. This may be due, for example, to an unexpected interaction between an application and the operating system or between two applications on the same host. A configuration error occurs when user controllable settings in a system are set such that the system is vulnerable. In an access validation error, the system is vulnerable because the access control mechanism is faulty. In an exceptional condition handling error, the system somehow becomes vulnerable due to an exceptional condition that has arisen.
Source: DUPUIS, Clement, Access Control Systems and Methodology CISSP Open Study Guide, version 10, march 2002 (page 106).

NEW QUESTION: 217
Which of the following is more suitable for a hardware implementation?
A. Stream ciphers
B. Block ciphers
C. Cipher block chaining
D. Electronic code book
Answer: (SHOW ANSWER)
A stream cipher treats the message as a stream of bits or bytes and performs mathematical functions on them individually. The key is a random value input into the stream cipher, which it uses to ensure the randomness of the keystream data. They are more suitable for hardware implementations, because they encrypt and decrypt one bit at a time. They are intensive because each bit must be manipulated, which works better at the silicon level. Block ciphers operate a the block level, dividing the message into blocks of bits. Cipher Block chaining (CBC) and Electronic Code Book (ECB) are operation modes of
DES, a block encryption algorithm.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 2).

NEW QUESTION: 218
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:
80 meters. It is only a distracter.
185 meters. Is incorrect because it is the maximum length for 10Base-2
500 meters. Is incorrect because it is the maximum length for 10Base-5

NEW QUESTION: 219
Which of the following problems is not addressed by using OAuth (Open Standard to Authorization) 2.0 to integrate a third-party identity provider for a service?
A. Compromise of the third party means compromise of all the users in the service.

B. Revocation of access of some users of the third party instead of all the users from the third party.
C. Guest users need to authenticate with the third party identity provider.
D. Resource Servers are required to use passwords to authenticate end users.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 220
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: C (LEAVE A REPLY)
This is a contactless smart card that has two chips with the capability of utilizing both contact and contactless formats. Two additional categories of cards are dual-interface cards and hybrid cards which is mentioned above. Hybrid Card A hybrid card has two chips, one with a contact interface and one with a contactless interface. The two chips are not interconnected.
Dual-Interface card Do not confuse this card with the Hybrid Card. This one has only one chip. A dual-interface card has a single chip with both contact and contactless interfaces. With dual-interface cards, it is possible to access the same chip using either a contact or contactless interface with a very high level of security.
Inner working of the cards The chips used in all of these cards fall into two categories as well: microcontroller chips and memory chips. A memory chip is like a small floppy disk with optional security. Memory chips are less expensive than microcontrollers but with a corresponding decrease in data management security. Cards that use memory chips depend on the security of the card reader for processing and are ideal for situations that require low or medium security. A microcontroller chip can add, delete, and otherwise manipulate information in its memory. A microcontroller is like a miniature computer, with an input/output port, operating system, and hard disk. Smart cards with an embedded microcontroller have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and digital signatures) and interact intelligently with a smart card reader.
The selection of a particular card technology is driven by a variety of issues, including:
Application dynamics Prevailing market infrastructure Economics of the business model Strategy for shared application cards
Smart cards are used in many applications worldwide, including:
Secure identity applications - employee ID badges, citizen ID documents, electronic passports, driver's licenses, online authentication devices Healthcare applications - citizen health ID cards, physician ID cards, portable medical records cards Payment applications - contact and contactless credit/debit cards, transit payment cards
Telecommunications applications - GSM Subscriber Identity Modules, pay telephone payment

cards
The following answers are incorrect:
Contact Smart Cards
A contact smart card must be inserted into a smart card reader with a direct connection to a conductive contact plate on the surface of the card (typically gold plated). Transmission of commands, data, and card status takes place over these physical contact points.
Contactless Smart Cards
A contactless card requires only close proximity to a reader. Both the reader and the card have antennae, and the two communicate using radio frequencies (RF) over this contactless link. Most contactless cards also derive power for the internal chip from this electromagnetic signal. The range is typically one-half to three inches for non-battery-powered cards, ideal for applications such as building entry and payment that require a very fast card interface.
Combi Card
Are similar to Hybrid cards only they contain only one set of circuitry as apposed to two.
The following reference(s) were/was used to create this question:
Smart Card Primer at: http://www.smartcardalliance.org/pages/smart-cards-intro-primer

NEW QUESTION: 221
Which statement is NOT true about the SOCKS protocol?
A. It operates in the transport layer of the OSI model.
B. It uses an ESP for authentication and encryption.
C. It is sometimes referred to as an application-level proxy.
D. Network applications need to be SOCKS-ified to operate.
Answer: B (LEAVE A REPLY)
The correct answer is "It uses an ESP for authentication and encryptio". The Encapsulating Security Payload, (ESP) is a component of IPSec. Socket Security (SOCKS) is a transport layer, secure networking proxy protocol. SOCKS replaces the standard network systems calls with its own calls. These calls open connections to
a SOCKS proxy server for client authentication, transparently to the user.
Common network utilities, like TELNET or FTP, need to be SOCKSified,
or have their network calls altered to recognize SOCKS proxy calls.
Source: Designing Network Security by Merike Kaeo (Cisco Press, 1999).

NEW QUESTION: 222
Which security model uses division of operations into different parts and requires different users to perform each part?
A. Bell-LaPadula model
B. Biba model
C. Clark-Wilson model
D. Non-interference model
Answer: (SHOW ANSWER)

The Clark-Wilson model uses separation of duties, which divides an operation into different parts and requires different users to perform each part. This prevents authorized users from making unauthorized modifications to data, thereby protecting its integrity.
The Clark-Wilson integrity model provides a foundation for specifying and analyzing an integrity policy for a computing system.
The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. An integrity policy describes how the data items in the system should be kept valid from one state of the system to the next and specifies the capabilities of various principals in the system. The model defines enforcement rules and certification rules.
The model's enforcement and certification rules define data items and processes that provide the basis for an integrity policy. The core of the model is based on the notion of a transaction.
A well-formed transaction is a series of operations that transition a system from one consistent state to another consistent state.
In this model the integrity policy addresses the integrity of the transactions.
The principle of separation of duty requires that the certifier of a transaction and the implementer be different entities.
The model contains a number of basic constructs that represent both data items and processes that operate on those data items. The key data type in the Clark-Wilson model is a Constrained Data Item (CDI). An Integrity Verification Procedure (IVP) ensures that all CDIs in the system are valid at a certain state. Transactions that enforce the integrity policy are represented by Transformation Procedures (TPs). A TP takes as input a CDI or Unconstrained Data Item (UDI) and produces a CDI. A TP must transition the system from one valid state to another valid state. UDIs represent system input (such as that provided by a user or adversary). A TP must guarantee
(via certification) that it transforms all possible values of a UDI to a "safe" CDI.
In general, preservation of data integrity has three goals:
Prevent data modification by unauthorized parties
Prevent unauthorized data modification by authorized parties
Maintain internal and external consistency (i.e. data reflects the real world)
Clark-Wilson addresses all three rules but BIBA addresses only the first rule of intergrity.
References:
HARRIS, Shon, All-In-One CISSP Certification Fifth Edition, McGraw-Hill/Osborne, Chapter 5: Security Architecture and Design (Page 341-344).
and
http://en.wikipedia.org/wiki/Clark-Wilson_model

NEW QUESTION: 223
Which of the following is BEST suited for exchanging authentication and authorization messages in a multi- party decentralized environment?
A. Lightweight Directory Access Protocol (LDAP)

B. Security Assertion Markup Language (SAML)
C. Internet Mail Access Protocol
D. Transport Layer Security (TLS)
Answer: B (LEAVE A REPLY)
Section: Software Development Security

NEW QUESTION: 224
Which of the following cable types is limited in length to 185 meters?
A. 10BaseT
B. RG8
C. RG58
D. 10Base5
Answer: C (LEAVE A REPLY)
10Base2, also known as RG58, or thinnet, is limited to 185 meters. 10Base5, also known as RG8/RG11 or thicknet, is limited to 500 meters. 10BaseT is only limited to 100 meters. Note that the 2 in 10Base2 refers to the maximum cable length (200 meters, 185, actually) and the 5 in 10Base5 is for 500 meters. Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 3: Telecommunications and Network Security (page 32).

NEW QUESTION: 225
Related to information security, availability is the opposite of which of the following?
A. delegation
B. distribution
C. documentation
D. destruction
Answer: D (LEAVE A REPLY)
Availability is the opposite of "destruction."
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

NEW QUESTION: 226
Which of the following is a BEST practice when traveling internationally with laptops containing Personally Identifiable Information (PII)?
A. Request international points of contact help scan the laptop on arrival to ensure it is protected.
B. Do not take unnecessary information, including sensitive information.
C. Use a thumb drive to transfer information from a foreign computer.
D. Connect the laptop only to well-known networks like the hotel or public Internet cafes.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 227
What is a Type 2 authentication factor?
A. Something you know
B. Something you are
C. Something you have
Answer: C (LEAVE A REPLY)
A Type 2 authentication factor is something you have, such as a smart card, ATM card, token device, memory card, etc.

NEW QUESTION: 228
Which of the following is required to determine classification and ownership?
A. Data file references are identified and linked
B. Access violations are logged and audited
C. System and data resources are properly identified
D. System security controls are fully integrated
Answer: C (LEAVE A REPLY)

NEW QUESTION: 229
The Transport Layer Security (TLS) 1.0 protocol is based on which Protocol Specification?
A. SSL-3.0
B. IPSEC
C. TCP/IP
D. SSH-2
Answer: (SHOW ANSWER)
The differences between TLS and SSL are not great, but there is enough of a difference such that TLS 1.0 and SSL 3.0 are not operationally compatible. If interoperability is desired, there is a capability in TLS that allows it to function as SSL. Question 5 provides additional discussion of the TLS protocol.

NEW QUESTION: 230
Identity Management solutions include such technologies as Directories services, Single

Sign-On and Web Access management. There are many reasons for management to choose an identity management solution.
Which of the following is a key management challenge regarding identity management solutions?
A. Increasing the number of points of failures.
B. Users will no longer be able to "recycle" their password for different applications.
C. Costs increase as identity management technologies require significant resources.
D. It must be able to scale to support high volumes of data and peak transaction rates.
Answer: D (LEAVE A REPLY)
Any identity management system used in an environment where there are tens of thousands of users must be able to scale to support the volumes of data and peak transaction rates.
The following answers are incorrect:
Increasing number of points of failures.
This is actually a potential negative impact of not implementing an identity management solution. Identity management is meant to decrease cost and inefficiencies that organizations struggle with so that failures can be managed more efficiently.
Users will no longer be able to "recycle" their password for different applications.
This is actually a function of an effective password management system. Consistency and efficiency are maintained by minimizing unique user authentication requirements.
Costs increase as identity management technologies require significant resources.
On the contrary, "When users access multiple systems, they may be presented with multiple log-in IDs, multiple passwords, and multiple sign-on screens. This complexity is burdensome to users, who consequently have problems accessing systems and incur productivity and support costs
The following reference(s) were/was used to create this question:
ISC2 Official Guide to the CISSP CBK 2007, pg 173
"Key management challenges regarding identity management solutions are:" [consistency, efficiency, usability, reliabliity and scalability.] "Scalability: Enterprises manage user profile data for large numbers of people. There are typically tens of thousands of internal users, and hundreds or thousands of partners or clients."

NEW QUESTION: 231
Who should NOT have access to the log files?
A. Security staff.
B. Internal audit staff.
C. System administration staff.
D. Manager's secretary.
Answer: D (LEAVE A REPLY)
Logs must be secured to prevent modification, deletion, and destruction. Only authorized persons should have access or permission to read logs. A person is authorized if he or she is a member of the internal audit staff, security staff, system administration staff, or he or she has a need for such access to perform regular duties.

NEW QUESTION: 232
Which of the following is an advantage of on-premise Credential Management Systems?
A. Improved credential interoperability
B. Control over system configuration
C. Lower infrastructure capital costs
D. Reduced administrative overhead
Answer: B (LEAVE A REPLY)

NEW QUESTION: 233
What is called the percentage of valid subjects that are falsely rejected by a Biometric Authentication system?
A. False Rejection Rate (FRR) or Type I Error
B. False Acceptance Rate (FAR) or Type II Error
C. Crossover Error Rate (CER)
D. True Rejection Rate (TRR) or Type III Error
Answer: A (LEAVE A REPLY)
The percentage of valid subjects that are falsely rejected is called the False Rejection Rate (FRR) or Type I Error.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38

NEW QUESTION: 234
Which of the following statements pertaining to software testing is incorrect?
A. Unit testing should be addressed and considered when the modules are being designed.
B. Test data should be part of the specifications.
C. Testing should be performed with live data to cover all possible situations.
D. Test data generators can be used to systematically generate random test data that can be used to test programs.
Answer: C (LEAVE A REPLY)
Live or actual field data is not recommended for use in the testing procedures because both data types may not cover out of range situations and the correct outputs of the test are unknown. Live data would not be the best data to use because of the lack of anomalies and also because of the risk of exposure to your live data. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 251).

NEW QUESTION: 235
Windows 2000 uses which of the following as the primary mechanism for authenticating users requesting access to a network?
A. Kerberos

B. Hash functions
C. Public key certificates
D. SESAME
Answer: A (LEAVE A REPLY)
While Kerberos is the primary mechanism, system administrators may also use alternative authentication services running under the Security Support Provider Interface (SSPI). Answer hash functions, are used for digital signature implementations. Answer SESAME is incorrect. It is the Secure European System for Applications in a Multivendor Environment. SESAME performs similar functions to Kerberos, but uses public key cryptography to distribute the secret keys. Answer "Public key certificates" is incorrect, since public key certificates are not used in the Windows 2000 primary authentication approach.

NEW QUESTION: 236
The main differences between a software process assessment and a software capability evaluation are:
A. Software process assessments and software capability evaluations are essentially identical, and there are no major differences between the two.
B. Software capability evaluations determine the state of an organizations current software process and are used to gain support from within the organization for a software process improvement program; software process assessments are used to identify contractors who are qualified to develop software or to monitor the state of the software process in a current software project.
C. Software process assessments are used to develop a risk profile for source selection; software capability evaluations are used to develop an action plan for continuous process improvement.
D. Software process assessments determine the state of an organizations current software process and are used to gain support from within the organization for a software process improvement program; software capability evaluations are used to identify contractors who are qualified to develop software or to monitor the state of the software process in a current software project.
Answer: (SHOW ANSWER)
The other answers are distracters. If, in answer "Software process assessments are used..." the terms software process assessments and software capability evaluations were interchanged, that result would also be correct. It would then read, Software capability evaluations are used to develop a risk profile for source selection; software process assessments are used to develop an action plan for continuous process improvement.

NEW QUESTION: 237
What is the BEST way to establish identity over the internet?
A. Internet Mail Access Protocol (IMAP) with Triple Data Encryption Standard (3DES)
B. Remote user authentication via Simple Object Access Protocol (SOAP)
C. Challenge Handshake Authentication Protocol (CHAP) and strong passwords

D. Remote Authentication Dial-In User Service (RADIUS) server with hardware tokens
Answer: B (LEAVE A REPLY)

NEW QUESTION: 238
Afirewall that performs stateful inspection of the data packet across all
layers is considered a:
A. Fourth-generation firewall.
B. Second-generation firewall.
C. Third-generation firewall.
D. First-generation firewall.
Answer: (SHOW ANSWER)
The correct answer is Third-generation firewall. A stateful inspection firewall is considered a third-generation firewall.

NEW QUESTION: 239
The ideal operating humidity range is defined as 40 percent to 60 percent. High humidity (greater than 60 percent) can produce what type of problem on computer parts?
A. Static electricity
B. Corrosion
C. Energy-plating
D. Element-plating
Answer: B (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 333.

NEW QUESTION: 240
Which of the following is covered under Crime Insurance Policy Coverage?
A. Inscribed, printed and Written documents
B. Manuscripts
C. Accounts Receivable
D. Money and Securities
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Crime Insurance policy protects organizations from loss of money, securities, or inventory resulting from crime.
Incorrect Answers:
A: Crime Insurance Policy does not protect Inscribed, printed and written documents. You would need Valuable paper insurance for that.
B: Crime Insurance Policy does not protect manuscripts. You would need Valuable paper insurance for that.

C: Crime Insurance Policy does not protect business records such as Accounts Receivable. You would need Valuable paper insurance for that.
References:
http://www.insurecast.com/html/crime_insurance.asp

NEW QUESTION: 241
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: 242
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: 243
What principle requires that for particular sets of transactions, no single individual be allowed to execute all transactions within the set?
A. Use of rights
B. Balance of power
C. Separation of duties
D. Fair use
Answer: C (LEAVE A REPLY)
Separation of duties is considered valuable in deterring fraud since fraud can occur if an opportunity exists for collaboration between various jobs related capabilities. Separation of duty requires that for particular sets of transactions, no single individual be allowed to execute all transactions within the set. The most commonly used examples are the separate transactions needed to initiate a payment and to authorize a payment. No single individual should be capable of executing both transactions.

NEW QUESTION: 244
A type of access control that supports the management of access rights
for groups of subjects is:
A. Discretionary
B. Rule-based
C. Role-based
D. Mandatory
Answer: C (LEAVE A REPLY)
Role-based access control assigns identical privileges to groups of users. This approach simplifies the management of access rights, particularly when members of the group change. Thus, access rights are assigned to a role, not to an individual. Individuals are entered as members of specific groups and are assigned the access privileges of that group. In answer Discretionary, the access rights to an object are assigned by the owner at the owner's discretion. For large numbers of people whose duties and participation may change frequently, this type of access control can become unwieldy. Mandatory access control, answer c, uses security labels or classifications assigned to data items and clearances assigned to users. A user has access rights

to data items with a classification equal to or less than the user's clearance. Another restriction is that the user has to have a need-to-know the information; this requirement is identical to the principle of least privilege. Answer 'rule-based access control' assigns access rights based on stated rules. An example of a rule is Access to trade-secret data is restricted to corporate officers, the data owner and the legal department.

NEW QUESTION: 245
The Data Encryption Algorithm performs how many rounds of substitution and permutation?
A. 4
B. 16
C. 54
D. 64
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
International Data Encryption Algorithm (IDEA) is a block cipher and operates on 64-bit blocks of data, which is divided into 16 smaller blocks, and each has eight rounds of mathematical functions performed on it.
Incorrect Answers:
A: This is the size of one of the smaller blocks.
C: This is not a valid block size for block ciphers.
D: This is incorrect as it is the initial size of the block.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, pp. 809, 810

NEW QUESTION: 246
Complete the following sentence. A digital signature is a ____
A. hash value that has been encrypted with the senders private key
B. hash value that has been encrypted with the senders public key
C. hash value that has been encrypted with the senders Session key
D. it is senders signature signed and scanned in a digital format
Answer: A (LEAVE A REPLY)
A digital signature is a hash value that has been encrypted with the senders private key. The act of signing means encrypting the messages hash value with the sender private key.
The following answers are incorrect:
hash value that has been encrypted with the senders public key Encrypting with a public key provide only one service, it is confidentiality. Only the receiver using the matching private key could get access to the clear text.
hash value that has been encrypted with the senders Session key Session keys are Symmetric keys that have a short lifespan, they are used to encrypt the data while a session is ongoing and then destroyed.

it is senders signature signed and scanned in a digital format This is only a distractor
The following reference(s) were/was used to create this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 829). McGraw-Hill . Kindle Edition.

NEW QUESTION: 247
The top speed of ISDN BRI is 256 KBS.(True/False)
A. True
B. False
Answer: B (LEAVE A REPLY)
The top speed of ISDN BRI is 128 KBS. Its two primary channels are each capable of carrying 64 KBS so the combined top speed is 128 KBS.

NEW QUESTION: 248
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: 249
Guards are appropriate whenever the function required by the security program involves which of the following?
A. The use of discriminating judgment
B. The use of physical force

C. The operation of access control devices
D. The need to detect unauthorized access
Answer: A (LEAVE A REPLY)
The answer: The use of discriminating judgment, a guard can make the determinations that hardware or other automated security devices cannot make due to its ability to
adjust to rapidly changing conditions, to learn and alter recognizable patterns, and to respond to various conditions in the environment. Guards are better at making value decisions at times of incidents. They are appropriate whenever immediate, discriminating judgment is required by the security entity.
The following answers are incorrect:
The use of physical force This is not the best answer. A guard provides discriminating judgment, and the ability to discern the need for physical force.
The operation of access control devices A guard is often uninvolved in the operations of an automated access control device such as a biometric reader, a smart lock, mantrap, etc.
The need to detect unauthorized access The primary function of a guard is not to detect unauthorized access, but to prevent unauthorized physical access attempts and may deter social engineering attempts.
The following reference(s) were/was used to create this question:
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 339).
Source: ISC2 Offical Guide to the CBK page 288-289.

NEW QUESTION: 250
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)
Explanation/Reference:
Explanation:
A typical PKI consists of hardware, software, policies and standards to manage the creation, administration, distribution and revocation of keys and digital certificates. Digital certificates are at the heart of PKI as they affirm the identity of the certificate subject and bind that identity to the public key contained in the certificate.
Incorrect Answers:
A: A public-key certificate contains a public key. However, it is the PKI (in particular the certificate authority) that verifies the subject's identity and binds the subject name to the public key value.
C: A secret key infrastructure is not a valid answer. A secret key can refer to a private key or more commonly to a shared key used in symmetric encryption.

D: A private key (and its corresponding public key) is usually generated by a user or application. The public key is then validated and signed by a CA. A private key does not bind a subject name to a public key value.
References:
http://searchsecurity.techtarget.com/definition/PKI

NEW QUESTION: 251
Which of the following controls related to physical security is NOT an administrative control?
A. Personnel controls
B. Alarms
C. Training
D. Emergency response and procedures
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Alarms are an example of a physical control type, not an administrative control.
Controls are put into place to reduce the risk an organization faces, and they come in three main flavors:
administrative, technical, and physical. Administrative controls are commonly referred to as "soft controls" because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.
Incorrect Answers:
A: Personnel controls are an example of an administrative control. Therefore, this answer is incorrect.
C: Training is an example of an administrative control. Therefore, this answer is incorrect.
D: Emergency response and procedures are an example of an administrative control. Therefore, this answer is incorrect.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 28

NEW QUESTION: 252
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: 253
Vulnerability scanners may allow for the administrator to assign which of the following in order to assist in prioritizing remediation activities?
A. Exploit code metrics
B. Asset values for networks
C. Vulnerability attack vectors
D. Definitions for each exposure type
Answer: B (LEAVE A REPLY)

NEW QUESTION: 254
For network based evidence, which of the following contains traffic details of all network sessions in order to detect anomalies?
A. Statistical data
B. Alert data
C. User data
D. Content data
Answer: (SHOW ANSWER)

NEW QUESTION: 255
Which of the following is the MOST important consideration when developing a Disaster Recovery Plan (DRP)?
A. The cost of downtime
B. A recovery strategy for all business processes
C. A containment strategy
D. The dynamic reconfiguration of systems
Answer: B (LEAVE A REPLY)

NEW QUESTION: 256
Degaussing is used to clear data from all of the following medias except:
A. Floppy Disks
B. Read-Only Media
C. Video Tapes
D. Magnetic Hard Disks
Answer: B (LEAVE A REPLY)
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"
The latest ISC2 book says:
"Degaussing can also be a form of media destruction. High-power degaussers are so strong in some cases that they can literally bend and warp the platters in a hard drive.
Shredding and burning are effective destruction methods for non-rigid magnetic media.
Indeed, some shredders are capable of shredding some rigid media such as an optical disk. This may be an effective alternative for any optical media containing nonsensitive information due to the residue size remaining after feeding the disk into the machine.
However, the residue size might be too large for media containing sensitive information.
Alternatively, grinding and pulverizing are acceptable choices for rigid and solid-state media.
Specialized devices are available for grinding the face of optical media that either sufficiently scratches the surface to render the media unreadable or actually grinds off the data layer of the disk. Several services also exist which will collect drives, destroy them on site if requested and provide certification of completion. It will be the responsibility of the security professional to help, select, and maintain the most appropriate solutions for media cleansing and disposal."
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 (from the "all about degaussers link below). 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 wich 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.
I will admit that this is a bit of a trick question. Determining the difference between "read- only media" and "read-only memory" is difficult for the question taker. However, I believe it is representative of the type of question you might one day see on an exam.
The other answers are incorrect because:
Floppy Disks, Magnetic Tapes, and Magnetic Hard Disks are all examples of magnetic storage, and therefore are erased by degaussing.
A videotape is a recording of images and sounds on to magnetic tape as opposed to film stock used in filmmaking or random access digital media. Videotapes are also used for storing scientific or medical data, such as the data produced by an electrocardiogram. In most cases, a helical scan video head rotates against the moving tape to record the data in two dimensions, because

video signals have a very high bandwidth, and static heads would require extremely high tape speeds. Videotape is used in both video tape recorders
(VTRs) or, more commonly and more recently, videocassette recorder (VCR) and camcorders. A Tape use a linear method of storing information and since nearly all video recordings made nowadays are digital direct to disk recording (DDR), videotape is expected to gradually lose importance as non-linear/random-access methods of storing digital video data become more common.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 25627-25630). McGraw-Hill. Kindle Edition.
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Security Operations (Kindle Locations 580-588). . Kindle Edition.
All About Degaussers and Erasure of Magnetic Media:
http://www.degausser.co.uk/degauss/degabout.htm
http://www.degaussing.net/
http://www.cerberussystems.com/INFOSEC/stds/ncsctg25.htm

NEW QUESTION: 257
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)
Explanation/Reference:
Explanation:
Availability ensures reliability and timely access to data and resources to authorized individuals. Network devices, computers, and applications should provide adequate functionality to perform in a predictable manner with an acceptable level of performance. They should be able to recover from disruptions in a secure and quick fashion so productivity is not negatively affected.

Necessary protection mechanisms must be in place to protect against inside and outside threats that could affect the availability and productivity of all business-processing components.
Incorrect Answers:
A: Confidentiality ensures that the necessary level of secrecy is enforced at each junction of data processing and prevents unauthorized disclosure. This is not what is described in the question.
C: Integrity ensures that data is unaltered. This is not what is described in the question.
D: Reliability could be used to describe the ability of system to serve data. However, data being accessible when required is described as availability, not reliability.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 23

NEW QUESTION: 258
Which of the following is an example of a symmetric key algorithm?(Choose all that apply)
A. Rijndael
B. RSA
C. Diffie-Hellman
D. Knapsack
E. IDEA
Answer: (SHOW ANSWER)
All the others except Rijndael and IDEA are examples of asymmetric key algorithms.

NEW QUESTION: 259
Which of the following alternatives should NOT be used by law
enforcement to gain access to a password?
A. Contacting the developer of the software for information to gain access to the computer or network through a back door
B. Compelling the suspect to provide the password
C. Data manipulation and trial procedures applied to the original version of the system hard disk
D. Using password cracker software
Answer: C (LEAVE A REPLY)
The original disk of a computer involved in a criminal investigation should not be used for any experimental purposes since data may be modified or destroyed. Any operations should be conducted on a copy of the system disk. However, the other answers are the preferred methods of gaining access to a password-protected system. Interestingly, in answer b, there is legal precedent to order a suspect to provide the password of a computer that is in the custody of law enforcement.

NEW QUESTION: 260
Which of the following is not a responsibility of an information (data) owner?
A. Determine what level of classification the information requires.
B. Periodically review the classification assignments against business needs.

C. Delegate the responsibility of data protection to data custodians.
D. Running regular backups and periodically testing the validity of the backup data.
Answer: D (LEAVE A REPLY)
This responsibility would be delegated to a data custodian rather than being performed directly by the information owner.
"Determine what level of classification the information requires" is incorrect. This is one of the major responsibilities of an information owner.
"Periodically review the classification assignments against business needs" is incorrect. This is one of the major responsibilities of an information owner.
"Delegates responsibility of maintenance of the data protection mechanisms to the data custodian" is incorrect. This is a responsibility of the information owner.
References:
CBK p. 105.
AIO3, p. 53-54, 960

NEW QUESTION: 261
Which of the following is a characteristic of a challenge/response authentication process?
A. Presenting distorted gravies of text for authentication
B. Transmitting a hash based on the user's password
C. Requiring the use of non-consecutive numeric characters
D. Using a password history blacklist
Answer: A (LEAVE A REPLY)

NEW QUESTION: 262
Which of the following is currently the most recommended water system for a computer room?
A. preaction
B. wet pipe
C. dry pipe
D. deluge
Answer: (SHOW ANSWER)
The answer: Preaction combines both the dry and wet pipe systems and allows manual intervention before a full discharge of water on the equipment occurs. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, page 334.

NEW QUESTION: 263
Which choice MOST accurately describes the difference between the role of a data owner versus the role of a data custodian?
A. The data owner implements the information classification scheme after the initial assignment by the custodian.

B. The custodian implements the information classification scheme after the initial assignment by the owner.
C. The custodian implements the information classification scheme after the initial assignment by the operations manager.
D. The custodian makes the initial information classification assignments, and the operations manager implements the scheme.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 264
Which of the following teams should NOT be included in an organization's contingency plan?
A. Damage assessment team
B. Hardware salvage team
C. Tiger team
D. Legal affairs team
Answer: (SHOW ANSWER)
According to NIST's Special publication 800-34, a capable recovery strategy will require some or all of the following functional groups: Senior management official, management team, damage assessment team, operating system administration team, systems software team, server recovery team, LAN/WAN recovery team, database recovery team, network operations recovery team, telecommunications team, hardware salvage team, alternate site recovery coordination team, original site restoration/salvage coordination team, test team, administrative support team, transportation and relocation team, media relations team, legal affairs team, physical/personal security team, procurements team. Ideally, these teams would be staffed with the personnel responsible for the same or similar operation under normal conditions. A tiger team, originally a U.S. military jargon term, defines a team (of sneakers) whose purpose is to penetrate security, and thus test security measures. Used today for teams performing ethical hacking. Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 23).

NEW QUESTION: 265
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: A (LEAVE A REPLY)
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: 266
When evaluating third-party applications, which of the following is the GREATEST responsibility of Information Security?
A. Accept the risk on behalf of the organization.
B. Report findings to the business to determine security gaps.
C. Quantify the risk to the business for product selection.
D. Approve the application that best meets security requirements.
Answer: (SHOW ANSWER)
Section: Software Development Security

NEW QUESTION: 267
Which statement below is accurate about the concept of Object Reuse?
A. Object reuse protects against physical attacks on the storage medium.
B. Object reuse applies to removable media only.
C. Object reuse controls the granting of access rights to objects.
D. Object reuse ensures that users do not obtain residual information from system resources.
Answer: D (LEAVE A REPLY)
Object reuse mechanisms ensure system resources are allocated and reassigned among authorized users in a way that prevents the leak of sensitive information, and ensure that the authorized user of the system does not obtain residual information from system resources. Object reuse is defined as The reassignment to some subject of a storage medium (e.g., page frame, disk sector, magnetic tape) that contained one or more objects. To be securely reassigned, no residual data can be available to the new subject through standard system mechanisms.7 The object reuse requirement of the TCSEC is intended to assure that system resources, in particular storage media, are allocated and reassigned among system users in a manner which prevents the disclosure of sensitive information. Answer a is incorrect. Object reuse does not necessarily protect against physical attacks on the storage medium. Answer c is also incorrect, as object reuse applies to all primary and secondary storage media, such as removable media, fixed media, real and virtual main memory (including registers), and cache memory. Answer d refers to authorization, the granting of access rights to a user, program, or process. Source: NCSC-TG-018, A Guide To Understanding Object Reuse in Trusted Systems [Light Blue Book].

NEW QUESTION: 268
Which of the following are controls that can be used to secure faxing of sensitive data?(Choose all that apply)
A. Send to email boxes instead of printing

B. Disable automatic printing
C. Print "sensitive document banner" on each page
D. Fax encryptor
E. Restrict the use of fax machines that use a ribbon or duplication cartridge
Answer: A,B,D,E (LEAVE A REPLY)

NEW QUESTION: 269
Which of the following was developed in order to protect against fraud in electronic fund transfers (EFT) by ensuring the message comes from its claimed originator and that it has not been altered in transmission?
A. Secure Electronic Transaction (SET)
B. Message Authentication Code (MAC)
C. Cyclic Redundancy Check (CRC)
D. Secure Hash Standard (SHS)
Answer: B (LEAVE A REPLY)
In order to protect against fraud in electronic fund transfers (EFT), the
Message Authentication Code (MAC), ANSI X9.9, was developed. The MAC is a check value, which is derived from the contents of the message itself, that is sensitive to the bit changes in a message. It is similar to a Cyclic Redundancy Check (CRC).
The aim of message authentication in computer and communication systems is to verify that he message comes from its claimed originator and that it has not been altered in transmission. It is particularly needed for EFT Electronic Funds Transfer). The protection mechanism is generation of a Message Authentication Code (MAC), attached to the message, which can be recalculated by the receiver and will reveal any alteration in transit.
One standard method is described in (ANSI, X9.9). Message authentication mechanisms an also be used to achieve non-repudiation of messages.
The Secure Electronic Transaction (SET) was developed by a consortium including
MasterCard and VISA as a means of preventing fraud from occurring during electronic payment.
The Secure Hash Standard (SHS), NIST FIPS 180, available at
http://www.itl.nist.gov/fipspubs/fip180-1.htm, specifies the Secure Hash Algorithm (SHA-1).
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 170)
also see:
http://luizfirmino.blogspot.com/2011/04/message-authentication-code-mac.html and
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.22.2312&rep=rep1&type=pdf

NEW QUESTION: 270
Which of the following is NOT a property of a Packet Filtering Firewall?
A. Uses ACLs

B. Operates at the Application Layer
C. Considered a first-generation firewall
D. Examines the source and destination addresses of the incoming packet
Answer: B (LEAVE A REPLY)
The correct answer is Operates at the Application Layer. A packet-filtering firewall can operate at the network or transport layers.

NEW QUESTION: 271
Which of the following would describe a type of biometric error refers to as FASLE rejection rate?
A. Type I error
B. Type II error
C. Type III error
D. CER error
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A Type I error, or false rejection rate, is when a biometric system rejects an authorized individual.
Incorrect Answers:
B: A Type II error, or false acceptance rate, is when the system accepts impostors who should be rejected.
C: A Type III error does not exist in biometrics.
D: The crossover error rate (CER) is a percentage that signifies the point at which the false rejection rate equals the false acceptance rate.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, pp. 188
http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=93
https://pciguru.wordpress.com/2010/05/01/one-two-and-three-factor-authentication/

NEW QUESTION: 272
What is the MAIN reason for testing a Disaster Recovery Plan (DRP)?
A. To ensure Information Technology (IT) staff knows and performs roles assigned to each of them
B. To validate backup sites' effectiveness

C. To find out what does not work and fix it
D. To create a high level DRP awareness among Information Technology (IT) staff
Answer: (SHOW ANSWER)
Section: Security Assessment and Testing

NEW QUESTION: 273
Which of the following groups represents the leading source of computer crime losses?
A. Hackers
B. Industrial saboteurs
C. Foreign intelligence officers
D. Employees
Answer: D (LEAVE A REPLY)
This can be checked at the computer crime static's on the web. Most of the attacks, actually 70% of them, come from inside the company, and 80% of them from employees of it. This is a reality, when we protect our infrastructure be sure to give great importance to internal security, we don't when is one of the company employees going to make a strike. Hackers are also important, but less than our own employees.

NEW QUESTION: 274
Which is NOT a property of a packet-switched network?
A. Connectionless network
B. Packets are assigned sequence numbers
C. Connection-oriented network
D. Characterized by bursty traffic
Answer: (SHOW ANSWER)
The correct answer is "Connection-oriented network". Packet-switched networks are considered connectionless networks; circuit-switched networks are considered connection-oriented.

NEW QUESTION: 275
Assessing a third party's risk by counting bugs in the code may not be the best measure of an attack surface within the supply chain.
Which of the following is LEAST associated with the attack surface?
A. Input protocols
B. Target processes
C. Error messages
D. Access rights
Answer: C (LEAVE A REPLY)
Explanation
Section: Security Assessment and Testing

NEW QUESTION: 276
Which of the following statements pertaining to ethical hacking is incorrect?
A. An organization should use ethical hackers who do not sell auditing, hardware, software, firewall, hosting, and/or networking services.
B. Testing should be done remotely to simulate external threats.
C. Ethical hacking should not involve writing to or modifying the target systems negatively.
D. Ethical hackers never use tools that have the potential of affecting servers or services.
Answer: D (LEAVE A REPLY)
This means that many of the tools used for ethical hacking have the potential of exploiting vulnerabilities and causing disruption to IT system. It is up to the individuals performing the tests to be familiar with their use and to make sure that no such disruption can happen or at least shoudl be avoided.
The first step before sending even one single packet to the target would be to have a signed agreement with clear rules of engagement and a signed contract. The signed contract explains to the client the associated risks and the client must agree to them before you even send one packet to the target range. This way the client understand that some of the test could lead to interruption of service or even crash a server. The client signs that he is aware of such risks and willing to accept them.
The following are incorrect answers:
An organization should use ethical hackers who do not sell auditing, hardware, software, firewall, hosting, and/or networking services. An ethical hacking firm's independence can be questioned if they sell security solutions at the same time as doing testing for the same client. There has to be independance between the judge (the tester) and the accuse (the client).
Testing should be done remotely to simulate external threats Testing simulating a cracker from the Internet is often time one of the first test being done, this is to validate perimeter security. By performing tests remotely, the ethical hacking firm emulates the hacker's approach more realistically.
Ethical hacking should not involve writing to or modifying the target systems negatively.
Even though ethical hacking should not involve negligence in writing to or modifying the target systems or reducing its response time, comprehensive penetration testing has to be performed using the most complete tools available just like a real cracker would.
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, Appendix F: The Case for Ethical Hacking (page 520).

NEW QUESTION: 277
Which of the following attack could be avoided by creating more security awareness in the organization and provide adequate security knowledge to all employees?
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.
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.
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.
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: 278
Which one of the following is a key agreement protocol used to enable two entities to agree and generate a session key (secret key used for one session) over an insecure medium without any prior secrets or communications between the entities? The negotiated key will subsequently be used for message encryption using Symmetric Cryptography.
A. RSA
B. PKI
C. Diffie_Hellmann
D. 3DES

Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Diffie-Hellman key exchange (D-H) is a specific method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle.
D-H is one of the earliest practical examples of public key exchange implemented within the field of cryptography. Traditionally, secure encrypted communication between two parties required that they first exchange keys by some secure physical channel, such as paper key lists transported by a trusted courier.
The Diffie-Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.
Incorrect Answers:
A: RSA is not the key agreement protocol described in the question.
B: PKI is not the key agreement protocol described in the question.
D: 3DES is not the key agreement protocol described in the question.
References:
https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

NEW QUESTION: 279
Which of the following Operation Security controls is intended to prevent unauthorized intruders from internally or externally accessing the system, and to lower the amount and impact of unintentional errors that are entering the system?
A. Detective Controls
B. Preventative Controls
C. Corrective Controls
D. Directive Controls
Answer: B (LEAVE A REPLY)
In the Operations Security domain, Preventative Controls are designed to prevent unauthorized intruders from internally or externally accessing the system, and to lower the amount and impact of unintentional errors that are entering the system.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 217.

NEW QUESTION: 280
*Directive controls are a form of change management policy and procedures. Which of the following subsections are recommended as part of the change management process?
A. Build and test
B. Implement security controls
C. Categorize Information System (IS)

D. Select security controls

Answer: A (LEAVE A REPLY)

Reference: https://books.google.com.pk/books?id=9gCn86CmsNQC&pg=PA570&lpg=PA570&dq=CISSP+Directive+controls+are+a+form+of+change+management+policy+and+procedures.+Which+o&source=bl&ots=riGvVpSS3E&sig=ACfU3U3dLYheW_GfTZcAYfN97fnDFlMmZg&hl=en&sa=X&ved=2ahUKEwjukoqK96npAhULtRoKHZEpBmcQ6AEwAHoECBQQAQ#v=onepage& q=CISSP%20Directive%20controls%20are%20a%20form%20of%20change%20management%20policy&f=false

NEW QUESTION: 281

In a PKI infrastructure where are list of revoked certificates stored?

A. CRL

B. Registration Authority

C. Recovery Agent

D. Key escrow

Answer: A (LEAVE A REPLY)

Certificate revocation is the process of revoking a certificate before it expires.

A certificate may need to be revoked because it was stolen, an employee moved to a new company, or someone has had their access revoked. A certificate revocation is handled either through a Certificate Revocation List (CRL) or by using the Online Certificate Status Protocol (OCSP).

A repository is simply a database or database server where the certificates are stored. The process of revoking a certificate begins when the CA is notified that a particular certificate needs to be revoked. This must be done whenever the private key becomes known/compromised.

The owner of a certificate can request it be revoked at any time, or the request can be made by the administrator. The CA marks the certificate as revoked. This information is published in the CRL. The revocation process is usually very quick; time is based on the publication interval for the CRL.

Disseminating the revocation information to users may take longer. Once the certificate has been revoked, it can never be used-or trusted-again. The CA publishes the CRL on a regular basis, usually either hourly or daily. The CA sends or publishes this list to organizations that have chosen to receive it; the publishing process occurs automatically in the case of PKI. The time between when the CRL is issued and when it reaches users may be too long for some applications. This time gap is referred to as latency.

OCSP solves the latency problem: If the recipient or relaying party uses OCSP for verification, the answer is available immediately.

The following answers are incorrect:

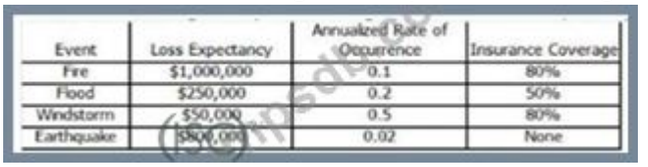
Registration Authority (RA) A registration authority (RA) is an authority in a network that verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it. RAs are part of a public key infrastructure (PKI), a networked system that enables companies and users to

exchange information and money safely and securely. The digital certificate contains a public key that is used to encrypt and decrypt messages and digital signatures.
Recovery agent Sometimes it is necessary to recover a lost key. One of the problems that often arises regarding PKI is the fear that documents will become lost forever-irrecoverable because someone loses or forgets his private key. Let's say that employees use Smart Cards to hold their private keys. If a user was to leave his Smart
Card in his or her wallet that was left in the pants that he or she accidentally threw into the washing machine, then that user might be without his private key and therefore incapable of accessing any documents or e-mails that used his existing private key.
Many corporate environments implement a key recovery server solely for the purpose of backing up and recovering keys. Within an organization, there typically is at least one key recovery agent. A key recovery agent has the authority and capability to restore a user's lost private key. Some key recovery servers require that two key recovery agents retrieve private user keys together for added security. This is similar to certain bank accounts, which require two signatures on a check for added security. Some key recovery servers also have the ability to function as a key escrow server, thereby adding the ability to split the keys onto two separate recovery servers, further increasing security.
Key escrow (also known as a "fair" cryptosystem) is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. These third parties may include businesses, who may want access to employees' private communications, or governments, who may wish to be able to view the contents of encrypted communications.
The following reference(s) were/was used to create this question:
Dulaney, Emmett (2011-06-03). CompTIA Security+ Study Guide: Exam SY0-301 (pp. 347-348). John Wiley and Sons. Kindle Edition.
and
http://en.wikipedia.org/wiki/Key_escrow
and
http://my.safaribooksonline.com/book/certification/securityplus/9781597494267/public-key-infrastructure/ch12lev1sec5 and
http://searchsecurity.techtarget.com/definition/registration-authority

NEW QUESTION: 282
Of the following, which is NOT a specific loss criteria that should be considered while developing a BIA?
A. Loss of skilled workers knowledge
B. Loss in revenue
C. Loss in profits
D. Loss in reputation
Answer: (SHOW ANSWER)
Although a loss of skilled workers knowledge would cause the company a great

loss, it is not identified as a specific loss criteria. It would fall under one of the three other criteria listed as distracters.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 598).

NEW QUESTION: 283
Which of the following would present the highert annualized loss expectancy (ALE)?



Event	Loss Expectancy	Annualized Rate of Occurrence	Insurance Coverage
Fire	$1,000,000	0.1	80%
Flood	$250,000	0.2	50%
Windstorm	$50,000	0.5	80%
Earthquake	$800,000	0.02	None

A. Flood
B. Earthquake
C. Windstorm
D. Fire
Answer: (SHOW ANSWER)

NEW QUESTION: 284
Which disaster recovery/emergency management plan testing type
below is considered the most cost-effective and efficient way to identify areas of overlap in the plan before conducting more demanding training exercises?
A. Evacuation drill
B. Table-top exercise test
C. Full-scale exercise
D. Walk-through drill
Answer: (SHOW ANSWER)
In a table-top exercise, members of the emergency management
group meet in a conference room setting to discuss their responsibilities and how they would react to emergency scenarios. Disaster recovery/emergency management plan testing scenarios have several
levels, and can be called different things. The primary hierarchy
of disaster/emergency testing plan types is shown below.
Checklist review. Plan is distributed and reviewed by business
units for its thoroughness and effectiveness.
Table-top exercise or structured walk-through test. Members of
the emergency management group meet in a conference room
setting to discuss their responsibilities and how they would
react to emergency scenarios by stepping through the plan.
Walk-through drill or simulation test. The emergency management
group and response teams actually perform their emergency
response functions by walking through the test, without

actually initiating recovery procedures. More thorough than the table-top exercise.
Functional drills. Test specific functions such as medical response, emergency notifications, warning and communications procedures, and equipment, although not necessarily all at once. Also includes evacuation drills, where personnel walk the evacuation route to a designated area where procedures for accounting for the personnel are tested.
Parallel test or full-scale exercise. A real-life emergency situation is simulated as closely as possible. Involves all of the participants that would be responding to the real emergency, including community and external organizations. The test may involve ceasing some real production processing.
Source: Emergency Management Guide for Business and Industry, Federal Emergency Management Agency, August 1998 and Computer Security Basics, by Deborah Russell and G.T. Gangemi, Sr. (OReilly, 1992).

NEW QUESTION: 285
Which of the following would best describe certificate path validation?
A. Verification of the validity of all certificates of the certificate chain to the root certificate
B. Verification of the integrity of the associated root certificate
C. Verification of the integrity of the concerned private key
D. Verification of the revocation status of the concerned certificate
Answer: (SHOW ANSWER)
With the advent of public key cryptography (PKI), it is now possible to communicate securely with untrusted parties over the Internet without prior arrangement.
One of the necessities arising from such communication is the ability to accurately verify someone's identity (i.e. whether the person you are communicating with is indeed the person who he/she claims to be). In order to be able to perform identity check for a given entity, there should be a fool-proof method of "binding" the entity's public key to its unique domain name (DN).
A X.509 digital certificate issued by a well known certificate authority (CA), like Verisign, Entrust, Thawte, etc., provides a way of positively identifying the entity by placing trust on the CA to have performed the necessary verifications. A X.509 certificate is a cryptographically sealed data object that contains the entity's unique DN, public key, serial number, validity period, and possibly other extensions.
The Windows Operating System offers a Certificate Viewer utility which allows you to double-click on any certificate and review its attributes in a human-readable format. For instance, the "General" tab in the Certificate Viewer Window (see below) shows who the certificate was issued to as well as the certificate's issuer, validation period and usage functions.
Certification Path graphic

The "Certification Path" tab contains the hierarchy for the chain of certificates. It allows you to select the certificate issuer or a subordinate certificate and then click on "View Certificate" to open the certificate in the Certificate Viewer.
Each end-user certificate is signed by its issuer, a trusted CA, by taking a hash value (MD5 or SHA-1) of ASN.1 DER (Distinguished Encoding Rule) encoded object and then encrypting the resulting hash with the issuer's private key (CA's Private Key) which is a digital signature. The encrypted data is stored in the "signatureValue" attribute of the entity's (CA) public certificate.
Once the certificate is signed by the issuer, a party who wishes to communicate with this entity can then take the entity's public certificate and find out who the issuer of the certificate is. Once the issuer's of the certificate (CA) is identified, it would be possible to decrypt the value of the "signatureValue" attribute in the entity's certificate using the issuer's public key to retrieve the hash value. This hash value will be compared with the independently calculated hash on the entity's certificate. If the two hash values match, then the information contained within the certificate must not have been altered and, therefore, one must trust that the CA has done enough background check to ensure that all details in the entity's certificate are accurate.
The process of cryptographically checking the signatures of all certificates in the certificate chain is called "key chaining". An additional check that is essential to key chaining is verifying that the value of the "subjectKeyIdentifier" extension in one certificate matches the same in the subsequent certificate.
Similarly, the process of comparing the subject field of the issuer certificate to the issuer field of the subordinate certificate is called "name chaining". In this process, these values must match for each pair of adjacent certificates in the certification path in order to guarantee that the path represents unbroken chain of entities relating directly to one another and that it has no missing links.
The two steps above are the steps to validate the Certification Path by ensuring the validity of all certificates of the certificate chain to the root certificate as described in the two paragraphs above.
Reference(s) used for this question:
FORD, Warwick & BAUM, Michael S., Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption (2nd Edition), 2000, Prentice Hall PTR, Page 262.
and
https://www.tibcommunity.com/docs/DOC-2197

NEW QUESTION: 286
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. Mandatory Access Control (MAC).
B. rule based access controls.
C. separation of duties.
D. least privilege.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 287
Refer to the information below to answer the question.
During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.
If it is discovered that large quantities of information have been copied by the unauthorized individual, what attribute of the data has been compromised?
A. Accountability
B. Availability
C. Integrity
D. Confidentiality
Answer: D (LEAVE A REPLY)

NEW QUESTION: 288
A screening router can perform packet filtering based upon what data?
A. Translated source destination addresses.
B. Inverse address resolution.
C. Source and destination port number.
D. Source and destination addresses and application data.
Answer: (SHOW ANSWER)
The original answer was A (translated source destination address). I did not come across this term in my reading. Screening router A screening router is one of the simplest firewall strategies to implement. This is a popular design because most companies already have the hardware in place to implement it. A screening router is an excellent first line of defense in the creation of your firewall strategy. It's just a router that has filters associated with it to screen outbound and inbound traffic based on IP address and UDP and TCP ports.
http://www.zdnet.co.uk/news/specials/2000/10/enterprise/techrepublic/2002/10/article002c.html

NEW QUESTION: 289
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 implementation

C. Plain text is encrypted with a public key and decrypted with a private key
D. Block ciphers can be operated as a stream
Answer: C (LEAVE A REPLY)
"Strong and efficient block cryptosystems use random key values so an attacker cannot find a pattern as to which S-boxes are chosen and used." Pg. 481 Shon Harris CISSP Certification All-in-One Exam Guide
Not A:
"When a block cipher algorithm is used for encryption and decryption purposes, the message is divided into blocks of bits. These blocks are then put through substitution, transposition, and other mathematical functions, on block at a time." Pg. 480 Shon Harris CISSP Certification All-in-One Exam Guide
Not B:
"Block ciphers are easier to implement in software because they work with blocks of data that the software is used to work with." Pg 483 Shon Harris CISSP Certification All-in-One Exam Guide
Not D:
"This encryption continues until the plaintext is exhausted." Pg. 196 Krutz The CISSP Prep Guide.
Not A or D:
"When a block a block cipher algorithm is used for encryption and decryption purposes, the message is divided into blocks of bits. These blocks are then put through substitution, transposition, and other mathematical functions, one block at a time." Pg 480 Shon Harris: All-in-One CISSP Certification

NEW QUESTION: 290
Which of the following is an effective method for avoiding magnetic media data remanence?
A. Degaussing
B. Authentication
C. Encryption
D. Data Loss Prevention (DLP)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 291
Relative to legal evidence, which one of the following correctly describes the difference between an expert and a nonexpert in delivering an opinion?
A. An expert can offer an opinion based on personal expertise and facts, but a nonexpert can testify only as to facts.
B. Anonexpert can offer an opinion based on personal expertise and facts, but an expert can testify only as to facts.
C. An expert can offer an opinion based on personal expertise and facts, but a nonexpert can testify only as to personal opinion.
D. An expert can offer an opinion based on facts only, but a nonexpert can testify only as to personal opinion.

Answer: A (LEAVE A REPLY)
The other answers are distracters.

NEW QUESTION: 292
Authentication Headers (AH) and Encapsulating Security Payload (ESP) protocols are the driving force of IPSec. Authentication Headers (AH) provides the following service except:
A. Authentication
B. Integrity
C. Replay resistance and non-repudiations
D. Confidentiality
Answer: D (LEAVE A REPLY)
AH provides integrity, authentication, and non-repudiation. AH does not provide encryption which means that NO confidentiality is in place if only AH is being used.
You must make use of the Encasulating Security Payload if you wish to get confidentiality.
IPSec uses two basic security protocols: Authentication Header (AH) and Encapsulation Security Payload.
AH is the authenticating protocol and the ESP is the authenticating and encrypting protocol that uses cryptographic mechanisms to provide source authentication, confidentiality and message integrity.
The modes of IPSEC, the protocols that have to be used are all negotiated using Security Association. Security Associations (SAs) can be combined into bundles to provide authentication, confidentialility and layered communication.
Source:
TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, page 164.
also see:
Shon Harris, CISSP All In One Exam Guide, 5th Edition, Page 758

NEW QUESTION: 293
While using IPsec, the ESP and AH protocols both provides integrity services. However when using AH, some special attention needs to be paid if one of the peers uses NAT for address translation service. Which of the items below would affects the use of AH and it's Integrity Check Value (ICV) the most?
A. Key session exchange
B. Packet Header Source or Destination address
C. VPN cryptographic key size
D. Crypotographic algorithm used
Answer: (SHOW ANSWER)
It may seem odd to have two different protocols that provide overlapping functionality. AH provides authentication and integrity, and ESP can provide those two functions and confidentiality.

Why even bother with AH then?

In most cases, the reason has to do with whether the environment is using network address translation (NAT). IPSec will generate an integrity check value (ICV), which is really the same thing as a MAC value, over a portion of the packet. Remember that the sender and receiver generate their own values. In IPSec, it is called an ICV value. The receiver compares her ICV value with the one sent by the sender. If the values match, the receiver can be assured the packet has not been modified during transmission. If the values are different, the packet has been altered and the receiver discards the packet.

The AH protocol calculates this ICV over the data payload, transport, and network headers. If the packet then goes through a NAT device, the NAT device changes the IP address of the packet. That is its job. This means a portion of the data (network header) that was included to calculate the ICV value has now changed, and the receiver will generate an ICV value that is different from the one sent with the packet, which means the packet will be discarded automatically.

The ESP protocol follows similar steps, except it does not include the network header portion when calculating its ICV value. When the NAT device changes the IP address, it will not affect the receiver's ICV value because it does not include the network header when calculating the ICV.

Here is a tutorial on IPSEC from the Shon Harris Blog:

The Internet Protocol Security (IPSec) protocol suite provides a method of setting up a secure channel for protected data exchange between two devices. The devices that share this secure channel can be two servers, two routers, a workstation and a server, or two gateways between different networks. IPSec is a widely accepted standard for providing network layer protection. It can be more flexible and less expensive than end-to end and link encryption methods.

IPSec has strong encryption and authentication methods, and although it can be used to enable tunneled communication between two computers, it is usually employed to establish virtual private networks (VPNs) among networks across the Internet.

IPSec is not a strict protocol that dictates the type of algorithm, keys, and authentication method to use. Rather, it is an open, modular framework that provides a lot of flexibility for companies when they choose to use this type of technology. IPSec uses two basic security protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP). AH is the authenticating protocol, and ESP is an authenticating and encrypting protocol that uses cryptographic mechanisms to provide source authentication, confidentiality, and message integrity.

IPSec can work in one of two modes: transport mode, in which the payload of the message is protected, and tunnel mode, in which the payload and the routing and header information are protected. ESP in transport mode encrypts the actual message information so it cannot be sniffed and uncovered by an unauthorized entity. Tunnel mode provides a higher level of protection by also protecting the header and trailer data an attacker may find useful. Figure 8-26 shows the high-level view of the steps of setting up an IPSec connection.

Each device will have at least one security association (SA) for each VPN it uses. The SA, which is critical to the IPSec architecture, is a record of the configurations the device needs to support an IPSec connection. When two devices complete their handshaking process, which means they

have agreed upon a long list of parameters they will use to communicate, these data must be recorded and stored somewhere, which is in the SA.

The SA can contain the authentication and encryption keys, the agreed-upon algorithms, the key lifetime, and the source IP address. When a device receives a packet via the IPSec protocol, it is the SA that tells the device what to do with the packet. So if device B receives a packet from device C via IPSec, device B will look to the corresponding SA to tell it how to decrypt the packet, how to properly authenticate the source of the packet, which key to use, and how to reply to the message if necessary.

SAs are directional, so a device will have one SA for outbound traffic and a different SA for inbound traffic for each individual communication channel. If a device is connecting to three devices, it will have at least six SAs, one for each inbound and outbound connection per remote device. So how can a device keep all of these SAs organized and ensure that the right SA is invoked for the right connection? With the mighty secu rity parameter index (SPI), that's how. Each device has an SPI that keeps track of the different SAs and tells the device which one is appropriate to invoke for the different packets it receives. The SPI value is in the header of an IPSec packet, and the device reads this value to tell it which SA to consult.

IPSec can authenticate the sending devices of the packet by using MAC (covered in the earlier section, "The One-Way Hash"). The ESP protocol can provide authentication, integrity, and confidentiality if the devices are configured for this type of functionality.

So if a company just needs to make sure it knows the source of the sender and must be assured of the integrity of the packets, it would choose to use AH. If the company would like to use these services and also have confidentiality, it would use the ESP protocol because it provides encryption functionality. In most cases, the reason ESP is employed is because the company must set up a secure VPN connection.

It may seem odd to have two different protocols that provide overlapping functionality. AH provides authentication and integrity, and ESP can provide those two functions and confidentiality. Why even bother with AH then? In most cases, the reason has to do with whether the environment is using network address translation (NAT). IPSec will generate an integrity check value (ICV), which is really the same thing as a MAC value, over a portion of the packet. Remember that the sender and receiver generate their own values. In IPSec, it is called an ICV value. The receiver compares her ICV value with the one sent by the sender. If the values match, the receiver can be assured the packet has not been modified during transmission. If the values are different, the packet has been altered and the receiver discards the packet.

The AH protocol calculates this ICV over the data payload, transport, and network headers. If the packet then goes through a NAT device, the NAT device changes the IP address of the packet. That is its job. This means a portion of the data (network header) that was included to calculate the ICV value has now changed, and the receiver will generate an ICV value that is different from the one sent with the packet, which means the packet will be discarded automatically.

The ESP protocol follows similar steps, except it does not include the network header portion when calculating its ICV value. When the NAT device changes the IP address, it will not affect the receiver's ICV value because it does not include the network header when calculating the ICV.

Because IPSec is a framework, it does not dictate which hashing and encryption algorithms are to be used or how keys are to be exchanged between devices. Key management can be handled manually or automated by a key management protocol. The de facto standard for IPSec is to use Internet Key Exchange (IKE), which is a combination of the ISAKMP and OAKLEY protocols. The Internet Security Association and Key Management Protocol (ISAKMP) is a key exchange architecture that is independent of the type of keying mechanisms used. Basically, ISAKMP provides the framework of what can be negotiated to set up an IPSec connection (algorithms, protocols, modes, keys). The OAKLEY protocol is the one that carries out the negotiation process. You can think of ISAKMP as providing the playing field (the infrastructure) and OAKLEY as the guy running up and down the playing field (carrying out the steps of the negotiation). IPSec is very complex with all of its components and possible configurations. This complexity is what provides for a great degree of flexibility, because a company has many different configuration
choices to achieve just the right level of protection. If this is all new to you and still confusing, please review one or more of the following references to help fill in the gray areas.
The following answers are incorrect:
The other options are distractors.
The following reference(s) were/was used to create this question:
Shon Harris, CISSP All-in-One Exam Guide- fiveth edition, page 759
and
https://neodean.wordpress.com/tag/security-protocol/

NEW QUESTION: 294
Which of the following is being considered as the most reliable kind of personal identification?
A. Token
B. Finger print
C. Password
D. Ticket Granting
Answer: B (LEAVE A REPLY)
Every person's fingerprint is unique and is a feature that stays with the person throughout his/her life. This makes the fingerprint the most reliable kind of personal identification because it cannot be forgotten, misplaced, or stolen. Fingerprint authorization is potentially the most affordable and convenient method of verifying a person's identity.

NEW QUESTION: 295
Which of the following choices is NOT part of a security policy?
A. statement of management intend, supporting the goals and principles of information security
B. description of specific technologies used in the field of information security
C. definition of general and specific responsibilities for information security management
D. definition of overall steps of information security and the importance of security
Answer: B (LEAVE A REPLY)

NEW QUESTION: 296
The standard process to certify and accredit
A. DIACAP
B. DITSCAP
C. CIAP
D. NIACAP
Answer: (SHOW ANSWER)
The correct answer is DITSCAP, the Defense Information Technology Security Certification and Accreditation Process.
* Answer NIACAP refers to the US government's non-defense Certification and Accreditation (C&A) process the National Information Assurance Certification and Accreditation Process.
* CIAP refers to the Commercial Information Security Analysis Process that is currently under development for application to commercial systems.
* Answer DIACAP is a distracter.

NEW QUESTION: 297
How does Encapsulating Security Payload (ESP) in transport mode affect in the Internet Protocol (IP)?
A. Encrypts and optionally authenticates the IP header, but not the IP payload
B. Encrypts and optionally authenticates the complete IP packet
C. Encrypts and optionally authenticates the IP payload, but not the IP header
D. Authenticates the IP payload and selected portions of the IP header
Answer: C (LEAVE A REPLY)

NEW QUESTION: 298
What types of computer attacks are most commonly reported by IDSs?
A. System penetration
B. Denial of service
C. System scanning
D. All of the choices
Answer: D (LEAVE A REPLY)
Three types of computer attacks are most commonly reported by IDSs: system scanning, denial of service (DOS), and system penetration. These attacks can be launched locally, on the attacked machine, or remotely, using a network to access the target. An IDS operator must understand the differences between these types of attacks, as each requires a different set of responses.

NEW QUESTION: 299
What is the MOST efficient way to verify the integrity of database backups?

A. Run DBCC CHECKDB on a regular basis to check the logical and physical integrity of the database objects.
B. Test restores on a regular basis.
C. Restore every file in the system to check its health.
D. Use checksum as part of the backup operation to make sure that no corruption has occurred.
Answer: (SHOW ANSWER)

NEW QUESTION: 300
Discretionary Access Control (DAC) restricts access according to
A. data classification labeling.
B. page views within an application.
C. management accreditation.
D. authorizations granted to the user.
Answer: (SHOW ANSWER)

NEW QUESTION: 301
What does the simple integrity axiom mean in the Biba model?
A. No write down
B. No read down
C. No read up
D. No write up
Answer: B (LEAVE A REPLY)
The simple integrity axiom of the Biba access control model states that a subject at one level of integrity is not permitted to observe an object of a lower integrity (no read down).
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 Architectures and Models (page 205).

NEW QUESTION: 302
Which of the following is the MOST common method of memory protection?
A. Segmentation
B. Virtual Local Area Network (VLAN) tagging
C. Error correction

D. Compartmentalization
Answer: A (LEAVE A REPLY)

NEW QUESTION: 303
Cryptography does NOT help in:
A. Detecting fraudulent insertion.
B. Detecting fraudulent deletion.
C. Detecting fraudulent modification.
D. Detecting fraudulent disclosure.
Answer: D (LEAVE A REPLY)
Cryptography is a detective control in the fact that it allows the detection of fraudulent insertion, deletion or modification. It also is a preventive control is the fact that it prevents disclosure, but it usually does not offers any means of detecting disclosure. Source: DUPUIS, Clement, CISSP Open Study Guide on domain 5, cryptography, April 1999.

NEW QUESTION: 304
The key benefits of a signed and encrypted e-mail include
A. confidentiality, non-repudiation, and authentication.
B. non-repudiation, authorization, and authentication.
C. non-repudiation, confidentiality, and authorization.
D. confidentiality, authentication, and authorization.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 305
Which of the following is NOT a characteristic of a cryptographic hash function, H (m), where m denotes the message being hashed by the function H?
A. H (m) is a one-way function.
B. H (m) is difficult to compute for any given m.
C. The output is of fixed length.
D. H (m) is collision free.
Answer: B (LEAVE A REPLY)
For a cryptographic hash function, H (m) is relatively easy to compute for a given m.
*Answer "H (m) is collision free" is a characteristic of a good cryptographic hash function, in that collision free means that for a given message, M, that produces H (M) = Z, it is computationally infeasible to find another message, M1, such that H (M1) = Z.
*Answer "The output is of fixed length" is part of the definition of a hash function since it generates a fixed-length result that is independent of the length of the input message. This characteristic is useful for generating digital signatures since the signature can be applied to the fixed-length hash that is uniquely characteristic of the message instead of to the entire message, which is usually much longer than the hash.

*Answer "H (m) is a one-way function" relates to answer "H (m) is difficult to compute for any given m" in that a one-way function is difficult or impossible to invert. This means that for a hash function H (M) = Z, it is computationally infeasible to reverse the process and find M given the hash Z and the function H.

NEW QUESTION: 306
Which of the following is a method of multiplexing data where a communication channel is divided into an arbitrary number of variable bit-rate digital channels or data streams. This method allocates bandwidth dynamically to physical channels having information to transmit?
A. Time-division multiplexing
B. Asynchronous time-division multiplexing
C. Statistical multiplexing
D. Frequency division multiplexing
Answer: (SHOW ANSWER)
Statistical multiplexing is a type of communication link sharing, very similar to dynamic bandwidth allocation (DBA). In statistical multiplexing, a communication channel is divided into an arbitrary number of variable bit-rate digital channels or data streams. The link sharing is adapted to the instantaneous traffic demands of the data streams that are transferred over each channel. This is an alternative to creating a fixed sharing of a link, such as in general time division multiplexing (TDM) and frequency division multiplexing (FDM). When performed correctly, statistical multiplexing can provide a link utilization improvement, called the statistical multiplexing gain. Generally, the methods for multiplexing data include the following : Time-division multiplexing (TDM): information from each data channel is allocated bandwidth based on pre-assigned time slots, regardless of whether there is data to transmit. Time-division multiplexing is used primarily for digital signals, but may be applied in analog multiplexing in which two or more signals or bit streams are transferred appearing simultaneously as sub-channels in one communication channel, but are physically taking turns on the channel. The time domain is divided into several recurrent time slots of fixed length, one for each sub-channel. A sample byte or data block of sub-channel 1 is transmitted during time slot 1, sub-channel 2 during time slot 2, etc. One TDM frame consists of one time slot per sub-channel plus a synchronization channel and sometimes error correction channel before the synchronization. After the last sub-channel, error correction, and synchronization, the cycle starts all over again with a new frame, starting with the second sample, byte or data block from sub-channel 1, etc.
Asynchronous time-division multiplexing (ATDM): information from data channels is allocated bandwidth as needed, via dynamically assigned time slots. ATM provides functionality that is similar to both circuit switching and packet switching networks: ATM uses asynchronous time-division multiplexing, and encodes data into small, fixed-sized packets (ISO-OSI frames) called cells. This differs from approaches such as the Internet Protocol or Ethernet that use variable sized packets and frames. ATM uses a connection-oriented model in which a virtual circuit must be established between two endpoints before the actual data exchange begins. These virtual circuits may be "permanent", i.e. dedicated connections that are usually preconfigured by the

service provider, or "switched", i.e. set up on a per-call basis using signalling and disconnected when the call is terminated.
Frequency division multiplexing (FDM): information from each data channel is allocated bandwidth based on the signal frequency of the traffic. In telecommunications, frequency-division multiplexing (FDM) is a technique by which the total bandwidth available in a communication medium is divided into a series of non-overlapping frequency sub-bands, each of which is used to carry a separate signal. This allows a single transmission medium such as the radio spectrum, a cable or optical fiber to be shared by many signals.
Reference used for this question: http://en.wikipedia.org/wiki/Statistical_multiplexing and http://en.wikipedia.org/wiki/Frequency_division_multiplexing and Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 114).

NEW QUESTION: 307
What is called the standard format that was established to set up and manage Security Associations (SA) on the Internet in IPSec?
A. Internet Key Exchange
B. Secure Key Exchange Mechanism
C. Oakley
D. Internet Security Association and Key Management Protocol
Answer: (SHOW ANSWER)
Reference: pg 221 Krutz

NEW QUESTION: 308
In an online transaction processing system (OLTP), which of the following actions should be taken when erroneous or invalid transactions are detected?
A. The transactions should be dropped from processing.
B. The transactions should be processed after the program makes adjustments.
C. The transactions should be written to a report and reviewed.
D. The transactions should be corrected and reprocessed.
Answer: (SHOW ANSWER)
In an online transaction processing system (OLTP) all transactions are recorded as they occur. When erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.
As explained in the ISC2 OIG: OLTP is designed to record all of the business transactions of an organization as they occur. It is a data processing system facilitating and managing transaction-oriented applications. These are characterized as a system used by many concurrent users who are actively adding and modifying data to effectively change real-time data.
OLTP environments are frequently found in the finance, telecommunications, insurance, retail, transportation, and travel industries. For example, airline ticket agents enter data in the database in real-time by creating and modifying travel reservations, and these are increasingly joined by

users directly making their own reservations and purchasing tickets through airline company Web sites as well as discount travel Web site portals. Therefore, millions of people may be accessing the same flight database every day, and dozens of people may be looking at a specific flight at the same time.

The security concerns for OLTP systems are concurrency and atomicity.

Concurrency controls ensure that two users cannot simultaneously change the same data, or that one user cannot make changes before another user is finished with it. In an airline ticket system, it is critical for an agent processing a reservation to complete the transaction, especially if it is the last seat available on the plane.

Atomicity ensures that all of the steps involved in the transaction complete successfully. If one step should fail, then the other steps should not be able to complete. Again, in an airline ticketing system, if the agent does not enter a name into the name data field correctly, the transaction should not be able to complete.

OLTP systems should act as a monitoring system and detect when individual processes abort, automatically restart an aborted process, back out of a transaction if necessary, allow distribution of multiple copies of application servers across machines, and perform dynamic load balancing.

A security feature uses transaction logs to record information on a transaction before it is processed, and then mark it as processed after it is done. If the system fails during the transaction,

the transaction can be recovered by reviewing the transaction logs.

Checkpoint restart is the process of using the transaction logs to restart the machine by running through the log to the last checkpoint or good transaction. All transactions following the last checkpoint are applied before allowing users to access the data again.

Wikipedia has nice coverage on what is OLTP:

Online transaction processing, or OLTP, refers to a class of systems that facilitate and manage transaction-oriented applications, typically for data entry and retrieval transaction processing. The term is somewhat ambiguous; some understand a "transaction" in the context of computer or database transactions, while others (such as the Transaction Processing Performance Council) define it in terms of business or commercial transactions.

OLTP has also been used to refer to processing in which the system responds immediately to user

requests. An automatic teller machine (ATM) for a bank is an example of a commercial transaction

processing application.

The technology is used in a number of industries, including banking, airlines, mailorder, supermarkets, and manufacturing. Applications include electronic banking, order processing, employee time clock systems, e-commerce, and eTrading.

There are two security concerns for OLTP system: Concurrency and Atomicity

ATOMICITY

In database systems, atomicity (or atomicness) is one of the ACID transaction properties. In an atomic transaction, a series of database operations either all occur, or nothing occurs. A

guarantee of atomicity prevents updates to the database occurring only partially, which can cause greater problems than rejecting the whole series outright.
The etymology of the phrase originates in the Classical Greek concept of a fundamental and indivisible component; see atom.
An example of atomicity is ordering an airline ticket where two actions are required: payment, and a seat reservation. The potential passenger must either:
both pay for and reserve a seat; OR
neither pay for nor reserve a seat.
The booking system does not consider it acceptable for a customer to pay for a ticket without securing the seat, nor to reserve the seat without payment succeeding.
CONCURRENCY Database concurrency controls ensure that transactions occur in an ordered fashion. The main job of these controls is to protect transactions issued by different users/applications from the effects of each other. They must preserve the four characteristics of database transactions ACID test: Atomicity, Consistency, Isolation, and Durability. Read http://en.wikipedia.org/wiki/ACID for more details on the ACID test. Thus concurrency control is an essential element for correctness in any system where two database transactions or more, executed with time overlap, can access the same data, e.g., virtually in any general-purpose database system. A well established concurrency control theory exists for database systems: serializability theory, which allows to effectively design and analyze concurrency control methods and mechanisms. Concurrency is not an issue in itself, it is the lack of proper concurrency controls that makes it a serious issue.
The following answers are incorrect:
The transactions should be dropped from processing. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs. The transactions should be processed after the program makes adjustments. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs. The transactions should be corrected and reprocessed. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.
References: Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 12749-12768). Auerbach Publications. Kindle Edition. and http://en.wikipedia.org/wiki/Online_transaction_processing and http://databases.about.com/od/administration/g/concurrency.htm

NEW QUESTION: 309
What are database views used for?
A. To ensure referential integrity.
B. To allow easier access to data in a database.
C. To restrict user access to data in a database.
D. To provide audit trails.

Answer: C (LEAVE A REPLY)
Through the use of a view we can provide security for the organization restricting users access to certain data or to the real tables containing the information in our database. For example, we can create a view that brings data from 3 tables, only showing 2 of the 4 columns in each. Instead of giving access to the tables that contain the information, we give access to the view, so the user can access this fixed information but does not have privileges over the tables containing it. This provides security.

NEW QUESTION: 310
What does the Maximum Tolerable Downtime (MTD) determine?
A. The fixed length of time in a DR process before redundant systems are engaged
B. The estimated period of time a business can remain interrupted beyond which it risks never recovering
C. The fixed length of time a company can endure a disaster without any Disaster Recovery (DR) planning
D. The estimated period of time a business critical database can remain down before customers are affected.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 311
Which one of these risk factors would be the LEAST important consideration in choosing a building site for a new computer facility?
A. Proximity to an airline flight path
B. Vulnerability to crime
C. Adjacent buildings and businesses
D. Vulnerability to natural disasters
Answer: A (LEAVE A REPLY)

NEW QUESTION: 312
A server farm consisting of multiple similar servers seen as a single IP address from users interacting with the group of servers is an example of which of the following?
A. Server clustering
B. Redundant servers
C. Multiple servers
D. Server fault tolerance
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
A server cluster is a group of servers that are viewed logically as one server to users and can be managed as a single logical system through a single IP address.
Incorrect Answers:

B: Redundant servers are not grouped together and can be managed through a single IP address.
C: In general, a group of multiple servers can be grouped together and managed through a single IP address.
D: Server fault tolerance is not related to managing a group of servers through a single IP address.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 1272

NEW QUESTION: 313
Primary storage is the:
A. Memory used in conjunction with real memory to present a CPU with a larger, apparent address space.
B. Memory directly addressable by the CPU, which is for the storage of instructions and data that are associated with the program being executed.
C. Memory, such as magnetic disks, that provide non-volatile storage.
D. Memory where information must be obtained by sequentially searching from the beginning of the memory space.
Answer: B (LEAVE A REPLY)
* Answer "Memory, such as magnetic disks, that provide non-volatile storage" refers to secondary storage.
* Answer "Memory used in conjunction with real memory to present a CPU with a larger, apparent address space" refers to virtual memory, and answer "Memory where information must be obtained by sequentially searching from the beginning of the memory space" refers to sequential memory.

NEW QUESTION: 314
A refinement to the basic Waterfall Model that states that software should be developed in increments of functional capability is called:
A. Functional development
B. Incremental development
C. Functional refinement
D. Incremental refinement
Answer: B (LEAVE A REPLY)
The advantages of incremental development include the ease of testing increments of functional capability and the opportunity to incorporate user experience into a successively refined product.
The other answers are distracters.

NEW QUESTION: 315

What maintenance activity is responsible for defining, implementing, and testing updates to application systems?
A. Export exception control
B. Program change control
C. User acceptance testing
D. Regression testing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 316
Examples of types of physical access controls include all EXCEPT which of the following?
A. badges
B. locks
C. guards
D. passwords
Answer: D (LEAVE A REPLY)
Passwords are considered a Preventive/Technical (logical) control.
The following answers are incorrect:
badges Badges are a physical control used to identify an individual. A badge can include a smart device which can be used for authentication and thus a Technical control, but the actual badge itself is primarily a physical control.
locks Locks are a Preventative Physical control and has no Technical association.
guards Guards are a Preventative Physical control and has no Technical association.
The following reference(s) were/was used to create this question:
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 35).

NEW QUESTION: 317
How many bits compose an IPv6 address?
A. 32 bits
B. 64 bits
C. 96 bits
D. 128 bits

Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
IPv6 uses 128 bits for its addresses.
Incorrect Answers:
A: IPv4 uses 32 bits for its addresses, while IPv6 uses 128 bits.
B: IPv6 uses 128 bits, not 64 bits, for its addresses.
C: IPv6 uses 128 bits, not 96 bits, for its addresses.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 541

NEW QUESTION: 318
A prolonged power supply that is below normal voltage is a:
A. brownout
B. blackout
C. surge
D. fault
Answer: A (LEAVE A REPLY)
A prolonged power supply that is below normal voltage is a brownout.
From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw-Hill/Osborne, 2005, page 368.

NEW QUESTION: 319
When considering an IT System Development Life-cycle, security should be:
A. Mostly considered during the initiation phase.
B. Mostly considered during the development phase.
C. Treated as an integral part of the overall system design.
D. Added once the design is completed.
Answer: C (LEAVE A REPLY)
Security must be considered in information system design. Experience has shown it is very difficult to implement security measures properly and successfully after a system has been developed, so it should be integrated fully into the system life-cycle process. This includes establishing security policies, understanding the resulting security requirements, participating in the evaluation of security products, and finally in the engineering, design, implementation, and disposal of the system. 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 (page 7).

NEW QUESTION: 320

A company whose Information Technology (IT) services are being delivered from a Tier 4 data center, is preparing a companywide Business Continuity Planning (BCP). Which of the following failures should the IT manager be concerned with?

A. Application

B. Network

C. Storage

D. Power

Answer: A (LEAVE A REPLY)

NEW QUESTION: 321

The ISC2 Code of Ethics does not include which of the following behaviors for a CISSP:

A. Honesty

B. Ethical behavior

C. Legality

D. Control

Answer: D (LEAVE A REPLY)

Control is not a behavior characteristic described in the Code of Ethics.

See a high level extract of the code below. I strongly suggest you visit the link below to get the full details of the code. You will be require to accept and agree to the code of ethics in order to become a CISSP.

https://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/Code_of_ethics/ISC2-Code-of-Ethics.pdf

Summary of the Code:

All information systems security professionals who are certified by (Isc)2 recognize that such certification is a privilege that must be both earned and maintained. In support of this principle, all (Isc)2 members are required to commit to fully support this Code of Ethics (the "Code"). (Isc)2 members who intentionally or knowingly violate any provision of the Code will be subject to action by a peer review panel, which may result in the revocation of certification. (Isc)2 members are obligated to follow the ethics complaint procedure upon observing any action by an (ISC)2 member that breach the Code. Failure to do so may be considered a breach of the Code pursuant to Canon IV.

There are only four mandatory canons in the Code. By necessity, such high-level guidance is not intended to be a substitute for the ethical judgment of the professional.

Code of Ethics Preamble:

The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.

Therefore, strict adherence to this Code is a condition of certification.

Code of Ethics Canons:

Protect society, the common good, necessary public trust and confidence, and the infrastructure.

Act honorably, honestly, justly, responsibly, and legally.

Provide diligent and competent service to principals.

Advance and protect the profession.
The following answers are incorrect:
morality Is incorrect because Morality is a behavior characteristic described in the Code of Ethics. Act honorably, honestly, justly, responsibly, and legally.
ethicality Is incorrect because Ethicality is a behavior characteristic described in the Code of Ethics. Act honorably, honestly, justly, responsibly, and legally.
legal. Is incorrect because Legality is a behavior characteristic described in the Code of Ethics. Act
honorably, honestly, justly, responsibly, and legally.
Reference(s) used for this question:
ISC2 Code of Ethics at https://www.isc2.org/ethics/Default.aspx
and
https://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/Code_of_ethics/ISC2-Code-of-Ethics.pdf

NEW QUESTION: 322
Examine the following characteristics and identify which answer best indicates the likely cause of this behavior:
- Core operating system files are hidden
- Backdoor access for attackers to return
- Permissions changing on key files
- A suspicious device driver
- Encryption applied to certain files without explanation
- Logfiles being wiped
A. Kernel-mode Rootkit
B. User-mode Rootkit
C. Malware
D. Kernel-mode Badware
Answer: A (LEAVE A REPLY)
Rootkits are software that is designed to get, keep and provide access to attackers by hooking into key components of the operating system like the kernel or system drivers.
Rootkits commonly try to hide their presence by affecting operating system functionality and can subvert detection software like Antivirus Scanners.
Removing a rootkit may be impossible because the software can irrevocably change components of the operating system. The OS may need to be completely reinstalled to remove the infestation. At any rate, a computer infected with ANY malware should never be trusted again and infestation should be mitigated by a completely new install of the OS from trusted media.
The following answers are incorrect:
- User-Mode Rootkit: This isn't correct because User-mode rootkits don't include device drivers.
- Malware: This isn't a bad answer but it isn't as specific as the correct answer. Malware is a very broad term that describes any software that is written to do something nefarious.

- Kernel-mode Badware: This isn't really a computer term. But it should be.
The following reference(s) was used to create this question:
2 013. Official Security+ Curriculum.

NEW QUESTION: 323
During which phase of an IT system life cycle are security requirements developed?
A. Operation
B. Initiation
C. Functional design analysis and Planning
D. Implementation
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Within the Systems Development Life Cycle (DSLC) model the design phase, also known as the security requirement phase, transforms requirements, including the security requirements, into a complete System Design Document.
Incorrect Answers:
A: The operation phase describes tasks to operate in a production environment, and is not concerned with development of security requirements.
B: The initiation phase starts when a sponsor identifies a need or an opportunity. During this phase a Concept Proposal, but no security requirements, is created.
D: In the implementation phase the system is implemented into a product production environment. The security requirements have already been developed long before this phase.
References:
Conrad, Eric, Seth Misenar and Joshua Feldman, CISSP Study Guide, 2nd Edition, Syngress, Waltham,
2012, p. 1095

NEW QUESTION: 324
Which of the following steps should be performed FIRST when purchasing Commercial Off-The-Shelf (COTS) software?
A. undergo a security assessment as part of authorization process
B. establish policies and procedures on system and services acquisition
C. establish a risk management strategy
D. harden the hosting server, and perform hosting and application vulnerability scans
Answer: B (LEAVE A REPLY)

NEW QUESTION: 325
Which one of the following operates at the session, transport, or network layer of the Open System Interconnection (OSI) model?
A. Data at rest encryption
B. Configuration Management

C. Cyclic redundancy check (CRC)
D. Integrity checking software
Answer: C (LEAVE A REPLY)

NEW QUESTION: 326
In biometrics, "one-to-many" search against database of stored biometric images is done in:
A. Authentication
B. Identification
C. Identities
D. Identity-based access control
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
A biometric system executes a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown user in identification mode. If the comparison of the biometric sample to a template in the database falls within a threshold previously set, identifying the individual will succeed.
Incorrect Answers:
A: In authentication mode, the biometric system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to confirm the individual is the person they claim to be.
C: Identities refer to who users are, not a mode used in biometrics.
D: An identity-based access control is a type of Discretionary Access Control (DAC) that is based on an individual's identity.
References:
https://en.wikipedia.org/wiki/Biometrics
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 220

NEW QUESTION: 327
Which of the following is true about Kerberos?
A. It utilized 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 relies upon symmetric key cryptography, specifically Data Encryption Standard (DES), and provides end-to-end security for authentication traffic between the client and the Key Distribution Center (KDC)." Pg. 15 Tittel: CISSP Study Guide

NEW QUESTION: 328
The term failover refers to:

A. A fail-soft system.
B. Terminating processing in a controlled fashion.
C. Resiliency.
D. Switching to a duplicate, hot backup component.
Answer: D (LEAVE A REPLY)
The correct answer is "Switching to a duplicate, hot backup component". Failover means switching to a hot backup system that maintains duplicate states with the primary system. Answer "Terminating processing in a controlled fashion" refers to fail safe, and answers Resiliency and A fail-soft system refer to fail soft.

NEW QUESTION: 329
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: (SHOW ANSWER)
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: 330
Which of the following ensures that a TCB is designed, developed, and maintained with formally controlled standards that enforces protection at each stage in the system's life cycle?
A. life cycle assurance
B. operational assurance
C. covert timing assurance
D. covert storage assurance
Answer: A (LEAVE A REPLY)
Life-cycle Assurance - Requirements specified in the Orange Book are:
security testing,
design specification and testing,
configuration management, and
trusted distribution.

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.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, page 219.
Also check out: HARRIS, Shon, All-In-One CISSP Certification Exam Guide 3rd Edition, McGraw-Hill/Osborne, 2005 (pages 904, 961).

NEW QUESTION: 331
Which term below BEST describes the concept of least privilege?
A. Active monitoring of facility entry access points.
B. Each user is granted the lowest clearance required for their tasks.
C. A formal separation of command, program, and interface functions.
D. A combination of classification and categories that represents the sensitivity of information.
Answer: B (LEAVE A REPLY)
The least privilege principle requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use. Applying this principle may limit the damage resulting from accidents, errors, or unauthorized use of system resources. *Answer "A formal separation of command, program, and interface functions." describes separation of privilege, which is the separation of functions, namely between the commands, programs, and interfaces implementing those functions, such that malicious or erroneous code in one function is prevented from affecting the code or data of another function. *Answer "A combination of classification and categories that represents the sensitivity of information." is a security level. A security level is the combination of hierarchical classification and a set of non-hierarchical categories that represents the sensitivity of information. *Answer "Active monitoring of facility entry access points." is a distracter. Source: DoD 5200.28STD Department of Defense Trusted Computer System Evaluation Criteria.

NEW QUESTION: 332
Which one of the following is a technical solution for the quality of service, speed, and security problems facing the Internet?

A. Random Early Detection (RED) queuing
B. Multi-protocol label-switching (MPLS)
C. Public Key Cryptography Standard (PKCS)
D. Resource Reservation Protocol (RSVP)
Answer: B (LEAVE A REPLY)
The original answer to this question was RED however I think this is incorrect because of this reason. Both Red and MPLS deal with qos/cos issues, there by increasing speed. Mpls more so the RED. However I have not been able to find any documents that state RED is a security implementation while MPLS is heavy used in the ISP VPN market. See this link for MPLS security http://www.nwfusion.com/research/2001/0521feat2.html Below are the link that are formation of the ration for this answer of B (MPLS)
Congestion avoidance algorithm in which a small percentage of packets are dropped when congestion is detected and before the queue in question overflows completely http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/r12.htm Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/m12.htm Resource Reservation Protocol. Protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams they want to receive. RSVP depends on IPv6. Also known as Resource Reservation Setup Protocol.
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/r12.htm Random Early Detection (RED) is the recommended approach for queue congestion management in routers (Braden et al., 1998). Although in its basic form RED can be implemented in a relatively short C program, as the speed of ports and the number of queues per port increase, the implementation moves more and more into hardware. Different vendors choose different ways to implement and support RED in their silicon implementations. The degree of programmability, the number of queues, the granularity among queues, and the calculation methods of the RED parameters all vary from implementation to implementation. Some of these differences are irrelevant to the behavior of the algorithm-and hence to the resulting network behavior. Some of the differences, however, may result in a very different behavior of the RED algorithm-and hence of the network efficiency.
http://www.cisco.com/en/US/products/hw/routers/ps167/products_white_paper09186a0080091fe4.shtml
Based on label swapping, a single forwarding mechanism provides opportunities for new control paradigms and applications. MPLS Label Forwarding is performed with a label lookup for an incoming label, which is then swapped with the outgoing label and finally sent to the next hop. Labels are imposed on the packets only once at the edge of the MPLS network and removed at the other end. These labels are assigned to packets based on groupings or forwarding equivalence classes (FECs). Packets belonging to the same FEC get similar treatment. The label is added between the Layer 2 and the Layer 3 header (in a packet environment) or in the virtual path identifier/virtual channel identifier (VPI/VCI) field (in ATM networks). The core network

merely reads labels, applies appropriate services, and forwards packets based on the labels. This MPLS lookup and forwarding scheme offers the ability to explicitly control routing based on destination and source addresses, allowing easier introduction of new IP services.
http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/xlsw_ds.htm

NEW QUESTION: 333
What is the correct sequence which enables an authorized agency to use the Law Enforcement Access Field (LEAF) to decrypt a message sent by using the Clipper Chip? The following designations are used for the respective keys involved Kf, the family key; Ks, the session key; U, a unique identifier for each Clipper Chip and Ku, the unit key that is unique to each Clipper Chip.
A. Decrypt the LEAF with the family key, Kf; recover U; obtain a court order to obtain Ks, the session key. Use the session key to decrypt the message.
B. Decrypt the LEAF with the family key, Kf; recover U; obtain a court order to obtain the two halves of Ku; recover Ku; and then recover Ks, the session key. Use the session key to decrypt the message.
C. Obtain a court order to acquire the family key, Kf; recover U and Ku; then recover Ks, the session key. Use the session key to decrypt the message.
D. Obtain a court order to acquire the two halves of Ku, the unit key. Recover Ku. Decrypt the LEAF with Ku and then recover Ks, the session key. Use the session key to decrypt the message.
Answer: B (LEAVE A REPLY)
The explanation is based on the LEAF as shown in the Figure.

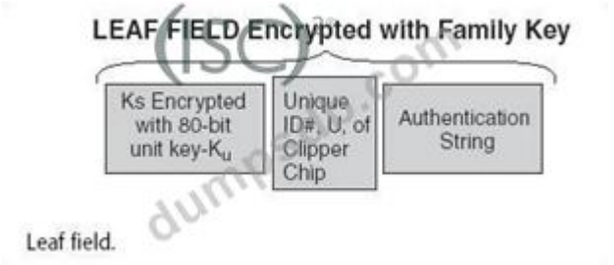


image018
The message is encrypted with the symmetric session key, Ks. In order to decrypt the message, then, Ks must be recovered. The LEAF contains the session key, but the LEAF is encrypted with the family key, Kf ,
that is common to all Clipper Chips. The authorized agency has access to Kf and decrypts the LEAf. However, the session key is still encrypted by the 80-bit unit key, Ku, that is unique to each Clipper Chip and is identified by the unique identifier, U. Ku is divided into two halves, and each half is deposited with an escrow agency. The law enforcement agency obtains the two halves of Ku by presenting the escrow agencies with a court order for the key identified by U.

The two halves of the key obtained by the court order are XORed
together to obtain Ku. Then, Ku is used to recover the session key, Ks, and Ks is used to decrypt the message.
The decryption sequence to obtain Ks can be summarized as:

$K_f \rightarrow U \rightarrow [1/2K_u \text{ XOR } 1/2\ K_u] \rightarrow K_u \rightarrow K_s$

image020
This is the sequence described in answer "Decrypt the LEAF with the family key, Kf; recover U; obtain a court order to obtain the two halves of Ku; recover Ku; and then recover
Ks,
the session key. Use the session key to decrypt the message". The sequences described in the other answers are incorrect.

NEW QUESTION: 334
When developing a business case for updating a security program, the security program owner MUST do which of the following?
A. Obtain resources for the security program
B. Interview executive management
C. Identify relevant metrics
D. Prepare performance test reports
Answer: (SHOW ANSWER)

NEW QUESTION: 335
Which of the following mail standards relies on a "Web of Trust"?
A. Secure Multipurpose Internet Mail extensions (S/MIME)
B. Pretty Good Privacy (PGP)
C. MIME Object Security Services (MOSS)
D. Privacy Enhanced Mail (PEM)
Answer: B (LEAVE A REPLY)
"PGP does not use a hierarchy of Cas, or any type of formal trust certificates, but relies on a "web of trust" in its key management approach. Each user generates and distributes his or her public key, and users sign each other's public keys, which creates a community of users who trust each other. This is different than the CA approach where no one trusts each other, they only trust the CA.

NEW QUESTION: 336
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: (SHOW ANSWER)

Explanation/Reference:

Explanation:

A chain of custody is a history that shows how evidence was collected, analyzed, transported, and preserved in order to be presented in court. Because electronic evidence can be easily modified, a clearly defined chain of custody demonstrates that the evidence is trustworthy.

Incorrect Answers:

A: The immateriality of the evidence is not the most important. It is more important to show how the evidence was collected, analyzed, transported, and preserved. This is called the chain of custody.

B: The reliability of the evidence is not the most important. It is more important to show how the evidence was collected, analyzed, transported, and preserved. This is called the chain of custody.

C: The process of producing the evidence is not the most important. It is more important to show how the evidence was collected, analyzed, transported, and preserved. This is called the chain of custody.

References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 1050

NEW QUESTION: 337

Which choice describes the Forest Green Book?

A. It is a Rainbow series book that defines the secure handling of storage media.

B. It is a Rainbow series book that defines guidelines for implementing access control lists.

C. It does not exist; there is no Forest Green Book.

D. It is a tool that assists vendors in data gathering for certifiers.

Answer: A (LEAVE A REPLY)

The Forest Green book is a Rainbow series book that defines the secure handling of sensitive or classified automated information system memory and secondary storage media, such as degaussers, magnetic tapes, hard disks, floppy disks, and cards. The Forest Green book details procedures for clearing, purging, declassifying, or destroying automated information system (AIS) storage media to prevent data remanence. Data remanence is the residual physical representation of data that has been erased in some way. After storage media is erased there may be some physical characteristics that allow data to be reconstructed.

* Answer "It is a tool that assists vendors in data gathering for certifiers." is the Blue Book, NCSC-TG-019 Trusted Product Evaluation Questionnaire Version-2. The Blue book is a tool to assist system developers and vendors in gathering data to assist evaluators and certifiers assessing trusted computer systems.

* Answer "It is a Rainbow series book that defines guidelines for implementing access control lists." is the Grey/Silver Book, NCSC-TG-020A, the Trusted
UNIX Working Group (TRUSIX) Rationale for Selecting Access Control.
The Grey/Silver book defines guidelines for implementing
access control lists (ACLs) in the UNIX system. Source: NCSC-TG-
0 25 A Guide to Understanding Data Remanence in Automated Information
Systems, NCSC-TG-020A Trusted UNIX Working Group
(TRUSIX) Rationale for Selecting Access Control, and NCSC-TG-019
Trusted Product Evaluation Questionnaire Version-2.

NEW QUESTION: 338
The application of a security patch to a product previously validate at Common Criteria (CC) Evaluation Assurance Level (EAL) 4 would
A. require an update of the Protection Profile (PP).
B. require recertification.
C. retain its current EAL rating.
D. reduce the product to EAL 3.
Answer: B (LEAVE A REPLY)
Section: Software Development Security

NEW QUESTION: 339
To understand the 'whys' in crime, many times it is necessary to understand MOM. Which of the following is not a component of MOM?
A. Opportunities
B. Methods
C. Motivation
D. Means
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
To understand the whys in crime, many times it is necessary to understand the Motivations, Opportunities, and Means (MOM). Motivations are the who and why of a crime. Opportunities are the where and when of a crime, and Means pertains to the capabilities a criminal would need to be successful. Methods is not a component of MOM.

NEW QUESTION: 340
Which access control model enables the OWNER of the resource to specify what subjects can access specific resources based on their identity?
A. Discretionary Access Control
B. Mandatory Access Control
C. Sensitive Access Control

D. Role-based Access Control
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Discretionary Access Control (DAC) allows data owners to dictate what subjects have access to the files and resources they own.
Incorrect Answers:
B: Mandatory Access control is considered nondiscretionary and is based on a security label system C: Sensitive access control is not a valid access control.
D: Role-based access control (RBAC) provides access to resources according to the role the user holds within the company or the tasks that the user has been assigned.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, pp. 220-228

NEW QUESTION: 341
Notifying the appropriate parties to take action in order to determine the extent of the severity of an incident and to remediate the incident's effects is part of:
A. Incident Evaluation
B. Incident Recognition
C. Incident Protection
D. Incident Response
Answer: C (LEAVE A REPLY)
These are core functions of the incident response process.
"Incident Evaluation" is incorrect. Evaluation of the extent and cause of the incident is a component of the incident response process.
"Incident Recognition" is incorrect. Recognition that an incident has occurred is the precursor to the initiation of the incident response process.
"Incident Protection" is incorrect. This is an almost-right-sounding nonsense answer to distract the unwary.
References:
CBK, pp. 698 - 703

NEW QUESTION: 342
An employee of a retail company has been granted an extended leave of absence by Human Resources (HR). This information has been formally communicated to the access provisioning team. Which of the following is the BEST action to take?
A. Revoke access temporarily.
B. Block user access and delete user account after six months.
C. Block access to the offices immediately.
D. Monitor account usage temporarily.
Answer: (SHOW ANSWER)

Section: Software Development Security

NEW QUESTION: 343
What works as an E-mail message transfer agent?
A. SMTP
B. SNMP
C. S-RPC
D. S/MIME
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
In e-mail clients SMTP works as a message transfer agent and moves the message from the user's computer to the mail server when the user sends the e-mail message.
Incorrect Answers:
B: SNMP is used for monitoring the network, not for sending email messages.
C: S-RPC is used for remote procedure not calls, and not for sending email messages.
D: S/MIME is a standard for email encryption. It is not used to send email messages.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 599

NEW QUESTION: 344
In a Public Key Infrastructure, how are public keys published?
A. Through digital certificates
B. They are sent by owners
C. They are not published
D. They are sent via e-mail
Answer: A (LEAVE A REPLY)

NEW QUESTION: 345
Which of the following is an essential step before performing Structured Query Language (SQL) penetration tests on a production system?
A. Confirm warm site is ready to accept connections.
B. Verify countermeasures have been deactivated.
C. Validate target systems have been backed up.
D. Ensure firewall logging has been activated.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 346
Frame relay and X.25 networks are part of which of the following?
A. Circuit-switched services
B. Cell-switched services

C. Packet-switched services
D. Dedicated digital services
Answer: C (LEAVE A REPLY)
Frame relay and X.25 are both examples of packet-switching technologies.
In packet-switched networks there are no dedicated connections between endpoints, and data is divided into packets and reassembled on the receiving end.
Frame Relay is an example of a packet-switched technology. Packet-switched networks enable end stations to dynamically share the network medium and the available bandwidth.
The following two techniques are used in packet-switching technology:
Variable-length packets
Statistical multiplexing
Variable-length packets are used for more efficient and flexible data transfers. These packets are switched between the various segments in the network until the destination is reached.
Statistical multiplexing techniques control network access in a packet-switched network.
The advantage of this technique is that it accommodates more flexibility and more efficient use of bandwidth. Most of today's popular LANs, such as Ethernet and Token Ring, are packet-switched networks.
Frame Relay often is described as a streamlined version of X.25, offering fewer of the robust capabilities, such as windowing and retransmission of last data that are offered in
X.25. This is because Frame Relay typically operates over WAN facilities that offer more reliable connection services and a higher degree of reliability than the facilities available during the late 1970s and early 1980s that served as the common platforms for X.25
WANs. As mentioned earlier, Frame Relay is strictly a Layer 2 protocol suite, whereas X.25 provides services at Layer 3 (the network layer) as well. This enables Frame Relay to offer higher performance and greater transmission efficiency than X.25, and makes Frame Relay suitable for current WAN applications, such as LAN interconnection.
The following answers are incorrect:
Circuit-switched services. An example of a circuit-switched service are Integrated Services Digital Network (ISDN) and Point-to-Point Protocol (PPP). Frame Relay and X.25 do not use circuit switching technology.
Cell-switched services. This is a distractor.
Dedicated digital services. A packet switched network is commonly via a digital method, but is not dedicated. Examples of a Dedicated digital service might be a Permanent Virtual
Circuit (PVC), which does not use packet switching.
The following reference(s) were/was used to create this question:
The CISCO Wiki on Frame Relay

NEW QUESTION: 347
Which choice below is the earliest and the most commonly found
Interior Gateway Protocol?
A. OSPF
B. RIP
C. IGRP
D. EAP
Answer: B (LEAVE A REPLY)
The Routing Information Protocol (RIP) bases its routing path on
the distance (number of hops) to the destination. RIP maintains optimum routing paths by sending out routing update messages if the network topology changes. For example, if a router finds that a particular link is faulty, it will update its routing table, then send a copy of the modified table to each of its neighbors.
* the Open Shortest Path First (OSPF) is a link-state hierarchical routing algorithm intended as a successor to RIP. It features least-cost routing, multipath routing, and load balancing.
* the Internet Gateway Routing Protocol (IGRP) is a Cisco protocol that uses a composite metric as its routing metric, including bandwidth, delay, reliability, loading, and maximum transmission unit.
* the Extensible Authentication Protocol (EAP), is a general protocol for PPP authentication that supports multiple remote authentication mechanisms. Source: Introduction to Cisco
Router Configuration edited by Laura Chappell (Cisco
Press, 1999).

NEW QUESTION: 348
What Service Organization Controls (SOC) report can be freely distributed and used by customers to gain confidence in a service organization's systems?
A. SOC 1 Type 1
B. SOC 1 Type 2
C. SOC 2
D. SOC 3
Answer: (SHOW ANSWER)
Section: Mixed questions
Explanation/Reference:
https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement.html

NEW QUESTION: 349

Which of the following BEST describes how access to a system is granted to federated user accounts?

A. Based on defined criteria by the Relying Party (RP)

B. Based on defined criteria by the Identity Provider (IdP)

C. With the identity assurance level

D. With the federation assurance level

Answer: B (LEAVE A REPLY)

NEW QUESTION: 350

Why would an information security policy require that communications test equipment be controlled?

A. The equipment is susceptible to damage

B. The equipment can be used to reconfigure the network multiplexers

C. The equipment must always be available for replacement if necessary

D. The equipment can be used to browse information passing on a network

Answer: D (LEAVE A REPLY)

NEW QUESTION: 351

Which backup type run at regular intervals would take the least time to complete?

A. Full Backup

B. Differential Backup

C. Incremental Backup

D. Disk Mirroring

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation:

An incremental backup copies only the files that have been modified since the previous backup. An incremental backup copies less data compared to full and differential backups.

Incorrect Answers:

A: A full backup copies all the data from the system to the backup medium. It copies more data compared to an incremental backup.

B: A differential backup is a type of data backup that preserves data, saving only the difference in the data since the last full backup. But a differential backup copies more data compared to an incremental backup.

D: Disk mirroring works dynamically in real-time. Disk mirroring does not take place at regular intervals.

References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 1410

NEW QUESTION: 352

What could be a major disadvantage to a mutual aid or reciprocal

type of backup service agreement?
A. The use of prefabricated buildings makes recovery easier.
B. It is free or at a low cost to the organization.
C. Annual testing by the Info Tech department is required to maintain
the site.
D. In a major emergency, the site might not have the capacity to handle the operations required.
Answer: (SHOW ANSWER)
The site might not have the capacity to
handle the operations required during a major disruptive event.
While mutual aid might be a good system for sharing resources during
a small or isolated outage, a major natural or other type of disaster can create serious resource contention between the two organizations.

NEW QUESTION: 353
What is RAD?
A. A development methodology
B. A project management technique
C. A measure of system complexity
D. Risk-assessment diagramming
Answer: (SHOW ANSWER)
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: 354
Which factor is critical in all systems to protect data integrity?
A. Data classification
B. Information ownership
C. Change control
D. System design
Answer: (SHOW ANSWER)
A Integrity is dependent on confidentiality, which relies on data classification. Also Biba integrity model relies on data classification.
"There are numerous countermeasures to ensure confidentiality against possible threats. These include the use of encryption, network traffic padding, strict access control, rigorous authentication
procedures, data classification, and extensive personnel training.
Confidentiality and integrity are dependent upon each other. Without object integrity, confidentiality
cannon be maintained. Other concepts, conditions, and aspects of confidentiality include sensitivity, discretion, criticality, concealment, secrecy, privacy, seclusion, and isolation." Pg 145 Tittel: CISSP Study Guide.
"Biba Integrity Model
Integrity is usually characterized by the three following goals:
1.)The data is protected from modification by unauthorized users.
2.)The data is protected from unauthorized modification by authorized users.
3.)The data is internally and externally consistent; the data held in a database must balance internally and correspond to the external, real world situation."
Pg. 277 Krutz: The CISSP Prep Guide: Gold Edition.

NEW QUESTION: 355
The MAIN reason an organization conducts a security authorization process is to
A. force the organization to enlist management support.
B. force the organization to make conscious risk decisions.
C. assure the effectiveness of security controls.
D. assure the correct security organization exists.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 356
The ANSI ASC X12 (American National Standards Institute Accredited
Standards Committee X12) Standard version 4010 applies to which one
of the following HIPAA categories?
A. Security
B. Privacy
C. Transactions

D. Code sets

Answer: C (LEAVE A REPLY)

The transactions addressed by HIPAA are:
Health claims or similar encounter information
Health care payment and remittance advice
Coordination of Benefits
Health claim status
Enrollment and disenrollment in a health plan
Eligibility for a health plan
Health plan premium payments
Referral certification and authorization
The HIPAA EDI transaction standards to address these HIPAA transactions include the following:
Health care claims or coordination of benefits
Retail drug NCPCP (National Council for Prescription Drug Programs) v. 32
Dental claim ASC X12N 837: dental
Professional claim ASC X12N 837: professional
Institutional claim ASC X12N 837: institutional
Payment and remittance advice ASC X12N 835
Health claim status ASC X12N 276/277
Plan enrollment ASC X12 834
Plan eligibility ASC X12 270/271
Plan premium payments ASC X12 820
Referral certification ASC X12 N 278
The American National Standards Institute was founded in 1917 and is the only source of American Standards. The ANSI Accredited Standards Committee X12 was chartered in 1979 and is responsible for cross-industry standards for electronic documents. The HIPAAprivacy standards, answer a, were finalized in April, 2001, and implementation must be accomplished by April 14, 2003. The privacy rule covers individually identifiable health care information transmitted, stored in electronic or paper form, or communicated orally. Protected health information (PHI) may not be disclosed unless disclosure is approved by the individual, permitted by the legislation, required for treatment, part of health care operations, required by law, or necessary for payment. PHI is defined as individually identifiable health information that is transmitted by electronic media, maintained in any medium described in the definition of electronic media under HIPAA, or is transmitted or maintained in any other form or medium. Answer b, code sets, refers to the codes that are used to fill in the data elements of the HIPAAtransaction standards. Examples of these codes are:

ICD-9-CM (vols. 1 and 2) International Classification of Diseases, 9th Ed., Clinical Modification Diseases, injuries, impairments, other health related problems, their manifestations, and causes of injury, disease, impairment, or other health-related problems
CPT (Current Procedural Terminology, 4th Ed. [CPT-4]), CDT (Code on Dental Procedures and Nomenclature, 2nd Ed. [CDT-2]) or ICD-9-CM (vol. 3) Procedures or other actions taken to prevent, diagnose, treat, or manage diseases, injuries, and impairments
NDC (National Drug Codes) drugs
HCPCS (Health Care Financing Administration Common Procedure Coding System)
Other health-related services, other substances, equipment, supplies, or other items used in health care services
The proposed HIPAA Security Rule, answer d, mandates the protection of the confidentiality, integrity, and availability of protected health information (PHI) through:
Administrative procedures
Physical safeguards
Technical services and mechanisms
The rule also addresses electronic signatures, but the final rule will depend on industry progress on reaching a standard. In addition, the proposed security rule requires the appointment of a security officer.

NEW QUESTION: 357
Within the realm of IT security, which of the following combinations best defines risk?
A. Threat coupled with a breach.
B. Threat coupled with a vulnerability.
C. Vulnerability coupled with an attack.
D. Threat coupled with a breach of security.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Risk is defined as "the probability of a threat agent exploiting a vulnerability and the associated impact".
The industry has different standardized methodologies when it comes to carrying out risk assessments.
Each of the individual methodologies has the same basic core components (identify vulnerabilities, associate threats, calculate risk values), but each has a specific focus. As a security professional it is your responsibility to know which is the best approach for your organization and its needs.

NIST developed a risk methodology, which is specific to IT threats and how they relate to information security risks. It lays out the following steps:

System characterization

- Threat identification
- Vulnerability identification
- Control analysis
- Likelihood determination
- Impact analysis
- Risk determination
- Control recommendations
- Results documentation

Incorrect Answers:

A: Threat coupled with a breach is not the definition of risk.

C: Vulnerability coupled with an attack is not the definition of risk.

D: Threat coupled with a breach of security is not the definition of risk.

References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, pp. 77-79

NEW QUESTION: 358

Which of the following is NOT a form of data erasure?

A. Remanence

B. Purging

C. Clearing

D. Destruction

Answer: (SHOW ANSWER)

Clearing refers to the overwriting of data
media intended to be reused in same organization. Purging refers to
degaussing or overwriting media intended to be removed from the
organization. Destruction refers to completely destroying the media.

NEW QUESTION: 359

Who determines the required level of independence for security control Assessors (SCA)?

A. System owner

B. Chief Information Security Officer (CISC)

C. Business owner

D. Authorizing Official (AO)

Answer: D (LEAVE A REPLY)

NEW QUESTION: 360
What can be defined as an abstract machine that mediates all access to objects by subjects to ensure that subjects have the necessary access rights and to protect objects from unauthorized access?
A. The Reference Monitor
B. The Security Kernel
C. The Trusted Computing Base
D. The Security Domain
Answer: A (LEAVE A REPLY)
The reference monitor refers to abstract machine that mediates all access to objects by subjects. This question is asking for the concept that governs access by subjects to objects, thus the reference monitor is the best answer. While the security kernel is similar in nature, it is what actually enforces the concepts outlined in the reference monitor.
In operating systems architecture a reference monitor concept defines a set of design requirements on a reference validation mechanism, which enforces an access control policy over subjects' (e.g., processes and users) ability to perform operations (e.g., read and write) on objects (e.g., files and sockets) on a system. The properties of a reference monitor are:
The reference validation mechanism must always be invoked (complete mediation).
Without this property, it is possible for an attacker to bypass the mechanism and violate the security policy.
The reference validation mechanism must be tamperproof (tamperproof). Without this property, an attacker can undermine the mechanism itself so that the security policy is not correctly enforced.
The reference validation mechanism must be small enough to be subject to analysis and tests, the completeness of which can be assured (verifiable). Without this property, the mechanism might be flawed in such a way that the policy is not enforced.
For example, Windows 3.x and 9x operating systems were not built with a reference monitor, whereas the Windows NT line, which also includes Windows 2000 and Windows
XP, was designed to contain a reference monitor, although it is not clear that its properties (tamperproof, etc.) have ever been independently verified, or what level of computer security it was intended to provide.
The claim is that a reference validation mechanism that satisfies the reference monitor concept will correctly enforce a system's access control policy, as it must be invoked to mediate all security-sensitive operations, must not be tampered, and has undergone complete analysis and testing to verify correctness. The abstract model of a reference monitor has been widely applied to any type of system that needs to enforce access control, and is considered to express the necessary and sufficient properties for any system making this security claim.
According to Ross Anderson, the reference monitor concept was introduced by James Anderson in an influential 1972 paper.
Systems evaluated at B3 and above by the Trusted Computer System Evaluation Criteria

(TCSEC) must enforce the reference monitor concept.
The reference monitor, as defined in AIO V5 (Harris) is: "an access control concept that refers to an abstract machine that mediates all access to objects by subjects."
The security kernel, as defined in AIO V5 (Harris) is: "the hardware, firmware, and software elements of a trusted computing based (TCB) that implement the reference monitor concept. The kernel must mediate all access between subjects and objects, be protected from modification, and be verifiable as correct."
The trusted computing based (TCB), as defined in AIO V5 (Harris) is: "all of the protection mechanisms within a computer system (software, hardware, and firmware) that are responsible for enforcing a security policy."
The security domain, "builds upon the definition of domain (a set of resources available to a subject) by adding the fact that resources withing this logical structure (domain) are working under the same security policy and managed by the same group."
The following answers are incorrect:
"The security kernel" is incorrect. One of the places a reference monitor could be implemented is in the security kernel but this is not the best answer.
"The trusted computing base" is incorrect. The reference monitor is an important concept in the TCB but this is not the best answer.
"The security domain is incorrect." The reference monitor is an important concept in the security domain but this is not the best answer.
Reference(s) used for this question:
Official ISC2 Guide to the CBK, page 324
AIO Version 3, pp. 272 - 274
AIOv4 Security Architecture and Design (pages 327 - 328)
AIOv5 Security Architecture and Design (pages 330 - 331)
Wikipedia article at https://en.wikipedia.org/wiki/Reference_monitor

NEW QUESTION: 361
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. A credential check-out process for a per-use basis
C. Full logging on affected systems
D. Reduce the group in size
Answer: (SHOW ANSWER)

NEW QUESTION: 362

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: C (LEAVE A REPLY)

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.

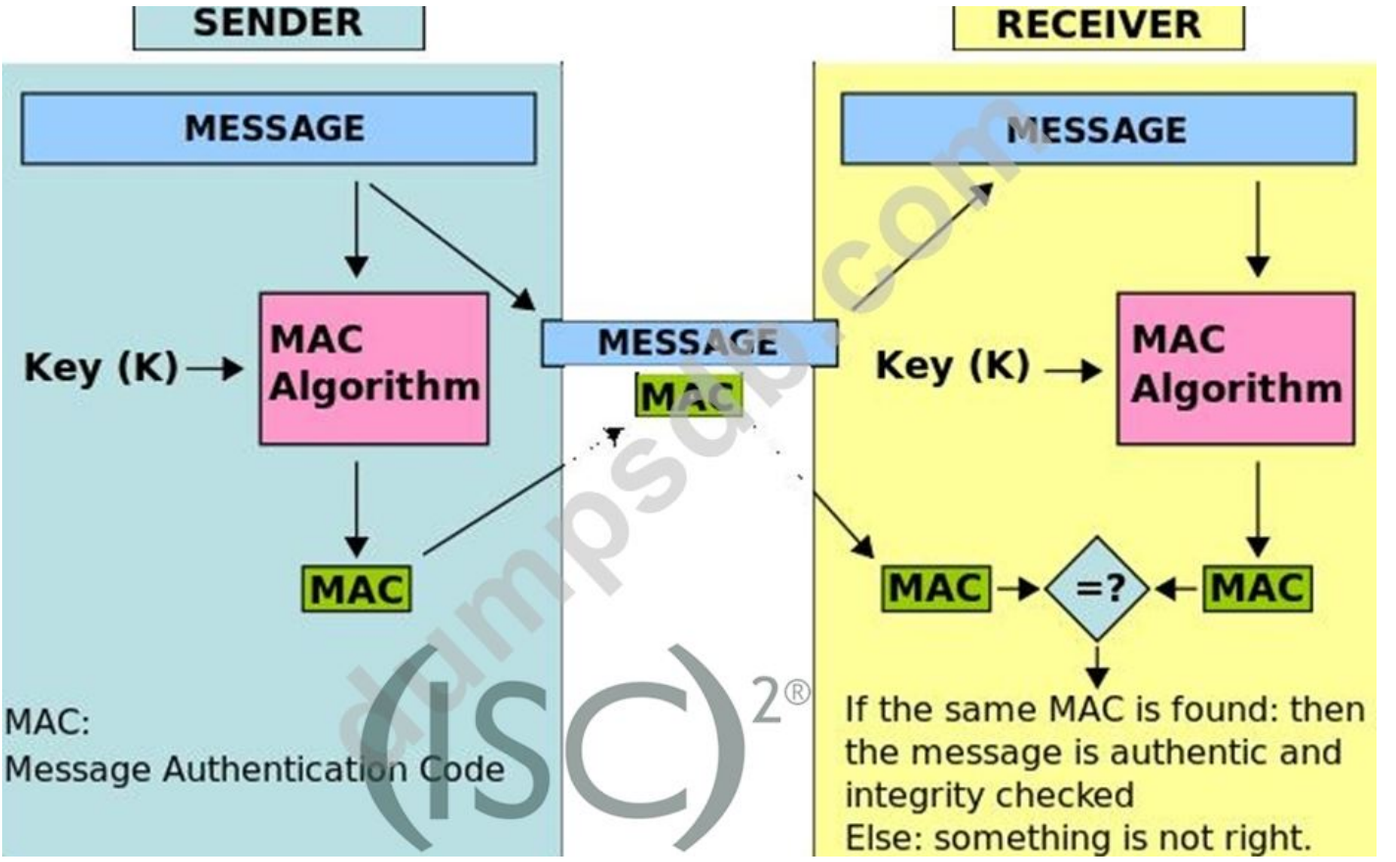
A MAC is a small representation of a message and has the following characteristics:

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: 363
Which choice below is the MOST accurate description of a warm site?
A. A backup processing facility with adequate electrical wiring and air conditioning, but no hardware or software installed
B. A backup processing facility with all hardware and software installed and 100% compatible with the original site, operational within hours
C. A mobile trailer with portable generators and air conditioning
D. A backup processing facility with most hardware and software installed, which can be operational within a matter of days
Answer: (SHOW ANSWER)
The three most common types of remote off-site backup processing facilities are hot sites, warm sites, and cold sites. They are primarily differentiated by how much preparation is devoted to the site, and therefore how quickly the site can be used as an alternate processing site.

NEW QUESTION: 364
Java follows which security model:
A. least priviledge
B. Sand box
C. CIA
D. OSI
Answer: B (LEAVE A REPLY)
Java follows a sand box security model. If a java program operates with the sand box it is considered safe.
However, hackers have found ways to make Java run outside of the sand box and thus is unsafe.
The following answers are incorrect:
A. least priviledge - minimum rights required to perform an authorized task are given. This is to limit damage or access to sensitive or confidential data.
B. CIA - stands for Confidentiality, Integrity and Availability. These are the fundamental principles of security.
D. OSI - this is a model is guideline on how devices/applications on a network are to communicate with each other.
This is defined in a seven layer approach.
The following reference(s) were/was used to create this question:

NEW QUESTION: 365
What are called user interfaces that limit the functions that can be selected by a user?
A. Constrained user interfaces
B. Limited user interfaces
C. Mini user interfaces
D. Unlimited user interfaces
Answer: A (LEAVE A REPLY)

Another method for controlling access is by restricting users to specific functions
based on their role in the system. This is typically implemented by limiting available menus, data views, encryption, or by physically constraining the user interfaces.
This is common on devices such as an automated teller machine (ATM). The advantage of a constrained user interface is that it limits potential avenues of attack and system failure by restricting the processing options that are available to the user.
On an ATM machine, if a user does not have a checking account with the bank he or she will not be shown the "Withdraw money from checking" option. Likewise, an information system might have an "Add/Remove Users" menu option for administrators, but if a normal, non-administrative user logs in he or she will not even see that menu option. By not even identifying potential options for non-qualifying users, the system limits the potentially harmful execution of unauthorized system
or application commands.
Many database management systems have the concept of "views." A database view is an extract of the data stored in the database that is filtered based on predefined user or system criteria. This permits multiple users to access the same database while only having the ability to access data they need (or are allowed to have) and not data for another user. The use of database views is another example of a constrained user interface.
The following were incorrect answers:
All of the other choices presented were bogus answers.
The following reference(s) were 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 1989-2002). Auerbach Publications. Kindle Edition.

NEW QUESTION: 366
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: (SHOW ANSWER)
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: 367
There are parallels between the trust models in Kerberos and Public Key Infrastructure (PKI). When we compare them side by side, Kerberos tickets correspond most closely to which of the following?
A. public keys
B. private keys
C. public-key certificates
D. private-key certificates
Answer: C (LEAVE A REPLY)
A Kerberos ticket is issued by a trusted third party. It is an encrypted data structure that includes the service encryption key. In that sense it is similar to a public-key certificate. However, the ticket is not the key.
The following answers are incorrect:
public keys. Kerberos tickets are not shared out publicly, so they are not like a PKI public key.
private keys. Although a Kerberos ticket is not shared publicly, it is not a private key.
Private keys are associated with Asymmetric crypto system which is not used by Kerberos. Kerberos uses only the Symmetric crypto system.
private key certificates. This is a detractor. There is no such thing as a private key certificate.

NEW QUESTION: 368
Which of the following BEST describes an exploit?
A. An intentional hidden message or feature in an object such as a piece of software or a movie.
B. A chunk of data, or sequence of commands that take advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software.
C. An anomalous condition where a process attempts to store data beyond the boundaries of a fixed- length buffer.
D. A condition where a program (either an application or part of the operating system) stops performing its expected function and also stops responding to other parts of the system.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
An exploit refers to a piece of software or data, or a sequence of commands that takes advantage of a bug or vulnerability with the aim of causing unplanned or unexpected behavior to take place on computerized hardware, or its software.
Incorrect Answers:
A: An intentional hidden message, in-joke, or feature in a work such as a computer program, web page, video game, movie, book, or crossword is known as a virtual Easter egg.

C: The anomalous condition where a process attempts to store data beyond the boundaries of a fixed- length buffer is known as buffer overflow.
D: In computing, a condition where a program (either an application or part of the operating system) stops performing its expected function and also stops responding to other parts of the system is known as a crash.
References:
https://en.wikipedia.org/wiki/Exploit_%28computer_security%29
https://www.quora.com/topic/Easter-Eggs-media
https://en.wikipedia.org/wiki/Buffer_overflow
http://www.article-buzz.com/Article/Avoiding-Data-Loss---A-Guide-To-The-Best-Online-Data-Storage- Websites/328757#.Vjc757crKHu

NEW QUESTION: 369
What is called an attack in which an attacker floods a system with connection requests but does not respond when the target system replies to those requests?
A. Ping of death attack
B. SYN attack
C. Smurf attack
D. Buffer overflow attack
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
A SYN flood DoS attack where an attacker sends a succession of SYN packets with the goal of overwhelming the victim system so that it is unresponsive to legitimate traffic.
Incorrect Answers:
A: The Ping of Death attack is based upon the use of oversized ICMP packets. It is not based on flooding the system with connection requests.
C: In a smurf attack the attacker sends an ICMP ECHO REQUEST packet, not a connection request, with a spoofed source address to a victim's network broadcast address.
D: In Buffer overflow attack is an anomaly where a program, while writing data to a buffer (not sending connection requests), overruns the buffer's boundary and overwrites adjacent memory locations.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 549

NEW QUESTION: 370
To be admissible in court, computer evidence must be which of the following?
A. Relevant
B. Decrypted
C. Edited
D. Incriminating

Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
For evidence to be admissible in court, it needs to be relevant, sufficient, and reliable.
Incorrect Answers:
B: The evidence should not be changed. If it is encrypted it should be kept encrypted.
C: Evidence should not be changed or edited.
D: Evidence does not need to be incriminating. It can very well be used in favor of the suspect, such as an alibi.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 1068

NEW QUESTION: 371
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. industry best practices.
B. organization policy.
C. industry laws and regulations.
D. management feedback.
Answer: (SHOW ANSWER)

NEW QUESTION: 372
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: (SHOW ANSWER)
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: 373
Which choice below is NOT an accurate statement about an
organization's incident-handling capability?
A. The organization's incident-handling capability should be used to
contain and repair damage done from incidents.
B. It should be used to prevent future damage from incidents.
C. The organization's incident-handling capability should be used to

detect and punish senior-level executive wrong-doing.
D. It should be used to provide the ability to respond quickly and effectively to an incident.
Answer: C (LEAVE A REPLY)
An organization should address computer security incidents by developing an incident-handling capability. The incident-handling capability should be used to:
Provide the ability to respond quickly and effectively.
Contain and repair the damage from incidents. When left unchecked, malicious software can significantly harm an organization's computing, depending on the technology and its connectivity.
Containing the incident should include an assessment of whether the incident is part of a targeted attack on the organization or an isolated incident.
Prevent future damage. An incident-handling capability should assist an organization in preventing (or at least minimizing) damage from future incidents. Incidents can be studied internally to gain a better understanding of the organization's threats and vulnerabilities.
Source: NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems.

NEW QUESTION: 374
This tape format can be used to backup data systems in addition to its original intended audio used by:
A. Digital Audio tape (DAT)
B. Digital video tape (DVT)
C. Digital Casio Tape (DCT)
D. Digital Voice Tape (DVT)
Answer: A (LEAVE A REPLY)
Digital Audio Tape (DAT or R-DAT) is a signal recording and playback medium introduced by Sony in 1987. In appearance it is similar to a compact audio cassette, using 1/8" magnetic tape enclosed in a protective shell, but is roughly half the size at 73 mm x 54 mm x 10.5 mm. As the name suggests the recording is digital rather than analog, DAT converting and recording at the same rate as a CD (44.1 kHz sampling rate and 16 bits quantization) without data compression. This means that the entire input signal is retained. If a digital source is copied then the DAT will produce an exact clone. The format was designed for audio use, but through an ISO standard it has been adopted for general data storage, storing from 4 to 40 GB on a 120 meter tape depending on the standard and compression (DDS-1 to DDS-4). It is, naturally, sequential-access media and is commonly used for backups. Due to the higher requirements for integrity in data backups a computer-grade DAT was introduced.

NEW QUESTION: 375
Which of the following is a symmetric encryption algorithm?
A. RSA
B. Elliptic Curve
C. RC5
D. El Gamal
Answer: (SHOW ANSWER)
RC5 is a symmetric encryption algorithm. It is a block cipher of variable block length, encrypts through integer addition, the application of a bitwise Exclusive OR (XOR), and variable rotations.
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 153).

NEW QUESTION: 376
Which of the following is BEST achieved through the use of eXtensible Access Markup Language (XACML)?
A. Minimize malicious attacks from third parties
B. Manage resource privileges
C. Share digital identities in hybrid cloud
D. Defined a standard protocol
Answer: D (LEAVE A REPLY)
Section: Communication and Network Security

NEW QUESTION: 377
Which of the following addresses a portion of the primary memory by specifying the actual address of the memory location?
A. direct addressing
B. Indirect addressing
C. implied addressing
D. indexed addressing
Answer: A (LEAVE A REPLY)
+------+-----+----------------------------------+
| load | reg | address |

+ ------+-----+-----------------------------------+
(Effective address = address as given in instruction)
This requires space in an instruction for quite a large address. It is often available on CISC machines which have variable-length instructions, such as x86.
Some RISC machines have a special Load Upper Literal instruction which places a 16-bit constant in the top half of a register. An OR literal instruction can be used to insert a 16-bit constant in the lower half of that register, so that a full 32-bit address can then be used via the register-indirect addressing mode, which itself is provided as "base-plus-offset" with an offset of 0.
http://en.wikipedia.org/wiki/Addressing_mode (Very good coverage of the subject) also see:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, page 186.
also see:
http://www.comsci.us/ic/notes/am.html

NEW QUESTION: 378
The PRIMARY outcome of a certification process is that it provides documented
A. system weaknesses for remediation.
B. standards for security assessment, testing, and process evaluation.
C. security analyses needed to make a risk-based decision.
D. interconnected systems and their implemented security controls.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 379
What protocol is often used between gateway hosts on the Internet' To control the scope of a Business Continuity Management (BCM) system, a security practitioner should identify which of the following?
A. Business needs of the security organization
B. Size, nature, and complexity of the organization
C. All possible risks
D. Adaptation model for future recovery planning
Answer: A (LEAVE A REPLY)

NEW QUESTION: 380
Which of the following is considered the PRIMARY security issue associated with encrypted e-mail messages?
A. Scanning for viruses and other malware
B. Greater costs associated for backups and restores
C. Storing attachments in centralized repositories
D. Key distribution
Answer: A (LEAVE A REPLY)

NEW QUESTION: 381

Refer to the information below to answer the question.

In a Multilevel Security (MLS) system, the following sensitivity labels are used in increasing levels of sensitivity: restricted, confidential, secret, top secret. Table A lists the clearance levels for four users, while Table B lists the security classes of four different files.

Table A

User	Clearance Level
A	Restricted
B	Confidential
C	Secret
D	Top Secret

Table B

Files	Security Class
1	Restricted
2	Confidential
3	Secret
4	Top Secret

In a Bell-LaPadula system, which user cannot write to File 3?

A. User C

B. User D

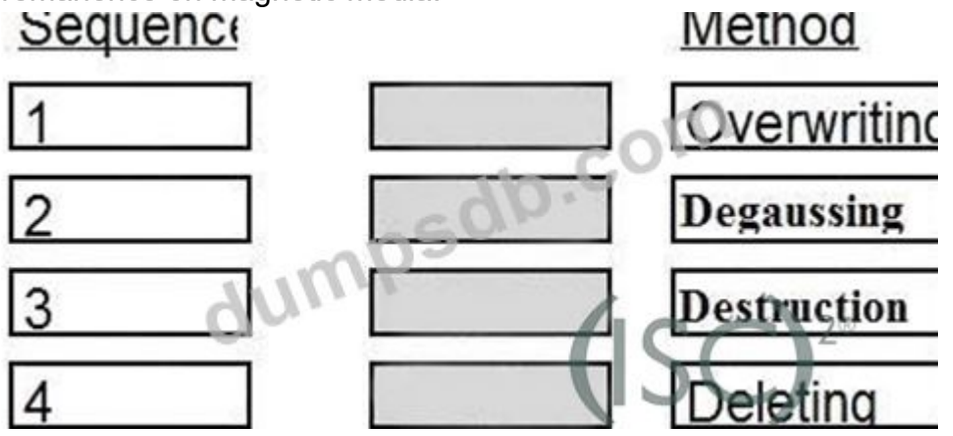
C. User A

D. User B

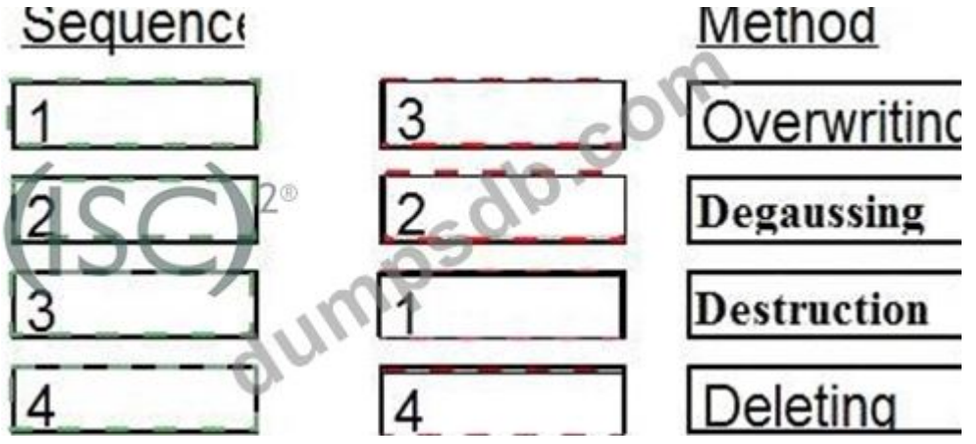
Answer: (SHOW ANSWER)

NEW QUESTION: 382

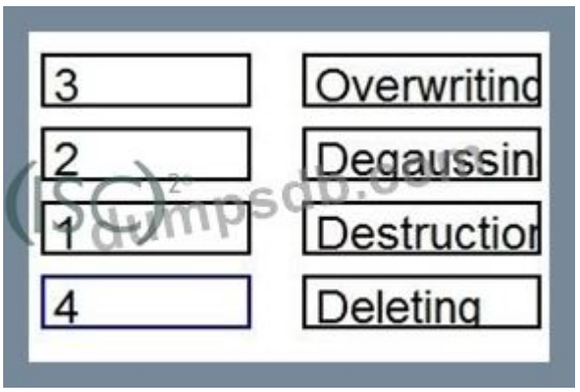
Place in order, from BEST (1) to WORST (4), the following methods to reduce the risk of data remanence on magnetic media.



Answer:



Explanation



NEW QUESTION: 383
Which Orange book security rating introduces security labels?
A. C2
B. B1
C. B2
D. B3
Answer: (SHOW ANSWER)
B1 is also called "Labeled Security" and each data object must have a classification label and each subject a clearence label. On each access attempt, the classification and clearence are checked to verify that the access is permissable.
C2 is incorrect. C2 is also called "Controlled Access Protection" and only requires that subjects be individually identified and that security-related events are auditable.
B2 is incorrect. B2 is also called "Structured Protection" and imposes additional controls on security policy and a more thorough review of system design and implementation.
B3 is incorrect. B3 is also called "Security Domains" and and imposes more granularity in each protection mechanism.
References:
CBK, pp. 329 - 330
AIO3 pp.302 - 307

NEW QUESTION: 384
Which of the following BEST describes the purpose of performing security certification?
A. To formalize the confirmation of completed risk mitigation and risk analysis
B. To identify system threats, vulnerabilities, and acceptable level of risk
C. To formalize the confirmation of compliance to security policies and standards
D. To verify that system architecture and interconnections with other systems are effectively implemented
Answer: (SHOW ANSWER)

NEW QUESTION: 385
The Diffie-Hellman algorithm is primarily used to provide which of the following?
A. Confidentiality

B. Key Agreement
C. Integrity
D. Non-repudiation
Answer: B (LEAVE A REPLY)
Diffie and Hellman describe a means for two parties to agree upon a shared secret in such a way that the secret will be unavailable to eavesdroppers. This secret may then be converted into cryptographic keying material for other (symmetric) algorithms. A large number of minor variants of this process exist. See RFC 2631 Diffie-Hellman Key
Agreement Method for more details.
In 1976, Diffie and Hellman were the first to introduce the notion of public key cryptography, requiring a system allowing the exchange of secret keys over non-secure channels. The Diffie-Hellman algorithm is used for key exchange between two parties communicating with each other, it cannot be used for encrypting and decrypting messages, or digital signature.
Diffie and Hellman sought to address the issue of having to exchange keys via courier and other unsecure means. Their efforts were the FIRST asymmetric key agreement algorithm.
Since the Diffie-Hellman algorithm cannot be used for encrypting and decrypting it cannot provide confidentiality nor integrity. This algorithm also does not provide for digital signature functionality and thus non-repudiation is not a choice.
NOTE: The DH algorithm is susceptible to man-in-the-middle attacks.
KEY AGREEMENT VERSUS KEY EXCHANGE
A key exchange can be done multiple way. It can be done in person, I can generate a key and then encrypt the key to get it securely to you by encrypting it with your public key. A
Key Agreement protocol is done over a public medium such as the internet using a mathematical formula to come out with a common value on both sides of the communication link, without the ennemy being able to know what the common agreement is.
The following answers were incorrect:
All of the other choices were not correct choices
Reference(s) used for this question:
Shon Harris, CISSP All In One (AIO), 6th edition . Chapter 7, Cryptography, Page 812.
http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
http://www.google.com/patents?vid=4200770

NEW QUESTION: 386
As one component of a physical security system, an Electronic Access Control (EAC) token is BEST known for its ability to
A. monitor the opening of windows and doors.
B. lock down a facility during an emergency.
C. overcome the problems of key assignments.
D. trigger alarms when intruders are detected.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 387
Which of the following is NOT a VPN communications protocol standard?
A. Point-to-point tunneling protocol (PPTP)
B. Challenge Handshake Authentication Protocol (CHAP)
C. Layer 2 tunneling protocol (L2TP)
D. IP Security
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The Challenge Handshake Authentication Protocol (CHAP) is used for authentication only. It is not a VPN communications protocol.
Incorrect Answers:
A: The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks.
C: Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs).
D: IP Security, Internet Protocol Security (IPsec), can be used to setup secure VPN connections.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 683

NEW QUESTION: 388
Convert Channel Analysis, Trusted Facility Management, and Trusted
Recovery are parts of which book in the TCSEC Rainbow Series?
A. Red Book
B. Dark Green Book
C. Orange Book
D. Green Book
Answer: C (LEAVE A REPLY)
The correct answer is Orange Book.
* Answer the Red Book is the Trusted Network
Interpretation (TNI) summary of network requirements (described
in the Telecommunications and Network Security domain).
* The Green Book, is the Department of Defense (DoD) Password Management Guide-line;
* The Dark Green Book, is The Guide to Understanding Data Rema-nence in Automated Information Systems.

NEW QUESTION: 389
A shared resource matrix is a technique commonly used to locate:
A. Malicious code
B. Security flaws
C. Trap doors

D. Covert channels

Answer: D (LEAVE A REPLY)

Analyzing resources of a system is one standard for locating covert channels because the basis of a covert channel is a shared resource.

The following properties must hold for a storage channel to exist:

1.Both sending and receiving process must have access to the same attribute of a shared object.

2.The sending process must be able to modify the attribute of the shared object.

3.The receiving process must be able to reference that attribute of the shared object.

4.A mechanism for initiating both processes and properly sequencing their respective accesses to the shared resource must exist.

Note: Similar properties for timing channel can be listed

The following answers are incorrect:

All other answers were not directly related to discovery of Covert Channels.

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

Auerbach Publications, Auerbach Publications (Test Series) - CRC Press LLC, Page No. 225

and

http://www.cs.ucsb.edu/~sherwood/cs290/papers/covert-kemmerer.pdf

and

http://www.cs.utexas.edu/~byoung/cs361/lecture16.pdf

and

http://www.cs.utexas.edu/~byoung/cs361/lecture16.pdf

NEW QUESTION: 390

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: 391
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: B (LEAVE A REPLY)
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: 392
The security term that is concerned with the same primary key existing at different classification levels in the same database is:
A. Polymorphism.
B. Inheritance.
C. Polyinstantiation.
D. Normalization.
Answer: C (LEAVE A REPLY)

The security term that is concerned with the same primary key existing at different classification levels in the same database is polyinstantiation.
Answer Polymorphism is incorrect because polymorphism is defined as objects of many different classes that are related by some common superclass; thus, any object denoted by this name is able to respond to some common set of operations in a different way. Answer Normalization is incorrect because normalization refers to removing redundant or incorrect data from a database. Answer Inheritance is incorrect because inheritance refers to methods from a class inherited by another subclass.

NEW QUESTION: 393
An organization plan on purchasing a custom software product developed by a small vendor to support its business model.
Which unique consideration should be made part of the contractual agreement potential long-term risks associated with creating this dependency?
A. Access to the technical documentation
B. Right to request an independent review of the software source code
C. Due diligence form requesting statements of compliance with security requirements
D. A source code escrow clause
Answer: (SHOW ANSWER)

NEW QUESTION: 394
Which of the following ciphers is a subset of the Vignere polyalphabetic cipher?
A. Caesar
B. Jefferson
C. Alberti
D. SIGABA
Answer: A (LEAVE A REPLY)
"The Caesar Cipher,...., is a simple substitution cipher that involves shifting the alphabet three positions to the right. The Caesar Cipher is a subset of the Vigenere polyalphabetic cipher. In the Caesar cipher, the message's characters and repetitions of the key are added together, modulo 26. In modulo 26, the letters A to Z of the alphabet are given a value of 0 to 25, respectively."
Pg. 189 Krutz: The CISSP Prep Guide: Gold Edition

NEW QUESTION: 395
The concentric circle approach is used to
A. Evaluate environmental threats.
B. Assess the physical security facility,
C. Assess the communications network security.
D. Develop a personnel security program.
Answer: B (LEAVE A REPLY)

The original answer for this question was C (assess the communications network security) however I think the concentric circle is defining what in the krutz book is know as the security perimeter. To this end this is a reference "A circular security perimeter that is under the access control defines the area or zone to be protected. Preventive/physical controls include fences, badges, multiple doors (man-traps that consists of two doors physically separated so that an individual can be 'trapped' in the space between the doors after entering one of the doors), magnetic card entry systems, biometrics (for identification), guards, dogs, environmental control systems (temperature, humidity, and so forth), and building and access area layout." -Ronald Krutz The CISSP PREP Guide (gold edition) pg 13 This is a standard concentric circle model shown in Figure 1 . If you've never seen this, you haven't had a security lecture. On the outside is our perimeter. We are fortunate to have some defenses on our base. Although some bases don't have people guarding the gates and checking IDs any longer, there's still the perception that it's tougher to commit a crime on a Naval base than it would be at GM. The point is: How much control do we have over fencing and guards? The answer: Not much. The next circle, the red circle, contains your internal access controls. For our purposes, the heart of the red circle is the computer. That's what I want to zero in on. The internal controls are the things you can do to keep people out of your PCs and off your network. http://www.chips.navy.mil/archives/96_oct/file5.htm

NEW QUESTION: 396
Which backup method listed below will probably require the backup
operator to use the most number of tapes for a complete system
restoration, if a different tape is used every night in a five-day rotation?
A. Incremental Backup Method
B. Ad Hoc Backup Method
C. Full Backup Method
D. Differential Backup Method
Answer: (SHOW ANSWER)
Most backup methods use the Archive file attribute to determine
whether the file should be backed up or not. The backup software
determines which files need to be backed up by checking to see if
the Archive file attribute has been set, and then resets the Archive bit value to null after the backup procedure. The Incremental Backup
Method backs up only files that have been created or modified since
the last backup was made, because the Archive file attribute is reset.
This can result in the backup operator needing several tapes to do a
complete restoration, as every tape with changed files as well as the
last full backup tape will need to be restored.
* a Full or Complete backup backs up all files in all directories
stored on the server regardless of when the last backup was
made and whether the files have already been backed up. The
Archive file attribute is changed to mark that the files have been

backed up, and the tapes or tapes will have all data and applications
on it. It's an incorrect answer for this question, however, as it's
assumed answers Differential Backup Method and Incremental Backup Method will additionally require differential or incremental tapes.
* the Differential Backup Method, backs up only files that
have been created or modified since the last backup was made, like an
incremental backup. However, the difference between an incremental
backup and a differential backup is that the Archive file attribute is not reset after the differential backup is completed, therefore the changed file is backed up every time the differential backup is run. The backup set grows in size until the next full backup as these files continue to be backed up during each subsequent differential backup, until the next complete backup occurs. The advantage of this backup method is that the backup operator should only need the full backup and the one differential backup to restore the system.
Table shows these three backup methods.
Exhibit:

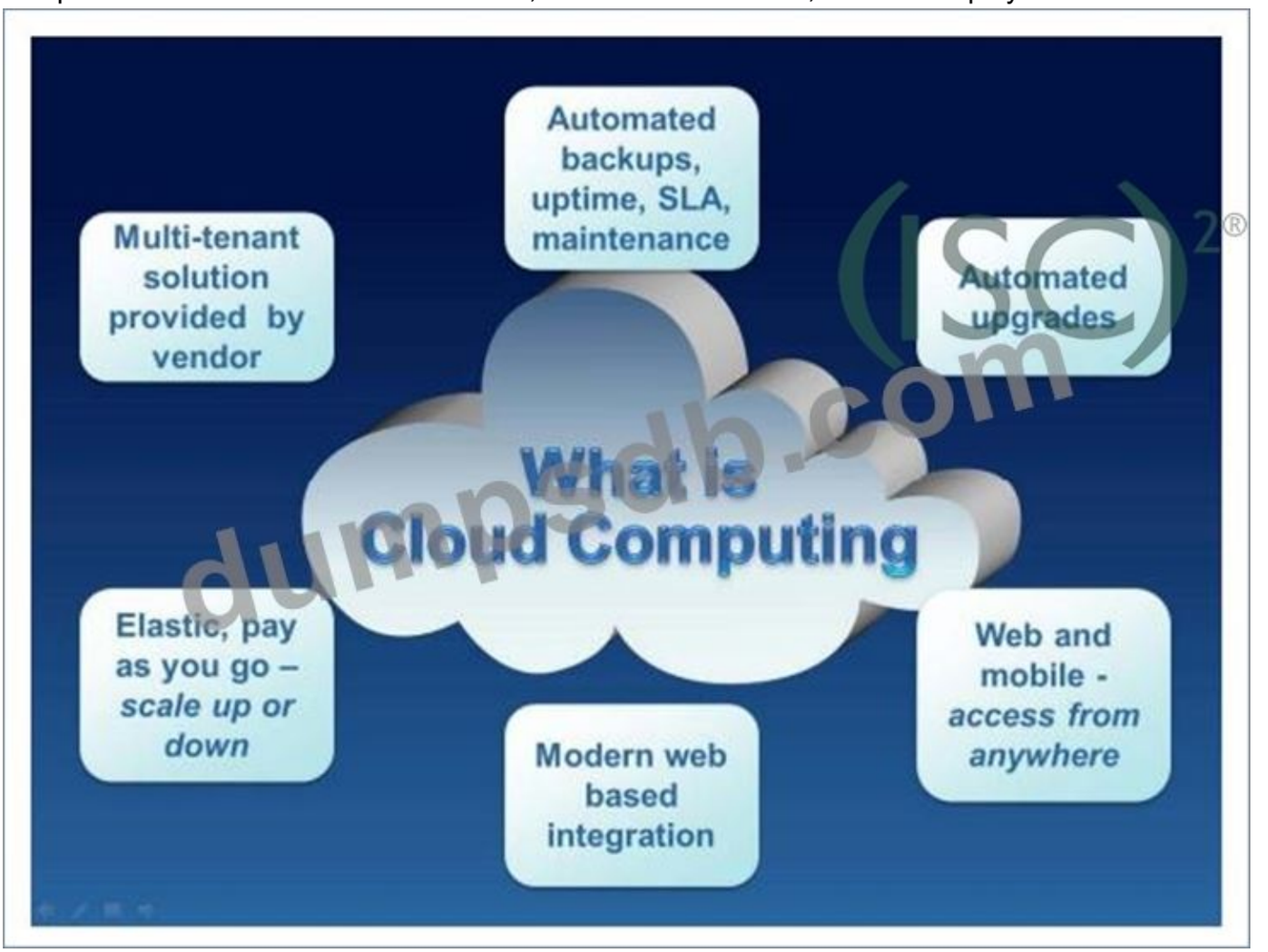
Differential versus Incremental Backup Tape Contents

BACKUP METHOD	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
Differential	Changed File A	Changed Files A & B	Files A, B, & C	Files A, B, C, & D	
Incremental	Changed File A	Changed File B	Changed File C	Changed File D	
Full Backup					All Files

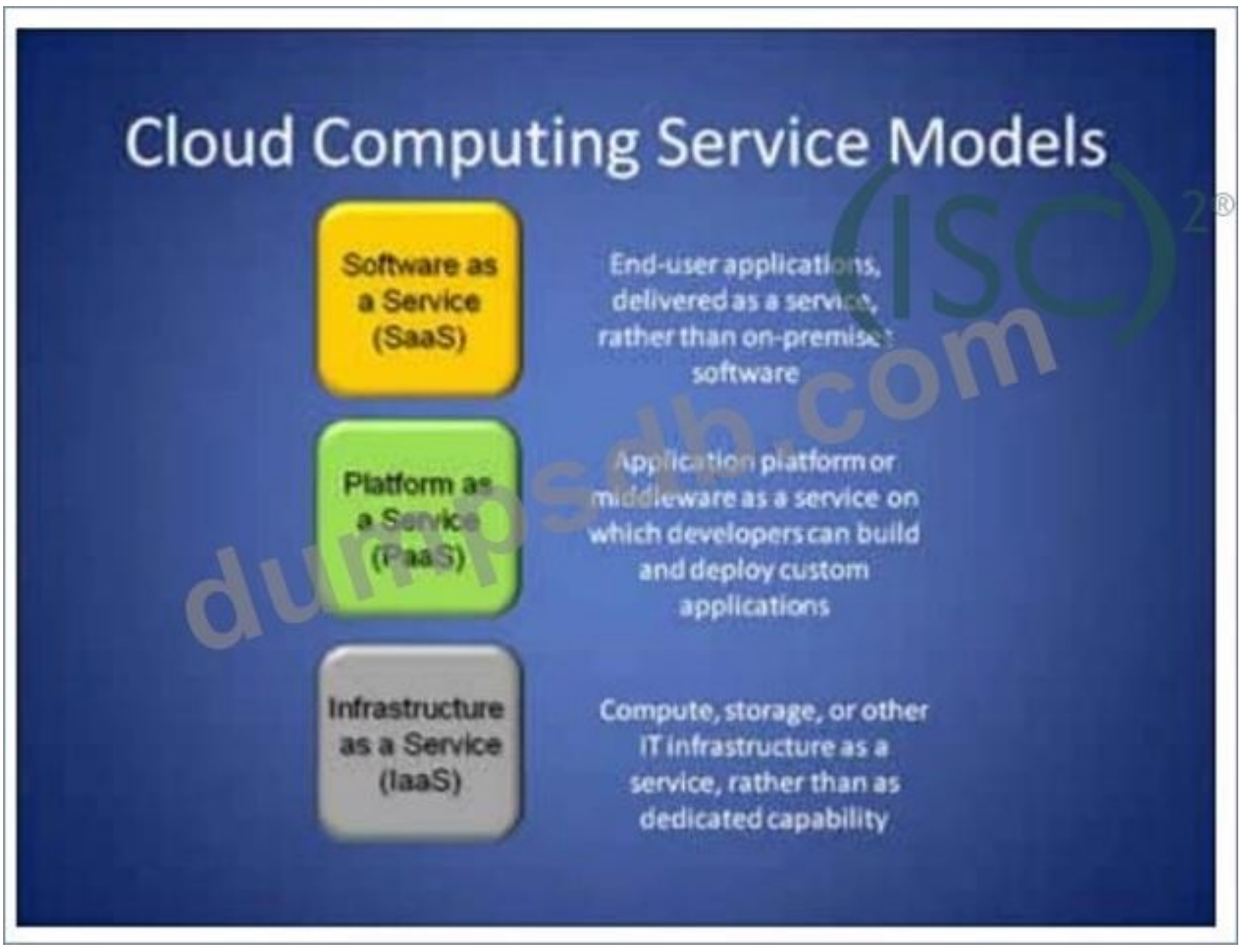
image008
Answer "Ad Hoc Backup Method" is a distracter.

NEW QUESTION: 397
In which of the following cloud computing service model are applications hosted by the service provider and made available to the customers over a network?
A. Software as a service
B. Data as a service
C. Platform as a service
D. Infrastructure as a service
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically, the Internet. SaaS is closely related to the ASP (application service provider) and on demand computing software delivery models. For your exam you should know below information about Cloud Computing: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal

management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.



Reference http://osarena.net/wp-content/uploads/2013/04/cloud-computing3.jpg Cloud computing service model



Cloud computing service models
Image Reference http://www.esri.com/news/arcwatch/0110/graphics/feature2.jpg Software as a Service (SaaS)
Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically, the Internet. SaaS is closely related to the ASP (application service provider) and on demand computing software delivery models. IDC identifies two slightly different delivery models for SaaS. The hosted application management (hosted AM) model is similar to ASP: a provider hosts commercially available software for customers and delivers it over the Web. In the software on demand model, the provider gives customers network- based access to a single copy of an application created specifically for SaaS distribution. Provider gives users access to specific application software (CRM, e-mail, games). The provider gives the customers network based access to a single copy of an application created specifically for SaaS distribution and use. Benefits of the SaaS model include: easier administration automatic updates and patch management compatibility: All users will have the same version of software. easier collaboration, for the same reason global accessibility.
Platform as a Service (PaaS) Platform as a Service (PaaS) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones. Cloud providers deliver a computing platform, which can include an operating system, database, and web server as a holistic execution environment.

Where IaaS is the "raw IT network," PaaS is the software environment that runs on top of the IT network.
Platform as a Service (PaaS) is an outgrowth of Software as a Service (SaaS), a software distribution model in which hosted software applications are made available to customers over the Internet. PaaS has several advantages for developers. With PaaS, operating system features can be changed and upgraded frequently. Geographically distributed development teams can work together on software development projects.
Services can be obtained from diverse sources that cross international boundaries. Initial and ongoing costs can be reduced by the use of infrastructure services from a single vendor rather than maintaining multiple hardware facilities that often perform duplicate functions or suffer from incompatibility problems.
Overall expenses can also be minimized by unification of programming development efforts. On the downside, PaaS involves some risk of "lock-in" if offerings require proprietary service interfaces or development languages. Another potential pitfall is that the flexibility of offerings may not meet the needs of some users whose requirements rapidly evolve. Infrastructure as a Service (IaaS) Cloud providers offer the infrastructure environment of a traditional data center in an on-demand delivery method. Companies deploy their own operating systems, applications, and software onto this provided infrastructure and are responsible for maintaining them. Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.
Incorrect Answers:
B: Data Provided as a service rather than needing to be loaded and prepared on premises.
C: Platform as a Service (PaaS) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.
D: Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.
References: CISA review manual 2014 page number 102 Official ISC2 guide to CISSP 3rd edition Page number 689
http://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service
http://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS
http://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS

NEW QUESTION: 398
Which of the following is a network intrusion detection technique?
A. Statistical anomaly

B. Port scanning
C. Perimeter intrusion
D. Network spoofing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 399
In the access control matrix, the rows are:
A. Capability lists.
B. Tuples.
C. Access Control Lists (ACLs).
D. Domains.
Answer: (SHOW ANSWER)
The correct answer is Capability lists.
* Answer "Access Control Lists (ACLs)" is incorrect because the access control list is not a row in the access control matrix.
* Answer Tuples is incorrect because a tuple is a row in the table of a relational database.
* Answer Domains is incorrect because a domain is the set of allowable values a column or attribute can take in a relational database.

NEW QUESTION: 400
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: 401
Which of the following PRIMARILY contributes to security incidents in web-based applications?
A. Improper stress testing and application interfaces
B. System incompatibility and patch management
C. Third-party applications and change controls
D. Systems administration and operating systems
Answer: C (LEAVE A REPLY)

NEW QUESTION: 402
In biometric identification systems, the parts of the body conveniently available for identification are:
A. neck and mouth
B. hands, face, and eyes
C. feet and hair
D. voice and neck
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Most identity authentication takes place when people are fully clothed (neck to feet and wrists), the parts of the body conveniently available for this purpose are hands, face, and eyes.
Incorrect Answers:
A: The neck is not convenient as it can be covered.
C: The feet normally have shoes on, and therefore not convenient.
D: The neck is not convenient as it can be covered.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, pp. 187-192

NEW QUESTION: 403
*Directive controls are a form of change management policy and procedures. Which of the following subsections are recommended as part of the change management process?
A. Build and test
B. Implement security controls
C. Categorize Information System (IS)
D. Select security controls

Answer: A (LEAVE A REPLY)
Reference:
https://books.google.com.pk/books?id=9gCn86CmsNQC&pg=PA570&lpg=PA570&dq=CISSP+Directive+cont

NEW QUESTION: 404
Which of the following are proprietarily implemented by CISCO?
A. RADIUS+
B. TACACS
C. XTACACS and TACACS+
D. RADIUS
Answer: C (LEAVE A REPLY)
Cisco implemented an enhanced version of TACACS, known as XTACACS (extended TACACS), which was also compatible with TACACS. It allowed for UDP and TCP encoding. XTACACS contained several improvements: It provided accounting functionality to track length of login and which hosts a user connected to, and it also separated the authentication, authorization, and accounting processes such that they could be independently implemented. None of the three functions are mandatory. XTACACS is described in RFC 1492. TACACS+ is the latest Cisco implementation. It is best described as XTACACS with improved attribute control (authorization) and accounting.

NEW QUESTION: 405
Which of the following statements pertaining to Kerberos is TRUE?
A. Kerberos does not address availability
B. Kerberos does not address integrity
C. Kerberos does not make use of Symmetric Keys
D. Kerberos cannot address confidentiality of information
Answer: (SHOW ANSWER)
The question was asking for a TRUE statement and the only correct statement is "Kerberos does not address availability".
Kerberos addresses the confidentiality and integrity of information. It does not directly address availability.
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 42).

NEW QUESTION: 406
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: (SHOW ANSWER)

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: 407
Which security model ensures that actions that take place at a higher security level do not affect actions that take place at a lower level?
A. The Bell-LaPadula model
B. The information flow model
C. The noninterference model
D. The Clark-Wilson model
Answer: C (LEAVE A REPLY)
The goal of a noninterference model is to strictly separate differing security levels to assure that higher-level actions do not determine what lower-level users can see. This is in contrast to other security models that control information flows between differing levels of users, By maintaining strict separation of security levels, a noninterference model minimizes leakages that might happen through a covert channel.
The model ensures that any actions that take place at a higher security level do not affect, or interfere with, actions that take place at a lower level.
It is not concerned with the flow of data, but rather with what a subject knows about the state of the system. So if an entity at a higher security level performs an action, it can not change the state
for the entity at the lower level.
The model also addresses the inference attack that occurs when some one has access to some type of information and can infer(guess) something that he does not have the clearance level or authority to know.
The following are incorrect answers:
The Bell-LaPadula model is incorrect. The Bell-LaPadula model is concerned only with confidentiality and bases access control decisions on the classfication of objects and the clearences of subjects.
The information flow model is incorrect. The information flow models have a similar framework to the Bell-LaPadula model and control how information may flow between objects based on security
classes. Information will be allowed to flow only in accordance with the security policy.
The Clark-Wilson model is incorrect. The Clark-Wilson model is concerned with change control and assuring that all modifications to objects preserve integrity by means of well-formed transactions and usage of an access triple (subjet - interface - object).
References:
CBK, pp 325 - 326
AIO3, pp. 290 - 291
AIOv4 Security Architecture and Design (page 345)
AIOv5 Security Architecture and Design (pages 347 - 348)

https://en.wikibooks.org/wiki/Security_Architecture_and_Design/Security_Models#Noninterference_Models

NEW QUESTION: 408
Making sure that the data has not been changed unintentionally, due to an accident or malice is:
A. Integrity.
B. Confidentiality.
C. Availability.
D. Auditability.
Answer: A (LEAVE A REPLY)
Integrity refers to the protection of information from unauthorized modification or deletion.
Confidentiality is incorrect. Confidentiality refers to the protection of information from unauthorized disclosure.
Availability is incorrect. Availability refers to the assurance that information and services will be available to authorized users in accordance with the service level objective.
Auditability is incorrect. Auditability refers to the ability to trace an action to the identity that performed it and identify the date and time at which it occurred.
References:
CBK, pp. 5 - 6
AIO3, pp. 56 - 57

NEW QUESTION: 409
Which of the following is less likely to be used today in creating a Virtual Private Network?
A. L2TP
B. PPTP
C. IPSec
D. L2F
Answer: D (LEAVE A REPLY)
L2F (Layer 2 Forwarding) provides no authentication or encryption. It is a
Protocol that supports the creation of secure virtual private dial-up networks over the Internet.
At one point L2F was merged with PPTP to produce L2TP to be used on networks and not only on dial up links.
IPSec is now considered the best VPN solution for IP environments.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 8: Cryptography (page 507).

NEW QUESTION: 410
What is the company benefit, in terms of risk, for people taking a vacation of a specified minimum length?
A. Reduces stress levels, thereby lowering insurance claims.

B. Improves morale, thereby decreasing errors.
C. Increases potential for discovering frauds.
D. Reduces dependence on critical individuals.
Answer: (SHOW ANSWER)
Mandatory vacations are another type of administrative control that may sound a bit odd at first. Chapter 3 touches on reasons to make sure that employees take their vacations; this has to do with being able to identify fraudulent activities and enable job rotation to take place. -Shon Harris All-in-one CISSP Certification Guide pg 810

NEW QUESTION: 411
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)
Security testing makes sure the modified or new system includes appropriate
access controls and does not introduce any security holes that might compromise other systems.
Recovery testing checks the system's ability to recover after a software or hardware failure.
Stress/volume testing involves testing an application with large quantities of data in order to evaluate performance during peak hours.
Interface testing evaluates the connection of two or more components that pass information from one area to another.
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 300).

NEW QUESTION: 412
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. Cookie manipulation
D. Structured Query Language (SQL) injection
Answer: D (LEAVE A REPLY)
Explanation
Section: Security Assessment and Testing

NEW QUESTION: 413

Which statement below is the BEST example of separation of duties?
A. Getting users to divulge their passwords.
B. An activity that checks on the system, its users, or the environment.
C. One person initiates a request for a payment and another authorizes that same payment.
D. A data entry clerk may not have access to run database analysis reports.
Answer: C (LEAVE A REPLY)
Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. In financial systems, no single individual should normally be given the authority to issue checks. Checks and balances need to be designed into both the process as well as the specific, individual positions of personnel who will implement the process. *Answer "An activity that checks on the system, its users, or the environment" describes system monitoring. *Answer "Getting users to divulge their passwords" is social engineering, a method of subverting system controls by getting users or administrators to divulge information about systems, including their passwords. *Answer "A data entry clerk may not have access to run database analysis reports" describes least privilege. Least privilege refers to the security objective of granting users only those accesses they need to perform their official duties. Least privilege does not mean that all users will have extremely little functional access; some employees will have significant access if it is required for their position. It is important to make certain that the implementation of least privilege does not interfere with the ability to have personnel substitute for each other without undue delay. Without careful planning, access control can interfere with contingency plans. Source: National Institute of Standards and Technology, An Introduction to Computer Security: The NIST Handbook Special Publication 800-12.

NEW QUESTION: 414
Readable is to unreadable just as plain text is to _____?
A. Cipher Text
B. Encryption
C. Unplain Text
D. Digitally Signed
Answer: (SHOW ANSWER)
When we encrypt text it is unreadable and referred to as Cipher Text.
The following answers are incorrect:
Encryption: Changing plain text to cipher text is the process of encryption but it isn't the right answer here. Sorry.
Unplain text: Sorry, that's not even a real word. Lol.
Digitally Signed: This answer is related to cryptography but isn't the right answer. We sign items so that the recipient can assure that the document came from the stated individual and it was not modified. A Digital Signature provides Authenticity and Integrity.
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. 4). Wiley. Kindle

Edition.

NEW QUESTION: 415
A pen register is a:
A. Device that records the caller-ID of incoming calls
B. Device that records the URLs accessed by an individual
C. Device that identifies the cell in which a mobile phone is operating
D. Device that records all the numbers dialed from a specific telephone line
Answer: D (LEAVE A REPLY)
(Electronic Privacy Information Center, Approvals for Federal Pen Registers and Trap and Trace Devices 1987-1998, www.epic. org). Gathering information as to which numbers are dialed from a specific telephone line is less costly and time-consuming than installing a wiretap and recording the information.
*There is also equipment that can record the information listed in answers "Device that identifies the cell in which a mobile phone is operating" and "Device that records the URLs accessed by an individual".
*The device referred to in answer "Device that records the caller-ID of incoming calls" is called a trap-and-trace device. All of the answers in this question are a subset of the category of traffic analysis wherein patterns and frequency associated with communications are studied instead of the content of the communications.

NEW QUESTION: 416
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: D (LEAVE A REPLY)
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: 417
Why do some sites choose not to implement Trivial File Transfer Protocol (TFTP)?

A. user authentication requirement
B. inherent security risks
C. list restrictions
D. directory restriction
Answer: (SHOW ANSWER)

NEW QUESTION: 418
Which of the following is related to physical security and is NOT considered a technical control?
A. Access control Mechanisms
B. Intrusion Detection Systems
C. Firewalls
D. Locks
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Locks are an example of a physical control type, not a technical control.
Controls are put into place to reduce the risk an organization faces, and they come in three main flavors:
administrative, technical, and physical. Administrative controls are commonly referred to as "soft controls" because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.
Incorrect Answers:
A: Access control Mechanisms are an example of a technical control. Therefore, this answer is incorrect.
B: Intrusion Detection Systems are an example of a technical control. Therefore, this answer is incorrect.
C: Firewalls are an example of a technical control. Therefore, this answer is incorrect.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 28

NEW QUESTION: 419
Which of the following is less likely to be included in the change control sub-phase of the maintenance phase of a software product?
A. Estimating the cost of the changes requested
B. Recreating and analyzing the problem
C. Determining the interface that is presented to the user
D. Establishing the priorities of requests

Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
To determine the user interface would not be part of the change control phase. This would be done in an earlier phase.
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 vulnerability, 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.
Incorrect Answers:
A: Calculation the cost of the change should be a part of analyzing a change request.
B: Testing is a part of change control. If a problem occurs during testing change control should recreate and analyze the problem.
D: If there are multiple change requests then they must be prioritized in the change control phase.
References:
Conrad, Eric, Seth Misenar and Joshua Feldman, CISSP Study Guide, 2nd Edition, Syngress, Waltham,
2012, p. 1122

NEW QUESTION: 420
Which of the following answers best describes the type of penetration testing where the analyst has full knowledge of the network on which he is going to perform his test?
A. White-Box Penetration Testing
B. Black-Box Pen Testing
C. Penetration Testing
D. Gray-Box Pen Testing
Answer: (SHOW ANSWER)
In general there are three ways a pen tester can test a target system.
-White-Box: The tester has full access and is testing from inside the system.
-Gray-Box: The tester has some knowledge of the system he's testing.
-Black-Box: The tester has no knowledge of the system.
Each of these forms of testing has different benefits and can test different aspects of the system from different approaches.
The following answers are incorrect:
-Black-Box Pen Testing: This is where no prior knowledge is given about the target network. Only a domain name or business name may be given to the analyst.
-Penetration Testing: This is half correct but more specifically it is white-box testing because the tester has full access.
-Gray-Box Pen Testing: This answer is not right because Gray-Box testing you are given a little information about the target network.

The following reference(s) was used to create this question: 2013. Official Security+ Curriculum. and tester is provided no information about the target's network or environment. The tester is simply left to his abilities Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 4742-4743). Auerbach Publications. Kindle Edition.

NEW QUESTION: 421
Which of the following is NOT true about IPSec Tunnel mode?
A. Fundamentally an IP tunnel with encryption and authentication
B. Works at the Transport layer of the OSI model
C. Have two sets of IP headers
D. Established for gateway service
Answer: (SHOW ANSWER)
IPSec can be run in either tunnel mode or transport mode. Each of these modes has
its own particular uses and care should be taken to ensure that the correct one is selected for the solution:
Tunnel mode is most commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it.
Transport mode is used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host-for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination.
As Figure 1 shows, basically transport mode should be used for end-to-end sessions and tunnel mode should be used for everything else. (Refer to the figure for the following discussion.)
Figure 1 Tunnel and transport modes in IPSec.
Figure 1 displays some examples of when to use tunnel versus transport mode:
Tunnel mode is most commonly used to encrypt traffic between secure IPSec gateways, such as between the Cisco router and PIX Firewall (as shown in example A in Figure 1). The IPSec gateways proxy IPSec for the devices behind them, such as Alice's PC and the HR servers in Figure 1. In example A, Alice connects to the HR servers securely through the IPSec tunnel set up
between the gateways.
Tunnel mode is also used to connect an end-station running IPSec software, such as the Cisco Secure VPN Client, to an IPSec gateway, as shown in example B.
In example C, tunnel mode is used to set up an IPSec tunnel between the Cisco router and a server running IPSec software. Note that Cisco IOS software and the PIX Firewall sets tunnel mode as the default IPSec mode.
Transport mode is used between end-stations supporting IPSec, or between an end-station and a gateway, if the gateway is being treated as a host. In example D, transport mode is used to set up an encrypted Telnet session from Alice's PC running Cisco Secure VPN Client software to terminate at the PIX Firewall, enabling Alice to remotely configure the PIX Firewall securely.
AH Tunnel Versus Transport Mode

Figure 2 shows the differences that the IPSec mode makes to AH. In transport mode, AH services protect the external IP header along with the data payload. AH services protect all the fields in the header that don't change in transport. The header goes after the IP header and before the ESP header, if present, and other higher-layer protocols.

In tunnel mode, the entire original header is authenticated, a new IP header is built, and the new IP header is protected in the same way as the IP header in transport mode.

Figure 2 AH tunnel versus transport mode.

AH is incompatible with Network Address Translation (NAT) because NAT changes the source IP address, which breaks the AH header and causes the packets to be rejected by the IPSec peer.

ESP Tunnel Versus Transport Mode

Figure 3 shows the differences that the IPSec mode makes to ESP. In transport mode, the IP payload is encrypted and the original headers are left intact. The ESP header is inserted after the IP header and before the upper-layer protocol header. The upper-layer protocols are encrypted and authenticated along with the ESP header. ESP doesn't authenticate the IP header itself.

NOTE

Higher-layer information is not available because it's part of the encrypted payload.

When ESP is used in tunnel mode, the original IP header is well protected because the entire original IP datagram is encrypted. With an ESP authentication mechanism, the original IP datagram and the ESP header are included; however, the new IP header is not included in the authentication.

When both authentication and encryption are selected, encryption is performed first, before authentication. One reason for this order of processing is that it facilitates rapid detection and rejection of replayed or bogus packets by the receiving node. Prior to decrypting the packet, the receiver can detect the problem and potentially reduce the impact of denial-of-service attacks.

Figure 3 ESP tunnel versus transport mode.

ESP can also provide packet authentication with an optional field for authentication. Cisco IOS software and the PIX Firewall refer to this service as ESP hashed message authentication code (HMAC). Authentication is calculated after the encryption is done. The current IPSec standard specifies SHA-1 and MD5 as the mandatory HMAC algorithms.

The main difference between the authentication provided by ESP and AH is the extent of the coverage. Specifically, ESP doesn't protect any IP header fields unless those fields are encapsulated by ESP (tunnel mode). Figure 4 illustrates the fields protected by ESP HMAC.

Figure 4 ESP encryption with a keyed HMAC.

IPSec Transforms

An IPSec transform specifies a single IPSec security protocol (either AH or ESP) with its corresponding security algorithms and mode. Example transforms include the following:

The AH protocol with the HMAC with MD5 authentication algorithm in tunnel mode is used for authentication.

The ESP protocol with the triple DES (3DES) encryption algorithm in transport mode is used for confidentiality of data.

The ESP protocol with the 56-bit DES encryption algorithm and the HMAC with SHA-1

authentication algorithm in tunnel mode is used for authentication and confidentiality.
Transform Sets
A transform set is a combination of individual IPSec transforms designed to enact a specific security policy for traffic. During the ISAKMP IPSec security association negotiation that occurs in IKE phase 2 quick mode, the peers agree to use a particular transform set for protecting a particular data flow. Transform sets combine the following IPSec factors:
Mechanism for payload authentication-AH transform
Mechanism for payload encryption-ESP transform
IPSec mode (transport versus tunnel)
Transform sets equal a combination of an AH transform, plus an ESP transform, plus the IPSec mode (either tunnel or transport mode).
This brings us to the end of the second part of this five-part series of articles covering IPSec. Be sure to catch the next installment.
Cisco Press at: http://www.ciscopress.com/articles/printerfriendly.asp?p=25477
and
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Pages 166-167.

NEW QUESTION: 422
In addition to the accuracy of the biometric systems, there are other factors that must also be considered:
A. These factors include the enrollment time and the throughput rate, but not acceptability.
B. These factors do not include the enrollment time, the throughput rate, and acceptability.
C. These factors include the enrollment time, the throughput rate, and acceptability.
D. These factors include the enrollment time, but not the throughput rate, neither the acceptability.
Answer: C (LEAVE A REPLY)
In addition to the accuracy of the biometric systems, there are OTHER factors that must also be considered. These factors include the enrollment time, the throughput rate, and acceptability. - Ronald Krutz The CISSP PREP Guide (gold edition) pg 51

NEW QUESTION: 423
What is the three way handshake sequence used to initiate TCP connections?
A. ACK, SYN/ACK, ACK

B. SYN, SYN/ACK, ACK
C. SYN, SYN, ACK/ACK
D. ACK, SYN/ACK, SYN
Answer: B (LEAVE A REPLY)
The TCP three way handshake:
1 . First, the client sends a SYN segment. This is a request to the server to synchronize the sequence numbers. It specifies its initial sequence number (ISN), which is incremented by 1 , and that is sent to the server. To initialize a connection, the client and server must synchronize each other's sequence numbers.
2 . Second, the server sends an ACK and a SYN in order to acknowledge the request of the client for synchronization. At the same time, the server is also sending its request to the client for synchronization of its sequence numbers. There is one major difference in this transmission from the first one. The server transmits an acknowledgement number to the client. The acknowledgement is just proof to the client that the ACK is specific to the SYN the client initiated. The process of acknowledging the client's request allows the server to increment the client's sequence number by one and uses it as its acknowledgement number.
3. Third, the client sends an ACK in order to acknowledge the request from the server for synchronization. The client uses the same algorithm the server implemented in providing an acknowledgement number. The client's acknowledgment of the server's request for synchronization completes the process of establishing a reliable connection.
The following answers are incorrect:
All of the other choices were incorrect answers
The following reference(s) were/was used to create this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 5560-5573). Auerbach Publications. Kindle Edition.

NEW QUESTION: 424
Management can expect penetration tests to provide all of the following EXCEPT
A. identification of security flaws
B. demonstration of the effects of the flaws
C. a method to correct the security flaws.
D. verification of the levels of existing infiltration resistance
Answer: (SHOW ANSWER)
Not B: It is not the objective of the pen tester to supply a method on how to correct the flaws. In fact management may decide to accept the risk and not repair the flaw. They may be able to demonstrate the effects of a flaw - especially if they manage to clobber a system!
Penetration testing is a set of procedures designed to test and possibly bypass security controls of a system. Its goal is to measure an organization's resistance to an attack and to uncover any weaknesses within the environment...The result of a penetration test is a report given to management describing the list of vulnerabilities that were identified and the severity of those

vulnerabilities. From here, it is up to management to determine how the vulnerabilities are dealt with and what countermeasures are implemented. - Shon Harris All-in-one CISSP Certification Guide pg 837-839

NEW QUESTION: 425
What is the second phase of Public Key Infrastructure (PKI) key/certificate life-cycle management?
A. Implementation Phase
B. Initialization Phase
C. Cancellation Phase
D. Issued Phase
Answer: D (LEAVE A REPLY)
Section: Security Architecture and Engineering
Explanation/Reference:

NEW QUESTION: 426
Attributable data should be:
A. always traced to individuals responsible for observing and recording the data
B. sometimes traced to individuals responsible for observing and recording the data
C. never traced to individuals responsible for observing and recording the data
D. often traced to individuals responsible for observing and recording the data
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
As per FDA data should be attributable, original, accurate, contemporaneous and legible.
In an automated system attributability could be achieved by a computer system designed to identify individuals responsible for any input.
References: U.S. Department of Health and Human Services, Food and Drug Administration, Guidance for Industry - Computerized Systems Used in Clinical Trials, April 1999, page 1.

NEW QUESTION: 427
Which SERVICE usually runs on port 25?
A. File Transfer Protocol (FTP)
B. Telnet
C. Simple Mail Transfer Protocol (SMTP)
D. Domain Name Service (DNS)
Answer: (SHOW ANSWER)
FTP - Port 21
Telnet - Port 23
SMTP - Port 25
DNS - Port 53

The port numbers are divided into three ranges: the Well Known Ports, the Registered Ports, and
the Dynamic and/or Private Ports.
The Well Known Ports are those from 0 through 1023.
The Registered Ports are those from 1024 through 49151.
The Dynamic and/or Private Ports are those from 49152 through 65535.
Reference : http://www.iana.org/assignments/port-numbers
For the purpose of the exam you DO NOT need to know all of the 65,535 ports but you must know the one that are very commonly used.

NEW QUESTION: 428
To what does 10Base-5 refer?
A. 100 Mbps unshielded twisted pair cabling
B. 10 Mbps thinnet coax cabling rated to 185 meters maximum length
C. 10 Mbps thicknet coax cabling rated to 500 meters maximum length
D. 10 Mbps baseband optical fiber
Answer: C (LEAVE A REPLY)
The correct answer is "10 Mbps thicknet coax cabling rated to 500 meters maximum length".
Answer "10 Mbps thinnet coax cabling rated to 185 meters maximum length" refers to 10Base-2.
10 Mbps baseband optical fiber refers to 10Base-F.
100 Mbps unshielded twisted pair cabling to 100Base-T.

NEW QUESTION: 429
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: 430
Which of the following questions is less likely to help in assessing controls over hardware and software maintenance?
A. Is access to all program libraries restricted and controlled?
B. Are integrity verification programs used by applications to look for evidences of data tampering, errors, and omissions?
C. Is there version control?
D. Are system components tested, documented, and approved prior to promotion to production?
Answer: (SHOW ANSWER)
Hardware and software maintenance access controls are used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a historical record of changes is maintained. Integrity verification programs are more integrity controls than software maintenance controls. Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Pages A-30 to A-32).

NEW QUESTION: 431
Which LAN transmission method below describes a packet sent from a
single source to multiple specific destinations?
A. Multicast
B. Unicast
C. Anycast
D. Broadcast

Answer: (SHOW ANSWER)
The correct answer is multicast.
Unicast describes a packet sent from a single source to a single destination.
Broadcast describes a packet sent to all nodes on the network segment.
Anycast, refers to communication between any sender and the nearest of a group of receivers in a
network.

NEW QUESTION: 432
A one-way hash provides which of the following?
A. Confidentiality
B. Availability
C. Integrity
D. Authentication
Answer: (SHOW ANSWER)
A one-way hash is a function that takes a variable-length string a message, and compresses and transforms it into a fixed length value referred to as a hash value. It provides integrity, but no confidentiality, availability or authentication. Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 5).

NEW QUESTION: 433
Which of the following biometric devices offers the LOWEST CER?
A. Keystroke dynamics
B. Voice verification
C. Iris scan
D. Fingerprint
Answer: C (LEAVE A REPLY)
From most effective (lowest CER) to least effective (highest CER) are:
Iris scan, fingerprint, voice verification, keystroke dynamics.
Reference : Shon Harris Aio v3 , Chapter-4 : Access Control , Page : 131
Also see: http://www.sans.org/reading_room/whitepapers/authentication/biometric- selection-body-parts-online_139

NEW QUESTION: 434
Which of the following server contingency solutions offers the highest availability?
A. System backups
B. Electronic vaulting/remote journaling
C. Redundant arrays of independent disks (RAID)
D. Load balancing/disk replication
Answer: (SHOW ANSWER)
Explanation/Reference:

Explanation:
With load balancing, often through clustering, each system takes a part of the processing load, and if one system fails there is an automatic failover to the other systems which continue to work. This guarantees a high availability of the service.
Incorrect Answers:
A: Systems backups only protects against data loss. It does not product a failure of server.
B: Electronic vaulting and remote journaling are transaction redundancy solutions. It protect the system by copying transaction information to a remote location. In case of server failure the database can be restored, but it would require a rebuild of the database.
C: RAID protects against a hard disk failures, but it does not protect against other type of server failures.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 1272

NEW QUESTION: 435
DESX is a variant of DES in which:
A. The output of DES is bitwise XORed with 64 bits of key material.
B. Input plaintext is bitwise XORed with 64 bits of additional key material before encryption with DES, and the output of DES is also bitwise XORed with another 64 bits of key material.
C. The input plaintext is encrypted X times with the DES algorithm using different keys for each encryption.
D. Input plaintext is bitwise XORed with 64 bits of additional key material before encryption with DES.
Answer: B (LEAVE A REPLY)
DESX was developed by Ron Rivest to increase the resistance of DES to brute force key search attacks; however, the resistance of DESX to differential and linear attacks is equivalent to that of DES with independent subkeys.

NEW QUESTION: 436
Which of the following is the MOST effective method of mitigating data theft from an active user workstation?
A. Enable multifactor authentication
B. Implement full-disk encryption
C. Disable use of portable devices
D. Deploy file integrity checkers
Answer: C (LEAVE A REPLY)

NEW QUESTION: 437
Which of the following is defined as 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?
A. Internet Key exchange (IKE)
B. Security Association Authentication Protocol (SAAP)
C. Simple Key-management for Internet Protocols (SKIP)
D. Key Exchange Algorithm (KEA)
Answer: A (LEAVE A REPLY)
RFC 2828 (Internet Security Glossary) defines IKE as 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.
The following are incorrect answers:
SKIP is a key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.
The Key Exchange Algorithm (KEA) is defined as a key agreement algorithm that is similar to the Diffie-Hellman algorithm, uses 1024-bit asymmetric keys, and was developed and formerly classified at the secret level by the NSA.
Security Association Authentication Protocol (SAAP) is a distracter.
Reference(s) used for this question:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 438
Which of the following value comparisons MOST accurately reflects the agile development approach?
A. Contract negotiation over customer collaboration
B. Processes and toots over individuals and interactions
C. Following a plan over responding to change
D. Working software over comprehensive documentation
Answer: (SHOW ANSWER)

NEW QUESTION: 439
The standard server port number for HTTP is which of the following?
A. 81
B. 80
C. 8080

D. 8180
Answer: B (LEAVE A REPLY)
HTTP is Port 80.
Reference: MAIWALD, Eric, Network Security: A Beginner's Guide, McGraw-Hill/Osborne Media, 2001, page 135.

NEW QUESTION: 440
Which of the following embodies all the detailed actions that personnel are required to follow?
A. Standards
B. Guidelines
C. Procedures
D. Baselines
Answer: C (LEAVE A REPLY)
Procedures are step-by-step instructions in support of of the policies, standards, guidelines and baselines. The procedure indicates how the policy will be implemented and who does what to accomplish the tasks."
Standards is incorrect. Standards are a "Mandatory statement of minimum requirements that support some part of a policy, the standards in this case is your own company standards and not standards such as the ISO standards"
Guidelines is incorrect. "Guidelines are discretionary or optional controls used to enable individuals to make judgments with respect to security actions."
Baselines is incorrect. Baselines "are a minimum acceptable level of security. This minimum is implemented using specific rules necessary to implement the security controls in support of the policy and standards." For example, requiring a password of at leat 8 character would be an example. Requiring all users to have a minimum of an antivirus, a personal firewall, and an anti spyware tool could be another example.
References:
CBK, pp. 12 - 16. Note especially the discussion of the "hammer policy" on pp. 16-17 for the differences between policy, standard, guideline and procedure.
AIO3, pp. 88-93.

NEW QUESTION: 441
The core component of Role Based Access control (RBAC) must be constructed of defined data elements, Which elements are required?
A. Users, rotes, operations, and protected objects
B. Users, permissions, operators, and protected objects
C. Roles, operations, accounts, and protected objects
D. Roles, accounts, permissions, and protected objects
Answer: (SHOW ANSWER)

NEW QUESTION: 442

What is the foundation of cryptographic functions?
A. Encryption
B. Cipher
C. Hash
D. Entropy
Answer: A (LEAVE A REPLY)
Section: Security Architecture and Engineering

NEW QUESTION: 443
Which of the following is NOT a characteristic of a client in the client/server model?
A. May be diskless
B. Systems backup and database protection
C. Extensive user interface
D. Data entry screens
Answer: B (LEAVE A REPLY)
In the client/server model, the server is the data storage resource and is responsible for data backups and protection/maintenance of the database.
Answer "May be diskless" refers to a diskless workstation or PC at the client side. By not providing local data storage capabilities at the client side, security is increased since the data is less vulnerable at a protected server location.
Also, because the client is the users path into the network, the client must have extensive, user friendly interfaces such as described in answers Extensive user interface and Data entry screens.

NEW QUESTION: 444
Which of the following is an example of discretionary access control?
A. Identity-based access control
B. Task-based access control
C. Role-based access control
D. Rule-based access control
Answer: A (LEAVE A REPLY)
An identity-based access control is an example of discretionary access control that is based on an individual's identity. Identity-based access control (IBAC) is access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity.
Rule Based Access Control (RuBAC) and Role Based Access Control (RBAC) are examples of non-discretionary access controls.
Rule-based access control is a type of non-discretionary access control because this access is determined by rules and the subject does not decide what those rules will be, the rules are uniformly applied to ALL of the users or subjects.

In general, all access control policies other than DAC are grouped in the category of non-discretionary access control (NDAC). As the name implies, policies in this category have rules that are not established at the discretion of the user. Non-discretionary policies establish controls that cannot be changed by users, but only through administrative action.
Both Role Based Access Control (RBAC) and Rule Based Access Control (RuBAC) fall within Non Discretionary Access Control (NDAC). If it is not DAC or MAC then it is most likely NDAC.
BELOW YOU HAVE A DESCRIPTION OF THE DIFFERENT CATEGORIES:
MAC = Mandatory Access Control
Under a mandatory access control environment, the system or security administrator will define what permissions subjects have on objects. The administrator does not dictate user's access but simply configure the proper level of access as dictated by the Data
Owner.
The MAC system will look at the Security Clearance of the subject and compare it with the object sensitivity level or classification level. This is what is called the dominance relationship.
The subject must DOMINATE the object sensitivity level. Which means that the subject must have a security clearance equal or higher than the object he is attempting to access.
MAC also introduce the concept of labels. Every objects will have a label attached to them indicating the classification of the object as well as categories that are used to impose the need to know (NTK) principle. Even thou a user has a security clearance of Secret it does not mean he would be able to access any Secret documents within the system. He would be allowed to access only Secret document for which he has a Need To Know, formal approval, and object where the user belong to one of the categories attached to the object.
If there is no clearance and no labels then IT IS NOT Mandatory Access Control.
Many of the other models can mimic MAC but none of them have labels and a dominance relationship so they are NOT in the MAC category.
DAC = Discretionary Access Control
DAC is also known as: Identity Based access control system.
The owner of an object is define as the person who created the object. As such the owner has the discretion to grant access to other users on the network. Access will be granted based solely on the identity of those users.
Such system is good for low level of security. One of the major problem is the fact that a user who has access to someone's else file can further share the file with other users without the knowledge or permission of the owner of the file. Very quickly this could become the wild wild west as there is no control on the dissimination of the information.
RBAC = Role Based Access Control
RBAC is a form of Non-Discretionary access control.
Role Based access control usually maps directly with the different types of jobs performed by employees within a company.
For example there might be 5 security administrator within your company. Instead of creating each of their profile one by one, you would simply create a role and assign the administrators to the role. Once an administrator has been assigned to a role, he will

IMPLICITLY inherit the permissions of that role.
RBAC is great tool for environment where there is a a large rotation of employees on a daily basis such as a very large help desk for example.
RBAC or RuBAC = Rule Based Access Control
RuBAC is a form of Non-Discretionary access control.
A good example of a Rule Based access control device would be a Firewall. A single set of rules is imposed to all users attempting to connect through the firewall.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33
and
NISTIR-7316 at http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316pdf and http://itlaw.wikia.com/wiki/Identity-based_access_control

NEW QUESTION: 445
The Biba model axiom An object at one level of integrity is not permitted to modify (write to) an object of a higher level of integrity (no write up) is called:
A. The Constrained Integrity Axiom
B. The Discretionary Integrity Axiom
C. The Simple Integrity Axiom
D. The * (star) Integrity Axiom
Answer: D (LEAVE A REPLY)
The correct answer is "The * (star) Integrity Axiom".
Answers a and d are distracters. Answer the Simple Integrity Axiom states, Asubject at one level of integrity is not permitted to observe (read) an object of lower integrity (no read down).

NEW QUESTION: 446
Three things that must be considered for the planning and implementation of access control mechanisms are:
A. Threats, assets, and objectives.
B. Threats, vulnerabilities, and risks.
C. Vulnerabilities, secret keys, and exposures.
D. Exposures, threats, and countermeasures.
Answer: B (LEAVE A REPLY)
The correct answer is "Threats, vulnerabilities, and risks". Threats define the possible source of security policy violations; vulnerabilities describe weaknesses in the system that might be exploited by the threats; and the risk determines the
probability of threats being realized. All three items must be present to meaningfully apply access control. Therefore, the other answers are incorrect.

NEW QUESTION: 447

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: (SHOW ANSWER)

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: 448
Passwords can be required to change monthly, quarterly, or any other intervals:
A. depending on the criticality of the information needing protection
B. not depending on the criticality of the information needing protection but depending on the password's frequency of use
C. depending on the criticality of the information needing protection and the password's frequency of use
D. depending on the password's frequency of use
Answer: C (LEAVE A REPLY)

NEW QUESTION: 449
Which of the following needs to be taken into account when assessing vulnerability?

A. Safeguard selection
B. Risk acceptance criteria
C. Threat mapping
D. Risk identification and validation
Answer: (SHOW ANSWER)

NEW QUESTION: 450
Computer-generated evidence is considered:
A. Best evidence
B. Second hand evidence
C. Demonstrative evidence
D. Direct evidence
Answer: B (LEAVE A REPLY)
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: 451
Which of the following control is intended to discourage a potential attacker?
A. Deterrent
B. Preventive
C. Corrective
D. Recovery
Answer: (SHOW ANSWER)
Deterrent Control are intended to discourage a potential attacker For your exam you should know below information about different security controls
Deterrent Controls Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with

the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions. The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events. When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers.

Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work

on the theory that it is easier to obey the control

rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is
damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use
of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective
device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to
correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must
work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management.

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy

requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.
The following answers are incorrect:
Preventive - Preventive controls are intended to avoid an incident from occurring
Corrective - Corrective control fixes components or systems after an incident has occurred
Recovery - Recovery controls are intended to bring the environment back to regular operations
The following reference(s) were/was used to create this question:
CISA Review Manual 2014 Page number 44 and Official ISC2 CISSP guide 3rd edition Page number 50 and 51

NEW QUESTION: 452
Which statement below is accurate about the reasons to implement a layered security architecture?
A. A layered approach doesn't really improve the security posture of the organization.
B. A layered security approach is intended to increase the work-factor for an attacker.
C. A good packet-filtering router will eliminate the need to implement a layered security architecture.
D. A layered security approach is not necessary when using COTS products.
Answer: (SHOW ANSWER)
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. The need for layered protections is important when commercialoff-the-shelf (COTS) products are used. The current state-of-the-art for security quality in COTS products do not provide a high degree of protection against sophisticated attacks. It is possible to help mitigate this situation by placing several controls in levels, requiring additional work by attackers to accomplish their goals.

Source: NIST Special Publication 800-27, Engineering Principles for Infor- mation Technology Security (A Baseline for Achieving Security).

NEW QUESTION: 453
There are some correlations between relational data base terminology and object-oriented database terminology. Which of the following relational model terms, respectively, correspond to the object model terms of class, attribute and instance object?
A. Relation, column, and tuple
B. Relation, domain, and column
C. Domain, relation, and column
D. Relation, tuple, and column
Answer: A (LEAVE A REPLY)
Table shows the correspondence between the two models. In comparing the two models, a class is similar to a relation; however, a relation does not have the inheritance property of a class. An attribute in the object model is similar to the column of a relational table. The column has limitations on the data types it can hold while an attribute in the object model can use all data types that are supported by the Java and C++ languages. An instance object in the object model corresponds to a tuple in the relational model. Again

Object and Relational Model Correspondence

OBJECT MODEL	RELATIONAL MODEL
CLASS	RELATION
ATTRIBUTE	COLUMN
INSTANCE OBJECT	TUPLE

the data structures of the tuple are limited while those of the instance object can use data structures of Java and C++.

NEW QUESTION: 454
Which of the following BEST represents the concept of least privilege?
A. Access to an object is only available to the owner.
B. Access to an object is denied unless access is specifically allowed.
C. Access to an object is allowed unless it is protected by the information security policy.
D. Access to an object is only allowed to authenticated users via an Access Control List (ACL).
Answer: B (LEAVE A REPLY)

NEW QUESTION: 455
Which of the following could be considered the MOST significant security challenge when adopting DevOps practices compared to a more traditional control framework?

A. Achieving Service Level Agreements (SLA) on how quickly patches will be released when a security flaw is found.
B. Maintaining segregation of duties.
C. Standardized configurations for logging, alerting, and security metrics.
D. Availability of security teams at the end of design process to perform last-minute manual audits and reviews.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 456
Which of the following is used to create parity information?
A. a hamming code
B. a clustering code
C. a mirroring code
D. a striping code
Answer: A (LEAVE A REPLY)
RAID Level 2 :- The parity information is created using a hamming code that detects errors and establishes which part of which drive is in error.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 66.

NEW QUESTION: 457
Which of the following is NOT an example of a detective control?
A. System Monitor
B. IDS
C. Monitor detector
D. Backup data restore
Answer: D (LEAVE A REPLY)
The word NOT is used as a keyword in the question. You need to find out a security control from an given options which in not detective control. Backup data restore is a corrective control and not a detective control.
For your exam you should know below information about different security controls
Deterrent Controls Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight

for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions. The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events. When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs. It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk. For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement. Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk. As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is

damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system. This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management. Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install. Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

For your exam you should know below information about different security controls

Deterrent Controls Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events.
When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.
It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.
Preventative Controls Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.
Compensating Controls Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.
For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.
Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.
Detective Controls Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.
As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform

once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.
This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.
Corrective Controls When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.
Recovery Controls Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management.
Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.
Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy
requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.
The following answers are incorrect:
The other examples are belongs to detective control.
The following reference(s) were/was used to create this question:
CISA Review Manual 2014 Page number 44
and
Official ISC2 CISSP guide 3rd edition Page number 50 and 51

NEW QUESTION: 458
Risk mitigation and risk reduction controls for providing information security are classified within three main categories, which of the following are being used?

A. preventive, corrective, and administrative
B. detective, corrective, and physical
C. Physical, technical, and administrative
D. Administrative, operational, and logical
Answer: C (LEAVE A REPLY)
Security is generally defined as the freedom from danger or as the condition of safety. Computer security, specifically, is the protection of data in a system against unauthorized disclosure, modification, or destruction and protection of the computer system itself against unauthorized use, modification, or denial of service. Because certain computer security controls inhibit productivity, security is typically a compromise toward which security practitioners, system users, and system operations and administrative personnel work to achieve a satisfactory balance between security and productivity.
Controls for providing information security can be physical, technical, or administrative. These three categories of controls can be further classified as either preventive or detective. Preventive controls attempt to avoid the occurrence of unwanted events, whereas detective controls attempt to identify unwanted events after they have occurred. Preventive controls inhibit the free use of computing resources and therefore can be applied only to the degree that the users are willing to accept. Effective security awareness programs can help increase users' level of tolerance for preventive controls by helping them understand how such controls enable them to trust their computing systems. Common detective controls include audit trails, intrusion detection methods, and checksums.
Three other types of controls supplement preventive and detective controls. They are usually described as deterrent, corrective, and recovery. Deterrent controls are intended to discourage individuals from intentionally violating information security policies or procedures. These usually take the form of constraints that make it difficult or undesirable to perform unauthorized activities or threats of consequences that influence a potential intruder to not violate security (e.g., threats ranging from embarrassment to severe punishment).
Corrective controls either remedy the circumstances that allowed the unauthorized activity or return conditions to what they were before the violation. Execution of corrective controls could result in changes to existing physical, technical, and administrative controls. Recovery controls restore lost computing resources or capabilities and help the organization recover monetary losses caused by a security violation.
Deterrent, corrective, and recovery controls are considered to be special cases within the major categories of physical, technical, and administrative controls; they do not clearly belong in either preventive or detective categories. For example, it could be argued that deterrence is a form of prevention because it can cause an intruder to turn away; however, deterrence also involves detecting violations, which may be what the intruder fears most. Corrective controls, on the other hand, are not preventive or detective, but they are clearly linked with technical controls when antiviral software eradicates a virus or with administrative controls when backup procedures enable restoring a damaged data base. Finally, recovery controls are neither preventive nor detective but are included in administrative controls as disaster recovery or contingency plans.

Reference(s) used for this question
Handbook of Information Security Management, Hal Tipton,

NEW QUESTION: 459
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: 460
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)
Explanation/Reference:
Explanation:
A zero-day is an undisclosed computer application vulnerability that could be misused to harmfully affect the computer programs, data, additional computers or a network.
Incorrect Answers:

B: An exploit refers to a piece of software or data, or a sequence of commands that takes advantage of a bug or vulnerability with the aim of causing unplanned or unexpected behavior to take place on computerized hardware, or its software.
C: A vulnerability is a weakness which allows an attacker to reduce a system's information assurance.
D: Software cracking is the modification of software to get rid of or deactivate features that are considered undesirable by the person cracking the software.
References:
https://en.wikipedia.org/wiki/Zero_day_attack
https://en.wikipedia.org/wiki/Exploit_%28computer_security%29
https://en.wikipedia.org/wiki/Vulnerability_(computing)
https://en.wikipedia.org/wiki/Software_cracking

NEW QUESTION: 461
Which of the following is an advantage of prototyping?
A. Prototype systems can provide significant time and cost savings.
B. Change control is often less complicated with prototype systems.
C. It ensures that functions or extras are not added to the intended system.
D. Strong internal controls are easier to implement.
Answer: A (LEAVE A REPLY)
Prototype systems can provide significant time and cost savings, however they also have several disadvantages. They often have poor internal controls, change control becomes much more complicated and it often leads to functions or extras being added to the system that were not originally intended. 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 306).

NEW QUESTION: 462
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: A (LEAVE A REPLY)
The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities. It does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-analysis of any recommended controls difficult. Since it involves a consensus of export and some guesswork based on the experience of Subject Matter Experts (SME's), it can not be easily automated.

Reference used for this question:
STONEBURNER, Gary et al., NIST Special publication 800-30, Risk management Guide for Information Technology Systems, 2001 (page 23).

NEW QUESTION: 463
The Physical Security domain focuses on three areas that are the basis to physically protecting enterprise's resources and sensitive information. Which of the following is not one of these areas?
A. Threats
B. Countermeasures
C. Vulnerabilities
D. Risks
Answer: B (LEAVE A REPLY)
Countermeasures are used to mitigate the risks, threats, and vulnerabilities and are not areas that are protected.
Security is very important to organizations and their infrastructures, and physical security is no exception. Physical security encompasses a different set of threats, vulnerabilities, and risks than the other types of security that have been addressed so far.
Physical security mechanisms include site design and layout, environmental components, emergency response readiness, training, access control, intrusion detection, and power andfire protection. Physical security mechanisms protect people, data, equipment, systems, facilities, and a long list of company assets.

NEW QUESTION: 464
Which is the MAIN advantage of having an application gateway?
A. To perform change control procedures for applications.
B. To provide a means for applications to move into production.
C. To log and control incoming and outgoing traffic.
D. To audit and approve changes to applications.
Answer: (SHOW ANSWER)
"An application-level gateway firewall is also called a proxy firewall. A proxy is a mechanism that copies packets from one network into another; the copy process also changes the source and destination address to protect the identity of the internal or private network. An application-level gateway firewall filters traffic based on the Internet service (i.e., application) used to transmit or receive the data." - Shon Harris All-in-one CISSP Certification Guide pg 92

NEW QUESTION: 465
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: (SHOW ANSWER)

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.