ISC.SSCP.v2023-03-16.q410

Exam Code:	SSCP
Exam Name:	System Security Certified Practitioner (SSCP)
Certification Provider:	ISC
Free Question Number:	410
Version:	v2023-03-16
# of views:	489
# of Questions views:	24882
https://www.freecram.net/torrent/ISC.SSCP.v2023-03-16.q410.html	

NEW QUESTION: 1
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: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
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: 2

What is called an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics?

A. Biometrics

B. Micrometrics

C. Macrometrics

D. MicroBiometrics

Answer: (SHOW ANSWER)

Biometrics; Biometrics are defined as an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 37,38.

NEW QUESTION: 3

Which device acting as a translator is used to connect two networks or applications from layer 4 up to layer 7 of the ISO/OSI Model?

A. Bridge

B. Repeater

C. Router

D. Gateway

Answer: (SHOW ANSWER)

A gateway is used to connect two networks using dissimilar protocols at the lower layers or it could also be at the highest level of the protocol stack.

Important Note:

For the purpose of the exam, you have to remember that a gateway is not synonymous to the term firewall.

The second thing you must remembers is the fact that a gateway act as a translation device.

It could be used to translate from IPX to TCP/IP for example. It could be used to convert different types of applications protocols and allow them to communicate together. A gateway could be at any of the OSI layers but usually tend to be higher up in the stack.

For your exam you should know the information below:

Repeaters

A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel. Repeaters can also work as line conditioners by actually cleaning up the signals. This works much better when amplifying digital signals than when amplifying analog signals, because digital signals are discrete units, which makes extraction of background noise from them much easier for the amplifier. If the device is amplifying analog signals, any accompanying noise often is amplified as well, which may further distort the signal. A hub is a multi-port repeater. A hub is often referred to as a concentrator because it is the physical

communication device that allows several computers and devices to communicate with each other. A hub does not understand or work with IP or MAC addresses. When one system sends a signal to go to another system connected to it, the signal is broadcast to all the ports, and thus to all the systems connected to the concentrator.

Repeater

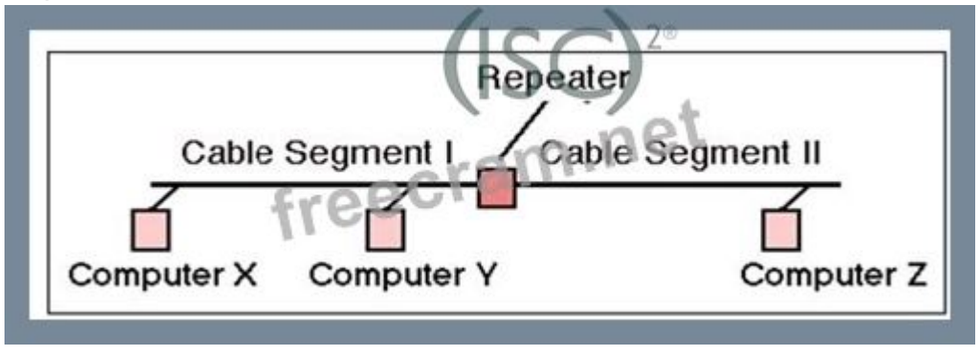


Image Reference- http://www.erg.abdn.ac.uk/~gorry/course/images/repeater.gif

Bridges A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.

Bridge C:\Users\MCS\Desktop\1.jpg

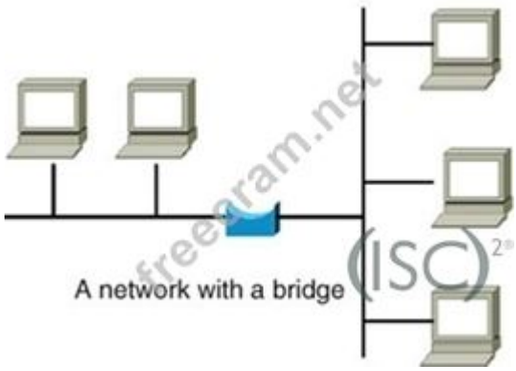


Image Reference- http://www.oreillynet.com/network/2001/01/30/graphics/bridge.jpg

Routers Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary. Because routers have more network-level knowledge, they can perform higher-level functions, such as calculating the shortest and most economical path between the sending and receiving hosts.

Router and Switch

Image Reference- http://www.computer-networking-success.com/images/router-switch.jpg
Switches Switches combine the functionality of a repeater and the functionality of a bridge. A switch amplifies the electrical signal, like a repeater, and has the built-in circuitry and intelligence of a bridge. It is a multi-port connection device that provides connections for individual computers or other hubs and switches.
Gateways Gateway is a general term for software running on a device that connects two different environments and that many times acts as a translator for them or somehow restricts their interactions. Usually a gateway is needed when one environment speaks a different language, meaning it uses a certain protocol that the other environment does not understand. The gateway can translate Internetwork Packet Exchange (IPX) protocol packets to IP packets, accept mail from one type of mail server and format it so another type of mail server can accept and understand it, or connect and translate different data link technologies such as FDDI to Ethernet.
Gateway Server C:\Users\MCS\Desktop\1.jpg

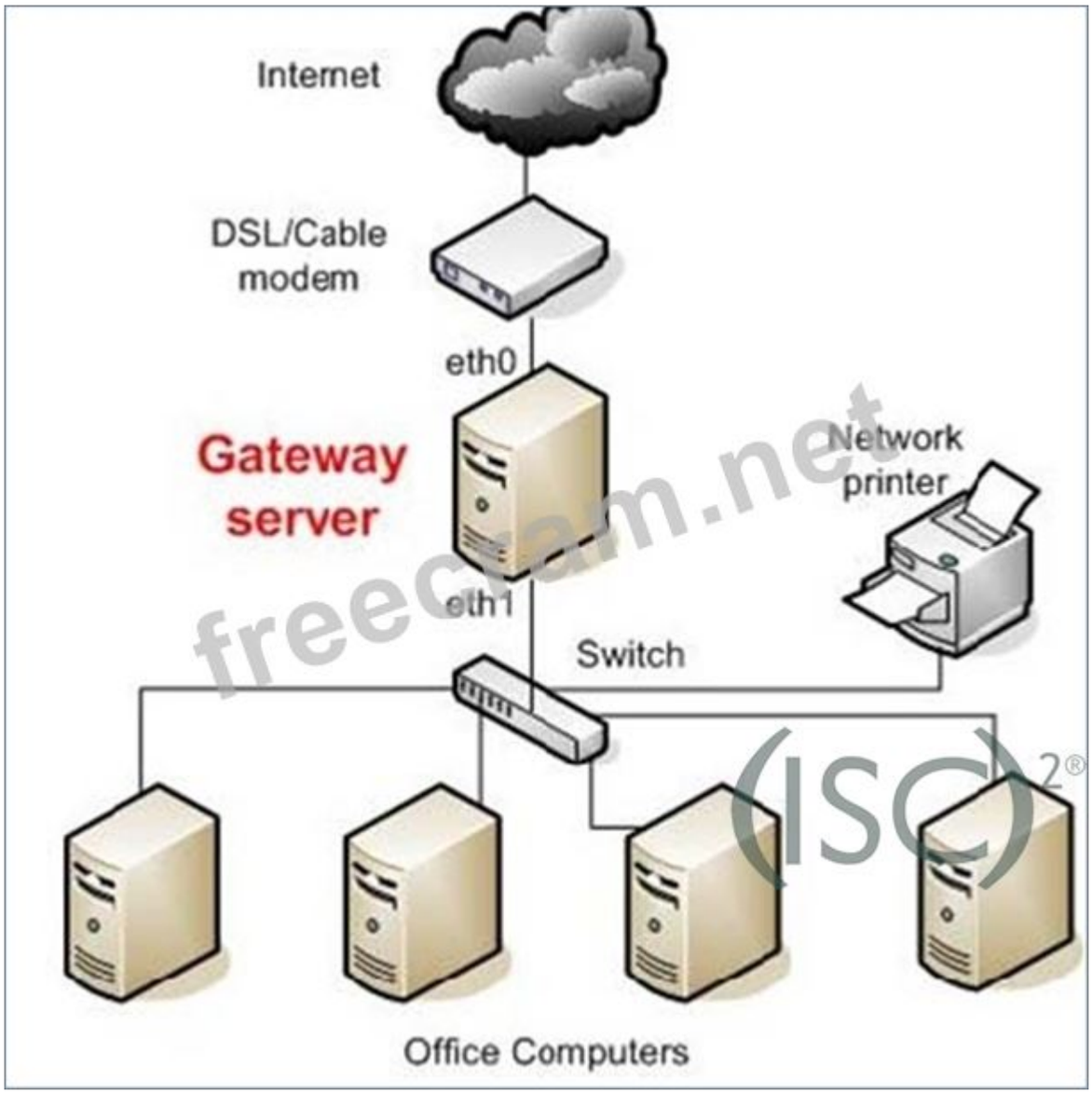


Image Referencehttp://static.howtoforge.com/images/screenshots/556af08d5e43aa768260f9e589dc547f3024.jpg
The following answers are incorrect:
Repeater - A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.
Bridges - A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.
Routers - Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to

their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary.
Following reference(s) were/was used to create this question: CISA review manual 2014 Page number 263 Official ISC2 guide to CISSP CBK 3rd Edition Page number 229 and 230

NEW QUESTION: 4
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: (SHOW ANSWER)
Section: Cryptography
Explanation/Reference:
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: 5
Which of the concepts best describes Availability in relation to computer resources?
A. None of the concepts describes Availability properly
B. Users can make authorized changes to data
C. Users can gain access to any resource upon request (assuming they have proper permissions)
D. Users can be assured that the data content has not been altered
Answer: (SHOW ANSWER)

NEW QUESTION: 6
What is the main problem of the renewal of a root CA certificate?
A. It requires key recovery of all end user keys
B. It requires the authentic distribution of the new root CA certificate to all PKI participants
C. It requires the collection of the old root CA certificates from all the users
D. It requires issuance of the new root CA certificate
Answer: (SHOW ANSWER)
Explanation/Reference:
The main task here is the authentic distribution of the new root CA certificate as new trust anchor to all the PKI participants (e.g. the users).
In some of the rollover-scenarios there is no automatic way, often explicit assignment of trust from each user is needed, which could be very costly.

Other methods make use of the old root CA certificate for automatic trust establishment (see PKIX-reference), but these solutions works only well for scenarios with currently valid root CA certificates (and not for emergency cases e.g. compromise of the current root CA certificate).
The rollover of the root CA certificate is a specific and delicate problem and therefore are often ignored during PKI deployment.
Reference: Camphausen, I.; Petersen, H.; Stark, C.: Konzepte zum Root CA Zertifikatswechsel, conference Enterprise Security 2002, March 26-27, 2002, Paderborn; RFC 2459 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

NEW QUESTION: 7
What is the main objective of proper separation of duties?
A. To prevent employees from disclosing sensitive information.
B. To ensure access controls are in place.
C. To ensure that no single individual can compromise a system.
D. To ensure that audit trails are not tampered with.
Answer: C (LEAVE A REPLY)
The primary objective of proper separation of duties is to ensure that one person acting alone cannot compromise the company's security in any way. A proper separation of duties does not prevent employees from disclosing information, nor does it ensure that access controls are in place or that audit trails are not tampered with. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 12: Operations Security (Page 808).

NEW QUESTION: 8
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)
Section: Network and Telecommunications
Explanation/Reference:
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: 9
What is called an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics?
A. Biometrics

B. Micrometrics
C. Macrometrics
D. MicroBiometrics
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
The Answer: Biometrics; Biometrics are defined as an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 37,38.

NEW QUESTION: 10
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: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
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: 11
Which xDSL flavour delivers both downstream and upstream speeds of 1.544 Mbps over two copper twisted pairs?
A. HDSL
B. SDSL
C. ADSL
D. VDSL
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
High-rate Digital Subscriber Line (HDSL) delivers 1.544 Mbps of bandwidth each way over two copper twisted pairs. SDSL also delivers 1.544 Mbps but over a single copper twisted pair. ADSL and VDSL offer a higher bandwidth downstream than upstream.
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
115).

NEW QUESTION: 12
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)
Explanation/Reference:
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: 13
A timely review of system access audit records would be an example of which of the basic security functions?

A. avoidance.
B. deterrence.
C. prevention.
D. detection.
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
By reviewing system logs you can detect events that have occured.
The following answers are incorrect:
avoidance. This is incorrect, avoidance is a distractor. By reviewing system logs you have not avoided anything.
deterrence. This is incorrect because system logs are a history of past events. You cannot deter something that has already occurred.
prevention. This is incorrect because system logs are a history of past events. You cannot prevent something that has already occurred.

NEW QUESTION: 14
Which of the following was developed as a simple mechanism for allowing simple network terminals to load their operating system from a server over the LAN?
A. DHCP
B. BootP
C. DNS
D. ARP
Answer: (SHOW ANSWER)
BootP was developed as a simple mechanism for allowing simple network terminals to load their operating system from a server over the LAN. Over time, it has expanded to allow centralized configuration of many aspects of a host's identity and behavior on the network. Note that DHCP, more complex, has replaced BootP over time. Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 4: Sockets and Services from a Security Viewpoint.

NEW QUESTION: 15
When gathering digital evidence it is very important to do the following: (Choose all that apply)
A. Shut down the compromised system to avoid further attacks
B. Reboot the victim system offline
C. Document the chain of evidence by taking good notes
D. Perform a bit-level back up of the data before analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Which of the following is an example of a connectionless communication protocol?
A. UDP

B. X.25
C. Packet switching
D. TCP
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
UDP is an example of connectionless communication protocol, wherein no connection needs to be established before data can be exchanged.
In telecommunications, connectionless describes communication between two network end points in which a message can be sent from one end point to another without prior arrangement. The device at one end of the communication transmits data addressed to the other, without first ensuring that the recipient is available and ready to receive the data. Some protocols allow for error correction by requested retransmission. Internet Protocol (IP) and User Datagram Protocol (UDP) are connectionless protocols.
Connectionless protocols are also described as stateless because the endpoints have no protocol-defined way to remember where they are in a "conversation" of message exchanges.
List of connectionless protocols
Hypertext Transfer Protocol
IP
UDP
ICMP
IPX
TIPC
NetBEUI
References:
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 86).
and
https://secure.wikimedia.org/wikipedia/en/wiki/Connectionless_protocol

NEW QUESTION: 17

MD5 is a _____ algorithm
A. PKI
B. 3DES
C. 192 bit
D. One way hash
Answer: D (LEAVE A REPLY)

NEW QUESTION: 18
In discretionary access environments, which of the following entities is authorized to grant information access to other people?
A. Manager
B. Group Leader
C. Security Manager
D. Data Owner
Answer: (SHOW ANSWER)
Explanation/Reference:
In Discretionary Access Control (DAC) environments, the user who creates a file is also considered the owner and has full control over the file including the ability to set permissions for that file.
The following answers are incorrect:
manager. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.
group leader. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/ user that is authorized to grant information access to other people.
security manager. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.
IMPORTANT NOTE:
The term Data Owner is also used within Classifications as well. Under the subject of classification the Data Owner is a person from management who has been entrusted with a data set that belongs to the company. For example it could be the Chief Financial Officer (CFO) who is entrusted with all of the financial data for a company. As such the CFO would determine the classification of the financial data and who can access as well. The Data Owner would then tell the Data Custodian (a technical person) what the classification and need to know is on the specific set of data.
The term Data Owner under DAC simply means whoever created the file and as the creator of the file the owner has full access and can grant access to other subjects based on their identity.

NEW QUESTION: 19
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)
Section: Network and Telecommunications
Explanation/Reference:
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: 20
A proxy is considered a:

A. first generation firewall.
B. third generation firewall.
C. second generation firewall.
D. fourth generation firewall.
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
The proxy (application layer firewall, circuit level proxy, or application proxy) is a second generation firewall
"First generation firewall" incorrect. A packet filtering firewall is a first generation firewall.
"Third generation firewall" is incorrect. Stateful Firewall are considered third generation firewalls

"Fourth generation firewall" is incorrect. Dynamic packet filtering firewalls are fourth generation firewalls
References:
CBK, p. 464
AIO3, pp. 482 - 484
Neither CBK or AIO3 use the generation terminology for firewall types but you will encounter it frequently as a practicing security professional. See http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/ scf4ch3.htm for a general discussion of the different generations.

NEW QUESTION: 21
What is the most secure way to dispose of information on a CD-ROM?
A. Sanitizing
B. Physical damage
C. Degaussing
D. Physical destruction
Answer: (SHOW ANSWER)
First you have to realize that the question is specifically talking about a CDROM. The information stored on a CDROM is not in electro magnetic format, so a degausser woud be inneffective.
You cannot sanitize a CDROM but you might be able to sanitize a RW/CDROM. A CDROM is a write once device and cannot be overwritten like a hard disk or other magnetic device.
Physical Damage would not be enough as information could still be extracted in a lab from the undamaged portion of the media or even from the pieces after the physical damage has been done.
Physical Destruction using a shredder, your microwave oven, melting it, would be very effective and the best choice for a non magnetic media such as a CDROM. Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 22
Which of the following security models does NOT concern itself with the flow of data?
A. The information flow model
B. The Biba model
C. The Bell-LaPadula model
D. The noninterference model
Answer: (SHOW ANSWER)
Explanation/Reference:
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 Bell-LaPadula model is incorrect. The Bell-LaPadula model is concerned with confidentiality and bases access control decsions 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.
The Biba model is incorrect. The Biba model is concerned with integrity and is a complement to the Bell-LaPadula model in that higher levels of integrity are more trusted than lower levels. Access control us based on these integrity levels to assure that read/write operations do not decrease an object's integrity.
References:
CBK, pp 325 - 326
AIO3, pp. 290 - 291

NEW QUESTION: 23
Which OSI/ISO layers are TCP and UDP implemented at?
A. Application layer
B. Presentation layer
C. Session layer
D. Transport layer
Answer: (SHOW ANSWER)
TCP and UDP are implemented at the transport layer (layer 4).
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 82).

NEW QUESTION: 24
Integrity = _____
A. Data being delivered from the source to the intended receiver without being altered
B. Protection of data from unauthorized users
C. Ability to access data when requested
D. Data being kept correct and current
E. All answers are correct
Answer: (SHOW ANSWER)

NEW QUESTION: 25
Which security model introduces access to objects only through programs?
A. The Biba model
B. The Bell-LaPadula model
C. The Clark-Wilson model
D. The information flow model
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
In the Clark-Wilson model, the subject no longer has direct access to objects but instead must access them through programs (well -formed transactions).

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.
Clark-Wilson is more clearly applicable to business and industry processes in which the integrity of the information content is paramount at any level of classification.
Integrity goals of Clark-Wilson model:
Prevent unauthorized users from making modification (Only this one is addressed by the Biba model).
Separation of duties prevents authorized users from making improper modifications.
Well formed transactions: maintain internal and external consistency i.e. it is a series of operations that are carried out to transfer the data from one consistent state to the other.
The following are incorrect answers:
The Biba model is incorrect. The Biba model is concerned with integrity and controls access to objects based on a comparison of the security level of the subject to that of the object.
The Bell-LaPdaula model is incorrect. The Bell-LaPaula model is concerned with confidentiality and controls access to objects based on a comparison of the clearence level of the subject to the classification level of the object.
The information flow model is incorrect. The information flow model uses a lattice where objects are labelled with security classes and information can flow either upward or at the same level. It is similar in framework to the Bell-LaPadula model.
References:
ISC2 Official Study Guide, Pages 325 - 327
AIO3, pp. 284 - 287
AIOv4 Security Architecture and Design (pages 338 - 342)
AIOv5 Security Architecture and Design (pages 341 - 344)
Wikipedia at: https://en.wikipedia.org/wiki/Clark-Wilson_model

NEW QUESTION: 26
Which of the following could be BEST defined as the likelihood of a threat agent taking advantage of a vulnerability?
A. A risk
B. A residual risk
C. An exposure
D. A countermeasure
Answer: (SHOW ANSWER)
Risk is the likelihood of a threat agent taking advantage of a vulnerability and
the corresponding business impact. If a firewall has several ports open , there is a higher
likelihood that an intruder will use one to access the network in an unauthorized method.

The following answers are incorrect :
Residual Risk is very different from the notion of total risk. Residual Risk would be the risks that still exists after countermeasures have been implemented. Total risk is the amount of risk a company faces if it chooses not to implement any type of safeguard.
Exposure: An exposure is an instance of being exposed to losses from a threat agent.
Countermeasure: A countermeasure or a safeguard is put in place to mitigate the potential risk. Examples of countermeasures include strong password management , a security guard.
REFERENCES : SHON HARRIS ALL IN ONE 3rd EDITION
Chapter - 3: Security Management Practices , Pages : 57-59

NEW QUESTION: 27
Business Continuity and Disaster Recovery Planning (Primarily) addresses the:
A. Availability of the CIA triad
B. Confidentiality of the CIA triad
C. Integrity of the CIA triad
D. Availability, Confidentiality and Integrity of the CIA triad
Answer: (SHOW ANSWER)
Explanation/Reference:
The Information Technology (IT) department plays a very important role in identifying and protecting the company's internal and external information dependencies. Also, the information technology elements of the BCP should address several vital issue, including:
Ensuring that the company employs sufficient physical security mechanisms to preserve vital network and hardware components. including file and print servers.
Ensuring that the organization uses sufficient logical security methodologies (authentication, authorization, etc.) for sensitive data.
Reference: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, page 279.

NEW QUESTION: 28
In what type of attack does an attacker try, from several encrypted messages, to figure out the key used in the encryption process?
A. Known-plaintext attack
B. Ciphertext-only attack
C. Chosen-Ciphertext attack
D. Plaintext-only attack
Answer: (SHOW ANSWER)
In a ciphertext-only attack, the attacker has the ciphertext of several messages encrypted with the same encryption algorithm. Its goal is to discover the plaintext of the messages by figuring out the key used in the encryption process. In a known-plaintext attack, the attacker has the plaintext and the ciphertext of

one or more messages. In a chosen-ciphertext attack, the attacker can chose the ciphertext to be decrypted and has access to the resulting plaintext.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 8: Cryptography (page 578).

NEW QUESTION: 29
Which of the following is NOT a defined ISO basic task related to network management?
A. Fault management
B. Accounting resources
C. Security management
D. Communications management
Answer: (SHOW ANSWER)
Explanation/Reference:
ISO has defined five basic tasks related to network management :
Fault management: Detects the devices that present some kind of fault.
Configuration management: Allows users to know, define and change remotely the configuration of any device.
Accounting resources: Holds the records of the resource usage in the WAN.
Performance management: Monitors usage levels and sets alarms when a threshold has been surpassed.
Security management: Detects suspicious traffic or users and generates alarms accordingly.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 137).

NEW QUESTION: 30
What can best be defined as a strongly protected computer that is in a network protected by a firewall (or is part of a firewall) and is the only host (or one of only a few hosts) in the network that can be directly accessed from networks on the other side of the firewall?

A. A bastion host
B. A screened subnet
C. A dual-homed host
D. A proxy server
Answer: (SHOW ANSWER)
Explanation/Reference:
The Internet Security Glossary (RFC2828) defines a bastion host as a strongly protected computer that is in a network protected by a firewall (or is part of a firewall) and is the only host (or one of only a few hosts) in the network that can be directly accessed from networks on the other side of the firewall.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 31

Which type of attack involves the alteration of a packet at the IP level to convince a system that it is communicating with a known entity in order to gain access to a system?

A. TCP sequence number attack

B. IP spoofing attack

C. Piggybacking attack

D. Teardrop attack

Answer: (SHOW ANSWER)

Explanation/Reference:

An IP spoofing attack is used to convince a system that it is communication with a known entity that gives an intruder access. It involves modifying the source address of a packet for a trusted source's address. A TCP sequence number attack involves hijacking a session between a host and a target by predicting the target's choice of an initial TCP sequence number. Piggybacking refers to an attacker gaining unauthorized access to a system by using a legitimate user's connection. A teardrop attack consists of modifying the length and fragmentation offset fields in sequential IP packets so the target system becomes confused and crashes after it receives contradictory instructions on how the fragments are offset on these packets.

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
77).

NEW QUESTION: 32

Which of the following prevents, detects, and corrects errors so that the integrity, availability, and confidentiality of transactions over networks may be maintained?

A. Communications security management and techniques

B. Information security management and techniques

C. Client security management and techniques

D. Server security management and techniques

Answer: (SHOW ANSWER)

Explanation/Reference:

Communications security and techniques are the best area for addressing this objective.

"Information security management and techniques" is incorrect. While the overall information security program would include this objective, communications security is the more specific and better answer.
"Client security management and techniques" is incorrect. While client security plays a part in this overall objective, communications security is the more specific and better answer.
"Server security management and techniques" is incorrect. While server security plays a part in this overall objective, communications security is the more specific and better answer.
References:
CBK, p. 408

NEW QUESTION: 33
What is the framing specification used for transmitting digital signals at 1.544 Mbps on a T1 facility?
A. DS-0
B. DS-1
C. DS-2
D. DS-3
Answer: (SHOW ANSWER)
Digital Signal level 1 (DS-1) is the framing specification used for transmitting digital signals at 1.544 Mbps on a T1 facility. DS-0 is the framing specification used in transmitting digital signals over a single 64 Kbps channel over a T1 facility. DS-3 is the framing specification used for transmitting digital signals at 44.736 Mbps on a T3 facility. DS-2 is not a defined framing specification.
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 114).

NEW QUESTION: 34
A program that intentionally leaves a security hole or covert method of access is referred to as a _____.
A. Logic bomb
B. Trojan horse
C. Back door
D. Honey pot
Answer: (SHOW ANSWER)

NEW QUESTION: 35
What can best be defined as high-level statements, beliefs, goals and objectives?
A. Standards
B. Policies
C. Guidelines
D. Procedures
Answer: (SHOW ANSWER)
Explanation/Reference:

Policies are high-level statements, beliefs, goals and objectives and the general means for their attainment for a specific subject area. Standards are mandatory activities, action, rules or regulations designed to provide policies with the support structure and specific direction they require to be effective. Guidelines are more general statements of how to achieve the policies objectives by providing a framework within which to implement procedures. Procedures spell out the specific steps of how the policy and supporting standards and how guidelines will be implemented.
Source: HARE, Chris, Security management Practices CISSP Open Study Guide, version 1.0, april 1999.

NEW QUESTION: 36
Which of the following would be best suited to oversee the development of an information security policy?
A. System Administrators
B. End User
C. Security Officers
D. Security administrators
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
The security officer would be the best person to oversea the development of such policies.
Security officers and their teams have typically been charged with the responsibility of creating the security policies. The policies must be written and communicated appropriately to ensure that they can be understood by the end users. Policies that are poorly written, or written at too high of an education level (common industry practice is to focus the content for general users at the sixth- to eighth-grade reading level), will not be understood.
Implementing security policies and the items that support them shows due care by the company and its management staff. Informing employees of what is expected of them and the consequences of noncompliance can come down to a liability issue.
While security officers may be responsible for the development of the security policies, the effort should be collaborative to ensure that the business issues are addressed.
The security officers will get better corporate support by including other areas in policy development. This helps build buy-in by these areas as they take on a greater ownership of the final product. Consider including areas such as HR, legal, compliance, various IT areas and specific business area representatives who represent critical business units.
When policies are developed solely within the IT department and then distributed without business input, they are likely to miss important business considerations. Once policy documents have been created, the basis for ensuring compliance is established. Depending on the organization, additional documentation may be necessary to support policy. This support may come in the form of additional controls described in standards, baselines, or procedures to help personnel with compliance. An important step after documentation is to make the most current version of the documents readily accessible to those who are expected to follow them. Many organizations place the documents on their intranets or in shared file folders to facilitate their accessibility.

Such placement of these documents plus checklists, forms, and sample documents can make awareness more effective.

For your exam you should know the information below:

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

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

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

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

Data/Information/Business/System Owners - A business executive or manager is typically responsible for an information asset. These are the individuals that assign the appropriate classification to information assets.

They ensure that the business information is protected with appropriate controls. Periodically, the information asset owners need to review the classification and access rights associated with information assets. The owners, or their delegates, may be required to approve access to the information. Owners also need to determine the criticality, sensitivity, retention, backups, and safeguards for the information. Owners or their delegates are responsible for understanding the risks that exist with regards to the information that they control.

Data/Information Custodian/Steward - A data custodian is an individual or function that takes care of the information on behalf of the owner. These individuals ensure that the information is available to the end users and is backed up to enable recovery in the event of data loss or corruption. Information may be stored in files, databases, or systems whose technical infrastructure must be managed, by systems administrators. This group administers access rights to the information assets.

Information Systems Auditor- IT auditors determine whether users, owners, custodians, systems, and networks are in compliance with the security policies, procedures, standards, baselines, designs, architectures, management direction, and other requirements placed on systems. The auditors provide independent assurance to the management on the appropriateness of the security controls. The auditor examines the information systems and determines whether they are designed, configured, implemented, operated, and managed in a way ensuring that the organizational objectives are being achieved. The

auditors provide top company management with an independent view of the controls and their effectiveness.

Business Continuity Planner - Business continuity planners develop contingency plans to prepare for any occurrence that could have the ability to impact the company's objectives negatively. Threats may include earthquakes, tornadoes, hurricanes, blackouts, changes in the economic/political climate, terrorist activities, fire, or other major actions potentially causing significant harm. The business continuity planner ensures that business processes can continue through the disaster and coordinates those activities with the business areas and information technology personnel responsible for disaster recovery.

Information Systems/ Technology Professionals- These personnel are responsible for designing security controls into information systems, testing the controls, and implementing the systems in production environments through agreed upon operating policies and procedures. The information systems professionals work with the business owners and the security professionals to ensure that the designed solution provides security controls commensurate with the acceptable criticality, sensitivity, and availability requirements of the application.

Security Administrator - A security administrator manages the user access request process and ensures that privileges are provided to those individuals who have been authorized for access by application/system/data owners. This individual has elevated privileges and creates and deletes accounts and access permissions. The security administrator also terminates access privileges when individuals leave their jobs or transfer between company divisions. The security administrator maintains records of access request approvals and produces reports of access rights for the auditor during testing in an access controls audit to demonstrate compliance with the policies.

Network/Systems Administrator - A systems administrator (sysadmin/netadmin) configures network and server hardware and the operating systems to ensure that the information can be available and accessible.

The administrator maintains the computing infrastructure using tools and utilities such as patch management and software distribution mechanisms to install updates and test patches on organization computers. The administrator tests and implements system upgrades to ensure the continued reliability of the servers and network devices. The administrator provides vulnerability management through either commercial off the shelf (COTS) and/or non-COTS solutions to test the computing environment and mitigate vulnerabilities appropriately.

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

Security Analyst - The security analyst role works at a higher, more strategic level than the previously described roles and helps develop policies, standards, and guidelines, as well as set various baselines.

Whereas the previous roles are "in the weeds" and focus on pieces and parts of the security program, a security analyst helps define the security program elements and follows through to ensure the elements are being carried out and practiced properly. This person works more at a design level than at an implementation level.

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

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

The help desk resets passwords, resynchronizes/reinitializes tokens and smart cards, and resolves other problems with access control.

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

Change Control Analyst Since the only thing that is constant is change, someone must make sure changes happen securely. The change control analyst is responsible for approving or rejecting requests to make changes to the network, systems, or software. This role must make certain that the change will not introduce any vulnerabilities, that it has been properly tested, and that it is properly rolled out. The change control analyst needs to understand how various changes can affect security, interoperability, performance, and productivity.

Or, a company can choose to just roll out the change and see what happens.

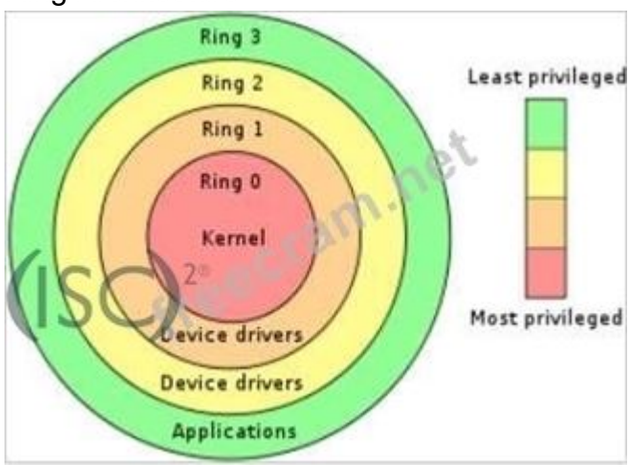
The following answers are incorrect:

Systems Administrator - A systems administrator (sysadmin/netadmin) configures network and server hardware and the operating systems to ensure that the information can be available and accessible. The administrator maintains the computing infrastructure using tools and utilities such as patch management and software distribution mechanisms to install updates and test patches on organization computers. The administrator tests and implements system upgrades to ensure the continued reliability of the servers and network devices. The administrator provides vulnerability management through either commercial off

the shelf (COTS) and/or non-COTS solutions to test the computing environment and mitigate vulnerabilities appropriately.
End User - The end user is responsible for protecting information assets on a daily basis through adherence to the security policies that have been communicated.
Security Administrator - A security administrator manages the user access request process and ensures that privileges are provided to those individuals who have been authorized for access by application/system/data owners. This individual has elevated privileges and creates and deletes accounts and access permissions. The security administrator also terminates access privileges when individuals leave their jobs or transfer between company divisions. The security administrator maintains records of access request approvals and produces reports of access rights for the auditor during testing in an access controls audit to demonstrate compliance with the policies.
Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 109
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 108). McGraw-Hill. Kindle Edition.

NEW QUESTION: 37
Detective/Technical measures:
A. include intrusion detection systems and automatically-generated violation reports from audit trail information.
B. do not include intrusion detection systems and automatically-generated violation reports from audit trail information.
C. include intrusion detection systems but do not include automatically-generated violation reports from audit trail information.
D. include intrusion detection systems and customised-generated violation reports from audit trail information.
Answer: (SHOW ANSWER)
Detective/Technical measures include intrusion detection systems and automatically-generated violation reports from audit trail information. These reports can indicate variations from "normal" operation or detect known signatures of unauthorized access episodes. In order to limit the amount of audit information flagged and reported by automated violation analysis and reporting mechanisms, clipping levels can be set. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35.

NEW QUESTION: 38
An Architecture where there are more than two execution domains or privilege levels is called:
A. Ring Architecture.
B. Ring Layering
C. Network Environment.
D. Security Models
Answer: (SHOW ANSWER)

Section: Security Operation Adimnistration
Explanation/Reference:
In computer science, hierarchical protection domains, often called protection rings, are a mechanism to protect data and functionality from faults (fault tolerance) and malicious behavior (computer security). This approach is diametrically opposite to that of capability-based security.
Computer operating systems provide different levels of access to resources. A protection ring is one of two or more hierarchical levels or layers of privilege within the architecture of a computer system. This is generally hardware-enforced by some CPU architectures that provide different CPU modes at the hardware or microcode level. Rings are arranged in a hierarchy from most privileged (most trusted, usually numbered zero) to least privileged (least trusted, usually with the highest ring number). On most operating systems, Ring 0 is the level with the most privileges and interacts most directly with the physical hardware such as the CPU and memory.
Special gates between rings are provided to allow an outer ring to access an inner ring's resources in a predefined manner, as opposed to allowing arbitrary usage. Correctly gating access between rings can improve security by preventing programs from one ring or privilege level from misusing resources intended for programs in another. For example, spyware running as a user program in Ring 3 should be prevented from turning on a web camera without informing the user, since hardware access should be a Ring 1 function reserved for device drivers. Programs such as web browsers running in higher numbered rings must request access to the network, a resource restricted to a lower numbered ring.
Ring Architecture


All of the other answers are incorrect because they are detractors.
References:
OIG CBK Security Architecture and Models (page 311)
and
https://en.wikipedia.org/wiki/Ring_%28computer_security%29

NEW QUESTION: 39
Who is responsible for providing reports to the senior management on the effectiveness of the security controls?
A. Information systems security professionals
B. Data owners

C. Data custodians
D. Information systems auditors
Answer: (SHOW ANSWER)
IT auditors determine whether systems are in compliance with the security policies, procedures, standards, baselines, designs, architectures, management direction and other requirements" and "provide top company management with an independent view of the controls that have been designed and their effectiveness."
"Information systems security professionals" is incorrect. Security professionals develop the security policies and supporting baselines, etc.
"Data owners" is incorrect. Data owners have overall responsibility for information assets and assign the appropriate classification for the asset as well as ensure that the asset is protected with the proper controls.
"Data custodians" is incorrect. Data custodians care for an information asset on behalf of the data owner.
References:
CBK, pp. 38 - 42. AIO3. pp. 99 - 104

NEW QUESTION: 40
A momentary power outage is a:
A. spike
B. blackout
C. surge
D. fault
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
A momentary power outage is a fault.
Power Excess
Spike --> Too much voltage for a short period of time.
Surge --> Too much voltage for a long period of time.
Power Loss
Fault --> A momentary power outage.
Blackout --> A long power interruption.
Power Degradation
Sag or Dip --> A momentary low voltage.
Brownout --> A prolonged power supply that is below normal voltage.
Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw-Hill/Osborne, 2005, page
368.
and
https://en.wikipedia.org/wiki/Power_quality

NEW QUESTION: 41
Sensitivity labels are an example of what application control type?
A. Preventive security controls
B. Detective security controls
C. Compensating administrative controls
D. Preventive accuracy controls
Answer: (SHOW ANSWER)
Explanation/Reference:
Sensitivity labels are a preventive security application controls, such as are firewalls, reference monitors, traffic padding, encryption, data classification, one-time passwords, contingency planning, separation of development, application and test environments.
The incorrect answers are:
Detective security controls - Intrusion detection systems (IDS), monitoring activities, and audit trails.
Compensating administrative controls - There no such application control.
Preventive accuracy controls - data checks, forms, custom screens, validity checks, contingency planning, and backups.
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 264).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Application Controls, Figure 7.1 (page 360).

NEW QUESTION: 42
Which of the following is the best reason for the use of an automated risk analysis tool?
A. Much of the data gathered during the review cannot be reused for subsequent analysis.
B. Automated methodologies require minimal training and knowledge of risk analysis.
C. Most software tools have user interfaces that are easy to use and does not require any training.
D. Information gathering would be minimized and expedited due to the amount of information already built into the tool.
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
The use of tools simplifies this process. Not only do they usually have a database of assests, threats, and vulnerabilities but they also speed up the entire process.
Using Automated tools for performing a risk assessment can reduce the time it takes to perform them and can simplify the process as well. The better types of these tools include a well-researched threat population and associated statistics. Using one of these tools virtually ensures that no relevant threat is overlooked, and associated risks are accepted as a consequence of the threat being overlooked.

In most situations, the assessor will turn to the use of a variety of automated tools to assist in the vulnerability assessment process. These tools contain extensive databases of specific known vulnerabilities as well as the ability to analyze system and network configuration information to predict where a particular system might be vulnerable to different types of attacks. There are many different types of tools currently available to address a wide variety of vulnerability assessment needs. Some tools will examine a system from the viewpoint of the network, seeking to determine if a system can be compromised by a remote attacker exploiting available services on a particular host system. These tools will test for open ports listening for connections, known vulnerabilities in common services, and known operating system exploits.
Michael Gregg says:
Automated tools are available that minimize the effort of the manual process. These programs enable users to rerun the analysis with different parameters to answer "what-ifs." They perform calculations quickly and can be used to estimate future expected losses easier than performing the calculations manually.
Shon Harris in her latest book says:
The gathered data can be reused, greatly reducing the time required to perform subsequent analyses. The risk analysis team can also print reports and comprehensive graphs to present 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 Locations 4655-4661). Auerbach Publications. Kindle Edition.
and
CISSP Exam Cram 2 by Michael Gregg
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 2333-2335). McGraw- Hill. Kindle Edition.
The following answers are incorrect:
Much of the data gathered during the review cannot be reused for subsequent analysis. Is incorrect because the data can be reused for later analysis.
Automated methodologies require minimal training and knowledge of risk analysis. Is incorrect because it is not the best answer. While a minimal amount of training and knowledge is needed, the analysis should still be performed by skilled professionals.
Most software tools have user interfaces that are easy to use and does not require any training. Is incorrect because it is not the best answer. While many of the user interfaces are easy to use it is better if the tool already has information built into it. There is always a training curve when any product is being used for the first time.

NEW QUESTION: 43
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: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
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: 44
_____, _____, and _____ are required to successfully complete a crime.
(Choose three)
A. Root kit
B. Motive
C. Buffer Overflow
D. Means
E. Opportunity
F. Advantage
Answer: (SHOW ANSWER)
Means, motive, and opportunity are the three items needed to commit a crime.

NEW QUESTION: 45
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: A (LEAVE A REPLY)
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

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: 46
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: B (LEAVE A REPLY)
Explanation/Reference:
In biometrics, identification is a "one-to-many" search of an individual's characteristics from a database of stored images.
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: 47
Which of the following is NOT a defined ISO basic task related to network management?
A. Fault management

B. Accounting resources
C. Security management
D. Communications management
Answer: D (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
ISO has defined five basic tasks related to network management :
Fault management: Detects the devices that present some kind of fault.
Configuration management: Allows users to know, define and change remotely the configuration of any device.
Accounting resources: Holds the records of the resource usage in the WAN.
Performance management: Monitors usage levels and sets alarms when a threshold has been surpassed.
Security management: Detects suspicious traffic or users and generates alarms accordingly.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 137).

NEW QUESTION: 48
Under United States law, an investigator's notebook may be used in court in which of the following scenarios?
A. When the investigator is unwilling to testify.
B. When other forms of physical evidence are not available.
C. To refresh the investigators memory while testifying.
D. If the defense has no objections.
Answer: (SHOW ANSWER)
Explanation/Reference:
An investigator's notebook cannot be used as evidence is court. It can only be used by the investigator to refresh his memory during a proceeding, but cannot be submitted as evidence in any form.
The following answers are incorrect:
When the investigator is unwilling to testify. Is incorrect because the notebook cannot be submitted as evidence in any form.
When other forms of physical evidence are not available. Is incorrect because the notebook cannot be submitted as evidence in any form.
If the defense has no objections. Is incorrect because the notebook cannot be submitted as evidence in any form.

NEW QUESTION: 49
Domain Name Service is a distributed database system that is used to map:
A. Domain Name to IP addresses.
B. MAC addresses to domain names.
C. MAC Address to IP addresses.

D. IP addresses to MAC Addresses.

Answer: (SHOW ANSWER)

The Domain Name Service is a distributed database system that is used to map domain names to IP addresses and IP addresses to domain names.

The Domain Name System is maintained by a distributed database system, which uses the client-server model. The nodes of this database are the name servers. Each domain has at least one authoritative DNS server that publishes information about that domain and the name servers of any domains subordinate to it. The top of the hierarchy is served by the root nameservers, the servers to query when looking up (resolving) a TLD.

Reference(s) used for this question:

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

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

NEW QUESTION: 50

Considerations of privacy, invasiveness, and psychological and physical comfort when using the system are important elements for which of the following?

A. Accountability of biometrics systems

B. Acceptability of biometrics systems

C. Availability of biometrics systems

D. Adaptability of biometrics systems

Answer: (SHOW ANSWER)

Section: Access Control

Explanation/Reference:

Acceptability refers to considerations of privacy, invasiveness, and psychological and physical comfort when using 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 39.

NEW QUESTION: 51

Sensitivity labels are an example of what application control type?

A. Preventive security controls

B. Detective security controls

C. Compensating administrative controls

D. Preventive accuracy controls

Answer: (SHOW ANSWER)

Section: Access Control

Explanation/Reference:

Sensitivity labels are a preventive security application controls, such as are firewalls, reference monitors, traffic padding, encryption, data classification, one-time passwords, contingency planning, separation of development, application and test environments.

The incorrect answers are:
Detective security controls - Intrusion detection systems (IDS), monitoring activities, and audit trails.
Compensating administrative controls - There no such application control.
Preventive accuracy controls - data checks, forms, custom screens, validity checks, contingency planning, and backups.
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 264).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter
7: Application Controls, Figure 7.1 (page 360).

NEW QUESTION: 52
Which of the following would be used to detect and correct errors so that integrity and confidentiality of transactions over networks may be maintained while preventing unauthorize interception of the traffic?
A. Information security
B. Server security
C. Client security
D. Communications security
Answer: (SHOW ANSWER)
Communications security is the discipline of preventing unauthorized interceptors from accessing telecommunications in an intelligible form, while still delivering content to the intended recipients. In the United States Department of Defense culture, it is often referred to by the abbreviation COMSEC. The field includes cryptosecurity, transmission security, emission security, traffic-flow security and physical security of COMSEC equipment.
All of the other answers are incorrect answers:
Information security Information security would be the overall program but communications security is the more specific and better answer. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.
These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms. Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.

Server security While server security plays a part in the overall information security program, communications security is a better answer when talking about data over the network and preventing interception. See publication 800-123 listed in the reference below to learn more.
Client security While client security plays a part in the overall information security program, communications security is a better answer. Securing the client would not prevent interception of data or capture of data over the network. Today people referred to this as endpoint security.
References:
http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf and
https://en.wikipedia.org/wiki/Information_security and
https://en.wikipedia.org/wiki/Communications_security

NEW QUESTION: 53
CORRECT TEXT
_____ is a tool used by network administrators to capture packets from a network.
Answer:

NEW QUESTION: 54
In a Public Key Infrastructure, how are public keys published?
A. They are sent via e-mail.
B. Through digital certificates.
C. They are sent by owners.
D. They are not published.
Answer: (SHOW ANSWER)
Explanation/Reference:
Public keys are published through digital certificates, signed by certification authority (CA), binding the certificate to the identity of its bearer.
A bit more details:
Although "Digital Certificates" is the best (or least wrong!) in the list of answers presented, for the past decade public keys have been published (ie: made known to the World) by the means of a LDAP server or a key distribution server (ex.: http://pgp.mit.edu/). An indirect publishing method is through OCSP servers (to validate digital signatures' CRL)
Reference used for this question:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
and
http://technet.microsoft.com/en-us/library/dd361898.aspx

NEW QUESTION: 55
When a biometric system is used, which error type deals with the possibility of GRANTING access to impostors who should be REJECTED?
A. Type I error
B. Type II error

C. Type III error

D. Crossover error

Answer: B (LEAVE A REPLY)

Explanation/Reference:

When the biometric system accepts impostors who should have been rejected , it is called a Type II error or False Acceptance Rate or False Accept Rate.

Biometrics verifies an individual's identity by analyzing a unique personal attribute or behavior, which is one of the most effective and accurate methods of verifying identification.

Biometrics is a very sophisticated technology; thus, it is much more expensive and complex than the other types of identity verification processes. A biometric system can make authentication decisions based on an individual's behavior, as in signature dynamics, but these can change over time and possibly be forged.

Biometric systems that base authentication decisions on physical attributes (iris, retina, fingerprint) provide more accuracy, because physical attributes typically don't change much, absent some disfiguring injury, and are harder to impersonate.

When a biometric system rejects an authorized individual, it is called a Type I error (False Rejection Rate (FRR) or False Reject Rate (FRR)).

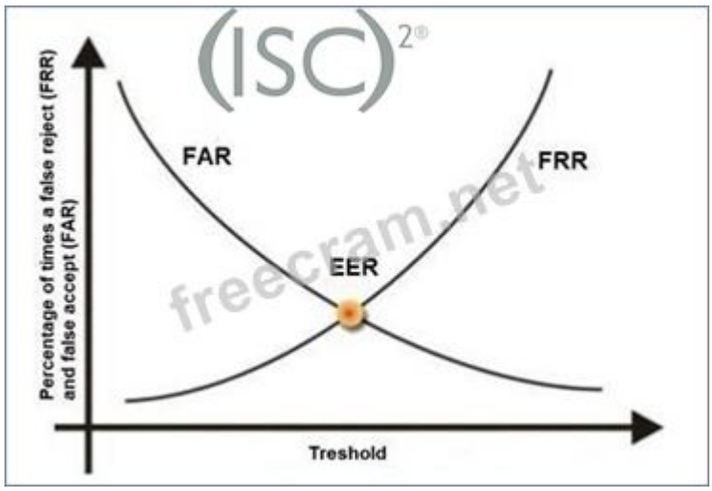
When the system accepts impostors who should be rejected, it is called a Type II error (False Acceptance Rate (FAR) or False Accept Rate (FAR)). Type II errors are the most dangerous and thus the most important to avoid.

The goal is to obtain low numbers for each type of error, but When comparing different biometric systems, many different variables are used, but one of the most important metrics is the crossover error rate (CER).

The accuracy of any biometric method is measured in terms of Failed Acceptance Rate (FAR) and Failed Rejection Rate (FRR). Both are expressed as percentages. The FAR is the rate at which attempts by unauthorized users are incorrectly accepted as valid. The FRR is just the opposite. It measures the rate at which authorized users are denied access.

The relationship between FRR (Type I) and FAR (Type II) is depicted in the graphic below . As one rate increases, the other decreases. The Cross-over Error Rate (CER) is sometimes considered a good indicator of the overall accuracy of a biometric system. This is the point at which the FRR and the FAR have the same value. Solutions with a lower CER are typically more accurate.

See graphic below from Biometria showing this relationship. The Cross-over Error Rate (CER) is also called the Equal Error Rate (EER), the two are synonymous.



Cross Over Error Rate
The other answers are incorrect:
Type I error is also called as False Rejection Rate where a valid user is rejected by the system.
Type III error : there is no such error type in biometric system.
Crossover error rate stated in percentage , represents the point at which false rejection equals the false acceptance rate.
Reference(s) used for this question:
http://www.biometria.sk/en/principles-of-biometrics.html
and
Shon Harris, CISSP All In One (AIO), 6th Edition , Chapter 3, Access Control, Page 188-189 and
Tech Republic, Reduce Multi_Factor Authentication Cost

NEW QUESTION: 56
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: (SHOW ANSWER)
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: 57

In regards to information classification what is the main responsibility of information (data) owner?
A. determining the data sensitivity or classification level
B. running regular data backups
C. audit the data users
D. periodically check the validity and accuracy of the data
Answer: (SHOW ANSWER)
Explanation/Reference:
Making the determination to decide what level of classification the information requires is the main responsibility of the data owner.
The data owner within classification is a person from Management who has been entrusted with a data set that belong to the company. It could be for example the Chief Financial Officer (CFO) who has been entrusted with all financial date or it could be the Human Resource Director who has been entrusted with all Human Resource data. The information owner will decide what classification will be applied to the data based on Confidentiality, Integrity, Availability, Criticality, and Sensitivity of the data.
The Custodian is the technical person who will implement the proper classification on objects in accordance with the Data Owner. The custodian DOES NOT decide what classification to apply, it is the Data Owner who will dictate to the Custodian what is the classification to apply.
NOTE:
The term Data Owner is also used within Discretionary Access Control (DAC). Within DAC it means the person who has created an object. For example, if I create a file on my system then I am the owner of the file and I can decide who else could get access to the file. It is left to my discretion. Within DAC access is granted based solely on the Identity of the subject, this is why sometimes DAC is referred to as Identity Based Access Control.
The other choices were not the best answer
Running regular backups is the responsibility of custodian.
Audit the data users is the responsibility of the auditors
Periodically check the validity and accuracy of the data is not one of the data owner responsibility
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, Page 14, Chapter 1: Security Management Practices.

NEW QUESTION: 58
The first step in the implementation of the contingency plan is to perform:
A. A firmware backup
B. A data backup
C. An operating systems software backup
D. An application software backup
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
A data backup is the first step in contingency planning.

Without data, there is nothing to process. "No backup, no recovery".
Backup for hardware should be taken care of next.
Formal arrangements must be made for alternate processing capability in case the need should arise.
Operating systems and application software should be taken care of afterwards.
Source: VALLABHANENI, S. Rao, CISSP Examination Textbooks, Volume 2: Practice, SRV Professional Publications, 2002, Chapter 8, Business Continuity Planning & Disaster Recovery Planning (page 506).

NEW QUESTION: 59
What is the act of obtaining information of a higher sensitivity by combining information from lower levels of sensitivity?
A. Polyinstantiation
B. Inference
C. Aggregation
D. Data mining
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
Aggregation is the act of obtaining information of a higher sensitivity by combining information from lower levels of sensitivity.
The incorrect answers are:
Polyinstantiation is the development of a detailed version of an object from another object using different values in the new object.
Inference is the ability of users to infer or deduce information about data at sensitivity levels for which they do not have access privilege.
Data mining refers to searching through a data warehouse for data correlations.
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 261).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter
7: Database Security Issues (page 358).

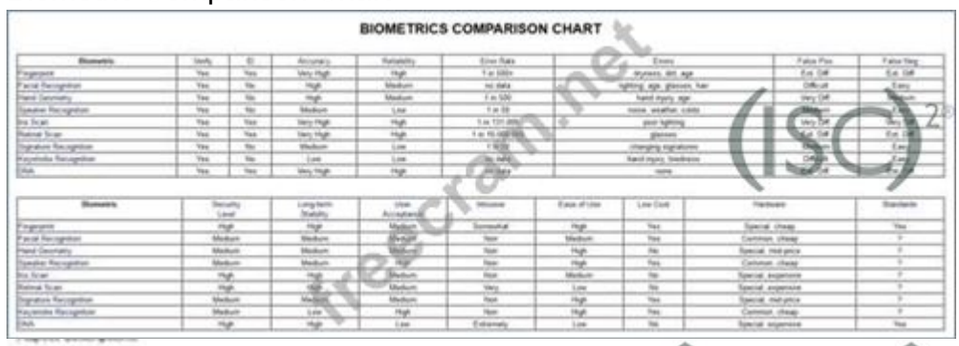
NEW QUESTION: 60
Attributable data should be:
A. always traced to individuals responsible for observing and recording the data
B. sometimes traced to individuals responsible for observing and recording the data
C. never traced to individuals responsible for observing and recording the data
D. often traced to individuals responsible for observing and recording the data
Answer: (SHOW ANSWER)
Explanation/Reference:

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.
Source: 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: 61
Which of the following statements pertaining to Asynchronous Transfer Mode (ATM) is false?
A. It can be used for voice
B. it can be used for data
C. It carries various sizes of packets
D. It can be used for video
Answer: C (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
ATM is an example of a fast packet-switching network that can be used for either data, voice or video, but packets are of fixed size.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 7:
Telecommunications and Network Security (page 455).

NEW QUESTION: 62
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: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:

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



lerify	Whether or not the Biometric is capable of verification. Verification is the process where an input is compared to specific data previously recorded from the user to see if the person is who they claim to be
D	Whether or not the Biometric is capable of identification. Identification is the process where an input is compared to a large data set previously recorded from many people to see which person the user is
ccuracy	How well the Biometric is able to tell individuals apart. This is partially determined by the amount of information gathered as well as the number of possible different data results
eliability	How dependable the Biometric is for recognition purposes
rror Rate	This is calculated as the crossing point when graphed of false positives and false negatives created using this Biometric
rrors	Typical causes of errors for this Biometric
alse Pos.	How easy it is to create a false positive reading with this biometric (someone is able to impersonate someone else)
alse Neg.	How easy it is to create a false negative reading with this biometric (someone is able to avoid identification as oneself)
ecurity Level	The highest level of security that this Biometric is capable of working at
ong-term itability	How well this Biometric continues to work without data updates over long periods of time
ser Acceptance	How willing the public is to use this Biometric
ntrusiveness	How much the Biometric is considered to invade one's privacy or require interaction by the user
ase of Use	How easy this Biometric is for both the user and the personnel involved
ow Cost	Whether or not there is a low-cost option for this Biometric to be used
ardware	Type and cost of hardware required to use this Biometric
tandards	Whether or not standards exist for this Biometric

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: 63
Which of the following is the core of fiber optic cables made of?
A. PVC
B. Glass fibers
C. Kevlar
D. Teflon

Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
Fiber optic cables have an outer insulating jacket made of Teflon or PVC, Kevlar fiber, which helps to strengthen the cable and prevent breakage, plastic coatings, used to cushion the fiber center. The center (core) of the cable is made of glass or plastic fibers.
Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 3: Telecommunications and Network Security (page 31).

NEW QUESTION: 64
What is the primary goal of setting up a honeypot?
A. To lure hackers into attacking unused systems
B. To entrap and track down possible hackers
C. To set up a sacrificial lamb on the network
D. To know when certain types of attacks are in progress and to learn about attack techniques so the network can be fortified.
Answer: (SHOW ANSWER)
Section: Analysis and Monitoring
Explanation/Reference:
The primary purpose of a honeypot is to study the attack methods of an attacker for the purposes of understanding their methods and improving defenses.
"To lure hackers into attacking unused systems" is incorrect. Honeypots can serve as decoys but their primary purpose is to study the behaviors of attackers.
"To entrap and track down possible hackers" is incorrect. There are a host of legal issues around enticement vs entrapment but a good general rule is that entrapment is generally prohibited and evidence gathered in a scenario that could be considered as "entrapping" an attacker would not be admissible in a court of law.
"To set up a sacrificial lamb on the network" is incorrect. While a honeypot is a sort of sacrificial lamb and may attract attacks that might have been directed against production systems, its real purpose is to study the methods of attackers with the goals of better understanding and improving network defenses.
References
AIO3, p. 213

NEW QUESTION: 65
Which of the following reviews system and event logs to detect attacks on the host and determine if the attack was successful?
A. host-based IDS
B. firewall-based IDS
C. bastion-based IDS
D. server-based IDS
Answer: (SHOW ANSWER)

A host-based IDS can review the system and event logs in order to detect an attack on the host and to determine if the attack was successful.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 48.

NEW QUESTION: 66
FTP, TFTP, SNMP, and SMTP are provided at what level of the Open Systems Interconnect (OSI) Reference Model?
A. Application
B. Network
C. Presentation
D. Transport
Answer: (SHOW ANSWER)
Application. The Layer 7 Application Layer of the Open Systems Interconnect (OSI) Reference Model is a service for applications and Operating Systems data transmission, for example FTP, TFTP, SNMP, and SMTP.
The following answers are incorrect: Network. The Network layer moves information between hosts that are not physically connected. It deals with routing of information. IP is a protocol that is used in Network Layer. FTP, TFTP, SNMP, and SMTP do not reside at the Layer 3 Network Layer in the OSI Reference Model.
Presentation. The Presentation Layer is concerned with the formatting of data into a standard presentation such as ASCII. FTP, TFTP, SNMP, and SMTP do not reside at the Layer 6 Presentation Layer in the OSI Reference Model.
Transport. The Transport Layer creates an end-to-end transportation between peer hosts. The transmission can be connectionless and unreliable such as UDP, or connection-oriented and ensure error-free delivery such as TCP. FTP, TFTP, SNMP, and SMTP do not reside at the Layer 4 Transportation Layer in the OSI Reference Model.
The following reference(s) were/was used to create this question: Reference: OSI/ISO.
Shon Harris AIO v.3 p. 420-421 ISC2 OIG, 2997 p.412-413

NEW QUESTION: 67
What does the directive of the European Union on Electronic Signatures deal with?
A. Encryption of classified data
B. Encryption of secret data
C. Non repudiation
D. Authentication of web servers
Answer: (SHOW ANSWER)
Explanation/Reference:
Reference: FORD, Warwick & BAUM, Michael S., Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption (2nd Edition), 2000, Prentice Hall PTR, Page 589; Directive 1999/93/ EC of 13 December 1999 on a Community framework for electronic signatures.

NEW QUESTION: 68
Which of the following was developed by the National Computer Security Center (NCSC) for the US Department of Defense ?
A. TCSEC
B. ITSEC
C. DIACAP
D. NIACAP
E. Explanation:
The
Answer: (SHOW ANSWER)
; The TCSEC, frequently referred to as the Orange
Book, is the centerpiece of the DoD Rainbow Series publications.
Initially issued by the National Computer Security Center (NCSC) an arm of the National Security Agency in 1983 and then updated in 1985, TCSEC was replaced with the development of the Common Criteria international standard originally published in 2005.
References:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, pages 197-199.
Wikepedia
http://en.wikipedia.org/wiki/TCSEC

NEW QUESTION: 69
PGP & PEM are programs that allow users to send encrypted messages to each other. What form of encryption do these programs use?
A. DES
B. Blowfish
C. 3RSA
D. RSA
E. 3DES
F. All of the above
Answer: (SHOW ANSWER)

NEW QUESTION: 70
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: (SHOW ANSWER)
Section: Risk, Response and Recovery

Explanation/Reference:
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Property Insurance overview, Page 589.

NEW QUESTION: 71
Recovery Site Strategies for the technology environment depend on how much downtime an organization can tolerate before the recovery must be completed. What would you call a strategy where the alternate site is internal, standby ready, with all the technology and equipment necessary to run the applications?
A. External Hot site
B. Warm Site
C. Internal Hot Site
D. Dual Data Center
Answer: (SHOW ANSWER)
Internal Hot Site-This site is standby ready with all the technology and equipment necessary to run the applications positioned there. The planner will be able to effectively restart an application in a hot site recovery without having to perform any bare metal recovery of servers. If this is an internal solution, then often the organization will run non-time sensitive processes there such as development or test environments, which will be pushed aside for recovery of production when needed. When employing this strategy, it is important that the two environments be kept as close to identical as possible to avoid problems with O/S levels, hardware differences, capacity differences, etc., from preventing or delaying recovery. Recovery Site Strategies Depending on how much downtime an organization has before the technology recovery must be complete, recovery strategies selected for the technology environment could be any one of the following: Dual Data Center-This strategy is employed for applications, which cannot accept any downtime without negatively impacting the organization. The applications are split between two geographically dispersed data centers and either load balanced between the two centers or hot swapped between the two centers. The surviving data center must have enough head room to carry the full production load in either case.
External Hot Site-This strategy has equipment on the floor waiting, but the environment must be rebuilt for the recovery. These are services contracted through a recovery service provider. Again, it is important that the two environments be kept as close to identical as possible to avoid problems with O/S levels, hardware differences, capacity differences, etc., from preventing or delaying recovery. Hot site vendors tend to have the most commonly used hardware and software products to attract the largest number of customers to utilize the site. Unique equipment or software would generally need to be provided by the organization either at time of disaster or stored there ahead of time.
Warm Site-A leased or rented facility that is usually partially configured with some equipment, but not the actual computers. It will generally have all the cooling, cabling, and networks in place to accommodate the recovery but the actual servers, mainframe, etc., equipment are delivered to the site at time of disaster.
Cold Site-A cold site is a shell or empty data center space with no technology on the floor. All technology must be purchased or acquired at the time of disaster.

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 21265-21291). Auerbach Publications. Kindle Edition.

NEW QUESTION: 72
Physically securing backup tapes from unauthorized access is obviously a security concern and is considered a function of the:
A. Operations Security Domain.
B. Operations Security Domain Analysis.
C. Telecommunications and Network Security Domain.
D. Business Continuity Planning and Disater Recovery Planning.
Answer: (SHOW ANSWER)
Physically securing the tapes from unauthorized access is obviously a security concern and is considered a function of the Operations Security Domain. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 71.

NEW QUESTION: 73
Packet Filtering Firewalls examines both the source and destination address of the:
A. incoming and outgoing data packets
B. outgoing data packets only
C. Incoming Data packets only
D. user data packet
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
Packeting filtering firewalls are devices that enforce administrative security policies by filtering incoming traffic as well as outgoing traffic based on rules that can include the source and/or destination addresses.
"Outgoing data packets" is incorrect. Firewalls filter incoming as well as outgoing traffic. This is sometimes called Egress and Ingress filtering.
"Incoming data packets only" is incorrect. (see previous explantion)
"User data packet" is incorrect. A packet filtering firewall does not typicallly look into the data portion of the packet.
References
CBK, p. 464
AIO3, pp. 482 - 484

NEW QUESTION: 74
Which of the following is a disadvantage of a statistical anomaly-based intrusion detection system?
A. it may truly detect a non-attack event that had caused a momentary anomaly in the system.

B. it may falsely detect a non-attack event that had caused a momentary anomaly in the system.
C. it may correctly detect a non-attack event that had caused a momentary anomaly in the system.
D. it may loosely detect a non-attack event that had caused a momentary anomaly in the system.
Answer: (SHOW ANSWER)
Section: Analysis and Monitoring
Explanation/Reference:
Some disadvantages of a statistical anomaly-based ID are that it will not detect an attack that does not significantly change the system operating characteristics, or it may falsely detect a non-attack event that had caused a momentary anomaly in 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 49.

NEW QUESTION: 75
Which of the following is best defined as an administrative declaration by a designated authority that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards?
A. Certification
B. Declaration
C. Audit
D. Accreditation
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
Accreditation: is an administrative declaration by a designated authority that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards. It is usually based on a technical certification of the system's security mechanisms.
Certification: Technical evaluation (usually made in support of an accreditation action) of an information system
\'s security features and other safeguards to establish the extent to which the system\'s design and implementation meet specified security requirements.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 76
Which of the following can be best defined as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data and for detecting or extracting the marks later?
A. Steganography
B. Digital watermarking
C. Digital enveloping
D. Digital signature
Answer: (SHOW ANSWER)

RFC 2828 (Internet Security Glossary) defines digital watermarking as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data-text, graphics, images, video, or audio#and for detecting or extracting the marks later. The set of embedded bits (the digital watermark) is sometimes hidden, usually imperceptible, and always intended to be unobtrusive. It is used as a measure to protect intellectual property rights. Steganography involves hiding the very existence of a message. A digital signature is a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity. A digital envelope is a combination of encrypted data and its encryption key in an encrypted form that has been prepared for use of the recipient.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 77
Which of the following embodies all the detailed actions that personnel are required to follow?
A. Standards
B. Guidelines
C. Procedures
D. Baselines
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
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: 78
A confidential number used as an authentication factor to verify a user's identity is called a:
A. PIN
B. User ID
C. Password
D. Challenge
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
PIN Stands for Personal Identification Number, as the name states it is a combination of numbers.
The following answers are incorrect:
User ID This is incorrect because a Userid is not required to be a number and a Userid is only used to establish identity not verify it.
Password. This is incorrect because a password is not required to be a number, it could be any combination of characters.
Challenge. This is incorrect because a challenge is not defined as a number, it could be anything.

NEW QUESTION: 79
A timely review of system access audit records would be an example of which of the basic security functions?
A. avoidance
B. deterrence
C. prevention
D. detection
Answer: D (LEAVE A REPLY)
Explanation/Reference:
By reviewing system logs you can detect events that have occured.
The following answers are incorrect:
avoidance. This is incorrect, avoidance is a distractor. By reviewing system logs you have not avoided anything.
deterrence. This is incorrect because system logs are a history of past events. You cannot deter something that has already occurred.
prevention. This is incorrect because system logs are a history of past events. You cannot prevent something that has already occurred.

NEW QUESTION: 80

What Orange Book security rating is reserved for systems that have been evaluated but fail to meet the criteria and requirements of the higher divisions?

A. A
B. D
C. E
D. F
Answer: (SHOW ANSWER)
D or "minimal protection" is reserved for systems that were evaluated under the TCSEC but did not meet the requirements for a higher trust level.
A is incorrect. A or "Verified Protectection" is the highest trust level under the TCSEC. E is incorrect. The trust levels are A - D so "E" is not a valid trust level.
F is incorrect. The trust levels are A - D so "F" is not a valid trust level.
CBK, pp. 329 - 330 AIO3, pp. 302 - 306

NEW QUESTION: 81
Which is the last line of defense in a physical security sense?
A. people
B. interior barriers
C. exterior barriers
D. perimeter barriers
Answer: (SHOW ANSWER)
Explanation/Reference:
"Ultimately, people are the last line of defense for your company's assets" (Pastore & Dulaney, 2006, p. 529).
Pastore, M. and Dulaney, E. (2006). CompTIA Security+ study guide: Exam SY0-101. Indianapolis, IN: Sybex.

NEW QUESTION: 82
A security policy is a rigid set of rules that must be followed explicitly in order to be effective.
A. False
B. True
Answer: (SHOW ANSWER)

NEW QUESTION: 83
Which of the following is unlike the other three choices presented?
A. El Gamal
B. Teardrop
C. Buffer Overflow
D. Smurf
Answer: A (LEAVE A REPLY)

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, pages 76, 157.

NEW QUESTION: 84

_____ states that users should only be given enough access to accomplish their jobs.

A. Concept of Least Privilege

B. All of the listed items are correct

C. Due Diligence

D. Separation of Duties

Answer: A (LEAVE A REPLY)

NEW QUESTION: 85

_____ is ultimately responsible for security and privacy violations.

A. Person committing the violation

B. CIO / CEO

C. OS Software

D. Security Officer

Answer: (SHOW ANSWER)

NEW QUESTION: 86

Public Key Infrastructure (PKI) uses asymmetric key encryption between parties. The originator encrypts information using the intended recipient's "public" key in order to get confidentiality of the data being sent. The recipients use their own "private" key to decrypt the information. The "Infrastructure" of this methodology ensures that:

A. The sender and recipient have reached a mutual agreement on the encryption key exchange that they will use.

B. The channels through which the information flows are secure.

C. The recipient's identity can be positively verified by the sender.

D. The sender of the message is the only other person with access to the recipient's private key.

Answer: (SHOW ANSWER)

Through the use of Public Key Infrastructure (PKI) the recipient's identity can be positively verified by the sender.

The sender of the message knows he is using a Public Key that belongs to a specific user. He can validate through the Certification Authority (CA) that a public key is in fact the valid public key of the receiver and the receiver is really who he claims to be. By using the public key of the recipient, only the recipient using the matching private key will be able to decrypt the message. When you wish to achieve confidentiality, you encrypt the message with the recipient public key.

If the sender would wish to prove to the recipient that he is really who he claims to be then the sender would apply a digital signature on the message before encrypting it with the public key of the receiver. This would provide Confidentiality and Authenticity of the message.

A PKI (Public Key Infrastructure) enables users of an insecure public network, such as the Internet, to securely and privately exchange data through the use of public key-pairs that are obtained and shared through a trusted authority, usually referred to as a Certificate Authority.
The PKI provides for digital certificates that can vouch for the identity of individuals or organizations, and for directory services that can store, and when necessary, revoke those
digital certificates. A PKI is the underlying technology that addresses the issue of trust in a normally untrusted environment.
The following answers are incorrect:
The sender and recipient have reached a mutual agreement on the encryption key exchange that they will use. Is incorrect because through the use of Public Key Infrastructure (PKI), the parties do not have to have a mutual agreement. They have a trusted 3rd party Certificate Authority to perform the verification of the sender.
The channels through which the information flows are secure. Is incorrect because the use of Public Key Infrastructure (PKI) does nothing to secure the channels.
The sender of the message is the only other person with access to the recipient's private key. Is incorrect because the sender does not have access to the recipient's private key though Public Key Infrastructure (PKI).
Reference(s) used for this question:
OIG CBK Cryptography (pages 253 - 254)

NEW QUESTION: 87
Which of the following layers provides end-to-end data transfer service?
A. Network Layer.
B. Data Link Layer.
C. Transport Layer.
D. Presentation Layer.
Answer: (SHOW ANSWER)
Explanation/Reference:
It is the Transport Layer that is responsible for reliable end-to-end data transfer between end systems.
The following answers are incorrect:
Network Layer. Is incorrect because the Network Layer is the OSI layer that is responsible for routing, switching, and subnetwork access across the entire OSI environment.
Data Link Layer. Is incorrect because the Data Link Layer is the serial communications path between nodes or devices without any intermediate switching nodes.
Presentation Layer. Is incorrect because the Presentation Layer is the OSI layer that determines how application information is represented (i.e., encoded) while in transit between two end systems.

NEW QUESTION: 88
What refers to legitimate users accessing networked services that would normally be restricted to them?
A. Spoofing
B. Piggybacking

C. Eavesdropping
D. Logon abuse
Answer: (SHOW ANSWER)
Unauthorized access of restricted network services by the circumvention of security access controls is known as logon abuse. This type of abuse refers to users who may be internal to the network but access resources they would not normally be allowed. 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 74).

NEW QUESTION: 89
Which of the following is an example of One-Time Password technology? (Choose all that apply)
A. LC3
B. OPIE
C. MD5
D. S/Key
Answer: (SHOW ANSWER)

NEW QUESTION: 90
How would nonrepudiation be best classified as?
A. A preventive control
B. A logical control
C. A corrective control
D. A compensating control
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Systems accountability depends on the ability to ensure that senders cannot deny sending information and that receivers cannot deny receiving it. Because the mechanisms implemented in nonrepudiation prevent the ability to successfully repudiate an action, it can be considered as a preventive control. Source: STONEBURNER, Gary, NIST Special Publication 800-33: Underlying Technical Models for Information Technology Security, National Institute of Standards and Technology, December 2001, page 7.

NEW QUESTION: 91
Which of the following choice is NOT normally part of the questions that would be asked in regards to an organization's information security policy?
A. Who is involved in establishing the security policy?
B. Where is the organization's security policy defined?
C. What are the actions that need to be performed in case of a disaster?
D. Who is responsible for monitoring compliance to the organization's security policy?
Answer: (SHOW ANSWER)

Section: Security Operation Adimnistration
Explanation/Reference:
Actions to be performed in case of a disaster are not normally part of an information security policy but part of a Disaster Recovery Plan (DRP).
Only personnel implicated in the plan should have a copy of the Disaster Recovery Plan whereas everyone should be aware of the contents of the organization's information security policy.
Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Appendix B, Practice-Level Policy Considerations (page 398).

NEW QUESTION: 92
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: (SHOW ANSWER)
Explanation/Reference:
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: 93
Smart cards are an example of which type of control?
A. Detective control

B. Administrative control
C. Technical control
D. Physical control
Answer: (SHOW ANSWER)
Explanation/Reference:
Logical or technical controls involve the restriction of access to systems and the protection of information. Smart cards and encryption are examples of these types of 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.
Many types of technical controls enable a user to access a system and the resources within that system. A technical control may be a username and password combination, a Kerberos implementation, biometrics, public key infrastructure (PKI), RADIUS, TACACS +, or authentication using a smart card through a reader connected to a system. These technologies verify the user is who he says he is by using different types of authentication methods. Once a user is properly authenticated, he can be authorized and allowed access to network resources.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 245). McGraw-Hill. Kindle Edition.
and
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 32).

NEW QUESTION: 94
Which of the following should be emphasized during the Business Impact Analysis (BIA) considering that the BIA focus is on business processes?
A. Composition
B. Priorities
C. Dependencies
D. Service levels
Answer: (SHOW ANSWER)
The Business Impact Analysis (BIA) identifies time-critical aspects of the critical business processes, and determines their maximum tolerable downtime. The BIA helps to Identify organization functions, the capabilities of each organization unit to handle outages, and the priority and sequence of functions and applications to be recovered, identify resources required for recovery of those areas and interdependencies

In performing the Business Impact Analysis (BIA) it is very important to consider what the dependencies are. You cannot bring a system up if it depends on another system to be operational. You need to look at not only internal dependencies but external as well. You might not be able to get the raw materials for your business so dependencies are very important aspect of a BIA.
The BIA committee will not truly understand all business processes, the steps that must take place, or the resources and supplies these processes require. So the committee must gather this information from the people who do know- department managers and specific employees throughout the organization.
The committee starts by identifying the people who will be part of the BIA data-gathering sessions. The committee needs to identify how it will collect the data from the selected employees, be it through surveys, interviews, or workshops. Next, the team needs to collect the information by actually conducting surveys, interviews, and workshops. Data points obtained as part of the information gathering will be used later during analysis. It is important that the team members ask about how different tasks- whether processes, transactions, or services, along with any relevant dependencies- get accomplished within the organization.
The following answers are incorrect: composition This is incorrect because it is not the best answer. While the make up of business may be important, if you have not determined the dependencies first you may not be able to bring the critical business processes to a ready state or have the materials on hand that are needed.
priorities This is incorrect because it is not the best answer. While the priorities of processes are important, if you have not determined the dependencies first you may not be able to bring the critical business processes to a ready state or have the materials on hand that are needed.
service levels This is incorrect because it is not the best answer. Service levels are not as important as dependencies.
Reference(s) used for this question:
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Business Continuity and Disaster Recovery Planning (Kindle Locations 188-191). . Kindle Edition.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 18562-18568). McGraw-Hill. Kindle Edition.

NEW QUESTION: 95
The IP header contains a protocol field. If this field contains the value of 6, what type of data is contained within the ip datagram?
A. TCP.
B. ICMP.
C. UDP.
D. IGMP.
Answer: (SHOW ANSWER)
Explanation/Reference:

If the protocol field has a value of 6 then it would indicate it was TCP.
The protocol field of the IP packet dictates what protocol the IP packet is using.
TCP=6, ICMP=1, UDP=17, IGMP=2
The following answers are incorrect:
ICMP. Is incorrect because the value for an ICMP protocol would be 1.
UDP. Is incorrect because the value for an UDP protocol would be 17.
IGMP. Is incorrect because the value for an IGMP protocol would be 2.
References:
SANS http://www.sans.org/resources/tcpip.pdf?ref=3871

NEW QUESTION: 96
Which method of password cracking takes the most time and effort?
A. Guessing
B. Shoulder Surfing
C. Hybrid
D. Brute Force
E. Dictionary attack
Answer: (SHOW ANSWER)

NEW QUESTION: 97
Which of the following is the WEAKEST authentication mechanism?
A. Passphrases
B. Passwords
C. One-time passwords
D. Token devices
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Most of the time users usually choose passwords which can be guessed , hence passwords is the BEST answer out of the choices listed above.
The following answers are incorrect because :
Passphrases is incorrect as it is more secure than a password because it is longer.
One-time passwords is incorrect as the name states , it is good for only once and cannot be reused.
Token devices is incorrect as this is also a password generator and is an one time password mechanism.
Reference : Shon Harris AIO v3 , Chapter-4 : Access Control , Page : 139 , 142.

NEW QUESTION: 98
Which of the following best allows risk management results to be used knowledgeably?
A. A vulnerability analysis
B. A likelihood assessment
C. An uncertainty analysis

D. A threat identification

Answer: (SHOW ANSWER)

Risk management consists of two primary and one underlying activity; risk assessment and risk mitigation are the primary activities and uncertainty analysis is the underlying one. After having performed risk assessment and mitigation, an uncertainty analysis should be performed. Risk management must often rely on speculation, best guesses, incomplete data, and many unproven assumptions. A documented uncertainty analysis allows the risk management results to be used knowledgeably. A vulnerability analysis, likelihood assessment and threat identification are all parts of the collection and analysis of data part of the risk assessment, one of the primary activities of risk management. Source: SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (pages 19-21).

NEW QUESTION: 99

In Discretionary Access Control the subject has authority, within certain limitations,

A. but he is not permitted to specify what objects can be accessible and so we need to get an independent third party to specify what objects can be accessible.

B. to specify what objects can be accessible.

C. to specify on a aggregate basis without understanding what objects can be accessible.

D. to specify in full detail what objects can be accessible.

Answer: (SHOW ANSWER)

Explanation/Reference:

With Discretionary Access Control, the subject has authority, within certain limitations, to specify what objects can be accessible.

For example, access control lists can be used. This type of access control is used in local, dynamic situations where the subjects must have the discretion to specify what resources certain users are permitted to access.

When a user, within certain limitations, has the right to alter the access control to certain objects, this is termed as user-directed discretionary access control. In some instances, a hybrid approach is used, which combines the features of user-based and identity-based discretionary access control.

References:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

and

HARRIS, Shon, All-In-One CISSP Certification Exam Guide 5th Edition, McGraw-Hill/Osborne, 2010, Chapter 4: Access Control (page 210-211).

NEW QUESTION: 100

Which of the following IEEE standards defines the token ring media access method?

A. 802.3

B. 802.11

C. 802.5
D. 802.2
Answer: (SHOW ANSWER)
The IEEE 802.5 standard defines the token ring media access method. 802.3 refers to Ethernet's CSMA/CD, 802.11 refers to wireless communications and 802.2 refers to the logical link control.
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 109).

NEW QUESTION: 101
Which of the following is the most secure firewall implementation?
A. Dual-homed host firewalls
B. Screened-subnet firewalls
C. Screened-host firewalls
D. Packet-filtering firewalls
Answer: (SHOW ANSWER)
One the most secure implementations of firewall architectures is the screened-subnet firewall. It employs two packet-filtering routers and a bastion host. Like a screened host firewall, this firewall supports both packet-filtering and proxy services. 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 93).

NEW QUESTION: 102
What are the three performance measurements used in biometrics?
(Choose three)
A. Crossover error rate
B. False rejection rate
C. Positive error rate
D. False acceptance rate
E. Negative error rate
Answer: (SHOW ANSWER)
The Crossover error rate, false reject rate, and the false acceptance rate are the three main performance measurements used in biometrics.

NEW QUESTION: 103
Which disaster recovery plan test involves functional representatives meeting to review the plan in detail?
A. Simulation test
B. Checklist test
C. Parallel test
D. Structured walk-through test
Answer: (SHOW ANSWER)

The structured walk-through test occurs when the functional representatives meet to review the plan in detail. This involves a thorough look at each of the plan steps, and the procedures that are invoked at that point in the plan. This ensures that the actual planned activities are accurately described in the plan. The checklist test is a method of testing the plan by distributing copies to each of the functional areas. The simulation test plays out different scenarios. The parallel test is essentially an operational test that is performed without interrupting current processing.
Source: HARE, Chris, CISSP Study Guide: Business Continuity Planning Domain,

NEW QUESTION: 104
Which integrity model defines a constrained data item, an integrity verification procedure and a transformation procedure?
A. The Take-Grant model
B. The Biba integrity model
C. The Clark Wilson integrity model
D. The Bell-LaPadula integrity model
Answer: (SHOW ANSWER)
Section: Access Control
Explanation
Explanation/Reference:
The Clark Wilson integrity model addresses the three following integrity goals: 1) data is protected from modification by unauthorized users; 2) data is protected from unauthorized modification by authorized users; and 3) data is internally and externally consistent. It also defines a Constrained Data Item (CDI), an Integrity Verification Procedure (IVP), a Transformation Procedure (TP) and an Unconstrained Data item. The Bell- LaPadula and Take-Grant models are not integrity models.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architecture and Models (page 205).

NEW QUESTION: 105
What level of assurance for a digital certificate verifies a user's name, address, social security number, and other information against a credit bureau database?
A. Level 1/Class 1
B. Level 2/Class 2
C. Level 3/Class 3
D. Level 4/Class 4
Answer: (SHOW ANSWER)
Users can obtain certificates with various levels of assurance. Here is a list that describe each of them:
-
Class 1/Level 1 for individuals, intended for email, no proof of identity For example, level 1 certificates verify electronic mail addresses. This is done through the use of a personal information number that a user would supply when asked to register. This level of certificate may also provide a name as well as an

electronic mail address; however, it may or may not be a genuine name (i.e., it could be an alias). This proves that a human being will reply back if you send an email to that name or email address.

-

Class 2/Level 2 is for organizations and companies for which proof of identity is required Level 2 certificates verify a user's name, address, social security number, and other information against a credit bureau database.

-

Class 3/Level 3 is for servers and software signing, for which independent verification and checking of identity and authority is done by the issuing certificate authority Level 3 certificates are available to companies. This level of certificate provides photo identification to accompany the other items of information provided by a level 2 certificate.

-

Class 4 for online business transactions between companies

-

Class 5 for private organizations or governmental security

References:

http://en.wikipedia.org/wiki/Digital_certificate veriSign introduced the concept of classes of digital certificates:

Also see:

Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 3, Secured Connections to External Networks (page 54).

NEW QUESTION: 106

What is defined as the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept?

A. The reference monitor

B. Protection rings

C. A security kernel

D. A protection domain

Answer: (SHOW ANSWER)

A security kernel is defined as the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept. A reference monitor is a system component that enforces access controls on an object. A protection domain consists of the execution and memory space assigned to each process. The use of protection rings is a scheme that supports multiple protection domains.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architecture and Models (page 194).

NEW QUESTION: 107
Cryptography does NOT help in:
A. Detecting fraudulent insertion.
B. Detecting fraudulent deletion.
C. Detecting fraudulent modification.
D. Detecting fraudulent disclosure.
Answer: (SHOW ANSWER)
Explanation/Reference:
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: 108
EDI (Electronic Data Interchange) differs from e-Commerce in that _____.
A. EDI allows companies to take credit cards directly to consumers via the web
B. EDI involves only computer to computer transactions
C. None of the items listed accurately reflect the differences between EDI and e-Commerce
D. E-Commerce involves only computer to computer transactions
Answer: (SHOW ANSWER)

NEW QUESTION: 109
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)
Explanation/Reference:
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: 110

Of the reasons why a Disaster Recovery plan gets outdated, which of the following is not true?

A. Personnel turnover
B. Large plans can take a lot of work to maintain
C. Continous auditing makes a Disaster Recovery plan irrelevant
D. Infrastructure and environment changes
Answer: (SHOW ANSWER)
Explanation/Reference:
Although a auditing is a part of corporate security, it in no way supercedes the requirments for a disaster recovery plan. All others can be blamed for a plan going out of date.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter
9: Disaster Recovery and Business continuity (page 609).

NEW QUESTION: 111
Of the reasons why a Disaster Recovery plan gets outdated, which of the following is not true?
A. Personnel turnover
B. Large plans can take a lot of work to maintain
C. Continous auditing makes a Disaster Recovery plan irrelevant
D. Infrastructure and environment changes
Answer: C (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation
Explanation/Reference:
Although a auditing is a part of corporate security, it in no way supercedes the requirments for a disaster recovery plan. All others can be blamed for a plan going out of date.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9:
Disaster Recovery and Business continuity (page 609).

NEW QUESTION: 112
Which of the following cannot be undertaken in conjunction or while computer incident handling is ongoing?
A. System development activity
B. Help-desk function
C. System Imaging
D. Risk management process
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
If Incident Handling is underway an incident has potentially been identified. At that point all use of the system should stop because the system can no longer be trusted and any changes could contaminate the evidence.

This would include all System Development Activity.
Every organization should have plans and procedures in place that deals with Incident Handling. Employees should be instructed what steps are to be taken as soon as an incident occurs and how to report it.
It is important that all parties involved are aware of these steps to protect not only any possible evidence but also to prevent any additional harm.
It is quite possible that the fraudster has planted malicous code that could cause destruction or even a Trojan Horse with a back door into the system. As soon as an incident has been identified the system can no longer be trusted and all use of the system should cease.
Shon Harris in her latest book mentions:
Although we commonly use the terms "event" and "incident" interchangeably, there are subtle differences between the two. An event is a negative occurrence that can be observed, verified, and documented, whereas an incident is a series of events that negatively affects the company and/ or impacts its security posture. This is why we call reacting to these issues "incident response" (or "incident handling"), because something is negatively affecting the company and causing a security breach.
Many types of incidents (virus, insider attack, terrorist attacks, and so on) exist, and sometimes it is just human error. Indeed, many incident response individuals have received a frantic call in the middle of the night because a system is acting "weird." The reasons could be that a deployed patch broke something, someone misconfigured a device, or the administrator just learned a new scripting language and rolled out some code that caused mayhem and confusion.
When a company endures a computer crime, it should leave the environment and evidence unaltered and contact whomever has been delegated to investigate these types of situations. Someone who is unfamiliar with the proper process of collecting data and evidence from a crime scene could instead destroy that evidence, and thus all hope of prosecuting individuals, and achieving a conviction would be lost.
Companies should have procedures for many issues in computer security such as enforcement procedures, disaster recovery and continuity procedures, and backup procedures. It is also necessary to have a procedure for dealing with computer incidents because they have become an increasingly important issue of today's information security departments. This is a direct result of attacks against networks and information systems increasing annually. Even though we don't have specific numbers due to a lack of universal reporting and reporting in general, it is clear that the volume of attacks is increasing. Just think about all the spam, phishing scams, malware, distributed denial-of-service, and other attacks you see on your own network and hear about in the news. Unfortunately, many companies are at a loss as to who to call or what to do right after they have been the victim of a cybercrime. Therefore, all companies should have an incident response policy that indicates who has the authority to initiate an incident response, with supporting procedures set up before an incident takes place.
This policy should be managed by the legal department and security department. They need to work together to make sure the technical security issues are covered and the legal issues that surround criminal activities are properly dealt with. The incident response policy should be clear and concise. For example, it should indicate if systems can be taken offline to try to save evidence or if systems have to continue functioning at the risk of destroying evidence. Each system and functionality should have a

priority assigned to it. For instance, if the file server is infected, it should be removed from the network, but not shut down. However, if the mail server is infected, it should not be removed from the network or shut down because of the priority the company attributes to the mail server over the file server. Tradeoffs and decisions will have to be made, but it is better to think through these issues before the situation occurs, because better logic is usually possible before a crisis, when there's less emotion and chaos.
The Australian Computer Emergency Response Team's General Guidelines for Computer Forensics:
Keep the handling and corruption of original data to a minimum.
Document all actions and explain changes.
Follow the Five Rules for Evidence (Admissible, Authentic, Complete, Accurate, Convincing).
* Bring in more experienced help when handling and/ or analyzing the evidence is beyond your knowledge, skills, or abilities.
Adhere to your organization's security policy and obtain written permission to conduct a forensics investigation.
Capture as accurate an image of the system(s) as possible while working quickly.
Be ready to testify in a court of law.
Make certain your actions are repeatable.
Prioritize your actions, beginning with volatile and proceeding to persistent evidence.
Do not run any programs on the system(s) that are potential evidence.
Act ethically and in good faith while conducting a forensics investigation, and do not attempt to do any harm.
The following answers are incorrect:
help-desk function. Is incorrect because during an incident, employees need to be able to communicate with a central source. It is most likely that would be the help-desk. Also the help-desk would need to be able to communicate with the employees to keep them informed.
system imaging. Is incorrect because once an incident has occured you should perform a capture of evidence starting with the most volatile data and imaging would be doen using bit for bit copy of storage medias to protect the evidence.
risk management process. Is incorrect because incident handling is part of risk management, and should continue.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 21468-21476). McGraw-Hill. Kindle Edition.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 21096-21121). McGraw-Hill. Kindle Edition.
and
NIST Computer Security incident handling http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter12.html

NEW QUESTION: 113
A proxy is considered a:

A. first generation firewall.
B. third generation firewall.
C. second generation firewall.
D. fourth generation firewall.
Answer: (SHOW ANSWER)
The proxy (application layer firewall, circuit level proxy, or application proxy) is a second generation firewall
"First generation firewall" incorrect. A packet filtering firewall is a first generation firewall. "Third generation firewall" is incorrect. Stateful Firewall are considered third generation firewalls "Fourth generation firewall" is incorrect. Dynamic packet filtering firewalls are fourth generation firewalls
References:
CBK, p. 464 AIO3, pp. 482 - 484
Neither CBK or AIO3 use the generation terminology for firewall types but you will encounter it frequently as a practicing security professional. See http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm for a general discussion of the different generations.

NEW QUESTION: 114
Which of the following should NOT be performed by an operator?
A. Implementing the initial program load
B. Monitoring execution of the system
C. Data entry
D. Controlling job flow
Answer: (SHOW ANSWER)
Explanation/Reference:
Under the principle of separation of duties, an operator should not be performing data entry. This should be left to data entry personnel.
System operators represent a class of users typically found in data center environments where mainframe systems are used. They provide day-to-day operations of the mainframe environment, ensuring that scheduled jobs are running effectively and troubleshooting problems that may arise. They also act as the arms and legs of the mainframe environment, load and unloading tape and results of job print runs.
Operators have elevated privileges, but less than those of system administrators. If misused, these privileges may be used to circumvent the system's security policy. As such, use of these privileges should be monitored through audit logs.
Some of the privileges and responsibilities assigned to operators include:
Implementing the initial program load: This is used to start the operating system. The boot process or initial program load of a system is a critical time for ensuring system security. Interruptions to this process may reduce the integrity of the system or cause the system to crash, precluding its availability.
Monitoring execution of the system: Operators respond to various events, to include errors, interruptions, and job completion messages.

Volume mounting: This allows the desired application access to the system and its data.
Controlling job flow: Operators can initiate, pause, or terminate programs. This may allow an operator to affect the scheduling of jobs. Controlling job flow involves the manipulation of configuration information needed by the system. Operators with the ability to control a job or application can cause output to be altered or diverted, which can threaten the confidentiality.
Bypass label processing: This allows the operator to bypass security label information to run foreign tapes (foreign tapes are those from a different data center that would not be using the same label format that the system could run). This privilege should be strictly controlled to prevent unauthorized access.
Renaming and relabeling resources: This is sometimes necessary in the mainframe environment to allow programs to properly execute. Use of this privilege should be monitored, as it can allow the unauthorized viewing of sensitive information.
Reassignment of ports and lines: Operators are allowed to reassign ports or lines. If misused, reassignment can cause program errors, such as sending sensitive output to an unsecured location. Furthermore, an incidental port may be opened, subjecting the system to an attack through the creation of a new entry point into the system.
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 19367-19395). Auerbach Publications. Kindle Edition.
129
Which of the following should be performed by an operator?
A. Changing profiles
B. Approving changes
C. Adding and removal of users
D. Installing system software
AnswerD
Of the listed tasks, installing system software is the only task that should normally be performed by an operator in a properly segregated environment.
Source: MOSHER, Richard & ROTHKE, Ben, CISSP CBK Review presentation on domain 7.

NEW QUESTION: 115
How should a risk be HANDLED when the cost of the countermeasure OUTWEIGHS the cost of the risk?
A. Reject the risk
B. Perform another risk analysis
C. Accept the risk
D. Reduce the risk
Answer: (SHOW ANSWER)
Explanation/Reference:
Which means the company understands the level of risk it is faced.
The following answers are incorrect because :
Reject the risk is incorrect as it means ignoring the risk which is dangerous.
Perform another risk analysis is also incorrect as the existing risk analysis has already shown the results.

Reduce the risk is incorrect is applicable after implementing the countermeasures.
Reference : Shon Harris AIO v3 , Chapter-3: Security Management Practices , Page : 39

NEW QUESTION: 116
Which one of the following is used to provide authentication and confidentiality for e-mail messages?
A. Digital signature
B. PGP
C. IPSEC AH
D. MD4
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
Instead of using a Certificate Authority, PGP uses a "Web of Trust", where users can certify each other in a mesh model, which is best applied to smaller groups.
In cryptography, a web of trust is a concept used in PGP, GnuPG, and other OpenPGP compatible systems to establish the authenticity of the binding between a public key and its owner. Its decentralized trust model is an alternative to the centralized trust model of a public key infrastructure (PKI), which relies exclusively on a certificate authority (or a hierarchy of such). The web of trust concept was first put forth by PGP creator Phil Zimmermann in 1992 in the manual for PGP version 2.0.
Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, E-mails, files, directories and whole disk partitions to increase the security of e-mail communications. It was created by Phil Zimmermann in 1991.
As per Shon Harris's book:
Pretty Good Privacy (PGP) was designed by Phil Zimmerman as a freeware e-mail security program and was released in 1991. It was the first widespread public key encryption program. PGP is a complete cryptosystem that uses cryptographic protection to protect e-mail and files. It can use RSA public key encryption for key management and use IDEA symmetric cipher for bulk encryption of data, although the user has the option of picking different types of algorithms for these functions. PGP can provide confidentiality by using the IDEA encryption algorithm, integrity by using the MD5 hashing algorithm, authentication by using the public key certificates, and nonrepudiation by using cryptographically signed messages. PGP initially used its own type of digital certificates rather than what is used in PKI, but they both have similar purposes. Today PGP support
X.509 V3 digital certificates.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 169).
Shon Harris, CISSP All in One book
https://en.wikipedia.org/wiki/Pretty_Good_Privacy
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 117
If any server in the cluster crashes, processing continues transparently, however, the cluster suffers some performance degradation. This implementation is sometimes called a:
A. server farm
B. client farm
C. cluster farm
D. host farm
Answer: (SHOW ANSWER)
If any server in the cluster crashes, processing continues transparently, however, the cluster suffers some performance degradation. This implementation is sometimes called a "server farm."
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: 118
CORRECT TEXT
Accounting, _____, and _____ are the AAAs of information security.
Answer:
Authorization

NEW QUESTION: 119
The throughput rate is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a biometric system. Acceptable throughput rates are in the range of:
A. 100 subjects per minute.
B. 25 subjects per minute.
C. 10 subjects per minute.
D. 50 subjects per minute.
Answer: (SHOW ANSWER)
Explanation/Reference:
The throughput rate is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a biometric system.
Acceptable throughput rates are in the range of 10 subjects per minute.
Things that may impact the throughput rate for some types of biometric systems may include:
A concern with retina scanning systems may be the exchange of body fluids on the eyepiece.
Another concern would be the retinal pattern that could reveal changes in a person's health, such as diabetes or high blood pressure.
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: 120
In order to be able to successfully prosecute an intruder:

A. A point of contact should be designated to be responsible for communicating with law enforcement and other external agencies.
B. A proper chain of custody of evidence has to be preserved.
C. Collection of evidence has to be done following predefined procedures.
D. Whenever possible, analyze a replica of the compromised resource, not the original, thereby avoiding inadvertently tamping with evidence.
Answer: (SHOW ANSWER)
Explanation/Reference:
If you intend on prosecuting an intruder, evidence has to be collected in a lawful manner and, most importantly, protected through a secure chain-of-custody procedure that tracks who has been involved in handling the evidence and where it has been stored. All other choices are all important points, but not the best answer, since no prosecution is possible without a proper, provable chain of custody of evidence.
Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Chapter 7: Responding to Intrusions (pages 282-285).

NEW QUESTION: 121
Identification and authentication are the keystones of most access control systems. Identification establishes:
A. User accountability for the actions on the system.
B. Top management accountability for the actions on the system.
C. EDP department accountability for the actions of users on the system.
D. Authentication for actions on the system
Answer: (SHOW ANSWER)
Identification and authentication are the keystones of most access control systems. Identification establishes user accountability for the actions on the system.
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.
Once a person has been identified through the user ID or a similar value, she must be authenticated, which means she must prove she is who she says she is. Three general factors can be used for authentication: something a person knows, something a person has, and something a person is. They are also commonly called authentication by knowledge, authentication by ownership, and authentication by characteristic.
For a user to be able to access a resource, he first must prove he is who he claims to be, has the necessary credentials, and has been given the necessary rights or privileges to perform the actions he is requesting. Once these steps are completed successfully, the user can access and use network resources; however, it is necessary to track the user's activities and enforce accountability for his actions. Identification describes a method of ensuring that a subject (user, program, or process) is the entity it claims to be. Identification can be provided with the use of a username or account number. To be

properly authenticated, the subject is usually required to provide a second piece to the credential set. This piece could be a password, passphrase, cryptographic key, personal identification number (PIN), anatomical attribute, or token.
These two credential items are compared to information that has been previously stored for this subject. If these credentials match the stored information, the subject is authenticated. But we are not done yet. Once the subject provides its credentials and is properly identified, the system it is trying to access needs to determine if this subject has been given the necessary rights and privileges to carry out the requested actions. The system will look at some type of access control matrix or compare security labels to verify that this subject may indeed access the requested resource and perform the actions it is attempting. If the system determines that the subject may access the resource, it authorizes the subject.
Although identification, authentication, authorization, and accountability have close and complementary definitions, each has distinct functions that fulfill a specific requirement in the process of access control. A user may be properly identified and authenticated to the network, but he may not have the authorization to access the files on the file server. On the other hand, a user may be authorized to access the files on the file server, but until she is properly identified and authenticated, those resources are out of reach.
Reference(s) used for this question:
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition: Access Control ((ISC)2 Press) (Kindle Locations 889-892). Auerbach Publications. Kindle Edition. and Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 3875-3878). McGraw-Hill. Kindle Edition. and Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 3833-3848). McGraw-Hill. Kindle Edition. and Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

NEW QUESTION: 122
Which type of firewall can be used to track connectionless protocols such as UDP and RPC?
A. Stateful inspection firewalls
B. Packet filtering firewalls
C. Application level firewalls
D. Circuit level firewalls
Answer: (SHOW ANSWER)

Explanation/Reference:
Packets in a stateful inspection firewall are queued and then analyzed at all OSI layers, providing a more complete inspection of the data. By examining the state and context of the incoming data packets, it helps to track the protocols that are considered "connectionless", such as UDP-based applications and Remote Procedure Calls (RPC).
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
91).

NEW QUESTION: 123
The three classic ways of authenticating yourself to the computer security software are: something you know, something you have, and something:
A. you need.
B. you read.
C. you are.
D. you do.
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 124
Secure Shell (SSH-2) provides all the following services except:
A. secure remote login
B. command execution
C. port forwarding
D. user authentication
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
This is one of the tricky negative question. You have to pay close attention to the word EXCEPT within the question.
The SSH transport layer is a secure, low level transport protocol. It provides strong encryption, cryptographic host authentication, and integrity protection.
Authentication in this protocol level is host-based; this protocol does not perform user authentication. A higher level protocol for user authentication can be designed on top of this protocol.
The protocol has been designed to be simple and flexible to allow parameter negotiation, and to minimize the number of round-trips. The key exchange method, public key algorithm, symmetric encryption algorithm, message authentication algorithm, and hash algorithm are all negotiated. It is expected that in

most environments, only 2 round-trips will be needed for full key exchange, server authentication, service request, and acceptance notification of service request. The worst case is 3 round-trips.
The following are incorrect answers:
"Remote log-on" is incorrect. SSH does provide remote log-on.
"Command execution" is incorrect. SSH does provide command execution.
"Port forwarding" is incorrect. SSH does provide port forwarding. SSH also has a wonderful feature called SSH Port Forwarding, sometimes called SSH Tunneling, which allows you to establish a secure SSH session and then tunnel arbitrary TCP connections through it. Tunnels can be created at any time, with almost no effort and no programming, which makes them very appealing. See the article below in the reference to take a look at SSH Port Forwarding in detail, as it is a very useful but often misunderstood technology. SSH Port Forwarding can be used for secure communications in a myriad of different ways.
You can see a nice tutorial on the PUTTY web site on how to use PUTTY to do port forwarding at:
http://www.cs.uu.nl/technical/services/ssh/putty/puttyfw.html
Reference(s) used for this question:
RFC 4253 at https://www.ietf.org/rfc/rfc4253.txt
and
SSH Port Forwarding by Symantec

NEW QUESTION: 125
Which of the following best corresponds to the type of memory addressing where the address location that is specified in the program instruction contains the address of the final desired location?
A. Direct addressing
B. Indirect addressing
C. Indexed addressing
D. Program addressing
Answer: (SHOW ANSWER)
Indirect addressing is when the address location that is specified in the program instruction contains the address of the final desired location. Direct addressing is when a portion of primary memory is accessed by specifying the actual address of the memory location. Indexed addressing is when the contents of the address defined in the program's instruction is added to that of an index register. Program addressing is not a defined memory addressing mode.
Source: WALLHOFF, John, CBK#6 Security Architecture and Models (CISSP Study Guide), April 2002 (page 2).

NEW QUESTION: 126
What can be defined as a data structure that enumerates digital certificates that were issued to CAs but have been invalidated by their issuer prior to when they were scheduled to expire?
A. Certificate revocation list
B. Certificate revocation tree
C. Authority revocation list
D. Untrusted certificate list

Answer: (SHOW ANSWER)

Explanation/Reference:

The Internet Security Glossary (RFC2828) defines the Authority Revocation List (ARL) as a data structure that enumerates digital certificates that were issued to CAs but have been invalidated by their issuer prior to when they were scheduled to expire.

Do not to confuse with an ARL with a Certificate Revocation List (CRL). A certificate revocation list is a mechanism for distributing notices of certificate revocations. The question specifically mentions "issued to CAs" which makes ARL a better answer than CRL.

http://rfclibrary.hosting.com/rfc/rfc2828/rfc2828-29.asp

$ certificate revocation list (CRL)

(I) A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were

scheduled to expire. (See: certificate expiration, X.509 certificate revocation list.)

http://rfclibrary.hosting.com/rfc/rfc2828/rfc2828-17.asp

$ authority revocation list (ARL)

(I) A data structure that enumerates digital certificates that were issued to CAs but have been invalidated by their issuer prior to when they were scheduled to expire. (See: certificate expiration, X.509 authority revocation list.)

In a few words: We use CRL's for end-user cert revocation and ARL's for CA cert revocation - both can be placed in distribution points.

NEW QUESTION: 127

Which of the following is NOT a technique used to perform a penetration test?

A. traffic padding

B. scanning and probing

C. war dialing

D. sniffing

Answer: (SHOW ANSWER)

Traffic padding is a countermeasure to traffic analysis.

Even if perfect cryptographic routines are used, the attacker can gain knowledge of the amount of traffic that was generated. The attacker might not know what Alice and Bob were talking about, but can know that they were talking and how much they talked. In certain circumstances this can be very bad. Consider for example when a military is organising a secret attack against another nation: it may suffice to alert the other nation for them to know merely that there is a lot of secret activity going on.

As another example, when encrypting Voice Over IP streams that use variable bit rate encoding, the number of bits per unit of time is not obscured, and this can be exploited to guess spoken phrases.

Padding messages is a way to make it harder to do traffic analysis. Normally, a number of random bits are appended to the end of the message with an indication at the end how much this random data is. The randomness should have a minimum value of 0, a maximum number of N and an even distribution between the two extremes. Note, that increasing 0 does not help, only increasing N helps, though that also means that a lower percentage of the channel will be used to transmit real data. Also note, that

since the cryptographic routine is assumed to be uncrackable (otherwise the padding length itself is crackable), it does not help to put the padding anywhere else, e.g. at the beginning, in the middle, or in a sporadic manner.
The other answers are all techniques used to do Penetration Testing.
References:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, pages 233, 238.
and https://secure.wikimedia.org/wikipedia/en/wiki/Padding_%28cryptography%29#Traffic_anal ysis

NEW QUESTION: 128
Network-based Intrusion Detection systems:
A. Commonly reside on a discrete network segment and monitor the traffic on that network segment.
B. Commonly will not reside on a discrete network segment and monitor the traffic on that network segment.
C. Commonly reside on a discrete network segment and does not monitor the traffic on that network segment.
D. Commonly reside on a host and and monitor the traffic on that specific host.
Answer: (SHOW ANSWER)
Network-based ID systems: -Commonly reside on a discrete network segment and monitor the traffic on that network segment
-Usually consist of a network appliance with a Network Interface Card (NIC) that is operating in promiscuous mode and is intercepting and analyzing the network packets in real time
"A passive NIDS takes advantage of promiscuous mode access to the network, allowing it to gain visibility into every packet traversing the network segment. This allows the system to inspect packets and monitor sessions without impacting the network, performance, or the systems and applications utilizing the network."
NOTE FROM CLEMENT:
A discrete network is a synonym for a SINGLE network. Usually the sensor will monitor a single network segment, however there are IDS today that allow you to monitor multiple LAN's at the same time.
References 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 62.
and
Official (ISC)2 Guide to the CISSP CBK, Hal Tipton and Kevin Henry, Page 196
and
Additional information on IDS systems can be found here:
http://en.wikipedia.org/wiki/Intrusion_detection_system

NEW QUESTION: 129
Which of the following would be the best reason for separating the test and development environments?

A. To restrict access to systems under test.
B. To control the stability of the test environment.
C. To segregate user and development staff.
D. To secure access to systems under development.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
The test environment must be controlled and stable in order to ensure that development projects are tested in a realistic environment which, as far as possible, mirrors the live environment.
Reference(s) used for this question:
Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 309).

NEW QUESTION: 130
What is the framing specification used for transmitting digital signals at 1.544 Mbps on a T1 facility?
A. DS-0
B. DS-1
C. DS-2
D. DS-3
Answer: (SHOW ANSWER)
Explanation/Reference:
Digital Signal level 1 (DS-1) is the framing specification used for transmitting digital signals at 1.544 Mbps on a T1 facility. DS-0 is the framing specification used in transmitting digital signals over a single 64 Kbps channel over a T1 facility. DS-3 is the framing specification used for transmitting digital signals at 44.736 Mbps on a T3 facility. DS-2 is not a defined framing specification.
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
114).

NEW QUESTION: 131
In order to ensure the privacy and integrity of the data, connections between firewalls over public networks should use:
A. Screened subnets
B. Digital certificates
C. An encrypted Virtual Private Network
D. Encryption
Answer: (SHOW ANSWER)
Virtual Private Networks allow a trusted network to communicate with another trusted network over untrusted networks such as the Internet.

Screened Subnet: A screened subnet is essentially the same as the screened host architecture, but adds an extra strata of security by creating a network which the bastion host resides (often call perimeter network) which is separated from the internal network. A screened subnet will be deployed by adding a perimeter network in order to separate the internal network from the external. This assures that if there is a successful attack on the bastion host, the attacker is restricted to the perimeter network by the screening router that is connected between the internal and perimeter network.
Digital Certificates: Digital Certificates will be used in the intitial steps of establishing a VPN but they would not provide the encryption and integrity by themselves.
Encryption: Even thou this seems like a choice that would include the other choices, encryption by itself does not provide integrity mechanims. So encryption would satisfy only half of the requirements of the question.
Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 3, Secured Connections to External Networks (page 65).

NEW QUESTION: 132
In a SSL session between a client and a server, who is responsible for generating the master secret that will be used as a seed to generate the symmetric keys that will be used during the session?
A. Both client and server
B. The client's browser
C. The web server
D. The merchant's Certificate Server
Answer: (SHOW ANSWER)
Explanation/Reference:
Once the merchant server has been authenticated by the browser client, the browser generates a master secret that is to be shared only between the server and client. This secret serves as a seed to generate the session (private) keys. The master secret is then encrypted with the merchant's public key and sent to the server. The fact that the master secret is generated by the client's browser provides the client assurance that the server is not reusing keys that would have been used in a previous session with another client.
Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 6: Cryptography (page 112).
Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, page 569.

NEW QUESTION: 133
Which of the following best corresponds to the type of memory addressing where the address location that is specified in the program instruction contains the address of the final desired location?
A. Direct addressing
B. Indirect addressing
C. Indexed addressing
D. Program addressing
Answer: (SHOW ANSWER)

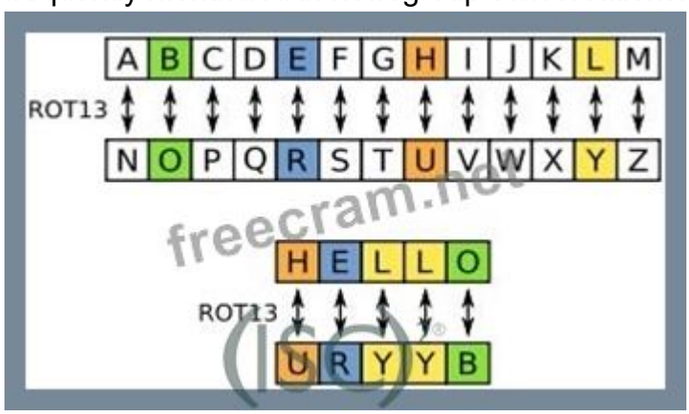
Explanation/Reference:
Indirect addressing is when the address location that is specified in the program instruction contains the address of the final desired location. Direct addressing is when a portion of primary memory is accessed by specifying the actual address of the memory location. Indexed addressing is when the contents of the address defined in the program's instruction is added to that of an index register. Program addressing is not a defined memory addressing mode.
Source: WALLHOFF, John, CBK#6 Security Architecture and Models (CISSP Study Guide), April 2002 (page 2).

NEW QUESTION: 134
What can best be defined as high-level statements, beliefs, goals and objectives?
A. Standards
B. Policies
C. Guidelines
D. Procedures
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
Policies are high-level statements, beliefs, goals and objectives and the general means for their attainment for a specific subject area. Standards are mandatory activities, action, rules or regulations designed to provide policies with the support structure and specific direction they require to be effective. Guidelines are more general statements of how to achieve the policies objectives by providing a framework within which to implement procedures. Procedures spell out the specific steps of how the policy and supporting standards and how guidelines will be implemented.
Source: HARE, Chris, Security management Practices CISSP Open Study Guide, version 1.0, april 1999.

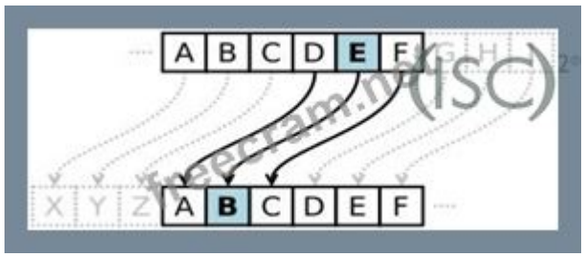
NEW QUESTION: 135
While there are many different models for IT system life cycle most contain five unique phases. Which of the following would be the first phase?
A. Development
B. Initiation
C. Disposal
D. Operation / Maintenance
E. Implementation
Answer: (SHOW ANSWER)
The order of implementation is: initiation, development, implementation, operation/maintenance, and disposal.

NEW QUESTION: 136
What is the name for a substitution cipher that shifts the alphabet by 13 places?
A. Caesar cipher

B. Polyalphabetic cipher
C. ROT13 cipher
D. Transposition cipher
Answer: (SHOW ANSWER)
An extremely simple example of conventional cryptography is a substitution cipher.
A substitution cipher substitutes one piece of information for another. This is most frequently done by offsetting letters of the alphabet. Two examples are Captain Midnight's Secret Decoder Ring, which you may have owned when you were a kid, and Julius Caesar's cipher. In both cases, the algorithm is to offset the alphabet and the key is the number of characters to offset it. So the offset could be one, two, or any number you wish. ROT-13 is an example where it is shifted 13 spaces. The Ceaser Cipher is another example where it is shifted 3 letters to the left.
ROT13 ("rotate by 13 places", sometimes hyphenated ROT-13) is a simple letter substitution cipher that replaces a letter with the letter 13 letters after it in the alphabet. ROT13 is an example of the Caesar cipher, developed in ancient Rome.
In the basic Latin alphabet, ROT13 is its own inverse; that is, to undo ROT13, the same algorithm is applied, so the same action can be used for encoding and decoding. The algorithm provides virtually no cryptographic security, and is often cited as a canonical example of weak encryption.
ROT13 is used in online forums as a means of hiding spoilers, puzzle solutions, and offensive materials from the casual glance. ROT13 has been described as the "Usenet equivalent of a magazine printing the answer to a quiz upside down". ROT13 has inspired a variety of letter and word games on-line, and is frequently mentioned in newsgroup conversations. See diagram Below:



Rot 13 Cipher
The following are incorrect: The Caesar cipher is a simple substitution cipher that involves shifting the alphabet three positions to the right. In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence.



Caesar Cipher Polyalphabetic cipher refers to using multiple alphabets at a time. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The Vigenere cipher is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case.

Viginere Cipher Transposition cipher is a different type of cipher. In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. That is, the order of the units is changed. See the reference below for multiple examples of Transpositio Ciphers.

An exemple of Transposition cipher could be columnar transposition, the message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order. Both the width of the rows and the permutation of the columns are usually defined by a keyword. For example, the word ZEBRAS is of length 6 (so the rows are of length 6), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "6 3 2 4 1 5".

In a regular columnar transposition cipher, any spare spaces are filled with nulls; in an irregular columnar transposition cipher, the spaces are left blank. Finally, the message is read off in columns, in the order specified by the keyword. For example, suppose we use the keyword ZEBRAS and the message WE ARE DISCOVERED. FLEE AT ONCE. In a regular columnar transposition, we write this into the grid as Follows:

Transposition Cipher
Providing five nulls (QKJEU) at the end. The ciphertext is then read off as:
EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE
Reference(s) used for this question:
http://en.wikipedia.org/wiki/ROT13
http://en.wikipedia.org/wiki/Caesar_cipher
http://en.wikipedia.org/wiki/Polyalphabetic_cipher
http://en.wikipedia.org/wiki/Transposition_cipher

NEW QUESTION: 137
As per the Orange Book, what are two types of system assurance?
A. Operational Assurance and Architectural Assurance.
B. Design Assurance and Implementation Assurance.
C. Architectural Assurance and Implementation Assurance.
D. Operational Assurance and Life-Cycle Assurance.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Are the two types of assurance mentioned in the Orange book.
The following answers are incorrect:
Operational Assurance and Architectural Assurance. Is incorrect because Architectural Assurance is not a type of assurance mentioned in the Orange book.
Design Assurance and Implementation Assurance. Is incorrect because neither are types of assurance mentioned in the Orange book.
Architectural Assurance and Implementation Assurance. Is incorrect because neither are types of assurance mentioned in the Orange book.

NEW QUESTION: 138
Which of the following statements pertaining to link encryption is false?
A. It encrypts all the data along a specific communication path.
B. It provides protection against packet sniffers and eavesdroppers.
C. Information stays encrypted from one end of its journey to the other.
D. User information, header, trailers, addresses and routing data that are part of the packets are encrypted.
Answer: (SHOW ANSWER)
Explanation/Reference:
When using link encryption, packets have to be decrypted at each hop and encrypted again.
Information staying encrypted from one end of its journey to the other is a characteristic of end-to-end encryption, not link encryption.
Link Encryption vs. End-to-End Encryption
Link encryption encrypts the entire packet, including headers and trailers, and has to be decrypted at each hop.
End-to-end encryption does not encrypt the IP Protocol headers, and therefore does not need to be decrypted at each hop.
Reference: All in one, Page 735 & Glossary
and
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 6).

NEW QUESTION: 139
Which of the following answers is described as a random value used in cryptographic algorithms to ensure that patterns are not created during the encryption process?
A. IV - Initialization Vector
B. Stream Cipher
C. OTP - One Time Pad
D. Ciphertext
Answer: (SHOW ANSWER)
Explanation/Reference:
The basic power in cryptography is randomness. This uncertainty is why encrypted data is unusable to someone without the key to decrypt.
Initialization Vectors are a used with encryption keys to add an extra layer of randomness to encrypted data. If no IV is used the attacker can possibly break the keyspace because of patterns resulting in the encryption process. Implementation such as DES in Code Book Mode (CBC) would allow frequency analysis attack to take place.
In cryptography, an initialization vector (IV) or starting variable (SV)is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message. For block ciphers, the use of an IV is described by so-called modes of operation. Randomization is also

required for other primitives, such as universal hash functions and message authentication codes based thereon.
It is define by TechTarget as:
An initialization vector (IV) is an arbitrary number that can be used along with a secret key for data encryption. This number, also called a nonce, is employed only one time in any session.
The use of an IV prevents repetition in data encryption, making it more difficult for a hacker using a dictionary attack to find patterns and break a cipher. For example, a sequence might appear twice or more within the body of a message. If there are repeated sequences in encrypted data, an attacker could assume that the corresponding sequences in the message were also identical. The IV prevents the appearance of corresponding duplicate character sequences in the ciphertext.
The following answers are incorrect:
- Stream Cipher: This isn't correct. A stream cipher is a symmetric key cipher where plaintext digits are combined with pseudorandom key stream to product cipher text.
- OTP - One Time Pad: This isn't correct but OTP is made up of random values used as key material. (Encryption key) It is considered by most to be unbreakable but must be changed with a new key after it is used which makes it impractical for common use.
- Ciphertext: Sorry, incorrect answer. Ciphertext is basically text that has been encrypted with key material (Encryption key)
The following reference(s) was used to create this question:
For more details on this TOPIC and other Qs of the Security+ CBK, subscribe to our Holistic Computer Based Tutorial (CBT) at http://www.cccure.tv
and
whatis.techtarget.com/definition/initialization-vector-IV
and
en.wikipedia.org/wiki/Initialization_vector

NEW QUESTION: 140
Crime Prevention Through Environmental Design (CPTED) is a discipline that:
A. Outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior.
B. Outlines how the proper design of the logical environment can reduce crime by directly affecting human behavior.
C. Outlines how the proper design of the detective control environment can reduce crime by directly affecting human behavior.
D. Outlines how the proper design of the administrative control environment can reduce crime by directly affecting human behavior.
Answer: (SHOW ANSWER)
Crime Prevention Through Environmental Design (CPTED) is a discipline that outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior. It provides guidance about lost and crime prevention through proper facility contruction and environmental components and procedures.

CPTED concepts were developed in the 1960s. They have been expanded upon and have matured as our environments and crime types have evolved. CPTED has been used not just to develop corporate physical security programs, but also for large-scale activities such as development of neighborhoods, towns, and cities. It addresses landscaping, entrances, facility and neighborhood layouts, lighting, road placement, and traffic circulation patterns. It looks at microenvironments, such as offices and rest-rooms, and macroenvironments, like campuses and cities.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 435). McGraw-Hill. Kindle Edition. and CPTED Guide Book

NEW QUESTION: 141
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: (SHOW ANSWER)
Section: Access Control
Explanation
Explanation/Reference:
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: 142
Which type of encryption is considered to be unbreakable if the stream is truly random and is as large as the plaintext and never reused in whole or part?
A. One Time Pad (OTP)
B. One time Cryptopad (OTC)
C. Cryptanalysis
D. Pretty Good Privacy (PGP)
Answer: A (LEAVE A REPLY)
Explanation/Reference:
OTP or One Time Pad is considered unbreakable if the key is truly random and is as large as the plaintext and never reused in whole or part AND kept secret.
In cryptography, a one-time pad is a system in which a key generated randomly is used only once to encrypt a message that is then decrypted by the receiver using the matching one-time pad and key.

Messages encrypted with keys based on randomness have the advantage that there is theoretically no way to "break the code" by analyzing a succession of messages. Each encryption is unique and bears no relation to the next encryption so that some pattern can be detected.
With a one-time pad, however, the decrypting party must have access to the same key used to encrypt the message and this raises the problem of how to get the key to the decrypting party safely or how to keep both keys secure. One-time pads have sometimes been used when the both parties started out at the same physical location and then separated, each with knowledge of the keys in the one-time pad.
The key used in a one-time pad is called a secret key because if it is revealed, the messages encrypted with it can easily be deciphered.
One-time pads figured prominently in secret message transmission and espionage before and during World War II and in the Cold War era. On the Internet, the difficulty of securely controlling secret keys led to the invention of public key cryptography.
The biggest challenge with OTP was to get the pad security to the person or entity you wanted to communicate with. It had to be done in person or using a trusted courrier or custodian. It certainly did not scale up very well and it would not be usable for large quantity of data that needs to be encrypted as we often time have today.
The following answers are incorrect:
- One time Cryptopad: Almost but this isn't correct. Cryptopad isn't a valid term in cryptography.
- Cryptanalysis: Sorry, incorrect. Cryptanalysis is the process of analyzing information in an effort to breach the cryptographic security systems.
- PGP - Pretty Good Privacy: PGP, written by Phil Zimmermann is a data encryption and decryption program that provides cryptographic privacy and authentication for data. Still isn't the right answer though.
Read more here about PGP.
The following reference(s) was used to create this question:
To get more info on this Qs or any Qs of Security+, subscribe to the CCCure Holistic Security+ CBT available at: http://www.cccure.tv
and
http://users.telenet.be/d.rijmenants/en/otp.htm
and
http://en.wikipedia.org/wiki/One-time_pad
and
http://searchsecurity.techtarget.com/definition/one-time-pad

NEW QUESTION: 143
Failure of a contingency plan is usually:
A. A technical failure.
B. A management failure.
C. Because of a lack of awareness.
D. Because of a lack of training.
Answer: (SHOW ANSWER)

Failure of a contingency plan is usually management failure to exhibit ongoing interest and concern about the BCP/DRP effort, and to provide financial and other resources as needed. Lack of management support will result in a lack awareness and training.
Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 9: Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) (page 163).

NEW QUESTION: 144
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: (SHOW ANSWER)
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: 145
Which of the following would be the MOST serious risk where a systems development life cycle methodology is inadequate?
A. The project will be completed late.
B. The project will exceed the cost estimates.
C. The project will be incompatible with existing systems.
D. The project will fail to meet business and user needs.
Answer: (SHOW ANSWER)
Explanation/Reference:
This is the most serious risk of inadequate systems development life cycle methodolgy.
The following answers are incorrect because :
The project will be completed late is incorrect as it is not most devastating as the above answer.
The project will exceed the cost estimates is also incorrect when compared to the above correct answer.
The project will be incompatible with existing systems is also incorrect when compared to the above correct answer.
Reference: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 290).

NEW QUESTION: 146

Organizations should not view disaster recovery as which of the following?
A. Committed expense.
B. Discretionary expense.
C. Enforcement of legal statutes.
D. Compliance with regulations.
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation
Explanation/Reference:
Disaster Recovery should never be considered a discretionary expense. It is far too important a task. In order to maintain the continuity of the business Disaster Recovery should be a commitment of and by the organization.
A discretionary fixed cost has a short future planning horizon-under a year. These types of costs arise from annual decisions of management to spend in specific fixed cost areas, such as marketing and research. DR would be an ongoing long term committment not a short term effort only.
A committed fixed cost has a long future planning horizon- more than on year. These types of costs relate to a company's investment in assets such as facilities and equipment. Once such costs have been incurred, the company is required to make future payments.
The following answers are incorrect:
committed expense. Is incorrect because Disaster Recovery should be a committed expense.
enforcement of legal statutes. Is incorrect because Disaster Recovery can include enforcement of legal statutes. Many organizations have legal requirements toward Disaster Recovery.
compliance with regulations. Is incorrect because Disaster Recovery often means compliance with regulations.
Many financial institutions have regulations requiring Disaster Recovery Plans and Procedures.

NEW QUESTION: 147
Related to information security, the guarantee that the message sent is the message received with the assurance that the message was not intentionally or unintentionally altered is an example of which of the following?
A. integrity
B. confidentiality
C. availability
D. identity
Answer: (SHOW ANSWER)
Explanation/Reference:
Integrity is the guarantee that the message sent is the message received, and that the message was not intentionally or unintentionally altered.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 60.

NEW QUESTION: 148
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: (SHOW ANSWER)
Explanation/Reference:
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: 149
Under the Business Exemption Rule to the hearsay evidence, which of the following exceptions would have no bearing on the inadmissibility of audit logs and audit trails in a court of law?
A. Records are collected during the regular conduct of business.
B. Records are collected by senior or executive management.
C. Records are collected at or near the time of occurrence of the act being investigated to generate automated reports.
D. You can prove no one could have changed the records/data/logs that were collected.
Answer: (SHOW ANSWER)
Hearsay evidence is not normally admissible in court unless it has firsthand evidence that can be used to prove the evidence's accuracy, trustworthiness, and reliability like a business person who generated the computer logs and collected them.
It is important that this person generates and collects logs as a normal part of his business and not just this one time for court. It has to be a documented process that is carried out daily.

The value of evidence depends upon the genuineness and competence of the source; therefore, since record collection is not an activity likely to be performed by senior or executive management, records collected by senior or executive management are not likely to be admissible in court.
Hearsay evidence is usually not admissible in court unless it meets the Business Records Exemption rule to the Hearsay evidence.
In certain instances computer records fall outside of the hearsay rule (e.g., business records exemption)
Information relates to regular business activities
Automatically computer generated data
No human intervention
Prove system was operating correctly
Prove no one changed the data
If you have a documented business process and you make use of intrusion detection tools, log analysis tools, and you produce daily reports of activities, then the computer generated data might be admissible in court and would not be considered Hearsay Evidence.
Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 10: Law, Investigation, and Ethics (page 676).

NEW QUESTION: 150

Which of the following would be true about Static password tokens?

A. The owner identity is authenticated by the token
B. The owner will never be authenticated by the token.
C. The owner will authenticate himself to the system.
D. The token does not authenticates the token owner but the system.

Answer: (SHOW ANSWER)

Section: Access Control
Explanation/Reference:
Password Tokens
Tokens are electronic devices or cards that supply a user's password for them. A token system can be used to supply either a static or a dynamic password. There is a big difference between the static and dynamic systems, a static system will normally log a user in but a dynamic system the user will often have to log themselves in.
Static Password Tokens:
The owner identity is authenticated by the token. This is done by the person who issues the token to the owner (normally the employer). The owner of the token is now authenticated by "something you have". The token authenticates the identity of the owner to the information system. An example of this occurring is when an employee swipes his or her smart card over an electronic lock to gain access to a store room.
Synchronous Dynamic Password Tokens:
This system is a lot more complex then the static token password. The synchronous dynamic password tokens generate new passwords at certain time intervals that are synched with the main system. The

password is generated on a small device similar to a pager or a calculator that can often be attached to the user's key ring.
Each password is only valid for a certain time period, typing in the wrong password in the wrong time period will invalidate the authentication. The time factor can also be the systems downfall. If a clock on the system or the password token device becomes out of synch, a user can have troubles authenticating themselves to the system.
Asynchronous Dynamic Password Tokens:
The clock synching problem is eliminated with asynchronous dynamic password tokens. This system works on the same principal as the synchronous one but it does not have a time frame. A lot of big companies use this system especially for employee's who may work from home on the companies VPN (Virtual private Network).
Challenge Response Tokens:
This is an interesting system. A user will be sent special "challenge" strings at either random or timed intervals.
The user inputs this challenge string into their token device and the device will respond by generating a challenge response. The user then types this response into the system and if it is correct they are authenticated.
Reference(s) used for this question:
http://www.informit.com/guides/content.aspx?g=security&seqNum=146
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

NEW QUESTION: 151
Contracts and agreements are often times unenforceable or hard to enforce in which of the following alternate facility recovery agreement?
A. hot site
B. warm site
C. cold site
D. reciprocal agreement
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
A reciprocal agreement is where two or more organizations mutually agree to provide facilities to the other if a disaster occurs. The organizations must have similiar hardware and software configurations. Reciprocal agreements are often not legally binding.
Reciprocal agreements are not contracts and cannot be enforced. You cannot force someone you have such an agreement with to provide processing to you.
Government regulators do not accept reciprocal agreements as valid disaster recovery sites.

Cold sites are empty computer rooms consisting only of environmental systems, such as air conditioning and raised floors, etc. They do not meet the requirements of most regulators and boards of directors that the disaster plan be tested at least annually.
Time Brokers promise to deliver processing time on other systems. They charge a fee, but cannot guaranty that processing will always be available, especially in areas that experienced multiple disasters.
With the exception of providing your own hot site, commercial hot sites provide the greatest protection. Most will allow you up to six weeks to restore your sites if you declare a disaster. They also permit an annual amount of time to test the Disaster Plan.
References:
OIG CBK Business Continuity and Disaster Recovery Planning (pages 368 - 369) The following answers are incorrect:
hot site. Is incorrect because you have a contract in place stating what services are to be provided.
warm site. Is incorrect because you have a contract in place stating what services are to be provided.
cold site. Is incorrect because you have a contract in place stating what services are to be provided.

NEW QUESTION: 152
What is a hot-site facility?
A. A site with pre-installed computers, raised flooring, air conditioning, telecommunications and networking equipment, and UPS.
B. A site in which space is reserved with pre-installed wiring and raised floors.
C. A site with raised flooring, air conditioning, telecommunications, and networking equipment, and UPS.
D. A site with ready made work space with telecommunications equipment, LANs, PCs, and terminals for work groups.
Answer: (SHOW ANSWER)
Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 153
Which type of attack consists of modifying the length and fragmentation offset fields in sequential IP packets?
A. Teardrop attack
B. Smurf attack

C. SYN attack
D. Buffer overflow attack
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
A teardrop attack consists of modifying the length and fragmentation offset fields in sequential IP packets so the target system becomes confused and crashes after it receives contradictory instructions on how the fragments are offset on these packets. A SYN attack is when an attacker floods a system with connection requests but does not respond when the target system replies to those requests. A smurf attack is an attack where the attacker spoofs the source IP address in an ICMP ECHO broadcast packet so it seems to have originated at the victim's system, in order to flood it with REPLY packets. A buffer overflow attack occurs when a process receives much more data than expected.
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
76).

NEW QUESTION: 154
Which of the following would be an example of the best password?
A. golf001
B. Elizabeth
C. T1me4g0lF
D. password
Answer: (SHOW ANSWER)
Explanation/Reference:
The best passwords are those that are both easy to remember and hard to crack using a dictionary attack.
The best way to create passwords that fulfil both criteria is to use two small unrelated words or phonemes, ideally with upper and lower case characters, a special character, and/or a number. Shouldn't be used:
common names, DOB, spouse, phone numbers, words found in dictionaries or system defaults.
Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 1.

NEW QUESTION: 155
Because all the secret keys are held and authentication is performed on the Kerberos TGS and the authentication servers, these servers are vulnerable to:
A. neither physical attacks nor attacks from malicious code.
B. physical attacks only
C. both physical attacks and attacks from malicious code.
D. physical attacks but not attacks from malicious code.
Answer: (SHOW ANSWER)

Section: Access Control
Explanation/Reference:
Since all the secret keys are held and authentication is performed on the Kerberos TGS and the authentication servers, these servers are vulnerable to both physical attacks and attacks from malicious code.
Because a client's password is used in the initiation of the Kerberos request for the service protocol, password guessing can be used to impersonate a client.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 42.

NEW QUESTION: 156
Which of the following statements pertaining to disaster recovery is incorrect?
A. A recovery team's primary task is to get the pre-defined critical business functions at the alternate backup processing site.
B. A salvage team's task is to ensure that the primary site returns to normal processing conditions.
C. The disaster recovery plan should include how the company will return from the alternate site to the primary site.
D. When returning to the primary site, the most critical applications should be brought back first.
Answer: (SHOW ANSWER)
It's interesting to note that the steps to resume normal processing operations will be different than the steps in the recovery plan; that is, the least critical work should be brought back first to the primary site.
My
Explanation:
at the point where the primary site is ready to receive operations again, less critical systems should be brought back first because one has to make sure that everything will be running smoothly at the primary site before returning critical systems, which are already
operating normally at the recovery site.
This will limit the possible interruption of processing to a minimum for most critical systems,
thus making it the best option.
Source: 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 291).

NEW QUESTION: 157
Which of the following statements pertaining to quantitative risk analysis is false?
A. Portion of it can be automated
B. It involves complex calculations
C. It requires a high volume of information
D. It requires little experience to apply
Answer: (SHOW ANSWER)

Assigning the values for the inputs to a purely quantitative risk assessment requires both a lot of time and significant experience on the part of the assessors. The most experienced employees or representatives from each of the departments would be involved in the process. It is NOT an easy task if you wish to come up with accurate values.
"It can be automated" is incorrect. There are a number of tools on the market that automate the process of conducting a quantitative risk assessment.
"It involves complex calculations" is incorrect. The calculations are simple for basic scenarios but could become fairly complex for large cases. The formulas have to be applied correctly.
"It requires a high volume of information" is incorrect. Large amounts of information are required in order to develop reasonable and defensible values for the inputs to the quantitative risk assessment.
References:
CBK, pp. 60-61 AIO3, p. 73, 78 The Cissp Prep Guide - Mastering The Ten Domains Of Computer Security - 2001, page 24

NEW QUESTION: 158
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)
Section: Security Operation Adimnistration
Explanation/Reference:
Change control sub-phase includes Recreating and analyzing the problem, Determining the interface that is presented to the user, and Establishing the priorities of requests.
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 252).

NEW QUESTION: 159
Which of the following is an advantage in using a bottom-up versus a top-down approach to software testing?
A. Interface errors are detected earlier.
B. Errors in critical modules are detected earlier.
C. Confidence in the system is achieved earlier.
D. Major functions and processing are tested earlier.
Answer: (SHOW ANSWER)
Explanation/Reference:
The bottom-up approach to software testing begins with the testing of atomic units, such as programs and modules, and work upwards until a complete system testing has taken place. The advantages of

using a bottom-up approach to software testing are the fact that there is no need for stubs or drivers and errors in critical modules are found earlier. The other choices refer to advantages of a top down approach which follows the opposite path.
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 299).

NEW QUESTION: 160

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)
Explanation/Reference:
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: 161
Which of the following is the most important consideration in locating an alternate computing facility during the development of a disaster recovery plan?
A. It is unlikely to be affected by the same disaster.
B. It is close enough to become operational quickly.
C. It is close enough to serve its users.
D. It is convenient to airports and hotels.
Answer: (SHOW ANSWER)
Explanation/Reference:
You do not want the alternate or recovery site located in close proximity to the original site because the same event that create the situation in the first place might very well impact that site also.
From NIST: "The fixed site should be in a geographic area that is unlikely to be negatively affected by the same disaster event (e.g., weather-related impacts or power grid failure) as the organization's primary site.
The following answers are incorrect:
It is close enough to become operational quickly. Is incorrect because it is not the best answer. You'd want the alternate site to be close but if it is too close the same event could impact that site as well.

It is close enough to serve its users. Is incorrect because it is not the best answer. You'd want the alternate site to be close to users if applicable, but if it is too close the same event could impact that site as well It is convenient to airports and hotels. Is incorrect because it is not the best answer, it is more important that the same event does not impact the alternate site then convenience.
References:
OIG CBK Business Continuity and Disaster Recovery Planning (pages 368 - 369) NIST document 800-34 pg 21

NEW QUESTION: 162
What is it called when a computer uses more than one CPU in parallel to execute instructions?
A. Multiprocessing
B. Multitasking
C. Multithreading
D. Parallel running
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
A system with multiple processors is called a multiprocessing system.
Multitasking is incorrect. Multitasking involves sharing the processor amoung all ready processes. Though it appears to the user that multiple processes are executing at the same time, only one process is running at any point in time.
Multithreading is incorrect. The developer can structure a program as a collection of independent threads to achieve better concurrency. For example, one thread of a program might be performing a calculation while another is waiting for additional input from the user.
"Parallel running" is incorrect. This is not a real term and is just a distraction.
References:
CBK, pp. 315-316
AIO3, pp. 234 - 239

NEW QUESTION: 163
Rule-Based Access Control (RuBAC) access is determined by rules. Such rules would fit within what category of access control ?
A. Discretionary Access Control (DAC)
B. Mandatory Access control (MAC)
C. Non-Discretionary Access Control (NDAC)
D. Lattice-based Access control
Answer: (SHOW ANSWER)
Explanation/Reference:
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.

IT IS NOT ALWAYS BLACK OR WHITE

The different access control models are not totally exclusive of each others. MAC is making use of Rules to be implemented. However with MAC you have requirements above and beyond having simple access rules. The subject would get formal approval from management, the subject must have the proper security clearance, objects must have labels/sensitivity levels attached to them, subjects must have the proper security clearance. If all of this is in place then you have MAC.

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.

NISTR-7316 Says:

Usually a labeling mechanism and a set of interfaces are used to determine access based on the MAC policy; for example, a user who is running a process at the Secret classification should not be allowed to read a file with a label of Top Secret. This is known as the "simple security rule," or "no read up." Conversely, a user who is running a process with a label of Secret should not be allowed to write to a file with a label of Confidential. This rule is called the "*-property" (pronounced "star property") or "no write down." The *-property is required to maintain system security in an automated environment. A variation on this rule called the "strict *-property" requires that information can be written at, but not above, the subject's clearance level. Multilevel security models such as the Bell-La Padula Confidentiality and Biba Integrity models are used to formally specify this kind of MAC policy.

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.
NOTE FROM CLEMENT:
Lot of people tend to confuse MAC and Rule Based Access Control.
Mandatory Access Control must make use of LABELS. If there is only rules and no label, it cannot be Mandatory Access Control. This is why they call it Non Discretionary Access control (NDAC).
There are even books out there that are WRONG on this subject. Books are sometimes opiniated and not strictly based on facts.
In MAC subjects must have clearance to access sensitive objects. Objects have labels that contain the classification to indicate the sensitivity of the object and the label also has categories to enforce the need to know.
Today the best example of rule based access control would be a firewall. All rules are imposed globally to any user attempting to connect through the device. This is NOT the case with MAC.
I strongly recommend you read carefully the following document:
NISTIR-7316 at http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf It is one of the best Access Control Study document to prepare for the exam. Usually I tell people not to worry about the hundreds of NIST documents and other reference. This document is an exception. Take some time to read it.
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 33.
and

NISTIR-7316 at http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf and
Conrad, Eric; Misenar, Seth; Feldman, Joshua (2012-09-01). CISSP Study Guide (Kindle Locations 651-652). Elsevier Science (reference). Kindle Edition.

NEW QUESTION: 164
Which of the following BEST describes a function relying on a shared secret key that is used along with a hashing algorithm to verify the integrity of the communication content as well as the sender?
A. Message Authentication Code - MAC
B. PAM - Pluggable Authentication Module
C. NAM - Negative Acknowledgement Message
D. Digital Signature Certificate
Answer: (SHOW ANSWER)
Section: Cryptography
Explanation/Reference:
The purpose of a message authentication code - MAC is to verify both the source and message integrity without the need for additional processes.
A MAC algorithm, sometimes called a keyed (cryptographic) hash function (however, cryptographic hash function is only one of the possible ways to generate MACs), accepts as input a secret key and an arbitrary- length message to be authenticated, and outputs a MAC (sometimes known as a tag). The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.
MACs differ from digital signatures as MAC values are both generated and verified using the same secret key.
This implies that the sender and receiver of a message must agree on the same key before initiating communications, as is the case with symmetric encryption. For the same reason, MACs do not provide the property of non-repudiation offered by signatures specifically in the case of a network-wide shared secret key:
any user who can verify a MAC is also capable of generating MACs for other messages.
In contrast, a digital signature is generated using the private key of a key pair, which is asymmetric encryption.
Since this private key is only accessible to its holder, a digital signature proves that a document was signed by none other than that holder. Thus, digital signatures do offer non-repudiation.
The following answers are incorrect:
PAM - Pluggable Authentication Module: This isn't the right answer. There is no known message authentication function called a PAM. However, a pluggable authentication module (PAM) is a mechanism to integrate multiple low-level authentication schemes and commonly used within the Linux Operating System.
NAM - Negative Acknowledgement Message: This isn't the right answer. There is no known message authentication function called a NAM. The proper term for a negative acknowledgement is NAK, it is a signal used in digital communications to ensure that data is received with a minimum of errors.

Digital Signature Certificate: This isn't right. As it is explained and contrasted in the explanations provided above.
The following reference(s) was used to create this question:
The CCCure Computer Based Tutorial for Security+, you can subscribe at http://www.cccure.tv and http://en.wikipedia.org/wiki/Message_authentication_code

NEW QUESTION: 165
What is Kerberos?
A. A three-headed dog from the egyptian mythology.
B. A trusted third-party authentication protocol.
C. A security model.
D. A remote authentication dial in user server.
Answer: (SHOW ANSWER)
Is correct because that is exactly what Kerberos is.
The following answers are incorrect:
A three-headed dog from Egyptian mythology. Is incorrect because we are dealing with Information Security and not the Egyptian mythology but the Greek Mythology.
A security model. Is incorrect because Kerberos is an authentication protocol and not just a security model.
A remote authentication dial in user server. Is incorrect because Kerberos is not a remote authentication dial in user server that would be called RADIUS.

NEW QUESTION: 166
Which of the following is the most reliable, secure means of removing data from magnetic storage media such as a magnetic tape, or a cassette?
A. Degaussing
B. Parity Bit Manipulation
C. Zeroization
D. Buffer overflow
Answer: (SHOW ANSWER)
A "Degausser (Otherwise known as a Bulk Eraser) has the main function of reducing to near zero the magnetic flux stored in the magnetized medium. Flux density is measured in Gauss or Tesla. The operation is speedier than overwriting and done in one short operation. This is achieved by subjecting the subject in bulk to a series of fields of alternating polarity and gradually decreasing strength.
The following answers are incorrect:Parity Bit Manipulation. Parity has to do with disk lerror detection, not data removal. A bit or series of bits appended to a character or block of characters to ensure that the information received is the same as the infromation that was sent.
Zeroization. Zeroization involves overwrting data to sanitize it. It is time-consuming and not foolproof. The potential of restoration of data does exist with this method. Buffer overflow. This is a detractor. Although many Operating Systems use a disk buffer to temporarily hold data read from disk, its primary purpose

has no connection to data removal. An overflow goes outside the constraints defined for the buffer and is a method used by an attacker to attempt access to a system.
The following reference(s) were/was used to create this question:
Shon Harris AIO v3. pg 908 Reference: What is degaussing.

NEW QUESTION: 167
Step-by-step instructions used to satisfy control requirements is called a:
A. policy
B. standard
C. guideline
D. procedure
Answer: (SHOW ANSWER)
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 168
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: (SHOW ANSWER)
Explanation/Reference:
Is a means of being 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.
Accountability is the ability to identify users and to be able to track user actions.
The following answers are incorrect:
Documented design as laid out in the Common Criteria. Is incorrect because the Common Criteria is an international standard to evaluate trust and would not be a factor in System Accountability.
Authorization. Is incorrect because Authorization is granting access to subjects, just because you have authorization does not hold the subject accountable for their actions.
Formal verification of system design. Is incorrect because all you have done is to verify the system design and have not taken any steps toward system accountability.

References:
OIG CBK Glossary (page 778)

NEW QUESTION: 169
Which of the following assertions is NOT true about pattern matching and anomaly detection in intrusion detection?
A. Anomaly detection tends to produce more data
B. A pattern matching IDS can only identify known attacks
C. Stateful matching scans for attack signatures by analyzing individual packets instead of traffic streams
D. An anomaly-based engine develops baselines of normal traffic activity and throughput, and alerts on deviations from these baselines
Answer: (SHOW ANSWER)
This is wrong which makes this the correct choice. This statement is not true as stateful matching scans for attack signatures by analyzing traffic streams rather than individual packets. Stateful matching intrusion detection takes pattern matching to the next level.
As networks become faster there is an emerging need for security analysis techniques that can keep up with the increased network throughput. Existing network-based intrusion detection sensors can barely keep up with bandwidths of a few hundred Mbps. Analysis tools that can deal with higher throughput are unable to maintain state between different steps of an attack or they are limited to the analysis of packet headers.
The following answers are all incorrect:
Anomaly detection tends to produce more data is true as an anomaly-based IDS produces a lot of data as any activity outside of expected behavior is recorded.
A pattern matching IDS can only identify known attacks is true as a pattern matching IDS works by comparing traffic streams against signatures. These signatures are created for known attacks.
An anomaly-based engine develops baselines of normal traffic activity and throughput, and alerts on deviations from these baselines is true as the assertion is a characteristic of a statistical anomaly-based IDS.
Reference:
Official guide to the CISSP CBK. Pages 198 to 201
http://cs.ucsb.edu/~vigna/publications/2003_vigna_robertson_kher_kemmerer_ACSAC03.p df

NEW QUESTION: 170
What can be defined as a list of subjects along with their access rights that are authorized to access a specific object?

A. A capability table
B. An access control list
C. An access control matrix
D. A role-based matrix
Answer: (SHOW ANSWER)
Explanation/Reference:

"It [ACL] specifies a list of users [subjects] who are allowed access to each object" CBK, p. 188 A capability table is incorrect. "Capability tables are used to track, manage and apply controls based on the object and rights, or capabilities of a subject. For example, a table identifies the object, specifies access rights allowed for a subject, and permits access based on the user's posession of a capability (or ticket) for the object." CBK, pp. 191-192. The distinction that makes this an incorrect choice is that access is based on posession of a capability by the subject.
To put it another way, as noted in AIO3 on p. 169, "A capabiltiy table is different from an ACL because the subject is bound to the capability table, whereas the object is bound to the ACL." An access control matrix is incorrect. The access control matrix is a way of describing the rules for an access control strategy. The matrix lists the users, groups and roles down the left side and the resources and functions across the top. The cells of the matrix can either indicate that access is allowed or indicate the type of access. CBK pp 317 - 318.
AIO3, p. 169 describes it as a table if subjects and objects specifying the access rights a certain subject possesses pertaining to specific objects.
In either case, the matrix is a way of analyzing the access control needed by a population of subjects to a population of objects. This access control can be applied using rules, ACL's, capability tables, etc.
A role-based matrix is incorrect. Again, a matrix of roles vs objects could be used as a tool for thinking about the access control to be applied to a set of objects. The results of the analysis could then be implemented using RBAC.
References:
CBK, Domain 2: Access Control.
AIO3, Chapter 4: Access Control

NEW QUESTION: 171
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: (SHOW ANSWER)
Explanation/Reference:
There are some conflicting figures as to which group is a bigger threat hackers or employees. Employees are still considered to the leading source of computer crime losses. Employees often have an easier time gaining access to systems or source code then ousiders or other means of creating computer crimes.
A word of caution is necessary: although the media has tended to portray the threat of cybercrime as existing almost exclusively from the outside, external to a company, reality paints a much different picture.
Often the greatest risk of cybercrime comes from the inside, namely, criminal insiders. Information security professionals must be particularly sensitive to the phenomena of the criminal or dangerous insider, as these individuals usually operate under the radar, inside of the primarily outward/external

facing security controls, thus significantly increasing the impact of their crimes while leaving few, if any, audit trails to follow and evidence for prosecution.
Some of the large scale crimes committed agains bank lately has shown that Internal Threats are the worst and they are more common that one would think. The definition of what a hacker is can vary greatly from one country to another but in some of the states in the USA a hacker is defined as Someone who is using resources in a way that is not authorized. A recent case in Ohio involved an internal employee who was spending most of his day on dating website looking for the love of his life. The employee was taken to court for hacking the company resources.
The following answers are incorrect:
hackers. Is incorrect because while hackers represent a very large problem and both the frequency of attacks and overall losses have grown hackers are considered to be a small segment of combined computer fraudsters.
industrial saboteurs. Is incorrect because industrial saboteurs tend to go after trade secrets. While the loss to the organization can be great, they still fall short when compared to the losses created by employees.
Often it is an employee that was involved in industrial sabotage.
foreign intelligence officers. Is incorrect because the losses tend to be national secrets. You really can't put t cost on this and the number of frequency and occurances of this is less than that of employee related losses.
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 22327-22331). Auerbach Publications. Kindle Edition.

NEW QUESTION: 172
Which of the following protocols does not operate at the data link layer (layer 2)?
A. PPP
B. RARP
C. L2F
D. ICMP
Answer: (SHOW ANSWER)
ICMP is the only of the mentioned protocols to operate at the network layer
(layer 3). Other protocols operate at layer 2.
Source: WALLHOFF, John, CBK#2 Telecommunications and Network Security (CISSP
Study Guide), April 2002 (page 1).

NEW QUESTION: 173
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)
Section: Risk, Response and Recovery
Explanation/Reference:
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: 174
Who first described the DoD multilevel military security policy in abstract, formal terms?
A. David Bell and Leonard LaPadula
B. Rivest, Shamir and Adleman
C. Whitfield Diffie and Martin Hellman
D. David Clark and David Wilson
Answer: A (LEAVE A REPLY)
Explanation/Reference:
It was David Bell and Leonard LaPadula who, in 1973, first described the DoD multilevel military security policy in abstract, formal terms. The Bell-LaPadula is a Mandatory Access Control (MAC) model concerned with confidentiality. Rivest, Shamir and Adleman (RSA) developed the RSA encryption algorithm. Whitfield Diffie and Martin Hellman published the Diffie-Hellman key agreement algorithm in 1976. David Clark and David Wilson developed the Clark-Wilson integrity model, more appropriate for security in commercial activities.
Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (pages 78,109).

NEW QUESTION: 175
Which of the following best describes the purpose of debugging programs?
A. To generate random data that can be used to test programs before implementing them.
B. To ensure that program coding flaws are detected and corrected.
C. To protect, during the programming phase, valid changes from being overwritten by other changes.

D. To compare source code versions before transferring to the test environment

Answer: (SHOW ANSWER)

Section: Security Operation Adimnistration

Explanation/Reference:

Debugging provides the basis for the programmer to correct the logic errors in a program under development before it goes into production.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 298).

NEW QUESTION: 176

The standard server port number for HTTP is which of the following?

A. 81

B. 80

C. 8080

D. 8180

Answer: (SHOW ANSWER)

Explanation/Reference:

HTTP is Port 80.

Reference: MAIWALD, Eric, Network Security: A Beginner's Guide, McGraw-Hill/Osborne Media, 2001, page 135.

NEW QUESTION: 177

:Which of the following is considered the LEAST secure?

A. Confidential

B. Public

C. Private

D. Sensitive

Answer: (SHOW ANSWER)

The order of classification from highest to lowest is: Sensitive, Confidential, Private, and Public. Review NIST Special Publication 800-26 for more details about information classifications.

NEW QUESTION: 178

Which of the following statements pertaining to Secure Sockets Layer (SSL) is false?

A. The SSL protocol was developed by Netscape to secure Internet client-server transactions.

B. The SSL protocol's primary use is to authenticate the client to the server using public key cryptography and digital certificates.

C. Web pages using the SSL protocol start with HTTPS

D. SSL can be used with applications such as Telnet, FTP and email protocols.

Answer: (SHOW ANSWER)

Section: Cryptography

Explanation/Reference:
All of these statements pertaining to SSL are true except that it is primary use is to authenticate the client to the server using public key cryptography and digital certificates. It is the opposite, Its primary use is to authenticate the server to the client.
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, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 170).

NEW QUESTION: 179
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:
Capacitance detectors monitor an electrical field surrounding the object being monitored. They are used for spot protection within a few inches of the object, rather than for overall room security monitoring used by wave detectors. Penetration of this field changes the electrical capacitance of the field enough to generate and alarm. Wave pattern motion detectors generate a frequency wave pattern and send an alarm if the pattern is disturbed as it is reflected back to its receiver. Field-powered devices are a type of personnel access control devices. Audio detectors simply monitor a room for any abnormal sound wave generation and trigger an alarm.
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 344).

NEW QUESTION: 180
CORRECT TEXT
A type of virus that resides in a Word or Excel document is called a _____ virus?

Answer:

NEW QUESTION: 181
Physical security is accomplished through proper facility construction, fire and water protection, anti-theft mechanisms, intrusion detection systems, and security procedures that are adhered to and enforced. Which of the following is not a component that achieves this type of security?
A. Administrative control mechanisms
B. Integrity control mechanisms
C. Technical control mechanisms
D. Physical control mechanisms
Answer: (SHOW ANSWER)

Explanation/Reference:
Integrity Controls Mechanisms are not part of physical security. All of the other detractors were correct this one was the wrong one that does not belong to Physical Security. Below you have more details extracted from the SearchSecurity web site:
Information security depends on the security and management of the physical space in which computer systems operate. Domain 9 of the CISSP exam's Common Body of Knowledge addresses the challenges of securing the physical space, its systems and the people who work within it by use of administrative, technical and physical controls. The following Qs are covered:
Facilities management: The administrative processes that govern the maintenance and protection of the physical operations space, from site selection through emergency response.
Risks, issues and protection strategies: Risk identification and the selection of security protection components.
Perimeter security: Typical physical protection controls.
Facilities management
Facilities management is a complex component of corporate security that ranges from the planning of a secure physical site to the management of the physical information system environment. Facilities management responsibilities include site selection and physical security planning (i.e. facility construction, design and layout, fire and water damage protection, antitheft mechanisms, intrusion detection and security procedures.) Protections must extend to both people and assets. The necessary level of protection depends on the value of the assets and data. CISSP® candidates must learn the concept of critical-path analysis as a means of determining a component's business function criticality relative to the cost of operation and replacement. Furthermore, students need to gain an understanding of the optimal location and physical attributes of a secure facility. Among the Qs covered in this domain are site inspection, location, accessibility and obscurity, considering the area crime rate, and the likelihood of natural hazards such as floods or earthquakes.
This domain also covers the quality of construction material, such as its protective qualities and load capabilities, as well as how to lay out the structure to minimize risk of forcible entry and accidental damage. Regulatory compliance is also touched on, as is preferred proximity to civil protection services, such as fire and police stations. Attention is given to computer and equipment rooms, including their location, configuration (entrance/egress requirements) and their proximity to wiring distribution centers at the site.
Physical risks, issues and protection strategies
An overview of physical security risks includes risk of theft, service interruption, physical damage, compromised system integrity and unauthorized disclosure of information. Interruptions to business can manifest due to loss of power, services, telecommunications connectivity and water supply. These can also seriously compromise electronic security monitoring alarm/response devices. Backup options are also covered in this domain, as is a strategy for quantifying the risk exposure by simple formula. Investment in preventive security can be costly. Appropriate redundancy of people skills, systems and infrastructure must be based on the criticality of the data and assets to be preserved. Therefore a strategy is presented that helps determine the selection of cost appropriate controls. Among the Qs covered in this domain are regulatory and legal requirements, common standard security protections

such as locks and fences, and the importance of establishing service level agreements for maintenance and disaster support.
Rounding out the optimization approach are simple calculations for determining mean time between failure and mean time to repair (used to estimate average equipment life expectancy) - essential for estimating the cost/benefit of purchasing and maintaining redundant equipment.
As the lifeblood of computer systems, special attention is placed on adequacy, quality and protection of power supplies. CISSP candidates need to understand power supply concepts and terminology, including those for quality (i.e. transient noise vs. clean power); types of interference (EMI and RFI); and types of interruptions such as power excess by spikes and surges, power loss by fault or blackout, and power degradation from sags and brownouts. A simple formula is presented for determining the total cost per hour for backup power. Proving power reliability through testing is recommended and the advantages of three power protection approaches are discussed (standby UPS, power line conditioners and backup sources) including minimum requirements for primary and alternate power provided.
Environmental controls are explored in this domain, including the value of positive pressure water drains and climate monitoring devices used to control temperature, humidity and reduce static electricity. Optimal temperatures and humidity settings are provided. Recommendations include strict procedures during emergencies, preventing typical risks (such as blocked fans), and the use of antistatic armbands and hygrometers. Positive pressurization for proper ventilation and monitoring for air born contaminants is stressed.
The pros and cons of several detection response systems are deeply explored in this domain. The concept of combustion, the classes of fire and fire extinguisher ratings are detailed. Mechanisms behind smoke- activated, heat-activated and flame-activated devices and Automatic Dial-up alarms are covered, along with their advantages, costs and shortcomings. Types of fire sources are distinguished and the effectiveness of fire suppression methods for each is included. For instance, Halon and its approved replacements are covered, as are the advantages and the inherent risks to equipment of the use of water sprinklers.
Administrative controls
The physical security domain also deals with administrative controls applied to physical sites and assets. The need for skilled personnel, knowledge sharing between them, separation of duties, and appropriate oversight in the care and maintenance of equipment and environments is stressed. A list of management duties including hiring checks, employee maintenance activities and recommended termination procedures is offered. Emergency measures include accountability for evacuation and system shutdown procedures, integration with disaster and business continuity plans, assuring documented procedures are easily available during different types of emergencies, the scheduling of periodic equipment testing, administrative reviews of documentation, procedures and recovery plans, responsibilities delegation, and personnel training and drills.
Perimeter security
Domain nine also covers the devices and techniques used to control access to a space. These include access control devices, surveillance monitoring, intrusion detection and corrective actions. Specifications are provided for optimal external boundary protection, including fence heights and placement, and lighting placement and types. Selection of door types and lock characteristics are covered. Surveillance

methods and intrusion-detection methods are explained, including the use of video monitoring, guards, dogs, proximity detection systems, photoelectric/photometric systems, wave pattern devices, passive infrared systems, and sound and motion detectors, and current flow sensitivity devices that specifically address computer theft. Room lock types - both preset and cipher locks (and their variations) -- device locks, such as portable laptop locks, lockable server bays, switch control locks and slot locks, port controls, peripheral switch controls and cable trap locks are also covered. Personal access control methods used to identify authorized users for site entry are covered at length, noting social engineering risks such as piggybacking.

Wireless proximity devices, both user access and system sensing readers are covered (i.e. transponder based, passive devices and field powered devices) in this domain.

Now that you've been introduced to the key concepts of Domain 9, watch the Domain 9, Physical Security video

Return to the CISSP Essentials Security School main page

See all SearchSecurity.com's resources on CISSP certification training

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 280.

NEW QUESTION: 182

Which of the following would best define a digital envelope?

A. A message that is encrypted and signed with a digital certificate.

B. A message that is signed with a secret key and encrypted with the sender's private key.

C. A message encrypted with a secret key attached with the message. The secret key is encrypted with the public key of the receiver.

D. A message that is encrypted with the recipient's public key and signed with the sender's private key.

Answer: (SHOW ANSWER)

A digital envelope for a recipient is a combination of encrypted data and its encryption key in an encrypted form that has been prepared for use of the recipient.

It consists of a hybrid encryption scheme in sealing a message, by encrypting the data and sending both it and a protected form of the key to the intended recipient, so that one else can open the message.

In PKCS #7, it means first encrypting the data using a symmetric encryption algorithm and a secret key, and then encrypting the secret key using an asymmetric encryption algorithm and the public key of the intended recipient.

Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 183
Configuration Management controls what?
A. Auditing of changes to the Trusted Computing Base.
B. Control of changes to the Trusted Computing Base.
C. Changes in the configuration access to the Trusted Computing Base.
D. Auditing and controlling any changes to the Trusted Computing Base.
Answer: (SHOW ANSWER)
Explanation/Reference:
All of these are components of Configuration Management.
The following answers are incorrect:
Auditing of changes to the Trusted Computing Base. Is incorrect because it refers only to auditing the changes, but nothing about controlling them.
Control of changes to the Trusted Computing Base. Is incorrect because it refers only to controlling the changes, but nothing about ensuring the changes will not lead to a weakness or fault in the system.
Changes in the configuration access to the Trusted Computing Base. Is incorrect because this does not refer to controlling the changes or ensuring the changes will not lead to a weakness or fault in the system.

NEW QUESTION: 184
What can be defined as a digital certificate that binds a set of descriptive data items, other than a public key, either directly to a subject name or to the identifier of another certificate that is a public-key certificate?
A. A public-key certificate
B. An attribute certificate
C. A digital certificate
D. A descriptive certificate
Answer: (SHOW ANSWER)
Section: Cryptography
Explanation/Reference:
The Internet Security Glossary (RFC2828) defines an attribute certificate as a digital certificate that binds a set of descriptive data items, other than a public key, either directly to a subject name or to the identifier of another certificate that is a public-key certificate. A public-key certificate binds a subject name to a public key value, along with information needed to perform certain cryptographic functions. Other attributes of a subject, such as a security clearance, may be certified in a separate kind of digital certificate, called an attribute certificate. A subject may have multiple attribute certificates associated with its name or with each of its public-key certificates.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 185

A proxy can control which services (FTP and so on) are used by a workstation , and also aids in protecting the network from outsiders who may be trying to get information about the:
A. network's design
B. user base
C. operating system design
D. net BIOS' design
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
To the untrusted host, all traffic seems to originate from the proxy server and addresses on the trusted network are not revealed.
"User base" is incorrect. The proxy hides the origin of the request from the untrusted host.
"Operating system design" is incorrect. The proxy hides the origin of the request from the untrusted host.
"Net BIOS' design" is incorrect. The proxy hides the origin of the request from the untrusted host.
References:
CBK, p. 467
AIO3, pp. 486 - 490

NEW QUESTION: 186
Which of the following elements of telecommunications is not used in assuring confidentiality?
A. Network security protocols
B. Network authentication services
C. Data encryption services
D. Passwords
Answer: (SHOW ANSWER)
Passwords are one of the multiple ways to authenticate (prove who you claim to be) an identity which allows confidentiality controls to be enforced to assure the identity can only access the information for which it is authorized. It is the authentication that assists assurance of confidentiality not the passwords.
"Network security protocols" is incorrect. Network security protocols are quite useful in assuring confidentiality in network communications.
"Network authentication services" is incorrect. Confidentiality is concerned with allowing only authorized users to access information. An important part of determining authorization is authenticating an identity and this service is supplied by network authentication services.
"Data encryption services" is incorrect. Data encryption services are quite useful in protecting the confidentiality of information.
Reference(s) used for this question:
Official ISC2 Guide to the CISSP CBK, pp. 407 - 520 AIO 3rd Edition, pp. 415 - 580

NEW QUESTION: 187
Which of the following protocols is designed to send individual messages securely?
A. Kerberos

B. Secure Electronic Transaction (SET).
C. Secure Sockets Layer (SSL).
D. Secure HTTP (S-HTTP).
Answer: (SHOW ANSWER)
Explanation/Reference:
An early standard for encrypting HTTP documents, Secure HTTP (S-HTTP) is designed to send individual messages securely. SSL is designed to establish a secure connection between two computers. SET was originated by VISA and MasterCard as an Internet credit card protocol using digital signatures. Kerberos is an authentication system.
Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 89.

NEW QUESTION: 188
Which of the following is NOT a characteristic or shortcoming of packet filtering gateways?
A. The source and destination addresses, protocols, and ports contained in the IP packet header are the only information that is available to the router in making a decision whether or not to permit traffic access to an internal network.
B. They don't protect against IP or DNS address spoofing.
C. They do not support strong user authentication.
D. They are appropriate for medium-risk environment.
Answer: (SHOW ANSWER)
Packet filtering firewalls use routers with packet filtering rules to grant or deny access based on source address, destination address, and port.
They offer minimum security but at a very low cost, and can be an appropriate choice for a low-risk environment.
Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 3, Secured Connections to External Networks (page 60).

NEW QUESTION: 189
Which of the following is an issue with signature-based intrusion detection systems?
A. Only previously identified attack signatures are detected.
B. Signature databases must be augmented with inferential elements.
C. It runs only on the windows operating system
D. Hackers can circumvent signature evaluations.
Answer: (SHOW ANSWER)
An issue with signature-based ID is that only attack signatures that are
stored in their database are detected.
New attacks without a signature would not be reported. They do require constant updates
in order to maintain their effectiveness.
Reference 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 49.

NEW QUESTION: 190

CORRECT TEXT

NIPC stands for _____ _____ _____ and is a government organization designed to help protect our nation's vital information resources.

Answer:

Infrastructure Protection Center

NEW QUESTION: 191

Asynchronous Communication transfers data by sending:

A. bits of data sequentially

B. bits of data sequentially in irregular timing patterns

C. bits of data in sync with a heartbeat or clock

D. bits of data simultaneously

Answer: (SHOW ANSWER)

Explanation/Reference:

Asynchronous Communication transfers data by sending bits of data in irregular timing patterns.

In asynchronous transmission each character is transmitted separately, that is one character at a time. The character is preceded by a start bit, which tells the receiving end where the character coding begins, and is followed by a stop bit, which tells the receiver where the character coding ends. There will be intervals of ideal time on the channel shown as gaps. Thus there can be gaps between two adjacent characters in the asynchronous communication scheme. In this scheme, the bits within the character frame (including start, parity and stop bits) are sent at the baud rate.

The START BIT and STOP BIT including gaps allow the receiving and sending computers to synchronise the data transmission. Asynchronous communication is used when slow speed peripherals communicate with the computer. The main disadvantage of asynchronous communication is slow speed transmission. Asynchronous communication however, does not require the complex and costly hardware equipments as is required for synchronous transmission.

Asynchronous communication is transmission of data without the use of an external clock signal. Any timing required to recover data from the communication symbols is encoded within the symbols. The most significant aspect of asynchronous communications is variable bit rate, or that the transmitter and receiver clock generators do not have to be exactly synchronized.

The asynchronous communication technique is a physical layer transmission technique which is most widely used for personal computers providing connectivity to printers, modems, fax machines, etc.

An asynchronous link communicates data as a series of characters of fixed size and format. Each character is preceded by a start bit and followed by 1-2 stop bits.

Parity is often added to provide some limited protection against errors occurring on the link.

The use of independent transmit and receive clocks constrains transmission to relatively short characters (<8 bits) and moderate data rates (< 64 kbps, but typically lower).

The asynchronous transmitter delimits each character by a start sequence and a stop sequence. The start bit (0), data (usually 8 bits plus parity) and stop bit(s) (1) are transmitted using a shift register clocked at the nominal data rate.
When asynchronous transmission is used to support packet data links (e.g. IP), then special characters have to be used ("framing") to indicate the start and end of each frame transmitted.
One character (none as an escape character) is reserved to mark any occurrence of the special characters within the frame. In this way the receiver is able to identify which characters are part of the frame and which are part of the "framing".
Packet communication over asynchronous links is used by some users to get access to a network using a modem.
Most Wide Area Networks use synchronous links and a more sophisticated link protocol Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 100.
and
http://en.wikipedia.org/wiki/Asynchronous_communication
and
http://www.erg.abdn.ac.uk/users/gorry/course/phy-pages/async.html
and
http://www.ligaturesoft.com/data_communications/async-data-transmission.html

NEW QUESTION: 192
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: (SHOW ANSWER)
Explanation/Reference:
Today implementation of fast, accurate, reliable, and user-acceptable biometric identification systems are already under way. Because most identity authentication takes place when a people are fully clothed (neck to feet and wrists), the parts of the body conveniently available for this purpose are hands, face, and eyes.
From: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Page 7.

NEW QUESTION: 193
Which of the following access control models requires security clearance for subjects?
A. Identity-based access control
B. Role-based access control
C. Discretionary access control
D. Mandatory access control

Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
With mandatory access control (MAC), the authorization of a subject's access to an object is dependant upon labels, which indicate the subject's clearance. Identity-based access control is a type of discretionary access control. A role-based access control is a type of non-discretionary access control.
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 33).

NEW QUESTION: 194
Which of the following is BEST defined as a physical control?
A. Monitoring of system activity
B. Fencing
C. Identification and authentication methods
D. Logical access control mechanisms
Answer: (SHOW ANSWER)
Physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.
The following answers are incorrect answers:
Monitoring of system activity is considered to be administrative control.
Identification and authentication methods are considered to be a technical control.
Logical access control mechanisms is also considered to be a technical control.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 1280-1282). McGraw-Hill. Kindle Edition.

NEW QUESTION: 195
Which of the following is true about Kerberos?
A. It utilizes public key cryptography.
B. It encrypts data after a ticket is granted, but passwords are exchanged in plain text.
C. It depends upon symmetric ciphers.
D. It is a second party authentication system.
Answer: (SHOW ANSWER)
Kerberos depends on secret keys (symmetric ciphers). Kerberos is a third party authentication protocol. It was designed and developed in the mid 1980's by MIT. It is considered open source but is copyrighted and owned by MIT. It relies on the user's secret keys. The password is used to encrypt and decrypt the keys.
The following answers are incorrect:
It utilizes public key cryptography. Is incorrect because Kerberos depends on secret keys (symmetric ciphers).
It encrypts data after a ticket is granted, but passwords are exchanged in plain text. Is

incorrect because the passwords are not exchanged but used for encryption and decryption of the keys.
It is a second party authentication system. Is incorrect because Kerberos is a third party authentication system, you authenticate to the third party (Kerberos) and not the system you are accessing.
References:
MIT http://web.mit.edu/kerberos/
Wikipedi http://en.wikipedia.org/wiki/Kerberos_%28protocol%29
OIG CBK Access Control (pages 181 - 184)
AIOv3 Access Control (pages 151 - 155)

NEW QUESTION: 196
Which of the following is less likely to accompany a contingency plan, either within the plan itself or in the form of an appendix?
A. Contact information for all personnel.
B. Vendor contact information, including offsite storage and alternate site.
C. Equipment and system requirements lists of the hardware, software, firmware and other resources required to support system operations.
D. The Business Impact Analysis.
Answer: (SHOW ANSWER)
Explanation/Reference:
Why is this the correct answer? Simply because it is WRONG, you would have contact information for your emergency personnel within the plan but NOT for ALL of your personnel. Be careful of words such as ALL.
According to NIST's Special publication 800-34, contingency plan appendices provide key details not contained in the main body of the plan. The appendices should reflect the specific technical, operational, and management contingency requirements of the given system. Contact information for recovery team personnel (not all personnel) and for vendor should be included, as well as detailed system requirements to allow for supporting of system operations. The Business Impact Analysis (BIA) should also be included as an appendix for reference should the plan be activated.
Reference(s) used for this question:
SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems

NEW QUESTION: 197
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: (SHOW ANSWER)
Explanation/Reference:
In the lattice model, users are assigned security clearences and the data is classified. Access decisions are made based on the clearence of the user and the classification of the object. Lattice-based access control is an essential ingredient of formal security models such as Bell-LaPadula, Biba, Chinese Wall, etc.
The bounds concept comes from the formal definition of a lattice as a "partially ordered set for which every pair of elements has a greatest lower bound and a least upper bound." To see the application, consider a file classified as "SECRET" and a user Joe with a security clearence of "TOP SECRET." Under Bell- LaPadula, Joe's "least upper bound" access to the file is "READ" and his least lower bound is "NO WRITE" (star property).
Role-based access control is incorrect. Under RBAC, the access is controlled by the permissions assigned to a role and the specific role assigned to the user.
Biba access control is incorrect. The Biba integrity model is based on a lattice structure but the context of the question disqualiifes it as the best answer.
Content-dependent access control is incorrect. In content dependent access control, the actual content of the information determines access as enforced by the arbiter.
References:
CBK, pp. 324-325.
AIO3, pp. 291-293. See aprticularly Figure 5-19 on p. 293 for an illustration of bounds in action.

NEW QUESTION: 198
The Orange Book is founded upon which security policy model?
A. The Biba Model
B. The Bell LaPadula Model
C. Clark-Wilson Model
D. TEMPEST
Answer: (SHOW ANSWER)
Explanation/Reference:
From the glossary of Computer Security Basics:
The Bell-LaPadula model is the security policy model on which the Orange Book requirements are based.

From the Orange Book definition, "A formal state transition model of computer security policy that describes a set of access control rules. In this formal model, the entities in a computer system are divided into abstract sets of subjects and objects. The notion of secure state is defined and it is proven that each state transition preserves security by moving from secure state to secure state; thus, inductively proving the system is secure. A system state is defined to be 'secure' if the only permitted access modes of subjects to objects are in accordance with a specific security policy. In order to determine whether or not a specific access mode is allowed, the clearance of a subject is compared to the classification of the object and a determination is made as to whether the subject is authorized for the specific access mode." The Biba Model is an integrity model of computer security policy that describes a set of rules. In this model, a subject may not depend on any object or other subject that is less trusted than itself.
The Clark Wilson Model is an integrity model for computer security policy designed for a commercial environment. It addresses such concepts as nondiscretionary access control, privilege separation, and least privilege. TEMPEST is a government program that prevents the compromising electrical and electromagnetic signals that emanate from computers and related equipment from being intercepted and deciphered.
Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, 1991.
Also: U.S. Department of Defense, Trusted Computer System Evaluation Criteria (Orange Book), DOD 5200.28-STD. December 1985 (also available here).

NEW QUESTION: 199
Which access control model would a lattice-based access control model be an example of?
A. Mandatory access control.
B. Discretionary access control.
C. Non-discretionary access control.
D. Rule-based access control.
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
In a lattice model, there are pairs of elements that have the least upper bound of values and greatest lower bound of values. In a Mandatory Access Control (MAC) model, users and data owners do not have as much freedom to determine who can access files.
TIPS FROM CLEMENT
Mandatory Access Control is in place whenever you have permissions that are being imposed on the subject and the subject cannot arbitrarily change them. When the subject/owner of the file can change permissions at will, it is discretionary access control.
Here is a breakdown largely based on explanations provided by Doug Landoll. I am reproducing below using my own word and not exactly how Doug explained it:
FIRST: The Lattice
A lattice is simply an access control tool usually used to implement Mandatory Access Control (MAC) and it could also be used to implement RBAC but this is not as common. The lattice model can be used

for Integrity level or file permissions as well. The lattice has a least upper bound and greatest lower bound. It makes use of pair of elements such as the subject security clearance pairing with the object sensitivity label.

SECOND: DAC (Discretionary Access Control)

Let's get into Discretionary Access Control: It is an access control method where the owner (read the creator of the object) will decide who has access at his own discretion. As we all know, users are sometimes insane.

They will share their files with other users based on their identity but nothing prevent the user from further sharing it with other users on the network. Very quickly you loose control on the flow of information and who has access to what. It is used in small and friendly environment where a low level of security is all that is required.

THIRD: MAC (Mandatory Access Control)

All of the following are forms of Mandatory Access Control:

Mandatory Access control (MAC) (Implemented using the lattice)

You must remember that MAC makes use of Security Clearance for the subject and also Labels will be assigned to the objects. The clearance of the Subject must dominate (be equal or higher) the clearance of the Object being accessed. The label attached to the object will indicate the sensitivity leval and the categories the object belongs to. The categories are used to implement the Need to Know.

All of the following are forms of Non Discretionary Access Control:

Role Based Access Control (RBAC)

Rule Based Access Control (Think Firewall in this case)

The official ISC2 book says that RBAC (synonymous with Non Discretionary Access Control) is a form of DAC but they are simply wrong. RBAC is a form of Non Discretionary Access Control. Non Discretionary DOES NOT equal mandatory access control as there is no labels and clearance involved.

I hope this clarifies the whole drama related to what is what in the world of access control.

In the same line of taught, you should be familiar with the difference between Explicit permission (the user has his own profile) versus Implicit (the user inherit permissions by being a member of a role for example).

The following answers are incorrect:

Discretionary access control. Is incorrect because in a Discretionary Access Control (DAC) model, access is restricted based on the authorization granted to the users. It is identity based access control only. It does not make use of a lattice.

Non-discretionary access control. Is incorrect because Non-discretionary Access Control (NDAC) uses the role-based access control method to determine access rights and permissions. It is often times used as a synonym to RBAC which is Role Based Access Control. The user inherit permission from the role when they are assigned into the role. This type of access could make use of a lattice but could also be implemented without the use of a lattice in some case. Mandatory Access Control was a better choice than this one, but RBAC could also make use of a lattice. The BEST answer was MAC.

Rule-based access control. Is incorrect because it is an example of a Non-discretionary Access Control (NDAC) access control mode. You have rules that are globally applied to all users. There is no such thing as a lattice being use in Rule-Based Access Control.

References:
AIOv3 Access Control (pages 161 - 168)
AIOv3 Security Models and Architecture (pages 291 - 293)

NEW QUESTION: 200

Out of the steps listed below, which one is not one of the steps conducted during the Business Impact Analysis (BIA)?

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

NEW QUESTION: 201
Which of the following is not a preventive operational control?
A. Protecting laptops, personal computers and workstations.
B. Controlling software viruses.
C. Controlling data media access and disposal.
D. Conducting security awareness and technical training.
Answer: (SHOW ANSWER)
Explanation/Reference:

Conducting security awareness and technical training to ensure that end users and system users are aware of the rules of behaviour and their responsibilities in protecting the organization's mission is an example of a preventive management control, therefore not an operational control.
Source: STONEBURNER, Gary et al., NIST Special publication 800-30, Risk management Guide for Information Technology Systems, 2001 (page 37).

NEW QUESTION: 202
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)
Explanation/Reference:
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: 203
When it comes to magnetic media sanitization, what difference can be made between clearing and purging information?
A. Clearing completely erases the media whereas purging only removes file headers, allowing the recovery of files.
B. Clearing renders information unrecoverable by a keyboard attack and purging renders information unrecoverable against laboratory attack.
C. They both involve rewriting the media.
D. Clearing renders information unrecoverable against a laboratory attack and purging renders information unrecoverable to a keyboard attack.
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
The removal of information from a storage medium is called sanitization. Different kinds of sanitization provide different levels of protection. A distinction can be made between clearing information (rendering it unrecoverable by a keyboard attack) and purging (rendering it unrecoverable against laboratory attack). There are three general methods of purging media: overwriting, degaussing, and destruction.
There should be continuous assurance that sensitive information is protected and not allowed to be placed in a circumstance wherein a possible compromise can occur. There are two primary levels of threat that the protector of information must guard against: keyboard attack (information scavenging through system software capabilities) and laboratory attack (information scavenging through laboratory

means). Procedures should be implemented to address these threats before the Automated Information System (AIS) is procured, and the procedures should be continued throughout the life cycle of the AIS.
Reference(s) use for this question:
SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (page 26).
and
A guide to understanding Data Remanence in Automated Information Systems

NEW QUESTION: 204
Only law enforcement personnel are qualified to do computer forensic investigations.
A. True
B. False
Answer: (SHOW ANSWER)

NEW QUESTION: 205
Which of the following statements pertaining to biometrics is FALSE?
A. User can be authenticated based on behavior.
B. User can be authenticated based on unique physical attributes.
C. User can be authenticated by what he knows.
D. A biometric system's accuracy is determined by its crossover error rate (CER).
Answer: C (LEAVE A REPLY)
As this is not a characteristic of Biometrics this is the rigth choice for this
question. This is one of the three basic way authentication can be performed and it is not related to Biometrics. Example of something you know would be a password or PIN for example.
Please make a note of the negative 'FALSE' within the question. This question may seem tricky to some of you but you would be amazed at how many people cannot deal with negative questions. There will be a few negative questions within the real exam, just like this one the keyword NOT or FALSE will be in Uppercase to clearly indicate that it is negative.
Biometrics verifies an individual's identity by analyzing a unique personal attribute or behavior, which is one of the most effective and accurate methods of performing authentication (one to one matching) or identification (a one to many matching).
A biometric system scans an attribute or behavior of a person and compares it to a template store within an authentication server datbase, such template would be created in an earlier enrollment process.
Because this system inspects the grooves of a person's fingerprint, the pattern of someone's retina, or the pitches of someone's voice, it has to be extremely sensitive.
The system must perform accurate and repeatable measurements of anatomical or physiological characteristics. This type of sensitivity can easily cause false positives or false negatives. The system must be calibrated so that these false positives and false negatives occur infrequently and the results are as accurate as possible.
There are two types of failures in biometric identification:

False Rejection also called False Rejection Rate (FRR) - The system fail to recognize a legitimate user. While it could be argued that this has the effect of keeping the protected area extra secure, it is an intolerable frustration to legitimate users who are refused access because the scanner does not recognize them.
False Acceptance or False Acceptance Rate (FAR) - This is an erroneous recognition, either by confusing one user with another or by accepting an imposter as a legitimate user.
Physiological Examples:
Unique Physical Attributes:
Fingerprint (Most commonly accepted)
Hand Geometry
Retina Scan (Most accurate but most intrusive)
Iris Scan
Vascular Scan
Behavioral Examples:
Repeated Actions
Keystroke Dynamics
(Dwell time (the time a key is pressed) and Flight time (the time between "key up" and the next "key down").
Signature Dynamics
(Stroke and pressure points)
EXAM TIP:
Retina scan devices are the most accurate but also the most invasive biometrics system available today. The continuity of the retinal pattern throughout life and the difficulty in fooling such a device also make it a great long-term, high-security option. Unfortunately, the cost of the proprietary hardware as well the stigma of users thinking it is potentially harmful to the eye makes retinal scanning a bad fit for most situations.
Remember for the exam that fingerprints are the most commonly accepted type of biometrics system.
The other answers are incorrect:
'Users can be authenticated based on behavior.' is incorrect as this choice is TRUE as it pertains to BIOMETRICS.
Biometrics systems makes use of unique physical characteristics or behavior of users.
'User can be authenticated based on unique physical attributes.' is also incorrect as this choice is also TRUE as it pertains to BIOMETRICS. Biometrics systems makes use of unique physical characteristics or behavior of users.
'A biometric system's accuracy is determined by its crossover error rate (CER)' is also incorrect as this is TRUE as it also pertains to BIOMETRICS. The CER is the point at which the false rejection rates and the false acceptance rates are equal. The smaller the value of the CER, the more accurate the system.
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 25353-25356). 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 25297-25303). Auerbach Publications. Kindle Edition.

NEW QUESTION: 206
Making sure that the data is accessible when and where it is needed is which of the following?
A. confidentiality
B. integrity
C. acceptability
D. availability
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Availability is making sure that the data is accessible when and where it is needed.
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: 207
Which of the following specifically addresses cyber attacks against an organization's IT systems?
A. Continuity of support plan
B. Business continuity plan
C. Incident response plan
D. Continuity of operations plan
Answer: C (LEAVE A REPLY)
The incident response plan focuses on information security responses to incidents affecting systems and/or networks. It establishes procedures to address cyber attacks against an organization's IT systems. These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware or software. The continuity of support plan is the same as an IT contingency plan. It addresses IT system disruptions and establishes procedures for recovering a major application or general support system. It is not business process focused. The business continuity plan addresses business processes and provides procedures for sustaining essential business operations while recovering from a significant disruption. The continuity of operations plan addresses the subset of an organization's missions that are deemed most critical and procedures to sustain these functions at an alternate site for up to 30 days.
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 8).

NEW QUESTION: 208
Which of the following elements of telecommunications is not used in assuring confidentiality?

A. Network security protocols
B. Network authentication services
C. Data encryption services
D. Passwords
Answer: (SHOW ANSWER)
Explanation/Reference:
Passwords are one of the multiple ways to authenticate (prove who you claim to be) an identity which allows confidentiality controls to be enforced to assure the identity can only access the information for which it is authorized. It is the authentication that assists assurance of confidentiality not the passwords.
"Network security protocols" is incorrect. Network security protocols are quite useful in assuring confidentiality in network communications.
"Network authentication services" is incorrect. Confidentiality is concerned with allowing only authorized users to access information. An important part of determining authorization is authenticating an identity and this service is supplied by network authentication services.
"Data encryption services" is incorrect. Data encryption services are quite useful in protecting the confidentiality of information.
Reference(s) used for this question:
Official ISC2 Guide to the CISSP CBK, pp. 407 - 520
AIO 3rd Edition, pp. 415 - 580

NEW QUESTION: 209
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: (SHOW ANSWER)
Explanation/Reference:
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: 210
Secure Shell (SSH-2) supports authentication, compression, confidentiality, and integrity, SSH is commonly used as a secure alternative to all of the following protocols below except:

A. telnet

B. rlogin
C. RSH
D. HTTPS
Answer: (SHOW ANSWER)
HTTPS is used for secure web transactions and is not commonly replaced by SSH.
Users often want to log on to a remote computer. Unfortunately, most early implementations to meet that need were designed for a trusted network. Protocols/programs, such as TELNET, RSH, and rlogin, transmit unencrypted over the network, which allows traffic to be easily intercepted. Secure shell (SSH) was designed as an alternative to the above insecure protocols and allows users to securely access resources on remote computers over an encrypted tunnel. SSH's services include remote log-on, file transfer, and command execution. It also supports port forwarding, which redirects other protocols through an encrypted SSH tunnel. Many users protect less secure traffic of protocols, such as X Windows and VNC (virtual network computing), by forwarding them through a SSH tunnel. The SSH tunnel protects the integrity of communication, preventing session hijacking and other man-in-the-middle attacks. Another advantage of SSH over its predecessors is that it supports strong authentication. There are several alternatives for SSH clients to authenticate to a SSH server, including passwords and digital certificates. Keep in mind that authenticating with a password is still a significant improvement over the other protocols because the password is transmitted encrypted.
The following were wrong answers:
telnet is an incorrect choice. SSH is commonly used as an more secure alternative to telnet. In fact Telnet should not longer be used today.
rlogin is and incorrect choice. SSH is commonly used as a more secure alternative to rlogin.
RSH is an incorrect choice. SSH is commonly used as a more secure alternative to RSH.
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 7077-7088). Auerbach Publications. Kindle Edition.

NEW QUESTION: 211
What is the appropriate role of the security analyst in the application system development or acquisition project?
A. policeman
B. control evaluator & consultant
C. data owner
D. application user
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:

The correct answer is "control evaluator & consultant". During any system development or acquisition, the security staff should evaluate security controls and advise (or consult) on the strengths and weaknesses with those responsible for making the final decisions on the project.
The other answers are not correct because:
policeman - It is never a good idea for the security staff to be placed into this type of role (though it is sometimes unavoidable). During system development or acquisition, there should be no need of anyone filling the role of policeman.
data owner - In this case, the data owner would be the person asking for the new system to manage, control, and secure information they are responsible for. While it is possible the security staff could also be the data owner for such a project if they happen to have responsibility for the information, it is also possible someone else would fill this role. Therefore, the best answer remains "control evaluator & consultant".
application user - Again, it is possible this could be the security staff, but it could also be many other people or groups. So this is not the best answer.
Reference:
Official ISC2 Guide page: 555 - 560
All in One Third Edition page: 832 - 846

NEW QUESTION: 212
The IP header contains a protocol field. If this field contains the value of 17, what type of data is contained within the ip datagram?
A. TCP.
B. ICMP.
C. UDP.
D. IGMP.
Answer: (SHOW ANSWER)
Explanation/Reference:
If the protocol field has a value of 17 then it would indicate it was UDP.
The following answers are incorrect answers:
TCP. Is incorrect because the value for a TCP protocol would be 6.
ICMP. Is incorrect because the value for an ICMP protocol would be 1.
IGMP. Is incorrect because the value for an IGMP protocol would be 2.

The protocol field of the IP packet dictates what protocol the IP packet is using.
TCP=6, ICMP=1, UDP=17, IGMP=2
Reference(s) used for this question:
SANS http://www.sans.org/resources/tcpip.pdf?ref=3871

NEW QUESTION: 213
Who should measure the effectiveness of Information System security related controls in an organization?
A. The local security specialist
B. The business manager
C. The systems auditor
D. The central security manager
Answer: (SHOW ANSWER)
Explanation/Reference:
It is the systems auditor that should lead the effort to ensure that the security controls are in place and effective. The audit would verify that the controls comply with polices, procedures, laws, and regulations where applicable. The findings would provide these to senior management.
The following answers are incorrect:
the local security specialist. Is incorrect because an independent review should take place by a third party.
The security specialist might offer mitigation strategies but it is the auditor that would ensure the effectiveness of the controls
the business manager. Is incorrect because the business manager would be responsible that the controls are in place, but it is the auditor that would ensure the effectiveness of the controls.
the central security manager. Is incorrect because the central security manager would be responsible for implementing the controls, but it is the auditor that is responsibe for ensuring their effectiveness.

NEW QUESTION: 214
Network-based Intrusion Detection systems:
A. Commonly reside on a discrete network segment and monitor the traffic on that network segment.
B. Commonly will not reside on a discrete network segment and monitor the traffic on that network segment.
C. Commonly reside on a discrete network segment and does not monitor the traffic on that network segment.
D. Commonly reside on a host and and monitor the traffic on that specific host.
Answer: (SHOW ANSWER)
Section: Analysis and Monitoring
Explanation/Reference:
Network-based ID systems:
- Commonly reside on a discrete network segment and monitor the traffic on that network segment

- Usually consist of a network appliance with a Network Interface Card (NIC) that is operating in promiscuous mode and is intercepting and analyzing the network packets in real time
"A passive NIDS takes advantage of promiscuous mode access to the network, allowing it to gain visibility into every packet traversing the network segment. This allows the system to inspect packets and monitor sessions without impacting the network, performance, or the systems and applications utilizing the network." NOTE FROM CLEMENT:
A discrete network is a synonym for a SINGLE network. Usually the sensor will monitor a single network segment, however there are IDS today that allow you to monitor multiple LAN's at the same time.
References 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 62.
and
Official (ISC)2 Guide to the CISSP CBK, Hal Tipton and Kevin Henry, Page 196 and Additional information on IDS systems can be found here: http://en.wikipedia.org/wiki/ Intrusion_detection_system

NEW QUESTION: 215
Which access control model is best suited in an environment where a high security level is required and where it is desired that only the administrator grants access control?
A. DAC
B. MAC
C. Access control matrix
D. TACACS
Answer: (SHOW ANSWER)
Explanation/Reference:
MAC provides high security by regulating access based on the clearance of individual users and sensitivity labels for each object. Clearance levels and sensitivity levels cannot be modified by individual users -- for example, user Joe (SECRET clearance) cannot reclassify the "Presidential Doughnut Recipe" from
"SECRET" to "CONFIDENTIAL" so that his friend Jane (CONFIDENTIAL clearance) can read it. The administrator is ultimately responsible for configuring this protection in accordance with security policy and directives from the Data Owner.
DAC is incorrect. In DAC, the data owner is responsible for controlling access to the object.
Access control matrix is incorrect. The access control matrix is a way of thinking about the access control needed by a population of subjects to a population of objects. This access control can be applied using rules, ACL's, capability tables, etc.
TACACS is incorrect. TACACS is a tool for performing user authentication.
References:
CBK, p. 187, Domain 2: Access Control.
AIO3, Chapter 4, Access Control.

NEW QUESTION: 216

Access Control techniques do not include which of the following?
A. Rule-Based Access Controls
B. Role-Based Access Control
C. Mandatory Access Control
D. Random Number Based Access Control
Answer: D (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Access Control Techniques
Discretionary Access Control
Mandatory Access Control
Lattice Based Access Control
Rule-Based Access Control
Role-Based Access Control
Source: DUPUIS, Clement, Access Control Systems and Methodology, Version 1, May 2002, CISSP Open Study Group Study Guide for Domain 1, Page 13.

NEW QUESTION: 217
Which of the following services relies on UDP?
A. FTP
B. Telnet
C. DNS
D. SMTP
Answer: (SHOW ANSWER)
DNS relies on connectionless UDP whereas services like FTP, Telnet and SMTP rely on TCP.
Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 2, August 1999.

NEW QUESTION: 218
Which of the following is best at defeating frequency analysis?
A. Substitution cipher
B. Polyalphabetic cipher
C. Transposition cipher
D. Ceasar Cipher
Answer: (SHOW ANSWER)
Simple substitution and transposition ciphers are vulnerable to attacks that
perform frequency analysis.
In every language, there are words and patterns that are used more than others.
Some patterns common to a language can actually help attackers figure out the
transformation between plaintext and ciphertext, which enables them to figure out the key
that was used to perform the transformation. Polyalphabetic ciphers use different alphabets
to defeat frequency analysis.

The ceasar cipher is a very simple substitution cipher that can be easily defeated and it does show repeating letters.
Out of list presented, it is the Polyalphabetic cipher that would provide the best protection against simple frequency analysis attacks.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 8: Cryptography (page 507).
And : DUPUIS, Clement, CISSP Open Study Guide on domain 5, cryptography, April 1999.

NEW QUESTION: 219
Which of the following best defines source routing?
A. The packets hold the forwarding information so they don't need to let bridges and routers decide what is the best route or way to get to the destination.
B. The packets hold source information in a fashion that source address cannot be forged.
C. The packets are encapsulated to conceal source information.
D. The packets hold information about redundant paths in order to provide a higher reliability.
Answer: (SHOW ANSWER)
Explanation/Reference:
With source routing, the packets hold the forwarding information so that they can find their way to the destination themselves without bridges and routers dictating their paths.
In computer networking, source routing allows a sender of a packet to specify the route the packet takes through the network.
With source routing the entire path to the destination is known to the sender and is included when sending data. Source routing differs from most other routing in that the source makes most or all of the routing decisions for each router along the way.
Source:
WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#2 Telecommunications and Network Security (page 5)
Wikipedia at http://en.wikipedia.org/wiki/Dynamic_Source_Routing

NEW QUESTION: 220
The control of communications test equipment should be clearly addressed by security policy for which of the following reasons?

A. Test equipment is easily damaged.
B. Test equipment can be used to browse information passing on a network.
C. Test equipment is difficult to replace if lost or stolen.
D. Test equipment must always be available for the maintenance personnel.
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:

Test equipment must be secured. There are equipment and other tools that if in the wrong hands could be used to "sniff" network traffic and also be used to commit fraud. The storage and use of this equipment should be detailed in the security policy for this reason.
The following answers are incorrect:
Test equipment is easily damaged. Is incorrect because it is not the best answer, and from a security point of view not relevent.
Test equipment is difficult to replace if lost or stolen. Is incorrect because it is not the best answer, and from a security point of view not relevent.
Test equipment must always be available for the maintenance personnel. Is incorrect because it is not the best answer, and from a security point of view not relevent.
References:
OIG CBK Operations Security (pages 642 - 643)

NEW QUESTION: 221
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: (SHOW ANSWER)
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: 222
Technical controls such as encryption and access control can be built into the operating system, be software applications, or can be supplemental hardware/software units. Such controls, also known as logical controls, represent which pairing?
A. Preventive/Administrative Pairing
B. Preventive/Technical Pairing
C. Preventive/Physical Pairing
D. Detective/Technical Pairing
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:

Preventive/Technical controls are also known as logical controls and can be built into the operating system, be software applications, or can be supplemental hardware/software units.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION: 223
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: 224
The DES algorithm is an example of what type of cryptography?
A. Secret Key
B. Two-key
C. Asymmetric Key
D. Public Key
Answer: (SHOW ANSWER)
Section: Cryptography
Explanation/Reference:
DES is also known as a Symmetric Key or Secret Key algorithm.
DES is a Symmetric Key algorithm, meaning the same key is used for encryption and decryption.
For the exam remember that:
DES key Sequence is 8 Bytes or 64 bits (8 x 8 = 64 bits)
DES has an Effective key length of only 56 Bits. 8 of the Bits are used for parity purpose only.
DES has a total key length of 64 Bits.
The following answers are incorrect:
Two-key This is incorrect because DES uses the same key for encryption and decryption.
Asymmetric Key This is incorrect because DES is a Symmetric Key algorithm using the same key for encryption and decryption and an Asymmetric Key algorithm uses both a Public Key and a Private Key.
Public Key. This is incorrect because Public Key or algorithm Asymmetric Key does not use the same key is used for encryption and decryption.
References used for this question:
http://en.wikipedia.org/wiki/Data_Encryption_Standard

NEW QUESTION: 225
What is called an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics?
A. Biometrics
B. Micrometrics
C. Macrometrics
D. MicroBiometrics
Answer: (SHOW ANSWER)
Explanation/Reference:
Biometrics; Biometrics are defined as an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 37,38.

NEW QUESTION: 226
Which of the following protocols is designed to send individual messages securely?
A. Kerberos
B. Secure Electronic Transaction (SET).
C. Secure Sockets Layer (SSL).
D. Secure HTTP (S-HTTP).
Answer: (SHOW ANSWER)
An early standard for encrypting HTTP documents, Secure HTTP (S-HTTP) is designed to send individual messages securely. SSL is designed to establish a secure connection between two computers. SET was originated by VISA and MasterCard as an Internet credit card protocol using digital signatures. Kerberos is an authentication system.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 89.

NEW QUESTION: 227
Which of the following is an example of an active attack?
A. Traffic analysis

B. Scanning
C. Eavesdropping
D. Wiretapping
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
Scanning is definitively a very active attack. The attacker will make use of a scanner to perform the attack, the scanner will send a very large quantity of packets to the target in order to illicit responses that allows the attacker to find information about the operating system, vulnerabilities, misconfiguration and more. The packets being sent are sometimes attempting to identify if a known vulnerability exist on the remote hosts.
A passive attack is usually done in the footprinting phase of an attack. While doing your passive reconnaissance you never send a single packet to the destination target. You gather information from public databases such as the DNS servers, public information through search engines, financial information from finance web sites, and technical infomation from mailing list archive or job posting for example.
An attack can be active or passive.
An "active attack" attempts to alter system resources or affect their operation.
A "passive attack" attempts to learn or make use of information from the system but does not affect system resources. (E.g., see: wiretapping.) The following are all incorrect answers because they are all passive attacks:
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 or counter-intelligence, and is a concern in computer security.
Eavesdropping - Eavesdropping is another security risk posed to networks. Because of the way some networks are built, anything that gets sent out is broadcast to everyone. Under normal circumstances, only the computer that the data was meant for will process that information. However, hackers can set up programs on their computers called "sniffers" that capture all data being broadcast over the network. By carefully examining the data, hackers can often reconstruct real data that was never meant for them. Some of the most damaging things that get sniffed include passwords and credit card information.
In the cryptographic context, Eavesdropping and sniffing data as it passes over a network are considered passive attacks because the attacker is not affecting the protocol, algorithm, key, message, or any parts of the encryption system. Passive attacks are hard to detect, so in most cases methods are put in place to try to prevent them rather than to detect and stop them. Altering messages, modifying system files, and masquerading as another individual are acts that are considered active attacks because the attacker is actually doing something instead of sitting back and gathering data. Passive attacks are usually used to gain information prior to carrying out an active attack." Wiretapping - Wiretapping refers to listening in on electronic communications on telephones, computers, and other devices. Many governments use it as a law enforcement tool, and it is also used in fields like corporate espionage to gain access to privileged

information. Depending on where in the world one is, wiretapping may be tightly controlled with laws that are designed to protect privacy rights, or it may be a widely accepted practice with little or no protections for citizens. Several advocacy organizations have been established to help civilians understand these laws in their areas, and to fight illegal wiretapping.
Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 6th Edition, Cryptography, Page 865 and
http://en.wikipedia.org/wiki/Attack_%28computing%29
and
http://www.wisegeek.com/what-is-wiretapping.htm
and
https://pangea.stanford.edu/computing/resources/network/security/risks.php and
http://en.wikipedia.org/wiki/Traffic_analysis

NEW QUESTION: 228
_____ and _____ are the primary controls of most access control systems.
(Choose two)
A. Tickets
B. Biometrics
C. Authorization
D. Identification
E. Authentication
Answer: (SHOW ANSWER)
Identifying a user and authenticating them into the system form the foundations of most access control systems.

NEW QUESTION: 229
Which of the following is true about link encryption?
A. Each entity has a common key with the destination node.
B. Encrypted messages are only decrypted by the final node.
C. This mode does not provide protection if anyone of the nodes along the transmission path is compromised.
D. Only secure nodes are used in this type of transmission.
Answer: (SHOW ANSWER)
Explanation/Reference:
In link encryption, each entity has keys in common with its two neighboring nodes in the transmission chain.
Thus, a node receives the encrypted message from its predecessor, decrypts it, and then re-encrypts it with a new key, common to the successor node. Obviously, this mode does not provide protection if anyone of the nodes along the transmission path is compromised.
Encryption can be performed at different communication levels, each with different types of protection and implications. Two general modes of encryption implementation are link encryption and end-to-end encryption.

Link encryption encrypts all the data along a specific communication path, as in a satellite link, T3 line, or telephone circuit. Not only is the user information encrypted, but the header, trailers, addresses, and routing data that are part of the packets are also encrypted. The only traffic not encrypted in this technology is the data link control messaging information, which includes instructions and parameters that the different link devices use to synchronize communication methods. Link encryption provides protection against packet sniffers and eavesdroppers.
In end-to-end encryption, the headers, addresses, routing, and trailer information are not encrypted, enabling attackers to learn more about a captured packet and where it is headed.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (pp. 845-846). McGraw-Hill.
And:
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 132).

NEW QUESTION: 230
Which of the following is the BEST way to detect software license violations?
A. Implementing a corporate policy on copyright infringements and software use.
B. Requiring that all PCs be diskless workstations.
C. Installing metering software on the LAN so applications can be accessed through the metered software.
D. Regularly scanning PCs in use to ensure that unauthorized copies of software have not been loaded on the PC.
Answer: (SHOW ANSWER)
Section: Analysis and Monitoring
Explanation/Reference:
The best way to prevent and detect software license violations is to regularly scan used PCs, either from the LAN or directly, to ensure that unauthorized copies of software have not been loaded on the PC.
Other options are not detective.
A corporate policy is not necessarily enforced and followed by all employees.
Software can be installed from other means than floppies or CD-ROMs (from a LAN or even downloaded from the Internet) and software metering only concerns applications that are registered.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 108).

NEW QUESTION: 231
Which of the following is not a logical control when implementing logical access security?
A. access profiles.
B. userids.
C. employee badges.
D. passwords.
Answer: (SHOW ANSWER)

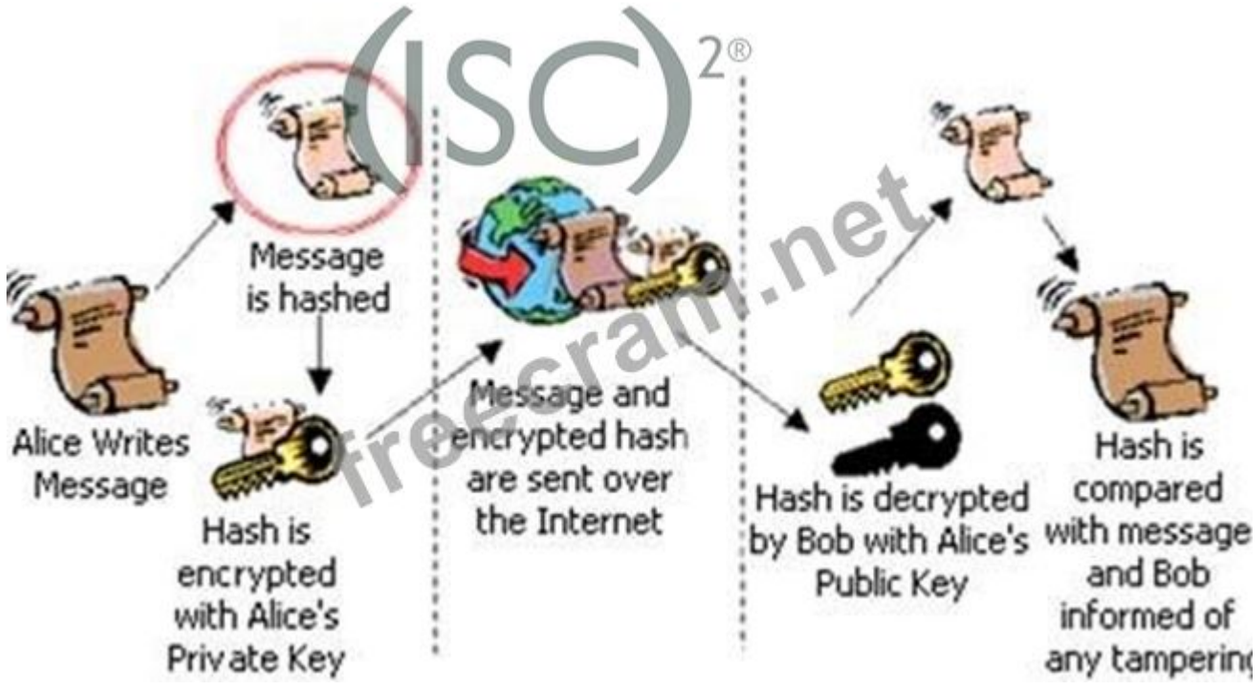
Explanation/Reference:
Employee badges are considered Physical so would not be a logical control.
The following answers are incorrect:
userids. Is incorrect because userids are a type of logical control.
access profiles. Is incorrect because access profiles are a type of logical control.
passwords. Is incorrect because passwords are a type of logical control.

NEW QUESTION: 232
Which of the following attacks could capture network user passwords?
A. Data diddling
B. Sniffing
C. IP Spoofing
D. Smurfing
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
A network sniffer captures a copy every packet that traverses the network segment the sniffer is connect to.
Sniffers are typically devices that can collect information from a communication medium, such as a network.
These devices can range from specialized equipment to basic workstations with customized software.
A sniffer can collect information about most, if not all, attributes of the communication. The most common method of sniffing is to plug a sniffer into an existing network device like a hub or switch. A hub (which is designed to relay all traffic passing through it to all of its ports) will automatically begin sending all the traffic on that network segment to the sniffing device. On the other hand, a switch (which is designed to limit what traffic gets sent to which port) will have to be specially configured to send all traffic to the port where the sniffer is plugged in.
Another method for sniffing is to use a network tap-a device that literally splits a network transmission into two identical streams; one going to the original network destination and the other going to the sniffing device. Each of these methods has its advantages and disadvantages, including cost, feasibility, and the desire to maintain the secrecy of the sniffing activity.
The packets captured by sniffer are decoded and then displayed by the sniffer. Therfore, if the username/password are contained in a packet or packets traversing the segment the sniffer is connected to, it will capture and display that information (and any other information on that segment it can see).
Of course, if the information is encrypted via a VPN, SSL, TLS, or similar technology, the information is still captured and displayed, but it is in an unreadable format.
The following answers are incorrect:
Data diddling involves changing data before, as it is enterred into a computer, or after it is extracted.
Spoofing is forging an address and inserting it into a packet to disguise the origin of the communication - or causing a system to respond to the wrong address.

Smurfing would refer to the smurf attack, where an attacker sends spoofed packets to the broadcast address on a gateway in order to cause a denial of service.
The following reference(s) were/was used to create this question:
CISA Review manual 2014 Page number 321
Official ISC2 Guide to the CISSP 3rd edition Page Number 153

NEW QUESTION: 233
Complete the blanks. When using PKI, I digitally sign a message using my _____ key. The recipient verifies my signature using my _____ key.
A. Private / Public
B. Public / Private
C. Symmetric / Asymmetric
D. Private / Symmetric
Answer: (SHOW ANSWER)
Explanation/Reference:
When we encrypt messages using our private keys which are only available to us. The person who wants to read and decrypt the message need only have our public keys to do so.
The whole point to PKI is to assure message integrity, authentication of the source, and to provide secrecy with the digital encryption.
See below a nice walktrough of Digital Signature creation and verification from the Comodo web site:
Digital Signatures apply the same functionality to an e-mail message or data file that a handwritten signature does for a paper-based document. The Digital Signature vouches for the origin and integrity of a message, document or other data file.
How do we create a Digital Signature?
The creation of a Digital Signature is a complex mathematical process. However as the complexities of the process are computed by the computer, applying a Digital Signature is no more difficult that creating a handwritten one!
The following text illustrates in general terms the processes behind the generation of a Digital Signature:
1. Alice clicks 'sign' in her email application or selects which file is to be signed.
2. Alice's computer calculates the 'hash' (the message is applied to a publicly known mathematical hashing function that coverts the message into a long number referred to as the hash).
3. The hash is encrypted with Alice's Private Key (in this case it is known as the Signing Key) to create the Digital Signature.
4. The original message and its Digital Signature are transmitted to Bob.
5. Bob receives the signed message. It is identified as being signed, so his email application knows which actions need to be performed to verify it.
6. Bob's computer decrypts the Digital Signature using Alice's Public Key.
7. Bob's computer also calculates the hash of the original message (remember - the mathematical function used by Alice to do this is publicly known).
8. Bob's computer compares the hashes it has computed from the received message with the now decrypted hash received with Alice's message.

digital signature creation and verification



If the message has remained integral during its transit (i.e. it has not been tampered with), when compared the two hashes will be identical.

However, if the two hashes differ when compared then the integrity of the original message has been compromised. If the original message is tampered with it will result in Bob's computer calculating a different hash value. If a different hash value is created, then the original message will have been altered. As a result the verification of the Digital Signature will fail and Bob will be informed.

Origin, Integrity, Non-Repudiation, and Preventing Men-In-The-Middle (MITM) attacks Eve, who wants to impersonate Alice, cannot generate the same signature as Alice because she does not have Alice's Private Key (needed to sign the message digest). If instead, Eve decides to alter the content of the message while in transit, the tampered message will create a different message digest to the original message, and Bob's computer will be able to detect that. Additionally, Alice cannot deny sending the message as it has been signed using her Private Key, thus ensuring non-repudiation.

creating and validating a digital signature

Due to the recent Global adoption of Digital Signature law, Alice may now sign a transaction, message or piece of digital data, and so long as it is verified successfully it is a legally permissible means of proof that Alice has made the transaction or written the message.
The following answers are incorrect:
- Public / Private: This is the opposite of the right answer.
- Symmetric / Asymmetric: Not quite. Sorry. This form of crypto is asymmetric so you were almost on target.
- Private / Symmetric: Well, you got half of it right but Symmetric is wrong.
The following reference(s) was used to create this question:
The CCCure Holistic Security+ CBT, you can subscribe at: http://www.cccure.tv and http://www.comodo.com/resources/small-business/digital-certificates3.php

NEW QUESTION: 234
Which of the following monitors network traffic in real time?
A. network-based IDS
B. host-based IDS
C. application-based IDS
D. firewall-based IDS
Answer: (SHOW ANSWER)
This type of IDS is called a network-based IDS because monitors network traffic in real time.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 48.

NEW QUESTION: 235
A deviation from an organization-wide security policy requires which of the following?
A. Risk Acceptance
B. Risk Assignment
C. Risk Reduction
D. Risk Containment
Answer: (SHOW ANSWER)
Explanation/Reference:
A deviation from an organization-wide security policy requires you to manage the risk. If you deviate from the security policy then you are required to accept the risks that might occur.
In some cases, it may be prudent for an organization to simply accept the risk that is presented in certain scenarios. Risk acceptance is the practice of accepting certain risk(s), typically based on a business decision that may also weigh the cost versus the benefit of dealing with the risk in another way.
The OIG defines Risk Management as: This term characterizes the overall process.
The first phase of risk assessment includes identifying risks, risk-reducing measures, and the budgetary impact of implementing decisions related to the acceptance, avoidance, or transfer of risk.

The second phase of risk management includes the process of assigning priority to, budgeting, implementing, and maintaining appropriate risk-reducing measures.
Risk management is a continuous process of ever-increasing complexity. It is how we evaluate the impact of exposures and respond to them. Risk management minimizes loss to information assets due to undesirable events through identification, measurement, and control. It encompasses the overall security review, risk analysis, selection and evaluation of safeguards, cost-benefit analysis, management decision, and safeguard identification and implementation, along with ongoing effectiveness review.
Risk management provides a mechanism to the organization to ensure that executive management knows current risks, and informed decisions can be made to use one of the risk management principles: risk avoidance, risk transfer, risk mitigation, or risk acceptance.
The 4 ways of dealing with risks are: Avoidance, Transfer, Mitigation, Acceptance The following answers are incorrect:
Risk assignment. Is incorrect because it is a distractor, assignment is not one of the ways to manage risk.
Risk reduction. Is incorrect because there was a deviation of the security policy. You could have some additional exposure by the fact that you deviated from the policy.
Risk containment. Is incorrect because it is a distractor, containment is not one of the ways to manage risk.
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 8882-8886). 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 10206-10208). Auerbach Publications. Kindle Edition.

NEW QUESTION: 236
The Orange Book states that "Hardware and software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB [Trusted Computing Base]." This statement is the formal requirement for:
A. Security Testing.
B. Design Verification.
C. System Integrity.
D. System Architecture Specification.
Answer: (SHOW ANSWER)
This is a requirement starting as low as C1 within the TCSEC rating.
The Orange book requires the following for System Integrity Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.
NOTE FROM CLEMENT:
This is a question that confuses a lot of people because most people take for granted that the orange book with its associated Bell LaPadula model has nothing to do with integrity.

However you have to be careful about the context in which the word integrity is being used. You can have Data Integrity and you can have System Integrity which are two completely different things.
Yes, the Orange Book does not specifically address the Integrity requirements, however it has to run on top of systems that must meet some integrity requirements.
This is part of what they call operational assurance which is defined as a level of confidence of a trusted system's architecture and implementation that enforces the system's security policy. It includes:
System architecture
Covert channel analysis
System integrity
Trusted recovery
DATA INTEGRITY
Data Integrity is very different from System Integrity. When you have integrity of the data, there are three goals:
1.Prevent authorized users from making unauthorized modifications
2.Preven unauthorized users from making modifications
3.Maintaining internal and external consistancy of the data
Bell LaPadula which is based on the Orange Book address does not address Integrity, it addresses only Confidentiality.
Biba address only the first goal of integrity.
Clark-Wilson addresses the three goals of integrity.
In the case of this question, there is a system integrity requirement within the TCB. As mentioned above here is an extract of the requirements: Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.
The following answers are incorrect:
Security Testing. Is incorrect because Security Testing has no set of requirements in the Orange book.
Design Verification. Is incorrect because the Orange book's requirements for Design Verification include: A formal model of the security policy must be clearly identified and documented, including a mathematical proof that the model is consistent with its axioms and is sufficient to support the security policy.
System Architecture Specification. Is incorrect because there are no requirements for System Architecture Specification in the Orange book.
The following reference(s) were used for this question:
Trusted Computer Security Evaluation Criteria (TCSEC), DoD 5200.28-STD, page 15, 18, 25, 31, 40, 50.
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Security Architecture and Design, Page 392-397, for users with the Kindle Version see Kindle Locations 28504-28505. and DOD TCSEC - http://www.cerberussystems.com/INFOSEC/stds/d520028.htm

NEW QUESTION: 237

Which of the following is not a DES mode of operation?
A. Cipher block chaining
B. Electronic code book
C. Input feedback
D. Cipher feedback
Answer: (SHOW ANSWER)
Section: Cryptography
Explanation
Explanation/Reference:
Output feedback (OFB) is a DES mode of operation, not input feedback.
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 149).

NEW QUESTION: 238
An area of the Telecommunications and Network Security domain that directly affects the Information Systems Security tenet of Availability can be defined as:
A. Netware availability
B. Network availability
C. Network acceptability
D. Network accountability
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
Network availability can be defined as an area of the Telecommunications and Network Security domain that directly affects the Information Systems Security tenet of Availability.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 64.

NEW QUESTION: 239
Which of the following service is a distributed database that translate host name to IP address to IP address to host name?
A. DNS
B. FTP
C. SSH
D. SMTP
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain

names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

For your exam you should know below information general Internet terminology:

Network access point - Internet service providers access internet using net access point.A Network Access Point (NAP) was a public network exchange facility where Internet service providers (ISPs) connected with one another in peering arrangements. The NAPs were a key component in the transition from the 1990s NSFNET era (when many networks were government sponsored and commercial traffic was prohibited) to the commercial Internet providers of today. They were often points of considerable Internet congestion.

Internet Service Provider (ISP) - An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet. Internet service providers may be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned. Internet services typically provided by ISPs include Internet access, Internet transit, domain name registration, web hosting, co- location.

Telnet or Remote Terminal Control Protocol -A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password.

Telnet is a common way to remotely control Web servers.

Internet Link- Internet link is a connection between Internet users and the Internet service provider.

Secure Shell or Secure Socket Shell (SSH) - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slogin, ssh, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

Domain Name System (DNS) - The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

File Transfer Protocol (FTP) - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit. FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available Simple Mail Transport Protocol (SMTP)

- SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.
The following answers are incorrect:
SMTP - Simple Mail Transport Protocol (SMTP) - SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix- based systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.
FTP - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit. FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available SSH - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slogin, ssh, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.
The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 273 and 274

NEW QUESTION: 240

Organizations should consider which of the following first before allowing external access to their LANs via the Internet?

A. plan for implementing workstation locking mechanisms.
B. plan for protecting the modem pool.
C. plan for providing the user with his account usage information.
D. plan for considering proper authentication options.
Answer: (SHOW ANSWER)
Explanation/Reference:

Before a LAN is connected to the Internet, you need to determine what the access controls mechanisms are to be used, this would include how you are going to authenticate individuals that may access your network externally through access control.
The following answers are incorrect:
plan for implementing workstation locking mechanisms. This is incorrect because locking the workstations have no impact on the LAN or Internet access.
plan for protecting the modem pool. This is incorrect because protecting the modem pool has no impact on the LAN or Internet access, it just protects the modem.
plan for providing the user with his account usage information. This is incorrect because the question asks what should be done first. While important your primary concern should be focused on security.

NEW QUESTION: 241
Which of the following statements pertaining to disk mirroring is incorrect?
A. Mirroring offers better performance in read operations but writing hinders system performance.
B. Mirroring is a hardware-based solution only.
C. Mirroring offers a higher fault tolerance than parity.
D. Mirroring is usually the less cost-effective solution.
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
With mirroring, the system writes the data simultaneously to separate drives or arrays.
The advantage of mirroring are minimal downtime, simple data recovery, and increased performance in reading from the disk.
The disadvantage of mirroring is that both drives or disk arrays are processing in the writing to disks function, which can hinder system performance.
Mirroring has a high fault tolerance and can be implemented either through a hardware RAID controller or through the operating system. Since it requires twice the disk space than actual data, mirroring is the less cost- efficient data redundancy strategy.
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
45).

NEW QUESTION: 242
Which type of control is concerned with restoring controls?
A. Compensating controls
B. Corrective controls
C. Detective controls
D. Preventive controls
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Corrective controls are concerned with remedying circumstances and restoring controls.
Detective controls are concerned with investigating what happen after the fact such as logs and video surveillance tapes for example.
Compensating controls are alternative controls, used to compensate weaknesses in other controls.
Preventive controls are concerned with avoiding occurrences of risks.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 243
What is NOT true about a one-way hashing function?
A. It provides authentication of the message
B. A hash cannot be reverse to get the message used to create the hash
C. The results of a one-way hash is a message digest
D. It provides integrity of the message
Answer: (SHOW ANSWER)
Section: Cryptography
Explanation/Reference:
A one way hashing function can only be use for the integrity of a message and not for authentication or confidentiality. Because the hash creates just a fingerprint of the message which cannot be reversed and it is also very difficult to create a second message with the same hash.
A hash by itself does not provide Authentication. It only provides a weak form or integrity. It would be possible for an attacker to perform a Man-In-The-Middle attack where both the hash and the digest could be changed without the receiver knowing it.
A hash combined with your session key will produce a Message Authentication Code (MAC) which will provide you with both authentication of the source and integrity. It is sometimes referred to as a Keyed Hash.
A hash encrypted with the sender private key produce a Digital Signature which provide authentication, but not the hash by itself.
Hashing functions by themselves such as MD5, SHA1, SHA2, SHA-3 does not provide authentication.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 548

NEW QUESTION: 244
What is the essential difference between a self-audit and an independent audit?
A. Tools used
B. Results
C. Objectivity
D. Competence
Answer: (SHOW ANSWER)
Section: Analysis and Monitoring
Explanation/Reference:
To maintain operational assurance, organizations use two basic methods: system audits and monitoring. Monitoring refers to an ongoing activity whereas audits are one-time or periodic events and can be either internal or external. The essential difference between a self-audit and an independent audit is objectivity, thus indirectly affecting the results of the audit. Internal and external auditors should have the same level of competence and can use the same tools.
Source: SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (page 25).

NEW QUESTION: 245
Which of the following refers to the data left on the media after the media has been erased?
A. remanence
B. recovery
C. sticky bits
D. semi-hidden
Answer: (SHOW ANSWER)
Actually the term "remanence" comes from electromagnetism, the study of the electromagnetics. Originally referred to (and still does in that field of study) the magnetic flux that remains in a magnetic circuit after an applied magnetomotive force has been removed. Absolutely no way a candidate will see anywhere near that much detail on any similar CISSP question, but having read this, a candidate won't be likely to forget it either.
It is becoming increasingly commonplace for people to buy used computer equipment, such as a hard drive, or router, and find information on the device left there by the previous owner; information they thought had been deleted. This is a classic example of data remanence: the remains of partial or even the entire data set of digital information. Normally, this refers to the data that remain on media after they are written over or degaussed. Data remanence is most common in storage systems but can also occur in memory.
Specialized hardware devices known as degaussers can be used to erase data saved to magnetic media. The measure of the amount of energy needed to reduce the magnetic field on the media to zero is known as coercivity.

It is important to make sure that the coercivity of the degausser is of sufficient strength to meet object reuse requirements when erasing data. If a degausser is used with insufficient coercivity, then a remanence of the data will exist. Remanence is the measure of the existing magnetic field on the media; it is the residue that remains after an object is degaussed or written over.
Data is still recoverable even when the remanence is small. While data remanence exists, there is no assurance of safe object reuse.
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 4207-4210). 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 19694-19699). Auerbach Publications. Kindle Edition.

NEW QUESTION: 246
Which of the following is the simplest type of firewall ?
A. Stateful packet filtering firewall
B. Packet filtering firewall
C. Dual-homed host firewall
D. Application gateway
Answer: B (LEAVE A REPLY)
A static packet filtering firewall is the simplest and least expensive type of firewalls, offering minimum security provisions to a low-risk computing environment.
A static packet filter firewall examines both the source and destination addresses of the incoming data packet and applies ACL's to them. They operates at either the Network or Transport layer. They are known as the First generation of firewall.
Older firewalls that were only packet filters were essentially routing devices that provided access control functionality for host addresses and communication sessions. These devices, also known as stateless inspection firewalls, do not keep track of the state of each flow of traffic that passes though the firewall; this means, for example, that they cannot associate multiple requests within a single session to each other. Packet filtering is at the core of most modern firewalls, but there are few firewalls sold today that only do stateless packet filtering. Unlike more advanced filters, packet filters are not concerned about the content of packets. Their access control functionality is governed by a set of directives referred to as a ruleset. Packet filtering capabilities are built into most operating systems and devices capable of routing; the most common example of a pure packet filtering device is a network router that employs access control lists.
There are many types of Firewall:
Application Level Firewalls - Often called a Proxy Server. It works by transferring a copy of each accepted data packet from one network to another. They are known as the Second generation of firewalls.
An application-proxy gateway is a feature of advanced firewalls that combines lower-layer access control with upper-layer functionality. These firewalls contain a proxy agent that

acts as an intermediary between two hosts that wish to communicate with each other, and never allows a direct connection between them. Each successful connection attempt actually results in the creation of two separate connections-one between the client and the proxy server, and another between the proxy server and the true destination. The proxy is meant to be transparent to the two hosts-from their perspectives there is a direct connection. Because external hosts only communicate with the proxy agent, internal IP addresses are not visible to the outside world. The proxy agent interfaces directly with the firewall ruleset to determine whether a given instance of network traffic should be allowed to transit the firewall.

Stateful Inspection Firewall - Packets are captured by the inspection engine operating at the network layer and then analyzed at all layers. They are known as the Third generation of firewalls.

Stateful inspection improves on the functions of packet filters by tracking the state of connections and blocking packets that deviate from the expected state. This is accomplished by incorporating greater awareness of the transport layer. As with packet filtering, stateful inspection intercepts packets at the network layer and inspects them to see if they are permitted by an existing firewall rule, but unlike packet filtering, stateful inspection keeps track of each connection in a state table. While the details of state table entries vary by firewall product, they typically include source IP address, destination IP address, port numbers, and connection state information.

Web Application Firewalls - The HTTP protocol used in web servers has been exploited by attackers in many ways, such as to place malicious software on the computer of someone browsing the web, or to fool a person into revealing private information that they might not have otherwise. Many of these exploits can be detected by specialized application firewalls called web application firewalls that reside in front of the web server. Web application firewalls are a relatively new technology, as compared to other firewall technologies, and the type of threats that they mitigate are still changing frequently. Because they are put in front of web servers to prevent attacks on the server, they are often considered to be very different than traditional firewalls.

Host-Based Firewalls and Personal Firewalls - Host-based firewalls for servers and personal firewalls for desktop and laptop personal computers (PC) provide an additional layer of security against network-based attacks. These firewalls are software-based, residing on the hosts they are protecting-each monitors and controls the incoming and outgoing network traffic for a single host. They can provide more granular protection than network firewalls to meet the needs of specific hosts.

Host-based firewalls are available as part of server operating systems such as Linux, Windows, Solaris, BSD, and Mac OS X Server, and they can also be installed as third-party add-ons. Configuring a host-based firewall to allow only necessary traffic to the server provides protection against malicious activity from all hosts, including those on the same subnet or on other internal subnets not separated by a network firewall. Limiting outgoing traffic from a server may also be helpful in preventing certain malware that infects a host from spreading to other hosts.11 Host-based firewalls usually perform logging, and can often be configured to perform address-based and application-based access controls

Dynamic Packet Filtering - Makes informed decisions on the ACL's to apply. They are known as the Fourth generation of firewalls.

Kernel Proxy - Very specialized architecture that provides modular kernel-based, multi-

layer evaluation and runs in the NT executive space. They are known as the Fifth generation of firewalls.
The following were incorrect answers:
All of the other types of firewalls listed are more complex than the Packet Filtering Firewall.
Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 6th Edition, Telecommunications and Network Security, Page 630.
and
NIST Guidelines on Firewalls and Firewalls policies, Special Publication 800-4 Revision 1

NEW QUESTION: 247
Another name for a VPN is a:
A. tunnel
B. one-time password
C. pipeline
D. bypass
Answer: (SHOW ANSWER)
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 248
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)
Explanation/Reference:
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: 249
What is the primary role of smartcards in a PKI?
A. Transparent renewal of user keys
B. Easy distribution of the certificates between the users
C. Fast hardware encryption of the raw data

D. Tamper resistant, mobile storage and application of private keys of the users

Answer: (SHOW ANSWER)

Section: Access Control

Explanation/Reference: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page
139;
SNYDER, J., What is a SMART CARD?.
Wikipedia has a nice definition at: http://en.wikipedia.org/wiki/Tamper_resistance Security Tamper-resistant microprocessors are used to store and process private or sensitive information, such as private keys or electronic money credit. To prevent an attacker from retrieving or modifying the information, the chips are designed so that the information is not accessible through external means and can be accessed only by the embedded software, which should contain the appropriate security measures. Examples of tamper-resistant chips include all secure cryptoprocessors, such as the IBM 4758 and chips used in smartcards, as well as the Clipper chip.
It has been argued that it is very difficult to make simple electronic devices secure against tampering, because numerous attacks are possible, including:
physical attack of various forms (microprobing, drills, files, solvents, etc.) freezing the device applying out-of-spec voltages or power surges applying unusual clock signals inducing software errors using radiation measuring the precise time and power requirements of certain operations (see power analysis) Tamper-resistant chips may be designed to zeroise their sensitive data (especially cryptographic keys) if they detect penetration of their security encapsulation or out-of-specification environmental parameters. A chip may even be rated for "cold zeroisation", the ability to zeroise itself even after its power supply has been crippled.
Nevertheless, the fact that an attacker may have the device in his possession for as long as he likes, and perhaps obtain numerous other samples for testing and practice, means that it is practically impossible to totally eliminate tampering by a sufficiently motivated opponent. Because of this, one of the most important elements in protecting a system is overall system design. In particular, tamper-resistant systems should "fail gracefully" by ensuring that compromise of one device does not compromise the entire system. In this manner, the attacker can be practically restricted to attacks that cost less than the expected return from compromising a single device (plus, perhaps, a little more for kudos). Since the most sophisticated attacks have been estimated to cost several hundred thousand dollars to carry out, carefully designed systems may be invulnerable in practice.

NEW QUESTION: 250

Which of the following is the primary security feature of a proxy server?

A. Virus Detection

B. URL blocking

C. Route blocking

D. Content filtering

Answer: (SHOW ANSWER)

Explanation/Reference:

In many organizations, the HTTP proxy is used as a means to implement content filtering, for instance, by logging or blocking traffic that has been defined as, or is assumed to be nonbusiness related for some reason.
Although filtering on a proxy server or firewall as part of a layered defense can be quite effective to prevent, for instance, virus infections (though it should never be the only protection against viruses), it will be only moderately effective in preventing access to unauthorized services (such as certain remote-access services or file sharing), as well as preventing the download of unwanted content. HTTP Tunneling.
HTTP tunneling is technically a misuse of the protocol on the part of the designer of such tunneling applications. It has become a popular feature with the rise of the first streaming video and audio applications and has been implemented into many applications that have a market need to bypass user policy restrictions.
Usually, HTTP tunneling is applied by encapsulating outgoing traffic from an application in an HTTP request and incoming traffic in a response. This is usually not done to circumvent security, but rather, to be compatible with existing firewall rules and allow an application to function through a firewall without the need to apply special rules, or additional configurations.
The following are incorrect choices:
Virus Detection A proxy is not best at detection malware and viruses within content. A antivirus product would be use for that purpose.
URL blocking This would be a subset of Proxying, based on the content some URL's may be blocked by the proxy but it is not doing filtering based on URL addresses only. This is not the BEST answer.
Route blocking This is a function that would be done by Intrusion Detection and Intrusion prevention system and not the proxy. This could be done by filtering devices such as Firewalls and Routers as well. Again, not the best choice.
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 6195-6201). Auerbach Publications. Kindle Edition.

NEW QUESTION: 251
Which of the following control pairing places emphasis on "soft" mechanisms that support the access control objectives?
A. Preventive/Technical Pairing
B. Preventive/Administrative Pairing
C. Preventive/Physical Pairing
D. Detective/Administrative Pairing
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Soft Control is another way of referring to Administrative control.
Technical and Physical controls are NOT soft control, so any choice listing them was not the best answer.

Preventative/Technical is incorrect because although access control can be technical control, it is commonly not referred to as a "soft" control Preventative/Administrative is correct because access controls are preventative in nature. it is always best to prevent a negative event, however there are times where controls might fail and you cannot prevent everything.
Administrative controls are roles, responsibilities, policies, etc which are usually paper based. In the administrative category you would find audit, monitoring, and security awareness as well.
Preventative/Physical pairing is incorrect because Access controls with an emphasis on "soft" mechanisms conflict with the basic concept of physical controls, physical controls are usually tangible objects such as fences, gates, door locks, sensors, etc...
Detective/Administrative Pairing is incorrect because access control is a preventative control used to control access, not to detect violations to access.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION: 252
Which of the following transmission media would NOT be affected by cross talk or interference?
A. Copper cable
B. Radio System
C. Satellite radiolink
D. Fiber optic cables
Answer: (SHOW ANSWER)
Only fiber optic cables are not affected by crosstalk or interference.
For your exam you should know the information about transmission media:
Copper Cable Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data. Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the 1820s.The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.
Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts. Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors.
Copper Cable

Image Source http://i00.i.aliimg.com/photo/v0/570456138/FRLS_HR_PVC_Copper_Cable.jpg

Coaxial cable Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line.

Coaxial cable are expensive and does not support many LAN's. It supports data and video Coaxial Cable

Image Source - http://www.tlc-direct.co.uk/Images/Products/size_3/CARG59.JPG

Fiber optics

An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Radio System

Radio systems are used for short distance,cheap and easy to tap.

Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.

Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width.

When radio waves strike an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.

Fiber Optics

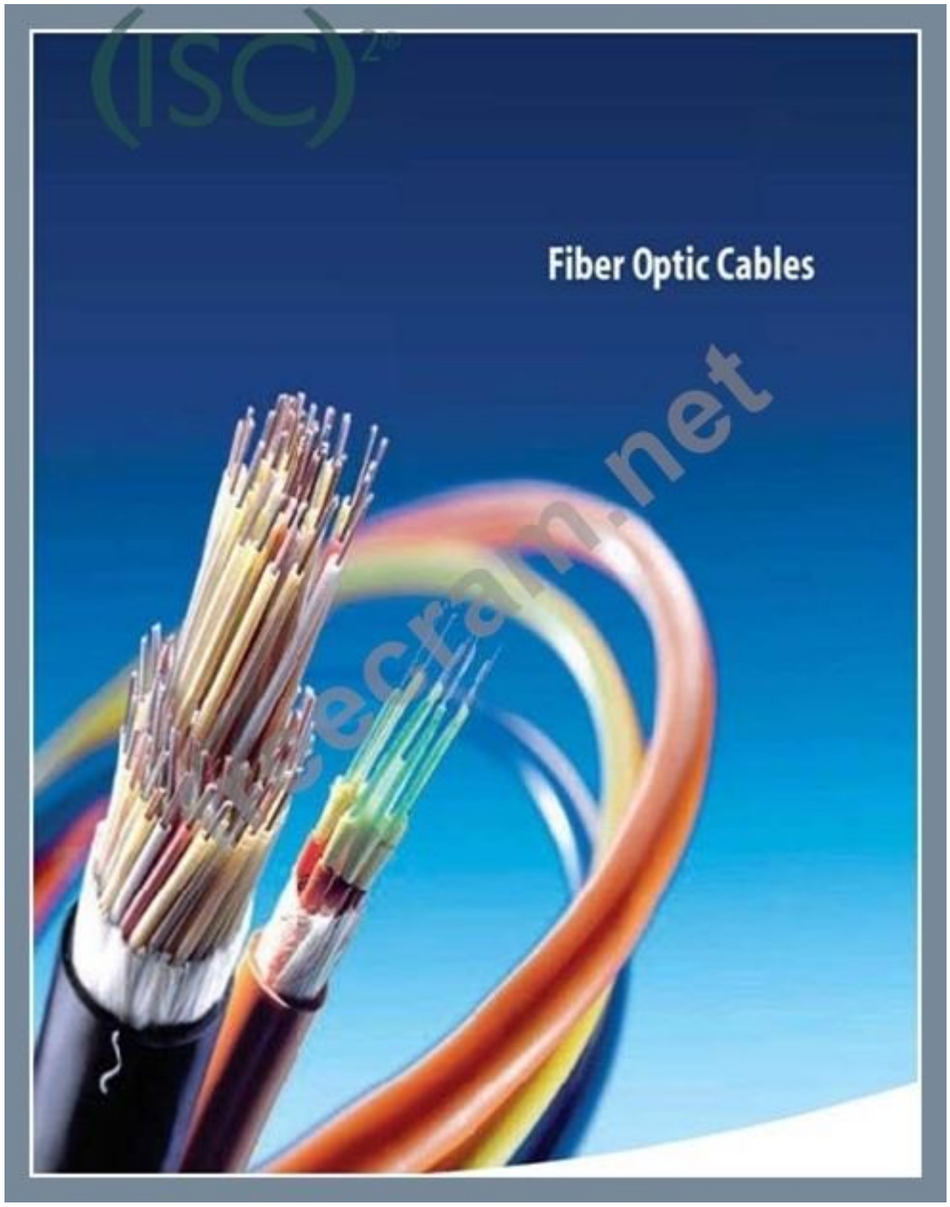


Image Source - http://aboveinfranet.com/wp-content/uploads/2014/04/fiber-optic-cablesabove-infranet-solutions.jpg

Microwave radio system Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimetre; these are called microwaves. Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum

below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can.
Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.
Microwave radio systems are carriers for voice data signal, cheap and easy to tap.
Microwave Radio System

Image Source http://www.valiantcom.com/images/applications/e1_digital_microwave_radio.gif
Satellite Radio Link Satellite radio is a radio service broadcast from satellites primarily to cars, with the signal broadcast nationwide, across a much wider geographical area than terrestrial radio stations. It is available by subscription, mostly commercial free, and offers subscribers more stations and a wider variety of programming options than terrestrial radio.
Satellite radio link uses transponder to send information and easy to tap.
The following answers are incorrect:
Copper Cable - Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.
Radio System - Radio systems are used for short distance,cheap and easy to tap.
Satellite Radio Link - Satellite radio link uses transponder to send information and easy to tap.
The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 265 &
Official ISC2 guide to CISSP CBK 3rd Edition Page number 233

NEW QUESTION: 253
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: (SHOW ANSWER)

Explanation/Reference:

The principle of least privilege refers to allowing users to have only the access they need and not anything more. Thus, certain users may have no need to access any of the files on specific systems.

The following answers are incorrect:

Users can access all systems. Although the principle of least privilege limits what access and systems users have authorization to, not all users would have a need to know to access all of the systems. The best answer is still Users would get access to only the info for which they have a need to know as some of the users may not have a need to access a system.

Users get new privileges when they change positions. Although true that a user may indeed require new privileges, this is not a given fact and in actuality a user may require less privileges for a new position. The principle of least privilege would require that the rights required for the position be closely evaluated and where possible rights revoked.

Authorization creep. Authorization creep occurs when users are given additional rights with new positions and responsibilities. The principle of least privilege should actually prevent authorization creep.

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

ISC2 OIG 2007 p.101,123

Shon Harris AIO v3 p148, 902-903

NEW QUESTION: 254

The IP header contains a protocol field. If this field contains the value of 2, what type of data is contained within the IP datagram?

A. TCP.

B. ICMP.

C. UDP.

D. IGMP.

Answer: (SHOW ANSWER)

If the protocol field has a value of 2 then it would indicate it was IGMP.

The following answers are incorrect:

TCP. Is incorrect because the value for a TCP protocol would be 6. UDP. Is incorrect because the value for an UDP protocol would be 17. ICMP. Is incorrect because the value for an ICMP protocol would be 1.

NEW QUESTION: 255

Within the OSI model, at what layer are some of the SLIP, CSLIP, PPP control functions provided?

A. Data Link

B. Transport

C. Presentation

D. Application

Answer: (SHOW ANSWER)

RFC 1661 - The Point-to-Point Protocol (PPP) specifies that the Point-to-

Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams

over point-to-point links. PPP is comprised of three main components:
1 A method for encapsulating multi-protocol datagrams.
2 A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection.
3 A family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols.

NEW QUESTION: 256
Which of the following protocols that provide integrity and authentication for IPSec, can also provide non-repudiation in IPSec?
A. Authentication Header (AH)
B. Encapsulating Security Payload (ESP)
C. Secure Sockets Layer (SSL)
D. Secure Shell (SSH-2)
Answer: (SHOW ANSWER)
Section: Cryptography
Explanation/Reference:
As per the RFC in reference, the Authentication Header (AH) protocol is a mechanism for providing strong integrity and authentication for IP datagrams. It might also provide non-repudiation, depending on which cryptographic algorithm is used and how keying is performed. For example, use of an asymmetric digital signature algorithm, such as RSA, could provide non-repudiation.
from a cryptography point of view, so we will cover it from a VPN point of view here. IPSec is a suite of protocols that was developed to specifically protect IP traffic. IPv4 does not have any integrated security, so IPSec was developed to bolt onto IP and secure the data the protocol transmits. Where PPTP and L2TP work at the data link layer, IPSec works at the network layer of the OSI model. The main protocols that make up the IPSec suite and their basic functionality are as follows: A. Authentication Header (AH) provides data integrity, data origin authentication, and protection from replay attacks. B. Encapsulating Security Payload (ESP) provides confidentiality, data-origin authentication, and data integrity. C. Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for security association creation and key exchange. D.
Internet Key Exchange (IKE) provides authenticated keying material for use with ISAKMP.
The following are incorrect answers:
ESP is a mechanism for providing integrity and confidentiality to IP datagrams. It may also provide authentication, depending on which lgorithm and algorithm mode are used. Non-repudiation and protection from traffic analysis are not provided by ESP (RFC 1827).
SSL is a secure protocol used for transmitting private information over the Internet. It works by using a public key to encrypt data that is transferred of the SSL connection. OIG 2007, page 976 SSH-2 is a secure, efficient, and portable version of SSH (Secure Shell) which is a secure replacement for telnet.
Reference(s) used for this question:
Shon Harris, CISSP All In One, 6th Edition , Page 705
and

RFC 1826, http://tools.ietf.org/html/rfc1826, paragraph 1.

NEW QUESTION: 257
What ensures that the control mechanisms correctly implement the security policy for the entire life cycle of an information system?
A. Accountability controls
B. Mandatory access controls
C. Assurance procedures
D. Administrative controls
Answer: (SHOW ANSWER)
Controls provide accountability for individuals accessing information.
Assurance procedures ensure that access control mechanisms correctly implement the security policy for the entire life cycle of an information system.
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 33).

NEW QUESTION: 258
Which encryption algorithm is BEST suited for communication with handheld wireless devices?
A. ECC (Elliptic Curve Cryptosystem)
B. RSA
C. SHA
D. RC4
Answer: (SHOW ANSWER)
Section: Cryptography
Explanation/Reference:
As it provides much of the same functionality that RSA provides: digital signatures, secure key distribution,and encryption. One differing factor is ECC's efficiency. ECC is more efficient that RSA and any other asymmetric algorithm.
The following answers are incorrect because :
RSA is incorrect as it is less efficient than ECC to be used in handheld devices.
SHA is also incorrect as it is a hashing algorithm.

RC4 is also incorrect as it is a symmetric algorithm.
Reference : Shon Harris AIO v3 , Chapter-8 : Cryptography , Page : 631 , 638.

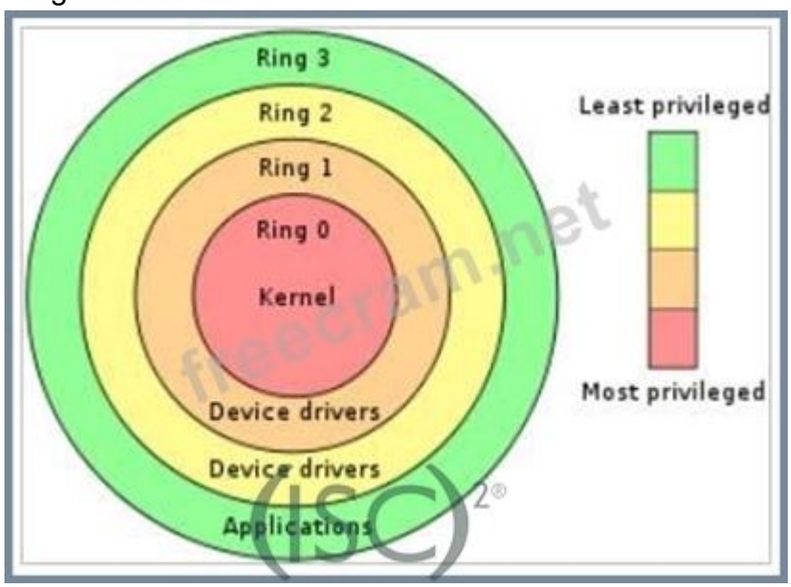
NEW QUESTION: 259
Physically securing backup tapes from unauthorized access is obviously a security concern and is considered a function of the:
A. Operations Security Domain.
B. Operations Security Domain Analysis.
C. Telecommunications and Network Security Domain.
D. Business Continuity Planning and Disater Recovery Planning.
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
Physically securing the tapes from unauthorized access is obviously a security concern and is considered a function of the Operations Security Domain.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 71.

NEW QUESTION: 260
The ability to adjust access control to the exact amount of permission necessary is called _____.

A. Detection
B. Separation of Duties
C. Granularity
D. Concept of Least Privilege
Answer: (SHOW ANSWER)

NEW QUESTION: 261
An Architecture where there are more than two execution domains or privilege levels is called:
A. Ring Architecture.
B. Ring Layering
C. Network Environment.
D. Security Models
Answer: (SHOW ANSWER)
Explanation/Reference:
In computer science, hierarchical protection domains, often called protection rings, are a mechanism to protect data and functionality from faults (fault tolerance) and malicious behavior (computer security). This approach is diametrically opposite to that of capability-based security.
Computer operating systems provide different levels of access to resources. A protection ring is one of two or more hierarchical levels or layers of privilege within the architecture of a computer system. This is generally hardware-enforced by some CPU architectures that provide different CPU modes at the

hardware or microcode level. Rings are arranged in a hierarchy from most privileged (most trusted, usually numbered zero) to least privileged (least trusted, usually with the highest ring number). On most operating systems, Ring 0 is the level with the most privileges and interacts most directly with the physical hardware such as the CPU and memory.
Special gates between rings are provided to allow an outer ring to access an inner ring's resources in a predefined manner, as opposed to allowing arbitrary usage. Correctly gating access between rings can improve security by preventing programs from one ring or privilege level from misusing resources intended for programs in another. For example, spyware running as a user program in Ring 3 should be prevented from turning on a web camera without informing the user, since hardware access should be a Ring 1 function reserved for device drivers. Programs such as web browsers running in higher numbered rings must request access to the network, a resource restricted to a lower numbered ring.
Ring Architecture



All of the other answers are incorrect because they are detractors.
References:
OIG CBK Security Architecture and Models (page 311)
and
https://en.wikipedia.org/wiki/Ring_%28computer_security%29

NEW QUESTION: 262
Which of the following tape formats can be used to backup data systems in addition to its original intended audio uses?
A. Digital Video Tape (DVT).
B. Digital Analog Tape (DAT).
C. Digital Voice Tape (DVT).
D. Digital Audio Tape (DAT).
Answer: (SHOW ANSWER)
Explanation/Reference:

Digital Audio Tape (DAT) can be used to backup data systems in addition to its original intended audio uses.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 70.

NEW QUESTION: 263
Which IPSec operational mode encrypts the entire data packet (including header and data) into an IPSec packet?
A. Authentication mode
B. Tunnel mode
C. Transport mode
D. Safe mode
Answer: (SHOW ANSWER)
In tunnel mode, the entire packet is encrypted and encased into an IPSec packet.
In transport mode, only the datagram (payload) is encrypted, leaving the IP address visible within the IP header.
Authentication mode and safe mode are not defined IPSec operational modes.
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 96).

NEW QUESTION: 264
Which of the following is NOT a proper component of Media Viability Controls?
A. Storage
B. Writing
C. Handling
D. Marking
Answer: (SHOW ANSWER)
Media Viability Controls include marking, handling and storage.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the
Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 231.

NEW QUESTION: 265
The Diffie-Hellman algorithm is used for:
A. Encryption
B. Digital signature
C. Key agreement
D. Non-repudiation
Answer: (SHOW ANSWER)
Explanation/Reference:

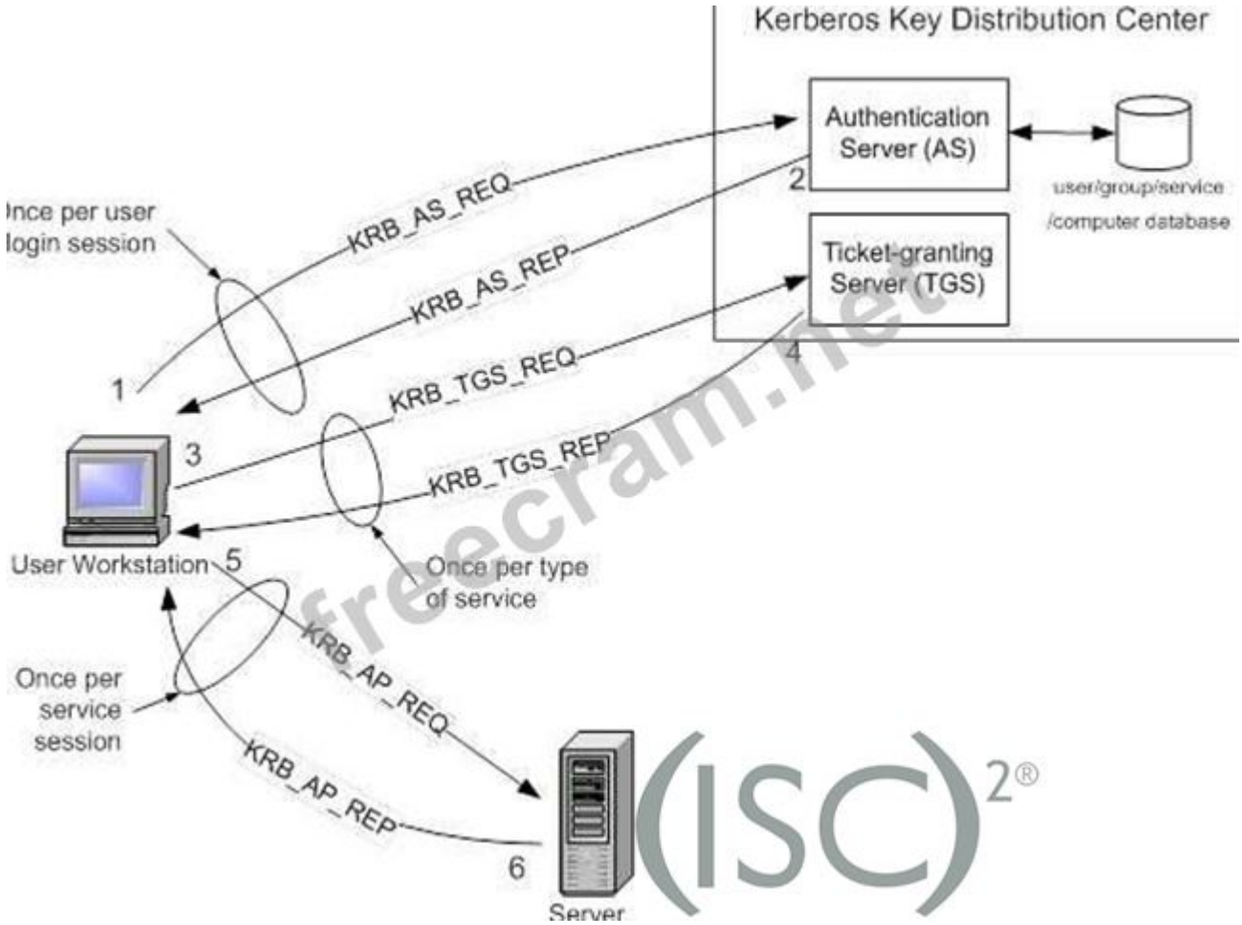
The Diffie-Hellman algorithm is used for Key agreement (key distribution) and cannot be used to encrypt and decrypt messages.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 4).
Note: key agreement, is different from key exchange, the functionality used by the other asymmetric algorithms.
References:
AIO, third edition Cryptography (Page 632)
AIO, fourth edition Cryptography (Page 709)

NEW QUESTION: 266
Which one of the following represents an ALE calculation?
A. single loss expectancy x annualized rate of occurrence.
B. gross loss expectancy x loss frequency.
C. actual replacement cost - proceeds of salvage.
D. asset value x loss expectancy.
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
Single Loss Expectancy (SLE) is the dollar amount that would be lost if there was a loss of an asset.
Annualized Rate of Occurrence (ARO) is an estimated possibility of a threat to an asset taking place in one year (for example if there is a change of a flood occuring once in 10 years the ARO would be .1, and if there was a chance of a flood occuring once in 100 years then the ARO would be .01).
The following answers are incorrect:
gross loss expectancy x loss frequency. Is incorrect because this is a distractor.
actual replacement cost - proceeds of salvage. Is incorrect because this is a distractor.
asset value x loss expectancy. Is incorrect because this is a distractor.

NEW QUESTION: 267
Which of the following statements pertaining to message digests is incorrect?
A. The original file cannot be created from the message digest.
B. Two different files should not have the same message digest.
C. The message digest should be calculated using at least 128 bytes of the file.
D. Messages digests are usually of fixed size.
Answer: (SHOW ANSWER)
Section: Cryptography
Explanation/Reference:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 160).

NEW QUESTION: 268
Which of the following is NOT true of the Kerberos protocol?

A. Only a single login is required per session.
B. The initial authentication steps are done using public key algorithm.
C. The KDC is aware of all systems in the network and is trusted by all of them
D. It performs mutual authentication
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. It has the following characteristics:
It is secure: it never sends a password unless it is encrypted.
Only a single login is required per session. Credentials defined at login are then passed between resources without the need for additional logins.
The concept depends on a trusted third party - a Key Distribution Center (KDC). The KDC is aware of all systems in the network and is trusted by all of them.
It performs mutual authentication, where a client proves its identity to a server and a server proves its identity to the client.
Kerberos introduces the concept of a Ticket-Granting Server/Service (TGS). A client that wishes to use a service has to receive a ticket from the TGS - a ticket is a time-limited cryptographic message - giving it access to the server. Kerberos also requires an Authentication Server (AS) to verify clients. The two servers combined make up a KDC.
Within the Windows environment, Active Directory performs the functions of the KDC. The following figure shows the sequence of events required for a client to gain access to a service using Kerberos authentication.
Each step is shown with the Kerberos message associated with it, as defined in RFC 4120 "The Kerberos Network Authorization Service (V5)".



Kerberos Authentication Step by Step

Step 1: The user logs on to the workstation and requests service on the host. The workstation sends a message to the Authorization Server requesting a ticket granting ticket (TGT).

Step 2: The Authorization Server verifies the user's access rights in the user database and creates a TGT and session key. The Authorization Sever encrypts the results using a key derived from the user's password and sends a message back to the user workstation.

The workstation prompts the user for a password and uses the password to decrypt the incoming message.

When decryption succeeds, the user will be able to use the TGT to request a service ticket.

Step 3: When the user wants access to a service, the workstation client application sends a request to the Ticket Granting Service containing the client name, realm name and a timestamp. The user proves his identity by sending an authenticator encrypted with the session key received in Step 2.

Step 4: The TGS decrypts the ticket and authenticator, verifies the request, and creates a ticket for the requested server. The ticket contains the client name and optionally the client IP address. It also contains the realm name and ticket lifespan. The TGS returns the ticket to the user workstation. The returned message contains two copies of a server session key - one encrypted with the client password, and one encrypted by the service password.

Step 5: The client application now sends a service request to the server containing the ticket received in Step

4 and an authenticator. The service authenticates the request by decrypting the session key. The server verifies that the ticket and authenticator match, and then grants access to the service. This step as described does not include the authorization performed by the Intel AMT device, as described later.
Step 6: If mutual authentication is required, then the server will reply with a server authentication message.
The Kerberos server knows "secrets" (encrypted passwords) for all clients and servers under its control, or it is in contact with other secure servers that have this information. These "secrets" are used to encrypt all of the messages shown in the figure above.
To prevent "replay attacks," Kerberos uses timestamps as part of its protocol definition. For timestamps to work properly, the clocks of the client and the server need to be in synch as much as possible. In other words, both computers need to be set to the same time and date. Since the clocks of two computers are often out of synch, administrators can establish a policy to establish the maximum acceptable difference to Kerberos between a client's clock and server's clock. If the difference between a client's clock and the server's clock is less than the maximum time difference specified in this policy, any timestamp used in a session between the two computers will be considered authentic. The maximum difference is usually set to five minutes.
Note that if a client application wishes to use a service that is "Kerberized" (the service is configured to perform Kerberos authentication), the client must also be Kerberized so that it expects to support the necessary message responses.
For more information about Kerberos, see http://web.mit.edu/kerberos/www/.
References:
Introduction to Kerberos Authentication from Intel
and
http://www.zeroshell.net/eng/kerberos/Kerberos-definitions/#1.3.5.3
and
http://www.ietf.org/rfc/rfc4120.txt

NEW QUESTION: 269
Which of the following is less likely to accompany a contingency plan, either within the plan itself or in the form of an appendix?
A. Contact information for all personnel.
B. Vendor contact information, including offsite storage and alternate site.
C. Equipment and system requirements lists of the hardware, software, firmware and other resources required to support system operations.
D. The Business Impact Analysis.
Answer: (SHOW ANSWER)
Why is this the correct answer? Simply because it is WRONG, you would have contact information for your emergency personnel within the plan but NOT for ALL of your personnel. Be careful of words such as ALL. According to NIST's Special publication 800-34, contingency plan appendices provide key details not contained in the main body of the plan. The appendices should reflect the specific technical, operational, and management contingency requirements of the given system. Contact information for

recovery team personnel (not all personnel) and for vendor should be included, as well as detailed system requirements to allow for supporting of system operations. The Business Impact Analysis (BIA) should also be included as an appendix for reference should the plan be activated.
Reference(s) used for this question: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems

NEW QUESTION: 270
Which of the following would assist the most in Host Based intrusion detection?
A. audit trails.
B. access control lists.
C. security clearances.
D. host-based authentication.
Answer: (SHOW ANSWER)
Explanation/Reference:
To assist in Intrusion Detection you would review audit logs for access violations.
The following answers are incorrect:
access control lists. This is incorrect because access control lists determine who has access to what but do not detect intrusions.
security clearances. This is incorrect because security clearances determine who has access to what but do not detect intrusions.
host-based authentication. This is incorrect because host-based authentication determine who have been authenticated to the system but do not dectect intrusions.

NEW QUESTION: 271
Which of the following control pairing places emphasis on "soft" mechanisms that support the access control objectives?
A. Preventive/Technical Pairing
B. Preventive/Administrative Pairing
C. Preventive/Physical Pairing
D. Detective/Administrative Pairing
Answer: B (LEAVE A REPLY)
Soft Control is another way of referring to Administrative control.
Technical and Physical controls are NOT soft control, so any choice listing them was not the best answer.
Preventative/Technical is incorrect because although access control can be technical control, it is commonly not referred to as a "soft" control
Preventative/Administrative is correct because access controls are preventative in nature. it is always best to prevent a negative event, however there are times where controls might fail and you cannot prevent everything. Administrative controls are roles, responsibilities, policies, etc which are usually paper based. In the administrative category you would find

audit, monitoring, and security awareness as well.
Preventative/Physical pairing is incorrect because Access controls with an emphasis on "soft" mechanisms conflict with the basic concept of physical controls, physical controls are usually tangible objects such as fences, gates, door locks, sensors, etc...
Detective/Administrative Pairing is incorrect because access control is a preventative control used to control access, not to detect violations to access.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION: 272
In response to Access-request from a client such as a Network Access Server (NAS), which of the following is not one of the response from a RADIUS Server?
A. Access-Accept
B. Access-Reject
C. Access-Granted
D. Access-Challenge
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
In response to an access-request from a client, a RADIUS server returns one of three authentication responses: access-accept, access-reject, or access-challenge, the latter being a request for additional authentication information such as a one-time password from a token or a callback identifier.
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, page 36.

NEW QUESTION: 273
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:
Radius, TACACS and DIAMETER are classified as authentication, authorization, and accounting (AAA) servers.
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 33.
also see:
The term "AAA" is often used, describing cornerstone concepts [of the AIC triad] Authentication, Authorization, and Accountability. Left out of the AAA acronym is Identification which is required before the three "A's" can follow. Identity is a claim, Authentication proves an identity, Authorization describes the action you can perform on a system once you have been identified and authenticated, and accountability holds users accountable for their actions.
Reference: CISSP Study Guide, Conrad Misenar, Feldman p. 10-11, (c) 2010 Elsevier.

NEW QUESTION: 274
Which communication method is characterized by very high speed transmission rates that are governed by electronic clock timing signals?
A. Asynchronous Communication.
B. Synchronous Communication.
C. Automatic Communication.
D. Full duplex Communication.
Answer: (SHOW ANSWER)
Synchronous Communication is characterized by very high speed transmission rates that are governed by electronic clock timing signals. 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: 275
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: (SHOW ANSWER)
Explanation/Reference:
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. Corrobative evidence takes many forms.
In a rape case for example, this could consist of torn clothing, soiled bed sheets, 911 emergency calls tapes, and
prompt complaint witnesses.

There are many types of evidence that exist. Below you have explanations of some of the most common types:

Physical Evidence

Physical evidence is any evidence introduced in a trial in the form of a physical object, intended to prove a fact in issue based on its demonstrable physical characteristics. Physical evidence can conceivably include all or part of any object.

In a murder trial for example (or a civil trial for assault), the physical evidence might include DNA left by the attacker on the victim's body, the body itself, the weapon used, pieces of carpet spattered with blood, or casts of footprints or tire prints found at the scene of the crime.

Real Evidence

Real evidence is a type of physical evidence and consists of objects that were involved in a case or actually played a part in the incident or transaction in question.

Examples include the written contract, the defective part or defective product, the murder weapon, the gloves used by an alleged murderer. Trace evidence, such as fingerprints and firearm residue, is a species of real evidence. Real evidence is usually reported upon by an expert witness with appropriate qualifications to give an opinion. This normally means a forensic scientist or one qualified in forensic engineering.

Admission of real evidence requires authentication, a showing of relevance, and a showing that the object is in "the same or substantially the same condition" now as it was on the relevant date. An object of real evidence is authenticated through the senses of witnesses or by circumstantial evidence called chain of custody.

Documentary

Documentary evidence is any evidence introduced at a trial in the form of documents. Although this term is most widely understood to mean writings on paper (such as an invoice, a contract or a will), the term actually include any media by which information can be preserved. Photographs, tape recordings, films, and printed emails are all forms of documentary evidence.

Documentary versus physical evidence

A piece of evidence is not documentary evidence if it is presented for some purpose other than the examination of the contents of the document. For example, if a blood-spattered letter is introduced solely to show that the defendant stabbed the author of the letter from behind as it was being written, then the evidence is physical evidence, not documentary evidence. However, a film of the murder taking place would be documentary evidence (just as a written description of the event from an eyewitness). If the content of that same letter is then introduced to show the motive for the murder, then the evidence would be both physical and documentary.

Documentary Evidence Authentication

Documentary evidence is subject to specific forms of authentication, usually through the testimony of an eyewitness to the execution of the document, or to the testimony of a witness able to identify the handwriting of the purported author. Documentary evidence is also subject to the best evidence rule, which requires that the original document be produced unless there is a good reason not to do so.

The role of the expert witness

Where physical evidence is of a complexity that makes it difficult for the average person to understand its significance, an expert witness may be called to explain to the jury the proper interpretation of the evidence at hand.

Digital Evidence or Electronic Evidence

Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial.

The use of digital evidence has increased in the past few decades as courts have allowed the use of e-mails, digital photographs, ATM transaction logs, word processing documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories, databases, the contents of computer memory, computer backups, computer printouts, Global Positioning System tracks, logs from a hotel's electronic door locks, and digital video or audio files.

While many courts in the United States have applied the Federal Rules of Evidence to digital evidence in the same way as more traditional documents, courts have noted very important differences. As compared to the more traditional evidence, courts have noted that digital evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive, and more readily available. As such, some courts have sometimes treated digital evidence differently for purposes of authentication, hearsay, the best evidence rule, and privilege. In December 2006, strict new rules were enacted within the Federal Rules of Civil Procedure requiring the preservation and disclosure of electronically stored evidence.

Demonstrative Evidence

Demonstrative evidence is evidence in the form of a representation of an object. This is, as opposed to, real evidence, testimony, or other forms of evidence used at trial.

Examples of demonstrative evidence include photos, x-rays, videotapes, movies, sound recordings, diagrams, forensic animation, maps, drawings, graphs, animation, simulations, and models. It is useful for assisting a finder of fact (fact-finder) in establishing context among the facts presented in a case. To be admissible, a demonstrative exhibit must "fairly and accurately" represent the real object at the relevant time.

Chain of custody

Chain of custody refers to the chronological documentation, and/or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic. Because evidence can be used in court to convict persons of crimes, it must be handled in a scrupulously careful manner to avoid later allegations of tampering or misconduct which can compromise the case of the prosecution toward acquittal or to overturning a guilty verdict upon appeal.

The idea behind recoding the chain of custody is to establish that the alleged evidence is fact related to the alleged crime - rather than, for example, having been planted fraudulently to make someone appear guilty.

Establishing the chain of custody is especially important when the evidence consists of fungible goods. In practice, this most often applies to illegal drugs which have been seized by law enforcement personnel. In such cases, the defendant at times disclaims any knowledge of possession of the controlled substance in question.

Accordingly, the chain of custody documentation and testimony is presented by the prosecution to establish that the substance in evidence was in fact in the possession of the defendant.
An identifiable person must always have the physical custody of a piece of evidence. In practice, this means that a police officer or detective will take charge of a piece of evidence, document its collection, and hand it over to an evidence clerk for storage in a secure place. These transactions, and every succeeding transaction between the collection of the evidence and its appearance in court, should be completely documented chronologically in order to withstand legal challenges to the authenticity of the evidence.
Documentation should include the conditions under which the evidence is gathered, the identity of all evidence handlers, duration of evidence custody, security conditions while handling or storing the evidence, and the manner in which evidence is transferred to subsequent custodians each time such a transfer occurs (along with the signatures of persons involved at each step).
Example
An example of "Chain of Custody" would be the recovery of a bloody knife at a murder scene:
Officer Andrew collects the knife and places it into a container, then gives it to forensics technician Bill.
Forensics technician Bill takes the knife to the lab and collects fingerprints and other evidence from the knife. Bill then gives the knife and all evidence gathered from the knife to evidence clerk Charlene.
Charlene then stores the evidence until it is needed, documenting everyone who has accessed the original evidence (the knife, and original copies of the lifted fingerprints).
The Chain of Custody requires that from the moment the evidence is collected, every transfer of evidence from person to person be documented and that it be provable that nobody else could have accessed that evidence. It is best to keep the number of transfers as low as possible.
In the courtroom, if the defendant questions the Chain of Custody of the evidence it can be proven that the knife in the evidence room is the same knife found at the crime scene. However, if there are discrepancies and it cannot be proven who had the knife at a particular point in time, then the Chain of Custody is broken and the defendant can ask to have the resulting evidence declared inadmissible.
"Chain of custody" is also used in most chemical sampling situations to maintain the integrity of the sample by providing documentation of the control, transfer, and analysis of samples. Chain of custody is especially important in environmental work where sampling can identify the existence of contamination and can be used to identify the responsible party.
REFERENCES:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 23173-23185). Auerbach Publications. Kindle Edition.
http://en.wikipedia.org/wiki/Documentary_evidence
http://en.wikipedia.org/wiki/Physical_evidence
http://en.wikipedia.org/wiki/Digital_evidence
http://en.wikipedia.org/wiki/Demonstrative_evidence
http://en.wikipedia.org/wiki/Real_evidence
http://en.wikipedia.org/wiki/Chain_of_custody

NEW QUESTION: 276

Which of the following remote access authentication systems is the most robust?
A. TACACS+
B. RADIUS
C. PAP
D. TACACS
Answer: (SHOW ANSWER)
TACACS+ is a proprietary Cisco enhancement to TACACS and is more
robust than RADIUS. PAP is not a remote access authentication system but a remote node
security protocol.
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 122).

NEW QUESTION: 277
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: (SHOW ANSWER)
Explanation/Reference:
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: 278
What attribute is included in a X.509-certificate?
A. Distinguished name of the subject
B. Telephone number of the department
C. secret key of the issuing CA
D. the key pair of the certificate holder
Answer: (SHOW ANSWER)
Explanation/Reference:
RFC 2459 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile; GUTMANN, P., X.509 style guide; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

NEW QUESTION: 279
Which of the following statements pertaining to message digests is incorrect?

A. The original file cannot be created from the message digest.
B. Two different files should not have the same message digest.
C. The message digest should be calculated using at least 128 bytes of the file.
D. Messages digests are usually of fixed size.
Answer: (SHOW ANSWER)
Explanation/Reference:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 160).

NEW QUESTION: 280
A Business Continuity Plan should be tested:
A. Once a month.
B. At least twice a year.
C. At least once a year.
D. At least once every two years.
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
It is recommended that testing does not exceed established frequency limits. For a plan to be effective, all components of the BCP should be tested at least once a year. Also, if there is a major change in the operations of the organization, the plan should be revised and tested not more than three months after the change becomes operational.
Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 165).

NEW QUESTION: 281
All of the following can be considered essential business functions that should be identified when creating a Business Impact Analysis (BIA) except one. Which of the following would not be considered an essential element of the BIA but an important TOPIC to include within the BCP plan:
A. IT Network Support
B. Accounting
C. Public Relations
D. Purchasing
Answer: (SHOW ANSWER)
Public Relations, although important to a company, is not listed as an
essential business function that should be identified and have loss criteria developed for.
All other entries are considered essential and should be identified and have loss criteria developed.
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: 282
Which of the following mechanisms was created to overcome the problem of collisions that occur on wired networks when traffic is simultaneously transmitted from different nodes?
A. Carrier sense multiple access with collision avoidance (CSMA/CA)
B. Carrier sense multiple access with collision detection (CSMA/CD)
C. Token-passing
D. Polling
Answer: (SHOW ANSWER)

NEW QUESTION: 283
Which of the following statements pertaining to the security kernel is incorrect?
A. The security kernel is made up of mechanisms that fall under the TCB and implements and enforces the reference monitor concept.
B. The security kernel must provide isolation for the processes carrying out the reference monitor concept and they must be tamperproof.
C. The security kernel must be small enough to be able to be tested and verified in a complete and comprehensive manner.
D. The security kernel is an access control concept, not an actual physical component.
Answer: (SHOW ANSWER)
Explanation/Reference:
The reference monitor, not the security kernel is an access control concept.
The security kernel is made up of software, and firmware components that fall within the TCB and implements and enforces the reference monitor concept. The security kernel mediates all access and functions between subjects and objects. The security kernel is the core of the TCB and is the most commonly used approach to building trusted computing systems.
There are three main requirements of the security kernel:
* It must provide isolation for the processes carrying out the reference monitor concept, and the processes must be tamperproof.
* It must be invoked for every access attempt and must be impossible to circumvent. Thus, the security kernel must be implemented in a complete and foolproof way.
* It must be small enough to be able to be tested and verified in a complete and comprehensive manner.
The following answers are incorrect:
The security kernel is made up of mechanisms that fall under the TCB and implements and enforces the reference monitor concept. Is incorrect because this is the definition of the security kernel.
The security kernel must provide isolation for the processes carrying out the reference monitor concept and they must be tamperproof. Is incorrect because this is one of the three requirements that make up the security kernel.
The security kernel must be small enough to be able to be tested and verified in a complete and comprehensive manner. Is incorrect because this is one of the three requirements that make up the security kernel.

NEW QUESTION: 284
Which of the following is NOT true concerning Application Control?
A. It limits end users use of applications in such a way that only particular screens are visible.
B. Only specific records can be requested through the application controls
C. Particular usage of the application can be recorded for audit purposes
D. It is non-transparent to the endpoint applications so changes are needed to the applications and databases involved
Answer: (SHOW ANSWER)
Explanation/Reference:
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, Auerbach.

NEW QUESTION: 285
How should a risk be HANDLED when the cost of the countermeasure OUTWEIGHS the cost of the risk?
A. Reject the risk
B. Perform another risk analysis
C. Accept the risk
D. Reduce the risk
Answer: (SHOW ANSWER)
Which means the company understands the level of risk it is faced.
The following answers are incorrect because :
Reject the risk is incorrect as it means ignoring the risk which is dangerous.
Perform another risk analysis is also incorrect as the existing risk analysis has already shown the results.
Reduce the risk is incorrect is applicable after implementing the countermeasures.
Reference : Shon Harris AIO v3 , Chapter-3: Security Management Practices , Page : 39

NEW QUESTION: 286
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: (SHOW ANSWER)
The software development life cycle (SDLC) (sometimes referred to as the System Development Life Cycle) is the process of creating or altering software systems, and the models and methodologies that people use to develop these systems.
The NIST SP 800-64 revision 2 has within the description section of para 3.2.1:
This section addresses security considerations unique to the second SDLC phase. Key security activities for this phase include:
Conduct the risk assessment and use the results to supplement the baseline security controls;

Analyze security requirements;
Perform functional and security testing;
Prepare initial documents for system certification and accreditation; and
Design security architecture.
Reviewing this publication you may want to pick development/acquisition. Although initiation would be a decent choice, it is correct to say during this phase you would only brainstorm the idea of security requirements. Once you start to develop and acquire hardware/software components then you would also develop the security controls for these. The Shon Harris reference below is correct as well.
Shon Harris' Book (All-in-One CISSP Certification Exam Guide) divides the SDLC differently:
Project initiation Functional design analysis and planning System design specifications Software development Installation Maintenance support Revision and replacement
According to the author (Shon Harris), security requirements should be developed during the functional design analysis and planning phase.
SDLC POSITIONING FROM NIST 800-64

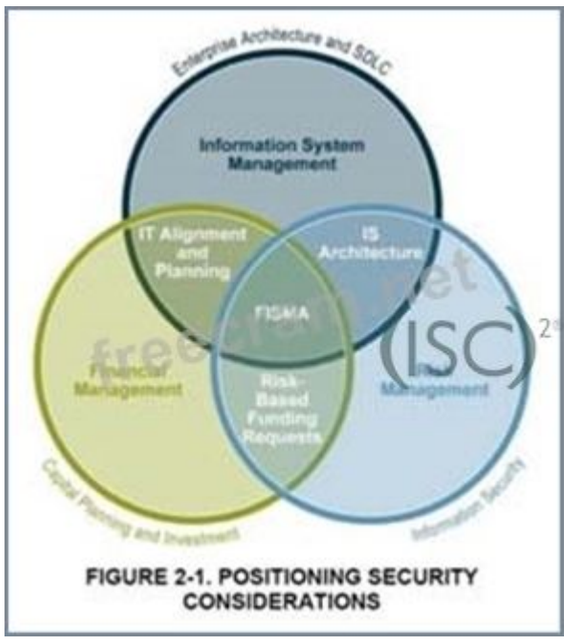


FIGURE 2-1. POSITIONING SECURITY CONSIDERATIONS

SDLC Positioning in the enterprise Information system security processes and activities provide valuable input into managing IT systems and their development, enabling risk identification, planning and mitigation. A risk management approach involves continually balancing the protection of agency information and assets with the cost of security controls and mitigation strategies throughout the complete information system development life cycle (see Figure 2-1 above). The most effective way to implement risk management is to identify critical assets and operations, as well as systemic vulnerabilities across the agency. Risks are shared and not bound by organization, revenue source, or topologies. Identification and verification of critical assets and operations and their interconnections can be achieved through the system security planning process, as well as through the compilation of information from the Capital Planning and Investment Control (CPIC) and Enterprise Architecture (EA) processes to establish insight into the agency's vital business operations, their supporting assets, and existing interdependencies and relationships.

With critical assets and operations identified, the organization can and should perform a business impact analysis (BIA). The purpose of the BIA is to relate systems and assets with the critical services they provide and assess the consequences of their disruption. By identifying these systems, an agency can manage security effectively by establishing priorities. This positions the security office to facilitate the IT program's cost-effective performance as well as articulate its business impact and value to the agency.
SDLC OVERVIEW FROM NIST 800-64 SDLC Overview from NIST 800-64 Revision 2

NIST 800-64 Revision 2 is one publication within the NISTstandards that I would recommend you look at for more details about the SDLC. It describe in great details what activities would take place and they have a nice diagram for each of the phases of the SDLC. You will find a copy at:
http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf
DISCUSSION:
Different sources present slightly different info as far as the phases names are concerned. People sometimes gets confused with some of the NIST standards. For example NIST 800-64 Security Considerations in the Information System Development Life Cycle has slightly different names, the activities mostly remains the same.
NIST clearly specifies that Security requirements would be considered throughout ALL of the phases. The keyword here is considered, if a question is about which phase they would be developed than Functional Design Analysis would be the correct choice.
Within the NIST standard they use different phase, howeverr under the second phase you will see that they talk specifically about Security Functional requirements analysis which confirms it is not at the initiation stage so it become easier to come out with the answer to this question. Here is what is stated:
The security functional requirements analysis considers the system security environment, including the enterprise information security policy and the enterprise security architecture. The analysis should address all requirements for confidentiality, integrity, and availability of information, and should include a review of all legal, functional, and other security requirements contained in applicable laws, regulations, and guidance.
At the initiation step you would NOT have enough detailed yet to produce the Security Requirements. You are mostly brainstorming on all of the issues listed but you do not develop them all at that stage.
By considering security early in the information system development life cycle (SDLC), you may be able to avoid higher costs later on and develop a more secure system from the start.

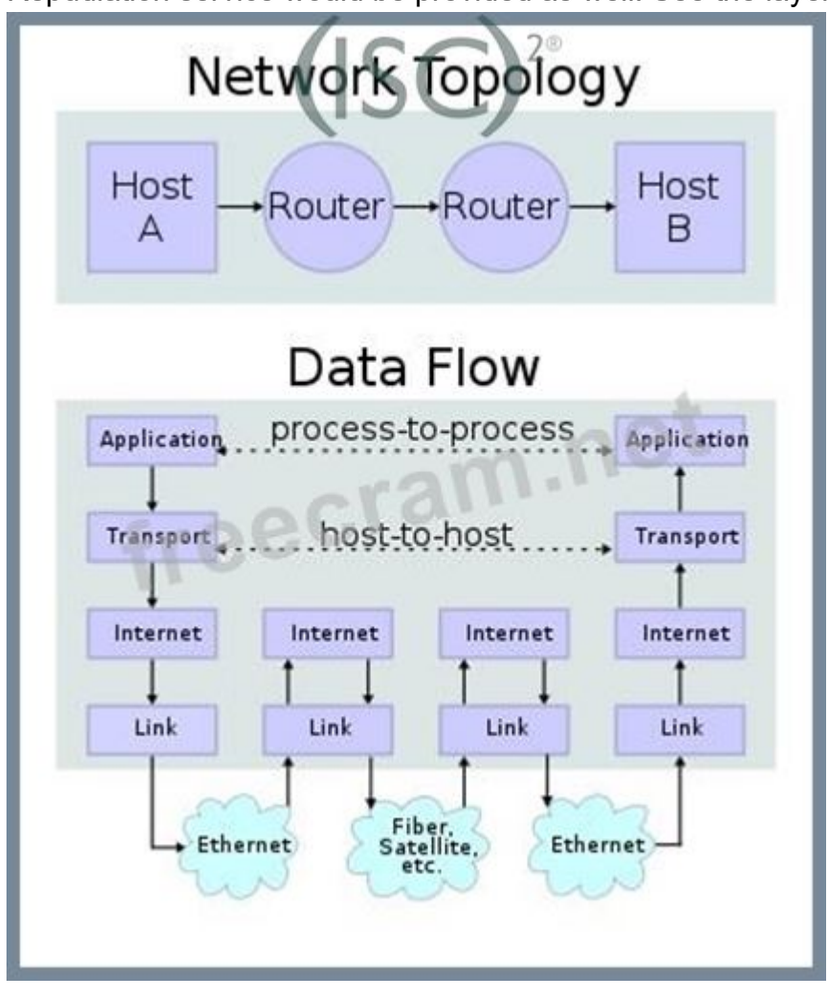
NIST says: NIST`s Information Technology Laboratory recently issued Special Publication (SP) 80064, Security Considerations in the Information System Development Life Cycle, by Tim Grance, Joan Hash, and Marc Stevens, to help organizations include security requirements in their planning for every phase of the system life cycle, and to select, acquire, and use appropriate and cost-effective security controls.
I must admit this is all very tricky but reading skills and paying attention to KEY WORDS is a must for this exam.
References:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, Fifth Edition, Page 956 and NIST S-64 Revision 2 at http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64Revision2.pdf and http://www.mks.com/resources/resource-pages/software-development-life-cycle-sdlcsystem-development

NEW QUESTION: 287
A _____ is an information path that is not normally used for communication within a computer system. It is not protected by the any of the systems security mechanisms.
A. Trojaned program
B. Backdoor
C. Covert channel
D. Hijacked session
E. Back-path
Answer: (SHOW ANSWER)
Covert channels can be used as a secret way to convey information to another person or program or for other illicit means.

NEW QUESTION: 288
What does the simple security (ss) property mean in the Bell-LaPadula model?
A. No read up
B. No write down
C. No read down
D. No write up
Answer: (SHOW ANSWER)
Explanation/Reference:

The ss (simple security) property of the Bell-LaPadula access control model states that reading of information by a subject at a lower sensitivity level from an object at a higher sensitivity level is not permitted (no read up).
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 202).

NEW QUESTION: 289
Which of the following DoD Model layer provides non-repudiation services?
A. network layer.
B. application layer.
C. transport layer.
D. data link layer.
Answer: (SHOW ANSWER)
Explanation/Reference:
The Application Layer determines the identity of the communication partners and this is where Non-Repudiation service would be provided as well. See the layers below:



DOD Model DoD Model
The following answers are incorrect:
network layer. Is incorrect because the Network Layer mostly has routing protocols, ICMP, IP, and IPSEC.

It it not a layer in the DoD Model. It is called the Internet Layer within the DoD model.
transport layer. Is incorrect because the Transport layer provides transparent transfer of data between end users. This is called Host-to-Host on the DoD model but sometimes some books will call it Transport as well on the DoD model.
data link layer. Is incorrect because the Data Link Layer defines the protocols that computers must follow to access the network for transmitting and receiving messages. It is part of the OSI Model. This does not exist on the DoD model, it is called the Link Layer on the DoD model.

NEW QUESTION: 290
All hosts on an IP network have a logical ID called a(n):
A. IP address.
B. MAC address.
C. TCP address.
D. Datagram address.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
All hosts on a network have a logical ID that is called an IP address. An IP address is a numeric identifier that is assigned to each machine on an IP network. It designates the location of a device on a network. A MAC address is typically called a hardware address because it is "burned" into the NIC card. TCP address and Datagram address are imposter answers.
Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

NEW QUESTION: 291
Which of the following would NOT violate the Due Diligence concept?
A. Security policy being outdated
B. Data owners not laying out the foundation of data protection
C. Network administrator not taking mandatory two-week vacation as planned
D. Latest security patches for servers being installed as per the Patch Management process
Answer: (SHOW ANSWER)
To be effective a patch management program must be in place (due diligence) and detailed procedures would specify how and when the patches are applied properly (Due Care). Remember, the question asked for NOT a violation of Due Diligence, in this case, applying patches demonstrates due care and the patch management process in place demonstrates due diligence.
Due diligence is the act of investigating and understanding the risks the company faces. A company practices by developing and implementing security policies, procedures, and standards. Detecting risks would be based on standards such as ISO 2700, Best Practices, and other published standards such as NIST standards for example.
Due Diligence is understanding the current threats and risks. Due diligence is practiced by activities that make sure that the protection mechanisms are continually maintained and operational where risks are

constantly being evaluated and reviewed. The security policy being outdated would be an example of violating the due diligence concept.
Due Care is implementing countermeasures to provide protection from those threats. Due care is when the necessary steps to help protect the company and its resources from possible risks that have been identifed. If the information owner does not lay out the foundation of data protection (doing something about it) and ensure that the directives are being enforced (actually being done and kept at an acceptable level), this would violate the due care concept.
If a company does not practice due care and due diligence pertaining to the security of its assets, it can be legally charged with negligence and held accountable for any ramifications of that negligence. Liability is usually established based on Due Diligence and Due Care or the lack of either.
A good way to remember this is using the first letter of both words within Due Diligence (DD) and Due Care (DC).
Due Diligence = Due Detect
Steps you take to identify risks based on best practices and standards.
Due Care = Due Correct.
Action you take to bring the risk level down to an acceptable level and maintaining that level over time.
The Following answer were wrong:
Security policy being outdated:
While having and enforcing a security policy is the right thing to do (due care), if it is outdated, you are not doing it the right way (due diligence). This questions violates due diligence and not due care.
Data owners not laying out the foundation for data protection:
Data owners are not recognizing the "right thing" to do. They don't have a security policy.
Network administrator not taking mandatory two week vacation:
The two week vacation is the "right thing" to do, but not taking the vacation violates due diligence (not doing the right thing the right way)
Reference(s) used for this question
Shon Harris, CISSP All In One, Version 5, Chapter 3, pg 110

NEW QUESTION: 292
The IP header contains a protocol field. If this field contains the value of 2, what type of data is contained within the IP datagram?
A. TCP.
B. ICMP.
C. UDP.
D. IGMP.
Answer: D (LEAVE A REPLY)
Explanation/Reference:

If the protocol field has a value of 2 then it would indicate it was IGMP.
The following answers are incorrect:
TCP. Is incorrect because the value for a TCP protocol would be 6.
UDP. Is incorrect because the value for an UDP protocol would be 17.
ICMP. Is incorrect because the value for an ICMP protocol would be 1.

NEW QUESTION: 293
A trusted system does NOT involve which of the following?
A. Enforcement of a security policy.
B. Sufficiency and effectiveness of mechanisms to be able to enforce a security policy.
C. Assurance that the security policy can be enforced in an efficient and reliable manner.
D. Independently-verifiable evidence that the security policy-enforcing mechanisms are sufficient and effective.
Answer: (SHOW ANSWER)
A trusted system is one that meets its intended security requirements. It involves sufficiency and effectiveness, not necessarily efficiency, in enforcing a security policy. Put succinctly, trusted systems have (1) policy, (2) mechanism, and (3) assurance. Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

NEW QUESTION: 294
Which must bear the primary responsibility for determining the level of protection needed for information systems resources?
A. IS security specialists
B. Senior Management
C. Senior security analysts
D. systems Auditors
Answer: (SHOW ANSWER)
If there is no support by senior management to implement, execute, and enforce security policies and procedure, then they won't work. Senior management must be involved in this because they have an obligation to the organization to protect the assests . The requirement here is for management to show "due diligence" in establishing an effective compliance, or security program. It is senior management that could face legal repercussions if they do not have sufficient controls in place.
The following answers are incorrect:
IS security specialists. Is incorrect because it is not the best answer. Senior management bears the primary responsibility for determining the level of protection needed.
Senior security analysts. Is incorrect because it is not the best answer. Senior management bears the primary responsibility for determining the level of protection needed.
systems auditors. Is incorrect because it is not the best answer, system auditors are responsible that the controls in place are effective. Senior management bears the primary responsibility for determining the level of protection needed.

NEW QUESTION: 295
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: (SHOW ANSWER)
Absolute/Direct
+------+-----+-----------------------------------+ | 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: 296
Smart cards are a secure alternative to which weak security mechanism?
A. Passwords
B. Public Key Encryption
C. Tokens
D. Biometrics
Answer: (SHOW ANSWER)

NEW QUESTION: 297
What is the main characteristic of a multi-homed host?
A. It is placed between two routers or firewalls.
B. It allows IP routing.
C. It has multiple network interfaces, each connected to separate networks.
D. It operates at multiple layers.
Answer: (SHOW ANSWER)

Explanation/Reference:
The main characteristic of a multi-homed host is that is has multiple network interfaces, each connected to logically and physically separate networks. IP routing should be disabled to prevent the firewall from routing packets directly from one interface to the other.
Source: FERREL, Robert G, Questions and Answers for the CISSP Exam, domain 2 (derived from the Information Security Management Handbook, 4th Ed., by Tipton & Krause).

NEW QUESTION: 298
Contracts and agreements are often times unenforceable or hard to enforce in which of the following alternate facility recovery agreement?
A. hot site
B. warm site
C. cold site
D. reciprocal agreement
Answer: (SHOW ANSWER)
A reciprocal agreement is where two or more organizations mutually agree to provide facilities to the other if a disaster occurs. The organizations must have similiar hardware and software configurations. Reciprocal agreements are often not legally binding. Reciprocal agreements are not contracts and cannot be enforced. You cannot force someone you have such an agreement with to provide processing to you.
Government regulators do not accept reciprocal agreements as valid disaster recovery sites.
Cold sites are empty computer rooms consisting only of environmental systems, such as air conditioning and raised floors, etc. They do not meet the requirements of most regulators and boards of directors that the disaster plan be tested at least annually.
Time Brokers promise to deliver processing time on other systems. They charge a fee, but cannot guaranty that processing will always be available, especially in areas that experienced multiple disasters.
With the exception of providing your own hot site, commercial hot sites provide the greatest protection. Most will allow you up to six weeks to restore your sites if you declare a disaster. They also permit an annual amount of time to test the Disaster Plan.
References:
OIG CBK Business Continuity and Disaster Recovery Planning (pages 368 - 369)
The following answers are incorrect:
hot site. Is incorrect because you have a contract in place stating what services are to be provided.
warm site. Is incorrect because you have a contract in place stating what services are to be provided.
cold site. Is incorrect because you have a contract in place stating what services are to be provided.

NEW QUESTION: 299
Which of the following rules appearing in an Internet firewall policy is inappropriate?
A. Source routing shall be disabled on all firewalls and external routers.
B. Firewalls shall be configured to transparently allow all outbound and inbound services.
C. Firewalls should fail to a configuration that denies all services, and require a firewall administrator to re-enable services after a firewall has failed.
D. Firewalls shall not accept traffic on its external interfaces that appear to be coming from internal network addresses.
Answer: (SHOW ANSWER)
Unless approved by the Network Services manager, all in-bound services shall be intercepted and processed by the firewall. Allowing unrestricted services inbound and outbound is certainly NOT recommended and very dangerous.
Pay close attention to the keyword: all
All of the other choices presented are recommended practices for a firewall policy.
Reference(s) used for this question:
GUTTMAN, Barbara & BAGWILL, Robert, NIST Special Publication 800-xx, Internet Security Policy: A Technical Guide, Draft Version, May 25, 2000 (page 78).

NEW QUESTION: 300
Which of the following is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism?

A. OAKLEY
B. Internet Security Association and Key Management Protocol (ISAKMP)
C. Simple Key-management for Internet Protocols (SKIP)
D. IPsec Key exchange (IKE)
Answer: (SHOW ANSWER)
Explanation/Reference:
RFC 2828 (Internet Security Glossary) defines the Internet Security Association and Key Management Protocol (ISAKMP) as an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism.
Let's clear up some confusion here first. Internet Key Exchange (IKE) is a hybrid protocol, it consists of 3 "protocols"
ISAKMP: It's not a key exchange protocol per se, it's a framework on which key exchange protocols operate. ISAKMP is part of IKE. IKE establishs the shared security policy and authenticated keys. ISAKMP is the protocol that specifies the mechanics of the key exchange.
Oakley: Describes the "modes" of key exchange (e.g. perfect forward secrecy for keys, identity protection, and authentication). Oakley describes a series of key exchanges and services.

SKEME: Provides support for public-key-based key exchange, key distribution centres, and manual installation, it also outlines methods of secure and fast key refreshment.
So yes, IPSec does use IKE, but ISAKMP is part of IKE.
The questions did not ask for the actual key negotiation being done but only for the "exchange of key generation and authentication data" being done. Under Oakly it would be Diffie Hellman (DH) that would be used for the actual key nogotiation.
The following are incorrect answers:
Simple Key-management for Internet Protocols (SKIP) is a key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.
OAKLEY is a key establishment protocol (proposed for IPsec but superseded by IKE) based on the Diffie- Hellman algorithm and designed to be a compatible component of ISAKMP.
IPsec Key Exchange (IKE) is an Internet, IPsec, key-establishment protocol [R2409] (partly based on OAKLEY) that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations, such as in AH and ESP.
Reference used for this question:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 301
_____ attacks capitalize on programming errors and can allow the originator to gain additional privileges on a machine.
A. SYN Flood
B. Distributed Denial of Service
C. Buffer Overflow
D. Coordinated
E. Denial of Service
Answer: (SHOW ANSWER)

NEW QUESTION: 302
Which of the following services relies on UDP?
A. FTP
B. Telnet
C. DNS

D. SMTP

Answer: (SHOW ANSWER)

Section: Network and Telecommunications

Explanation/Reference:

DNS relies on connectionless UDP whereas services like FTP, Telnet and SMTP rely on TCP.

Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 2, August 1999.

NEW QUESTION: 303

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: (SHOW ANSWER)

Explanation/Reference:

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: 304

Recovery Site Strategies for the technology environment depend on how much downtime an organization can tolerate before the recovery must be completed. What would you call a strategy where the alternate site is internal, standby ready, with all the technology and equipment necessary to run the applications?

A. External Hot site

B. Warm Site

C. Internal Hot Site

D. Dual Data Center

Answer: (SHOW ANSWER)

Explanation/Reference:
Internal Hot Site-This site is standby ready with all the technology and equipment necessary to run the applications positioned there. The planner will be able to effectively restart an application in a hot site recovery without having to perform any bare metal recovery of servers. If this is an internal solution, then often the organization will run non-time sensitive processes there such as development or test environments, which will be pushed aside for recovery of production when needed. When employing this strategy, it is important that the two environments be kept as close to identical as possible to avoid problems with O/S levels, hardware differences, capacity differences, etc., from preventing or delaying recovery.
Recovery Site Strategies Depending on how much downtime an organization has before the technology recovery must be complete, recovery strategies selected for the technology environment could be any one of the following:
Dual Data Center-This strategy is employed for applications, which cannot accept any downtime without negatively impacting the organization. The applications are split between two geographically dispersed data centers and either load balanced between the two centers or hot swapped between the two centers. The surviving data center must have enough head room to carry the full production load in either case.
External Hot Site-This strategy has equipment on the floor waiting, but the environment must be rebuilt for the recovery. These are services contracted through a recovery service provider. Again, it is important that the two environments be kept as close to identical as possible to avoid problems with O/S levels, hardware differences, capacity differences, etc., from preventing or delaying recovery. Hot site vendors tend to have the most commonly used hardware and software products to attract the largest number of customers to utilize the site. Unique equipment or software would generally need to be provided by the organization either at time of disaster or stored there ahead of time.
Warm Site-A leased or rented facility that is usually partially configured with some equipment, but not the actual computers. It will generally have all the cooling, cabling, and networks in place to accommodate the recovery but the actual servers, mainframe, etc., equipment are delivered to the site at time of disaster.
Cold Site-A cold site is a shell or empty data center space with no technology on the floor. All technology must be purchased or acquired at the time of disaster.
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 21265-21291). Auerbach Publications. Kindle Edition.

NEW QUESTION: 305
Which access model is most appropriate for companies with a high employee turnover?
A. Role-based access control
B. Mandatory access control
C. Lattice-based access control
D. Discretionary access control
Answer: (SHOW ANSWER)
Explanation/Reference:

The underlying problem for a company with a lot of turnover is assuring that new employees are assigned the correct access permissions and that those permissions are removed when they leave the company.
Selecting the best answer requires one to think about the access control options in the context of a company with a lot of flux in the employee population. RBAC simplifies the task of assigning permissions because the permissions are assigned to roles which do not change based on who belongs to them. As employees join the company, it is simply a matter of assigning them to the appropriate roles and their permissions derive from their assigned role. They will implicitely inherit the permissions of the role or roles they have been assigned to. When they leave the company or change jobs, their role assignment is revoked/changed appropriately.
Mandatory access control is incorrect. While controlling access based on the clearence level of employees and the sensitivity of obects is a better choice than some of the other incorrect answers, it is not the best choice when RBAC is an option and you are looking for the best solution for a high number of employees constantly leaving or joining the company.
Lattice-based access control is incorrect. The lattice is really a mathematical concept that is used in formally modeling information flow (Bell-Lapadula, Biba, etc). In the context of the question, an abstract model of information flow is not an appropriate choice. CBK, pp. 324-325.
Discretionary access control is incorrect. When an employee joins or leaves the company, the object owner must grant or revoke access for that employee on all the objects they own. Problems would also arise when the owner of an object leaves the company. The complexity of assuring that the permissions are added and removed correctly makes this the least desirable solution in this situation.
References
Alll in One, third edition page 165
RBAC is discussed on pp. 189 through 191 of the ISC(2) guide.

NEW QUESTION: 306
Which of the following are NOT a countermeasure to traffic analysis?
A. Padding messages.
B. Eavesdropping.
C. Sending noise.
D. Faraday Cage
Answer: (SHOW ANSWER)
Explanation/Reference:
Eavesdropping is not a countermeasure, it is a type of attack where you are collecting traffic and attempting to see what is being send between entities communicating with each other.
The following answers are incorrect:
Padding Messages. Is incorrect because it is considered a countermeasure you make messages uniform size, 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 patterns.
Sending Noise. Is incorrect because it is considered a countermeasure, tansmitting non-informational data elements to disguise real data.

Faraday Cage Is incorrect because it is a tool used to prevent emanation of electromagnetic waves. It is a very effective tool to prevent traffic analysis.

NEW QUESTION: 307
Transport Layer Security (TLS) is a two-layered socket layer security protocol that contains the TLS Record Protocol and the::
A. Transport Layer Security (TLS) Internet Protocol.
B. Transport Layer Security (TLS) Data Protocol.
C. Transport Layer Security (TLS) Link Protocol.
D. Transport Layer Security (TLS) Handshake Protocol.
Answer: (SHOW ANSWER)
Section: Network and Telecommunications

NEW QUESTION: 308
What security control provides a method to insure that a transaction did or did not occur?
A. Identification
B. Accountability
C. Nonrepudiation
D. Verification
E. Access control
Answer: (SHOW ANSWER)
Nonrepudiation serves to validate whether or not a claimed event or action occurred in order to resolve disputes about the validity of the event. Nonrepudiation is vital in electronic commerce because it protects both the seller and the consumer from fraudulent behavior by the other party.

NEW QUESTION: 309
The concept of best effort delivery is best associated with?
A. TCP
B. HTTP
C. RSVP
D. IP
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
The Internet Protocol (IP) is a data-oriented protocol used for communicating data across a packet-switched internetwork. IP provides an unreliable service (i.e., best effort delivery). This means that the network makes no guarantees about the packet.
Low-level connectionless protocols such as DDP (under Appletalk) and IP usually provide best-effort delivery of data.

Best-effort delivery means that the protocol attempts to deliver any packets that meet certain requirements, such as containing a valid destination address, but the protocol does not inform the sender when it is unable to deliver the data, nor does it attempt to recover from error conditions and data loss. Higher-level protocols such as TCP on the other hand, can provide reliable delivery of data. Reliable delivery includes error checking and recovery from error or loss of data.
HTTP is the HyperText Transport Protocol used to establish connections to a web server and thus one of the higher level protocol using TCP to ensure delivery of all bytes between the client and the server. It was not a good choice according to the question presented.
Here is another definition from the TCP/IP guide at: http://www.tcpipguide.com/free/t_IPOverviewandKeyOperationalCharacteristics.htm Delivered Unreliably: IP is said to be an "unreliable protocol". That doesn't mean that one day your IP software will decide to go fishing rather than run your network. J It does mean that when datagrams are sent from device A to device B, device A just sends each one and then moves on to the next. IP doesn't keep track of the ones it sent. It does not provide reliability or service quality capabilities such as error protection for the data it sends (though it does on the IP header), flow control or retransmission of lost datagrams.
For this reason, IP is sometimes called a best-effort protocol. It does what it can to get data to where it needs to go, but "makes no guarantees" that the data will actually get there.

NEW QUESTION: 310
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: (SHOW ANSWER)
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: 311
Which division of the Orange Book deals with discretionary protection (need-to-know)?
A. D
B. C
C. B
D. A

Answer: (SHOW ANSWER)

Section: Access Control

Explanation/Reference:

C deals with discretionary protection. See matric below:

TNI/TCSEC MATRIX

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

TCSEC Matric

The following are incorrect answers:

D is incorrect. D deals with minimal security.

B is incorrect. B deals with mandatory protection.

A is incorrect. A deals with verified protection.

Reference(s) used for this question:

CBK, p. 329 - 330

and

Shon Harris, CISSP All In One (AIO), 6th Edition , page 392-393

NEW QUESTION: 312
In the CIA triad, what does the letter A stand for?
A. Auditability
B. Accountability
C. Availability
D. Authentication
Answer: (SHOW ANSWER)
The CIA triad stands for Confidentiality, Integrity and Availability.

NEW QUESTION: 313
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: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation
Explanation/Reference:
Controls are implemented to mitigate risk and reduce the potential for loss. Preventive controls are put in place to inhibit harmful occurrences; detective controls are established to discover harmful occurrences; corrective controls are used to restore systems that are victims of harmful attacks.
It is not feasible and possible to eliminate all risks and the potential for loss as risk/threats are constantly changing.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 32.

NEW QUESTION: 314
How do you distinguish between a bridge and a router?
A. A bridge simply connects multiple networks, a router examines each packet to determine which network to forward it to.
B. "Bridge" and "router" are synonyms for equipment used to join two networks.
C. The bridge is a specific type of router used to connect a LAN to the global Internet.
D. The bridge connects multiple networks at the data link layer, while router connects multiple networks at the network layer.
Answer: (SHOW ANSWER)
A bridge operates at the Data Link Layer and a router operates at the Network Layer.
The following answers are incorrect:
A bridge simply connects multiple networks, a router examines each packet to determine which network to forward it to. Is incorrect because both forward packets this is not distinctive enough.

"Bridge" and "router" are synonyms for equipment used to join two networks. Is incorrect because the two are unique and operate at different layers of the OSI model.
The bridge is a specific type of router used to connect a LAN to the global Internet. Is incorrect because a bridge does not connect a LAN to the global internet, but connects networks together creating a LAN.

NEW QUESTION: 315
Digital Certificates use which protocol?
A. X.400
B. X.500
C. X.525
D. X.511
E. X.509
F. None of the above
Answer: (SHOW ANSWER)

NEW QUESTION: 316
What mechanism automatically causes an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters?
A. Central station alarm
B. Proprietary alarm
C. A remote station alarm
D. An auxiliary station alarm
Answer: (SHOW ANSWER)
Auxiliary station alarms automatically cause an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters. They are usually Municipal Fire Alarm Boxes are installed at your business or building, they are wired directly into the fire station.
Central station alarms are operated by private security organizations. It is very similar to a proprietary alarm system (see below). However, the biggest difference is the monitoring and receiving of alarm is done off site at a central location manned by non staff members. It is a third party.
Proprietary alarms are similar to central stations alarms except that monitoring is performed directly on the protected property. This type of alarm is usually use to protect large industrials or commercial buildings. Each of the buildings in the same vincinity has their own alarm system, they are all wired together at a central location within one of the building acting as a common receiving point. This point is usually far away from the other building so it is not under the same danger. It is usually man 24 hours a day by a trained team who knows how to react under different conditions.
A remote station alarm is a direct connection between the signal-initiating device at the protected property and the signal-receiving device located at a remote station, such as the fire station or usually a monitoring service. This is the most popular type of implementation and the owner of the premise must

pay a monthly monitoring fee. This is what most people use in their home where they get a company like ADT to receive the alarms on their behalf.
A remote system differs from an auxiliary system in that it does not use the municipal fire of police alarm circuits.
Reference(s) used for this question:
ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 11: Physical Security (page 211). and Great presentation J.T.A. Stone on SlideShare

NEW QUESTION: 317
What mechanism does a system use to compare the security labels of a subject and an object?
A. Validation Module.
B. Reference Monitor.
C. Clearance Check.
D. Security Module.
Answer: (SHOW ANSWER)
Because the Reference Monitor is responsible for access control to the objects by the subjects it compares the security labels of a subject and an object.
According to the OIG: The reference monitor is an access control concept referring to an abstract machine that mediates all accesses to objects by subjects based on information in an access control database. The reference monitor must mediate all access, be protected from modification, be verifiable as correct, and must always be invoked. The reference monitor, in accordance with the security policy, controls the checks that are made in the access control database.
The following are incorrect:
Validation Module. A Validation Module is typically found in application source code and is used to validate data being inputted.
Clearance Check. Is a distractor, there is no such thing other than what someone would do when checking if someone is authorized to access a secure facility.
Security Module. Is typically a general purpose module that prerforms a variety of security related functions.
References:
OIG CBK, Security Architecture and Design (page 324)

AIO, 4th Edition, Security Architecture and Design, pp 328-328.
Wikipedia - http://en.wikipedia.org/wiki/Reference_monitor

NEW QUESTION: 318
What is called a sequence of characters that is usually longer than the allotted number for a password?
A. passphrase
B. cognitive phrase
C. anticipated phrase
D. Real phrase
Answer: (SHOW ANSWER)
Explanation/Reference:
A passphrase is a sequence of characters that is usually longer than the allotted number for a password.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, page 37.

NEW QUESTION: 319
Which of the following is not an encryption algorithm?
A. Skipjack
B. SHA-1
C. Twofish
D. DEA
Answer: B (LEAVE A REPLY)
The SHA-1 is a hashing algorithm producing a 160-bit hash result from any data. It does not perform encryption.
In cryptography, SHA-1 is a cryptographic hash function designed by the United States National Security Agency and published by the United States NIST as a U.S. Federal Information Processing Standard. SHA stands for "secure hash algorithm". The four SHA algorithms are structured differently and are distinguished as SHA-0, SHA-1, SHA-2, and SHA-3. SHA-1 is very similar to SHA0, but corrects an error in the original SHA hash specification that led to significant weaknesses. The SHA-0 algorithm was not adopted by many applications. SHA-2 on the other hand significantly differs from the SHA-1 hash function.
SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols.
In 2005, cryptanalysts found attacks on SHA-1 suggesting that the algorithm might not be secure enough for ongoing use. NIST required many applications in federal agencies to move to SHA-2 after 2010 because of the weakness. Although no successful attacks have yet been reported on SHA-2, they are algorithmically similar to SHA-1.
In 2012, following a long-running competition, NIST selected an additional algorithm, Keccak, for standardization as SHA-3
NOTE: A Cryptographic Hash Function is not the same as an Encryption Algorithm even thou both are Algorithms. An algorithm is defined as a step-by-step procedure for calculations. Hashing Algorithm do

not encrypt the data. People sometimes will say they encrypted a password with SHA-1 but really they simply created a Message Digest of the password using SHA-1, putting the input through a series of steps to come out with the message digest or hash value.
A cryptographic hash function is a hash function; that is, an algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that any (accidental or intentional) change to the data will (with very high probability) change the hash value. The data to be encoded are often called the "message," and the hash value is sometimes called the message digest or simply digest.
Encryption Algorithms are reversible but Hashing Algorithms are not meant to be reversible if the input is large enough.
The following are incorrect answers:
The Skipjack algorithm is a Type II block cipher with a block size of 64 bits and a key size of 80 bits that was developed by NSA and formerly classified at the U.S. Department of Defense "Secret" level.
Twofish is a freely available 128-bit block cipher designed by Counterpane Systems (Bruce Schneier et al.).
DEA is a symmetric block cipher, defined as part of the U.S. Government's Data Encryption Standard (DES). DEA uses a 64-bit key, of which 56 bits are independently chosen and 8 are parity bits, and maps a 64-bit block into another 64-bit block.
Reference(s) used for this question:
http://en.wikipedia.org/wiki/SHA-1 and SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000. and Counterpane Labs, at http://www.counterpane.com/twofish.html.

NEW QUESTION: 320

Which of the following is commonly used for retrofitting multilevel security to a database management system?

A. trusted front-end.
B. trusted back-end.
C. controller.
D. kernel.
Answer: (SHOW ANSWER)
Explanation/Reference:
If you are "retrofitting" that means you are adding to an existing database management system (DBMS). You could go back and redesign the entire DBMS but the cost of that could be expensive and there is no telling what the effect will be on existing applications, but that is redesigning and the question states retrofitting. The most cost effective way with the least effect on existing applications while adding a layer of security on top is through a trusted front-end.
Clark-Wilson is a synonym of that model as well. It was used to add more granular control or control to database that did not provide appropriate controls or no controls at all. It is one of the most popular model today. Any dynamic website with a back-end database is an example of this today.
Such a model would also introduce separation of duties by allowing the subject only specific rights on the objects they need to access.
The following answers are incorrect:

trusted back-end. Is incorrect because a trusted back-end would be the database management system (DBMS). Since the question stated "retrofitting" that eliminates this answer.
controller. Is incorrect because this is a distractor and has nothing to do with "retrofitting".
kernel. Is incorrect because this is a distractor and has nothing to do with "retrofitting". A security kernel would provide protection to devices and processes but would be inefficient in protecting rows or columns in a table.

NEW QUESTION: 321
Which of the following statements pertaining to key management is incorrect?
A. The more a key is used, the shorter its lifetime should be.
B. When not using the full keyspace, the key should be extremely random.
C. Keys should be backed up or escrowed in case of emergencies.
D. A key's lifetime should correspond with the sensitivity of the data it is protecting.
Answer: (SHOW ANSWER)
A key should always be using the full spectrum of the keyspace and be extremely random. Other statements are correct.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 6).

NEW QUESTION: 322
Which of the following forms of authentication would most likely apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier?
A. Dynamic authentication
B. Continuous authentication
C. Encrypted authentication
D. Robust authentication
Answer: (SHOW ANSWER)
Explanation/Reference:
Continuous authentication is a type of authentication that provides protection against impostors who can see, alter, and insert information passed between the claimant and verifier even after the claimant/verifier authentication is complete. These are typically referred to as active attacks, since they assume that the imposter can actively influence the connection between claimant and verifier. One way to provide this form of authentication is to apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier. There are other combinations of cryptography that can provide this form of authentication but current strategies rely on applying some type of cryptography to every bit of data sent. Otherwise, any unprotected bit would be suspect. Robust authentication relies on dynamic authentication data that changes with each authenticated session between a claimant and a verifier, but does not provide protection against active attacks. Encrypted authentication is a distracter.
Source: GUTTMAN, Barbara & BAGWILL, Robert, NIST Special Publication 800-xx, Internet Security Policy: A Technical Guide, Draft Version, May 25, 2000 (page 34).

NEW QUESTION: 323
CORRECT TEXT
When an employee leaves the company, their network access account should be _____?
Answer:

NEW QUESTION: 324
Within the legal domain what rule is concerned with the legality of how the evidence was gathered ?
A. Exclusionary rule
B. Best evidence rule
C. Hearsay rule
D. Investigation rule
Answer: (SHOW ANSWER)
Explanation/Reference:
The exclusionary rule mentions that evidence must be gathered legally or it can't be used.
The principle based on federal Constitutional Law that evidence illegally seized by law enforcement officers in violation of a suspect's right to be free from unreasonable searches and seizures cannot be used against the suspect in a criminal prosecution.
The exclusionary rule is designed to exclude evidence obtained in violation of a criminal defendant's Fourth Amendment rights. The Fourth Amendment protects against unreasonable searches and seizures by law enforcement personnel. If the search of a criminal suspect is unreasonable, the evidence obtained in the search will be excluded from trial.
The exclusionary rule is a court-made rule. This means that it was created not in statutes passed by legislative bodies but rather by the U.S. Supreme Court. The exclusionary rule applies in federal courts by virtue of the Fourth Amendment. The Court has ruled that it applies in state courts although the due process clause of the Fourteenth Amendment.(The Bill of Rights-the first ten amendments- applies to actions by the federal government. The Fourteenth Amendment, the Court has held, makes most of the protections in the Bill of Rights applicable to actions by the states.) The exclusionary rule has been in existence since the early 1900s. Before the rule was fashioned, any evidence was admissible in a criminal trial if the judge found the evidence to be relevant. The manner in which the evidence had been seized was not an issue. This began to change in 1914, when the U.S.
Supreme Court devised a way to enforce the Fourth Amendment. In Weeks v. United States, 232 U.S. 383, 34 S. Ct. 341, 58 L. Ed. 652 (1914), a federal agent had conducted a warrantless search for evidence of gambling at the home of Fremont Weeks. The evidence seized in the search was used at trial, and Weeks was convicted. On appeal, the Court held that the Fourth Amendment barred the use of evidence secured through a warrantless search. Weeks's conviction was reversed, and thus was born the exclusionary rule.
The best evidence rule concerns limiting potential for alteration. The best evidence rule is a common law rule of evidence which can be traced back at least as far as the 18th century. In Omychund v Barker (1745) 1 Atk, 21, 49; 26 ER 15, 33, Lord Harwicke stated that no evidence was admissible unless it was

"the best that the nature of the case will allow". The general rule is that secondary evidence, such as a copy or facsimile, will be not admissible if an original document exists, and is not unavailable due to destruction or other circumstances indicating unavailability.
The rationale for the best evidence rule can be understood from the context in which it arose: in the eighteenth century a copy was usually made by hand by a clerk (or even a litigant). The best evidence rule was predicated on the assumption that, if the original was not produced, there was a significant chance of error or fraud in relying on such a copy.
The hearsay rule concerns computer-generated evidence, which is considered second-hand evidence. Hearsay is information gathered by one person from another concerning some event, condition, or thing of which the first person had no direct experience. When submitted as evidence, such statements are called hearsay evidence. As a legal term, "hearsay" can also have the narrower meaning of the use of such information as evidence to prove the truth of what is asserted. Such use of "hearsay evidence" in court is generally not allowed. This prohibition is called the hearsay rule.
For example, a witness says "Susan told me Tom was in town". Since the witness did not see Tom in town, the statement would be hearsay evidence to the fact that Tom was in town, and not admissible. However, it would be admissible as evidence that Susan said Tom was in town, and on the issue of her knowledge of whether he was in town.
Hearsay evidence has many exception rules. For the purpose of the exam you must be familiar with the business records exception rule to the Hearsay Evidence. The business records created during the ordinary course of business are considered reliable and can usually be brought in under this exception if the proper foundation is laid when the records are introduced into evidence. Depending on which jurisdiction the case is in, either the records custodian or someone with knowledge of the records must lay a foundation for the records. Logs that are collected as part of a document business process being carried at regular interval would fall under this exception. They could be presented in court and not be considered Hearsay.
Investigation rule is a detractor.
Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 9.
and
The FREE Online Law Dictionary at: http://legal-dictionary.thefreedictionary.com/Exclusionary+Rule and Wikipedia has a nice article on this subject at: http://en.wikipedia.org/wiki/Exclusionary_rule and http://en.wikipedia.org/wiki/Hearsay_in_United_States_law#Hearsay_exceptions

NEW QUESTION: 325
A server cluster looks like a:
A. single server from the user's point of view
B. dual server from the user's point of view
C. triple server from the user's point of view
D. quardle server from the user's point of view
Answer: A (LEAVE A REPLY)
Explanation/Reference:
The cluster looks like a single server from the user's point of view.

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: 326
Which of the following protocols suite does the Internet use?
A. IP/UDP/TCP
B. IP/UDP/ICMP/TCP
C. TCP/IP
D. IMAP/SMTP/POP3
Answer: (SHOW ANSWER)
Explanation/Reference:
Transmission Control Protocol/Internet Protocol (TCP/IP) is the common name for the suite of protocols that was developed by the Department of Defense (DoD) in the 1970's to support the construction of the internet. The Internet is based on TCP/IP.
The Internet protocol suite is the networking model and a set of communications protocols used for the Internet and similar networks. It is commonly known as TCP/IP, because its most important protocols, the Transmission Control Protocol (TCP) and the Internet Protocol (IP), were the first networking protocols defined in this standard. It is occasionally known as the DoD model, because the development of the networking model was funded by DARPA, an agency of the United States Department of Defense.
TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. This functionality has been organized into four abstraction layers within the DoD Model which are used to sort all related protocols according to the scope of networking involved.
From lowest to highest, the layers are:
The link layer, containing communication technologies for a single network segment (link), The internet layer, connecting independent networks, thus establishing internetworking, The transport layer handling process-to-process communication,
The application layer, which interfaces to the user and provides support services.
The TCP/IP model and related protocols are maintained by the Internet Engineering Task Force (IETF).
The following answers are incorrect:
IP/UDP/TCP. This is incorrect, all three are popular protocol and they are not considered a suite of protocols.
IP/UDP/ICMP/TCP. This is incorrect, all 4 are some of the MOST commonly used protocol but they are not called a suite of protocol.
IMAP/SMTP/POP3 . This is incorrect because they are all email protocol and consist of only a few of the protocol that would be included in the TCP/IP suite of protocol.
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 5267-5268). Auerbach Publications. Kindle Edition.
http://en.wikipedia.org/wiki/Internet_protocol_suite

NEW QUESTION: 327
Because all the secret keys are held and authentication is performed on the Kerberos TGS and the authentication servers, these servers are vulnerable to:
A. neither physical attacks nor attacks from malicious code.
B. physical attacks only
C. both physical attacks and attacks from malicious code.
D. physical attacks but not attacks from malicious code.
Answer: (SHOW ANSWER)
Since all the secret keys are held and authentication is performed on the Kerberos TGS and the authentication servers, these servers are vulnerable to both physical attacks and attacks from malicious code.
Because a client's password is used in the initiation of the Kerberos request for the service protocol, password guessing can be used to impersonate a client.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 42.

NEW QUESTION: 328
Cryptography does not concern itself with which of the following choices?
A. Availability
B. Integrity
C. Confidentiality
D. Validation
Answer: (SHOW ANSWER)
The cryptography domain addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality, and authenticity. Unlike the other domains, cryptography does not completely support the standard of availability.
Availability Cryptography supports all three of the core principles of information security. Many access control systems use cryptography to limit access to systems through the use of passwords.
Many token-based authentication systems use cryptographic-based hash algorithms to compute one-time passwords. Denying unauthorized access prevents an attacker from entering and damaging the system or network, thereby denying access to authorized users if they damage or currupt the data.
Confidentiality
Cryptography provides confidentiality through altering or hiding a message so that ideally it cannot be understood by anyone except the intended recipient.
Integrity
Cryptographic tools provide integrity checks that allow a recipient to verify that a message has not been altered. Cryptographic tools cannot prevent a message from being altered, but they are effective to detect either intentional or accidental modification of the message.
Additional Features of Cryptographic Systems In addition to the three core principles of information security listed above, cryptographic tools provide several more benefits.

Nonrepudiation

In a trusted environment, the authentication of the origin can be provided through the simple control of the keys. The receiver has a level of assurance that the message was encrypted by the sender, and the sender has trust that the message was not altered once it was received. However, in a more stringent, less trustworthy environment, it may be necessary to provide assurance via a third party of who sent a message and that the message was indeed delivered to the right recipient. This is accomplished through the use of digital signatures and public key encryption. The use of these tools provides a level of nonrepudiation of origin that can be verified by a third party.

Once a message has been received, what is to prevent the recipient from changing the message and contesting that the altered message was the one sent by the sender? The nonrepudiation of delivery prevents a recipient from changing the message and falsely claiming that the message is in its original state. This is also accomplished through the use of public key cryptography and digital signatures and is verifiable by a trusted third party.

Authentication

Authentication is the ability to determine if someone or something is what it declares to be. This is primarily done through the control of the keys, because only those with access to the key are able to encrypt a message. This is not as strong as the nonrepudiation of origin, which will be reviewed shortly Cryptographic functions use several methods to ensure that a message has not been changed or altered. These include hash functions, digital signatures, and message authentication codes (MACs). The main concept is that the recipient is able to detect any change that has been made to a message, whether accidentally or intentionally.

Access Control

Through the use of cryptographic tools, many forms of access control are supported-from log-ins via passwords and passphrases to the prevention of access to confidential files or messages. In all cases, access would only be possible for those individuals that had access to the correct cryptographic keys.

NOTE FROM CLEMENT:

As you have seen this question was very recently updated with the latest content of the Official ISC2 Guide (OIG) to the CISSP CBK, Version 3.

Myself, I agree with most of you that cryptography does not help on the availability side and it is even the contrary sometimes if you loose the key for example. In such case you would loose access to the data and negatively impact availability. But the ISC2 is not about what I think or what you think, they have their own view of the world where they claim and state clearly that cryptography does address availability even thou it does not fully address it. They look at crypto as the ever emcompassing tool it has become today. Where it can be use for authentication purpose for example where it would help to avoid corruption of the data through illegal access by an unauthorized user.

The question is worded this way in purpose, it is VERY specific to the CISSP exam context where ISC2 preaches that cryptography address availability even thou they state it does

not fully address it. This is something new in the last edition of their book and something you must be aware of.
Best regards
Clement
The following terms are from the Software Development Security domain:
Validation: The assurance that a product, service, or system meets the needs of the customer and other identified stakeholders. It often involves acceptance and suitability with external customers. Contrast with verification below."
Verification: The evaluation of whether or not a product, service, or system complies with a regulation, requirement, specification, or imposed condition. It is often an internal process. Contrast with validation."
The terms above are from the Software Development Security Domain.
Reference(s) used for this question:
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Cryptography (Kindle Locations 227-244). . Kindle Edition.
and
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Cryptography (Kindle Locations 206-227). . Kindle Edition.
and
http://en.wikipedia.org/wiki/Verification_and_validation

NEW QUESTION: 329
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: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
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: 330
How would an IP spoofing attack be best classified?
A. Session hijacking attack
B. Passive attack
C. Fragmentation attack
D. Sniffing attack

Answer: (SHOW ANSWER)

Explanation/Reference:

IP spoofing is used to convince a system that it is communicating with a known entity that gives an intruder access. IP spoofing attacks is a common session hijacking attack.

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
77).

NEW QUESTION: 331

Which of the following computer crime is MORE often associated with INSIDERS?

A. IP spoofing

B. Password sniffing

C. Data diddling

D. Denial of service (DOS)

Answer: (SHOW ANSWER)

It refers to the alteration of the existing data , most often seen before it is entered into an application.This type of crime is extremely common and can be prevented by using appropriate access controls and proper segregation of duties. It will more likely be perpetrated by insiders, who have access to data before it is processed.

The other answers are incorrect because :

IP Spoofing is not correct as the questions asks about the crime associated with the insiders. Spoofing is generally accomplished from the outside.

Password sniffing is also not the BEST answer as it requires a lot of technical knowledge in understanding the encryption and decryption process.

Denial of service (DOS) is also incorrect as most Denial of service attacks occur over the internet.

Reference : Shon Harris , AIO v3 , Chapter-10 : Law , Investigation & Ethics , Page : 758
760.

NEW QUESTION: 332

Which of the following statements pertaining to quantitative risk analysis is false?

A. Portion of it can be automated

B. It involves complex calculations
C. It requires a high volume of information
D. It requires little experience to apply
Answer: (SHOW ANSWER)
Explanation/Reference:
Assigning the values for the inputs to a purely quantitative risk assessment requires both a lot of time and significant experience on the part of the assessors. The most experienced employees or representatives from each of the departments would be involved in the process. It is NOT an easy task if you wish to come up with accurate values.
"It can be automated" is incorrect. There are a number of tools on the market that automate the process of conducting a quantitative risk assessment.
"It involves complex calculations" is incorrect. The calculations are simple for basic scenarios but could become fairly complex for large cases. The formulas have to be applied correctly.
"It requires a high volume of information" is incorrect. Large amounts of information are required in order to develop reasonable and defensible values for the inputs to the quantitative risk assessment.
References:
CBK, pp. 60-61
AIO3, p. 73, 78
The Cissp Prep Guide - Mastering The Ten Domains Of Computer Security - 2001, page 24

NEW QUESTION: 333
Which of the following best describes what would be expected at a "hot site"?
A. Computers, climate control, cables and peripherals
B. Computers and peripherals
C. Computers and dedicated climate control systems.
D. Dedicated climate control systems
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
A Hot Site contains everything needed to become operational in the shortest amount of time.
The following answers are incorrect:
Computers and peripherals. Is incorrect because no mention is made of cables. You would not be fully operational without those.
Computers and dedicated climate control systems. Is incorrect because no mention is made of peripherals.
You would not be fully operational without those.
Dedicated climate control systems. Is incorrect because no mentionis made of computers, cables and peripherals. You would not be fully operational without those.
According to the OIG, a hot site is defined as a fully configured site with complete customer required hardware and software provided by the service provider. A hot site in the context of the CBK is always a RENTAL place.

If you have your own site fully equipped that you make use of in case of disaster that would be called a redundant site or an alternate site.
Wikipedia: "A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data." References:
OIG CBK, Business Continuity and Disaster Recovery Planning (pages 367 - 368) AIO, 3rd Edition, Business Continuity Planning (pages 709 - 714) AIO, 4th Edition, Business Continuity Planning , p 790.
Wikipedia - http://en.wikipedia.org/wiki/Hot_site#Hot_Sites

NEW QUESTION: 334
Some Unix systems use a very simple cipher called _____.
A. Block
B. ROT13
C. Stream
D. SOT14
E. DES
Answer: (SHOW ANSWER)

NEW QUESTION: 335
What is called the formal acceptance of the adequacy of a system's overall security by the management?
A. Certification
B. Acceptance
C. Accreditation
D. Evaluation
Answer: (SHOW ANSWER)
Explanation/Reference:
Accreditation is the authorization by management to implement software or systems in a production environment. This authorization may be either provisional or full.
The following are incorrect answers:
Certification is incorrect. Certification is the process of evaluating the security stance of the software or system against a selected set of standards or policies. Certification is the technical evaluation of a product. This may precede accreditation but is not a required precursor.
Acceptance is incorrect. This term is sometimes used as the recognition that a piece of software or system has met a set of functional or service level criteria (the new payroll system has passed its acceptance test).
Certification is the better tem in this context.
Evaluation is incorrect. Evaluation is certainly a part of the certification process but it is not the best answer to the question.
Reference(s) used for this question:
The Official Study Guide to the CBK from ISC2, pages 559-560
AIO3, pp. 314 - 317
AIOv4 Security Architecture and Design (pages 369 - 372)

AIOv5 Security Architecture and Design (pages 370 - 372)

NEW QUESTION: 336
Which of the following is the best reason for the use of an automated risk analysis tool?
A. Much of the data gathered during the review cannot be reused for subsequent analysis.
B. Automated methodologies require minimal training and knowledge of risk analysis.
C. Most software tools have user interfaces that are easy to use and does not require any training.
D. Information gathering would be minimized and expedited due to the amount of information already built into the tool.
Answer: (SHOW ANSWER)
The use of tools simplifies this process. Not only do they usually have a database of assests, threats, and vulnerabilities but they also speed up the entire process.
Using Automated tools for performing a risk assessment can reduce the time it takes to perform them and can simplify the process as well. The better types of these tools include a well-researched threat population and associated statistics. Using one of these tools virtually ensures that no relevant threat is overlooked, and associated risks are accepted as a consequence of the threat being overlooked.
In most situations, the assessor will turn to the use of a variety of automated tools to assist in the vulnerability assessment process. These tools contain extensive databases of specific known vulnerabilities as well as the ability to analyze system and network configuration information to predict where a particular system might be vulnerable to different types of attacks. There are many different types of tools currently available to address a wide variety of vulnerability assessment needs. Some tools will examine a
system from the viewpoint of the network, seeking to determine if a system can be compromised by a remote attacker exploiting available services on a particular host system. These tools will test for open ports listening for connections, known vulnerabilities in common services, and known operating system exploits.
Michael Gregg says:
Automated tools are available that minimize the effort of the manual process. These programs enable users to rerun the analysis with different parameters to answer "what-ifs." They perform calculations quickly and can be used to estimate future expected losses easier than performing the calculations manually.
Shon Harris in her latest book says:
The gathered data can be reused, greatly reducing the time required to perform subsequent analyses. The risk analysis team can also print reports and comprehensive graphs to present 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 Locations 4655-4661). Auerbach Publications. Kindle Edition.
and
CISSP Exam Cram 2 by Michael Gregg

and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 2333-2335). McGraw-Hill. Kindle Edition.
The following answers are incorrect:
Much of the data gathered during the review cannot be reused for subsequent analysis. Is incorrect because the data can be reused for later analysis.
Automated methodologies require minimal training and knowledge of risk analysis. Is incorrect because it is not the best answer. While a minimal amount of training and knowledge is needed, the analysis should still be performed by skilled professionals.
Most software tools have user interfaces that are easy to use and does not require any training. Is incorrect because it is not the best answer. While many of the user interfaces are easy to use it is better if the tool already has information built into it. There is always a training curve when any product is being used for the first time.

NEW QUESTION: 337
Which of the following phases of a system development life-cycle is most concerned with maintaining proper authentication of users and processes to ensure appropriate access control decisions?
A. Development/acquisition
B. Implementation
C. Operation/Maintenance
D. Initiation
Answer: (SHOW ANSWER)
Explanation/Reference:
The operation phase of an IT system is concerned with user authentication.
Authentication is the process where a system establishes the validity of a transmission, message, or a means of verifying the eligibility of an individual, process, or machine to carry out a desired action, thereby ensuring that security is not compromised by an untrusted source.
It is essential that adequate authentication be achieved in order to implement security policies and achieve security goals. Additionally, level of trust is always an issue when dealing with cross-domain interactions.
The solution is to establish an authentication policy and apply it to cross-domain interactions as required.
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 15).

NEW QUESTION: 338
Which of the following packets should NOT be dropped at a firewall protecting an organization's internal network?
A. Inbound packets with Source Routing option set
B. Router information exchange protocols
C. Inbound packets with an internal address as the source IP address

D. Outbound packets with an external destination IP address

Answer: (SHOW ANSWER)

Section: Network and Telecommunications

Explanation/Reference:

Normal outbound traffic has an internal source IP address and an external destination IP address. Traffic with an internal source IP address should only come from an internal interface. Such packets coming from an external interface should be dropped.

Packets with the source-routing option enabled usually indicates a network intrusion attempt.

Router information exchange protocols like RIP and OSPF should be dropped to avoid having internal routing equipment being reconfigured by external agents.

Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 10: The Perfect Firewall.

NEW QUESTION: 339

What is a big difference between Java Applets and Active X controls?

A. Java Applets have access to the full Windows OS

B. Active X controls have access to the full Windows OS

C. Active X controls can run on any platform

D. Java Applets only run in Windows

Answer: (SHOW ANSWER)

NEW QUESTION: 340

Organizations should consider which of the following first before allowing external access to their LANs via the Internet?

A. plan for implementing workstation locking mechanisms.

B. plan for protecting the modem pool.

C. plan for providing the user with his account usage information.

D. plan for considering proper authentication options.

Answer: (SHOW ANSWER)

Before a LAN is connected to the Internet, you need to determine what the access controls mechanisms are to be used, this would include how you are going to authenticate individuals that may access your network externally through access control.

The following answers are incorrect:

plan for implementing workstation locking mechanisms. This is incorrect because locking the workstations have no impact on the LAN or Internet access.

plan for protecting the modem pool. This is incorrect because protecting the modem pool has no impact on the LAN or Internet access, it just protects the modem.

plan for providing the user with his account usage information. This is incorrect because the question asks what should be done first. While important your primary concern should be focused on security.

NEW QUESTION: 341

Which of the following countermeasures would be the most appropriate to prevent possible intrusion or damage from wardialing attacks?
A. Monitoring and auditing for such activity
B. Require user authentication
C. Making sure only necessary phone numbers are made public
D. Using completely different numbers for voice and data accesses
Answer: (SHOW ANSWER)
Explanation/Reference:
Knowlege of modem numbers is a poor access control method as an attacker can discover modem numbers by dialing all numbers in a range. Requiring user authentication before remote access is granted will help in avoiding unauthorized access over a modem line.
"Monitoring and auditing for such activity" is incorrect. While monitoring and auditing can assist in detecting a wardialing attack, they do not defend against a successful wardialing attack.
"Making sure that only necessary phone numbers are made public" is incorrect. Since a wardialing attack blindly calls all numbers in a range, whether certain numbers in the range are public or not is irrelevant.
"Using completely different numbers for voice and data accesses" is incorrect. Using different number ranges for voice and data access might help prevent an attacker from stumbling across the data lines while wardialing the public voice number range but this is not an adequate countermeaure.
References:
CBK, p. 214
AIO3, p. 534-535

NEW QUESTION: 342
Countermeasures have three main objectives, what are they? (Choose all that apply)
A. Prevent
B. Recover
C. Detect
D. Retaliate
E. Trace
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 343
Which backup method copies only files that have changed since the last full backup, but does not clear the archive bit?
A. Differential backup method.
B. Full backup method.
C. Incremental backup method.
D. Tape backup method.
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:

One of the key item to understand regarding backup is the archive bit. The archive bit is used to determine what files have been backuped already. The archive bit is set if a file is modified or a new file is created, this indicates to the backup program that it has to be saved on the next backup. When a full backup is performed the archive bit will be cleared indicating that the files were backup. This allows backup programs to do an incremental or differential backup that only backs up the changes to the filesystem since the last time the bit was cleared Full Backup (or Reference Backup) A Full backup will backup all the files and folders on the drive every time you run the full backup. The archive bit is cleared on all files indicating they were all backuped.

Advantages:

All files from the selected drives and folders are backed up to one backup set.

In the event you need to restore files, they are easily restored from the single backup set.

Disadvantages:

A full backup is more time consuming than other backup options.

Full backups require more disk, tape, or network drive space.

Incremental Backup

An incremental backup provides a backup of files that have changed or are new since the last incremental backup.

For the first incremental backup, all files in the file set are backed up (just as in a full backup). If you use the same file set to perform a incremental backup later, only the files that have changed are backed up. If you use the same file set for a third backup, only the files that have changed since the second backup are backed up, and so on.

Incremental backup will clear the archive bit.

Advantages:

Backup time is faster than full backups.

Incremental backups require less disk, tape, or network drive space.

You can keep several versions of the same files on different backup sets.

Disadvantages:

In order to restore all the files, you must have all of the incremental backups available.

It may take longer to restore a specific file since you must search more than one backup set to find the latest version of a file.

Differential Backup

A differential backup provides a backup of files that have changed since a full backup was performed. A differential backup typically saves only the files that are different or new since the last full backup. Together, a full backup and a differential backup include all the files on your computer, changed and unchanged.

Differential backup do not clear the archive bits.

Advantages:

Differential backups require even less disk, tape, or network drive space than incremental backups.

Backup time is faster than full or incremental backups.

Disadvantages:

Restoring all your files may take considerably longer since you may have to restore both the last differential and full backup.
Restoring an individual file may take longer since you have to locate the file on either the differential or full backup.
For more info see: http://support.microsoft.com/kb/136621
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

NEW QUESTION: 344
Which OSI/ISO layer is responsible for determining the best route for data to be transferred?
A. Session layer
B. Physical layer
C. Network layer
D. Transport layer
Answer: (SHOW ANSWER)
Explanation/Reference:
The main responsibility of the network layer is to insert information into the packet's header so that it can be properly routed. The protocols at the network layer must determine the best path for the packet to take.
The following answers are incorrect:
Session layer. The session layer is responsible for establishing a connection between two applications.
Physical layer. The physical layer if responsible for converting electronic impulses into bits and vice-versa.
Transport layer. The transport layer is responsible for data transmission and error detection.
The following reference(s) were/was used to create this question:
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, v3, chapter 7:
Telecommunications and Network Security (page 422-428).
ISC2 Official ISC2 Guide to the CBK (OIG) 2007, p. 409-412

NEW QUESTION: 345
What is called an event or activity that has the potential to cause harm to the information systems or networks?
A. Vulnerability
B. Threat agent
C. Weakness
D. Threat
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 16, 32.

NEW QUESTION: 346
In which of the following security models is the subject's clearance compared to the object's classification such that specific rules can be applied to control how the subject-to-object interactions take place?
A. Bell-LaPadula model
B. Biba model
C. Access Matrix model
D. Take-Grant model
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
The Bell-LAPadula model is also called a multilevel security system because users with different clearances use the system and the system processes data with different classifications. Developed by the US Military in the 1970s.
A security model maps the abstract goals of the policy to information system terms by specifying explicit data structures and techniques necessary to enforce the security policy. A security model is usually represented in mathematics and analytical ideas, which are mapped to system specifications and then developed by programmers through programming code. So we have a policy that encompasses security goals, such as
"each subject must be authenticated and authorized before accessing an object." The security model takes this requirement and provides the necessary mathematical formulas, relationships, and logic structure to be followed to accomplish this goal.
A system that employs the Bell-LaPadula model is called a multilevel security system because users with different clearances use the system, and the system processes data at different classification levels. The level at which information is classified determines the handling procedures that should be used. The Bell-LaPadula model is a state machine model that enforces the confidentiality aspects of access control. A matrix and security levels are used to determine if subjects can access different objects. The subject's clearance is compared to the object's classification and then specific rules are applied to control how subject-to-object subject-to-object interactions can take place.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 369). McGraw-Hill. Kindle Edition.

NEW QUESTION: 347
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: (SHOW ANSWER)
Explanation/Reference:
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: 348
Once evidence is seized, a law enforcement officer should emphasize which of the following?
A. Chain of command
B. Chain of custody
C. Chain of control
D. Chain of communications
Answer: B (LEAVE A REPLY)
All people that handle the evidence from the time the crime was committed through the final disposition must be identified. This is to ensure that the evidence can be used and has not been tampered with.
The following answers are incorrect:
chain of command. Is incorrect because chain of command is the order of authority and
does not apply to evidence.
chain of control. Is incorrect because it is a distractor.

chain of communications. Is incorrect because it is a distractor.

NEW QUESTION: 349
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)
Explanation/Reference:
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: 350
Which Network Address Translation (NAT) is the most convenient and secure solution?
A. Hiding Network Address Translation
B. Port Address Translation
C. Dedicated Address Translation
D. Static Address Translation
Answer: (SHOW ANSWER)
Explanation/Reference:
Static network address translation offers the most flexibility, but it is not normally practical given the shortage of IP version 4 addresses. Hiding network address translation is was an interim step in the development of network address translation technology, and is seldom used because port address translation offers additional features above and beyond those present in hiding network address translation while maintaining the same basic design and engineering considerations. PAT is often the most convenient and secure solution.
Source: WACK, John et al., NIST Special publication 800-41, Guidelines on Firewalls and Firewall Policy, January 2002 (page 18).

NEW QUESTION: 351
Within the context of the CBK, which of the following provides a MINIMUM level of security ACCEPTABLE for an environment ?

A. A baseline
B. A standard
C. A procedure
D. A guideline
Answer: (SHOW ANSWER)
Baselines provide the minimum level of security necessary throughout the organization.
Standards specify how hardware and software products should be used throughout the organization.
Procedures are detailed step-by-step instruction on how to achieve certain tasks.
Guidelines are recommendation actions and operational guides to personnel when a specific standard does not apply.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 3: Security Management Practices (page 94).

NEW QUESTION: 352
In the context of network enumeration by an outside attacker and possible Distributed Denial of Service (DDoS) attacks, which of the following firewall rules is not appropriate to protect an organization's internal network?
A. Allow echo reply outbound
B. Allow echo request outbound
C. Drop echo request inbound
D. Allow echo reply inbound
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
Echo replies outbound should be dropped, not allowed. There is no reason for any internet users to send ICMP ECHO Request to your interal hosts from the internet. If they wish to find out if a service is available, they can use a browser to connect to your web server or simply send an email if they wish to test your mail service.
Echo replies outbound could be used as part of the SMURF amplification attack where someone will send ICMP echo requests to gateways broadcast addresses in order to amplify the request by X number of users sitting behind the gateway.
By allowing inbound echo requests and outbound echo replies, it makes it easier for attackers to learn about the internal network as well by performing a simply ping sweep. ICMP can also be used to find out which host has been up and running the longest which would indicates which patches are missing on the host if a critical patch required a reboot.
ICMP can also be use for DDoS attacks, so you should strictly limit what type of ICMP traffic would be allowed to flow through your firewall.
On top of all this, tools such as LOKI could be use as a client-server application to transfer files back and forward between the internat and some of your internal hosts. LOKI is a client/server program published

in the online publication Phrack . This program is a working proof-of-concept to demonstrate that data can be transmitted somewhat secretly across a network by hiding it in traffic that normally does not contain payloads.
The example code can tunnel the equivalent of a Unix RCMD/RSH session in either ICMP echo request (ping) packets or UDP traffic to the DNS port. This is used as a back door into a Unix system after root access has been compromised. Presence of LOKI on a system is evidence that the system has been compromised in the past.
The outbound echo request and inbound echo reply allow internal users to verify connectivity with external hosts.
The following answers are incorrect:
Allow echo request outbound The outbound echo request and inbound echo reply allow internal users to verify connectivity with external hosts.
Drop echo request inbound There is no need for anyone on the internet to attempt pinging your internal hosts.
Allow echo reply inbound The outbound echo request and inbound echo reply allow internal users to verify connectivity with external hosts.
Reference(s) used for this question:
http://www.phrack.org/issues.html?issue=49&id=6
STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 10: The Perfect Firewall.

NEW QUESTION: 353
Which of the following terms can be described as the process to conceal data into another file or media in a practice known as security through obscurity?
A. Steganography
B. ADS - Alternate Data Streams
C. Encryption
D. NTFS ADS
Answer: (SHOW ANSWER)
Explanation/Reference:
It is the art and science of encoding hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message or could claim there is a message.
It is a form of security through obscurity.
The word steganography is of Greek origin and means "concealed writing." It combines the Greek words steganos (στεγανός), meaning "covered or protected," and graphei (γραφή) meaning "writing." The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages will appear to be (or be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter.
The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how

unbreakable, will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

It is sometimes referred to as Hiding in Plain Sight. This image of trees blow contains in it another image of a cat using Steganography.

ADS Tree with Cat inside

This image below is hidden in the picture of the trees above:

Hidden Kitty

As explained here the image is hidden by removing all but the two least significant bits of each color component and subsequent normalization.

ABOUT MSF and LSF

One of the common method to perform steganography is by hiding bits within the Least Significant Bits of a media (LSB) or what is sometimes referred to as Slack Space. By modifying only the least significant bit, it is not possible to tell if there is an hidden message or not looking at the picture or the media. If you would change the Most Significant Bits (MSB) then it would be possible to view or detect the changes just by looking at the picture. A person can perceive only up to 6 bits of depth, bit that are changed past the first sixth bit of the color code would be undetectable to a human eye.

If we make use of a high quality digital picture, we could hide six bits of data within each of the pixel of the image. You have a color code for each pixel composed of a Red, Green, and Blue value. The color

code is 3 sets of 8 bits each for each of the color. You could change the last two bit to hide your data. See below a color code for one pixel in binary format. The bits below are not real they are just example for illustration purpose:
RED GREEN BLUE
0101 0101 1100 1011 1110 0011
MSB LSB MSB LSB MSB LSB
Let's say that I would like to hide the letter A uppercase within the pixels of the picture. If we convert the letter "A" uppercase to a decimal value it would be number 65 within the ASCII table , in binary format the value 65 would translet to 01000001
You can break the 8 bits of character A uppercase in group of two bits as follow: 01 00 00 01 Using the pixel above we will hide those bits within the last two bits of each of the color as follow:
RED GREEN BLUE
0101 0101 1100 1000 1110 0000
MSB LSB MSB LSB MSB LSB
As you can see above, the last two bits of RED was already set to the proper value of 01, then we move to the GREEN value and we changed the last two bit from 11 to 00, and finally we changed the last two bits of blue to 00. One pixel allowed us to hide 6 bits of data. We would have to use another pixel to hide the remaining two bits.
The following answers are incorrect:
- ADS - Alternate Data Streams: This is almost correct but ADS is different from steganography in that ADS hides data in streams of communications or files while Steganography hides data in a single file.
- Encryption: This is almost correct but Steganography isn't exactly encryption as much as using space in a file to store another file.
- NTFS ADS: This is also almost correct in that you're hiding data where you have space to do so. NTFS, or New Technology File System common on Windows computers has a feature where you can hide files where they're not viewable under normal conditions. Tools are required to uncover the ADS-hidden files.
The following reference(s) was used to create this question:
The CCCure Security+ Holistic Tutorial at http://www.cccure.tv
and
Steganography tool
and
http://en.wikipedia.org/wiki/Steganography

NEW QUESTION: 354
Which of the following BEST explains why computerized information systems frequently fail to meet the needs of users?
A. Inadequate quality assurance (QA) tools.
B. Constantly changing user needs.
C. Inadequate user participation in defining the system's requirements.
D. Inadequate project management.
Answer: (SHOW ANSWER)

Section: Security Operation Adimnistration
Explanation/Reference:
Inadequate user participation in defining the system's requirements. Most projects fail to meet the needs of the users because there was inadequate input in the initial steps of the project from the user community and what their needs really are.
The other answers, while potentially valid, are incorrect because they do not represent the most common problem assosciated with information systems failing to meet the needs of users.
References: All in One pg 834
Only users can define what their needs are and, therefore, what the system should accomplish. Lack of adequate user involvement, especially in the systems requirements phase, will usually result in a system that doesn't fully or adequately address the needs of the user.
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 296).

NEW QUESTION: 355
A central authority determines what subjects can have access to certain objects based on the organizational security policy is called:
A. Mandatory Access Control
B. Discretionary Access Control
C. Non-Discretionary Access Control
D. Rule-based Access control
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
A central authority determines what subjects can have access to certain objects based on the organizational security policy.
The key focal point of this question is the 'central authority' that determines access rights.
Cecilia one of the quiz user has sent me feedback informing me that NIST defines MAC as: "MAC Policy means that Access Control Policy Decisions are made by a CENTRAL AUTHORITY. Which seems to indicate there could be two good answers to this question.
However if you read the NISTR document mentioned in the references below, it is also mentioned that: MAC is the most mentioned NDAC policy. So MAC is a form of NDAC policy.
Within the same document it is also mentioned: "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." Under NDAC you have two choices:
Rule Based Access control and Role Base Access Control
MAC is implemented using RULES which makes it fall under RBAC which is a form of NDAC. It is a subset of NDAC.

This question is representative of what you can expect on the real exam where you have more than once choice that seems to be right. However, you have to look closely if one of the choices would be higher level or if one of the choice falls under one of the other choice. In this case NDAC is a better choice because MAC is falling under NDAC through the use of Rule Based Access Control.

The following are incorrect answers:

MANDATORY ACCESS CONTROL

In Mandatory Access Control the labels of the object and the clearance of the subject determines access rights, not a central authority. Although a central authority (Better known as the Data Owner) assigns the label to the object, the system does the determination of access rights automatically by comparing the Object label with the Subject clearance. The subject clearance MUST dominate (be equal or higher) than the object being accessed.

The need for a MAC mechanism arises when the security policy of a system dictates that:

1. Protection decisions must not be decided by the object owner.
2. The system must enforce the protection decisions (i.e., the system enforces the security policy over the wishes or intentions of the object owner).

Usually a labeling mechanism and a set of interfaces are used to determine access based on the MAC policy; for example, a user who is running a process at the Secret classification should not be allowed to read a file with a label of Top Secret. This is known as the "simple security rule," or "no read up." Conversely, a user who is running a process with a label of Secret should not be allowed to write to a file with a label of Confidential. This rule is called the "*-property" (pronounced "star property") or "no write down." The *- property is required to maintain system security in an automated environment.

DISCRETIONARY ACCESS CONTROL

In Discretionary Access Control the rights are determined by many different entities, each of the persons who have created files and they are the owner of that file, not one central authority.

DAC leaves a certain amount of access control to the discretion of the object's owner or anyone else who is authorized to control the object's access. For example, it is generally used to limit a user's access to a file; it is the owner of the file who controls other users' accesses to the file. Only those users specified by the owner may have some combination of read, write, execute, and other permissions to the file.

DAC policy tends to be very flexible and is widely used in the commercial and government sectors. However, DAC is known to be inherently weak for two reasons:

First, granting read access is transitive; for example, when Ann grants Bob read access to a file, nothing stops Bob from copying the contents of Ann's file to an object that Bob controls. Bob may now grant any other user access to the copy of Ann's file without Ann's knowledge.

Second, DAC policy is vulnerable to Trojan horse attacks. Because programs inherit the identity of the invoking user, Bob may, for example, write a program for Ann that, on the surface, performs some useful function, while at the same time destroys the contents of Ann's files. When investigating the problem, the audit files would indicate that Ann destroyed her own files. Thus, formally, the drawbacks of DAC are as follows:

Discretionary Access Control (DAC) Information can be copied from one object to another; therefore, there is no real assurance on the flow of information in a system.

No restrictions apply to the usage of information when the user has received it.

The privileges for accessing objects are decided by the owner of the object, rather than through a system-wide policy that reflects the organization's security requirements.
ACLs and owner/group/other access control mechanisms are by far the most common mechanism for implementing DAC policies. Other mechanisms, even though not designed with DAC in mind, may have the capabilities to implement a DAC policy.
RULE BASED ACCESS CONTROL
In Rule-based Access Control a central authority could in fact determine what subjects can have access when assigning the rules for access. However, the rules actually determine the access and so this is not the most correct answer.
RuBAC (as opposed to RBAC, role-based access control) allow users to access systems and information based on pre determined and configured rules. It is important to note that there is no commonly understood definition or formally defined standard for rule-based access control as there is for DAC, MAC, and RBAC.
"Rule-based access" is a generic term applied to systems that allow some form of organization-defined rules, and therefore rule-based access control encompasses a broad range of systems. RuBAC may in fact be combined with other models, particularly RBAC or DAC. A RuBAC system intercepts every access request and compares the rules with the rights of the user to make an access decision. Most of the rule-based access control relies on a security label system, which dynamically composes a set of rules defined by a security policy. Security labels are attached to all objects, including files, directories, and devices. Sometime roles to subjects (based on their attributes) are assigned as well. RuBAC meets the business needs as well as the technical needs of controlling service access. It allows business rules to be applied to access control-for example, customers who have overdue balances may be denied service access. As a mechanism for MAC, rules of RuBAC cannot be changed by users. The rules can be established by any attributes of a system related to the users such as domain, host, protocol, network, or IP addresses. For example, suppose that a user wants to access an object in another network on the other side of a router. The router employs RuBAC with the rule composed by the network addresses, domain, and protocol to decide whether or not the user can be granted access. If employees change their roles within the organization, their existing authentication credentials remain in effect and do not need to be re configured. Using rules in conjunction with roles adds greater flexibility because rules can be applied to people as well as to devices. Rule-based access control can be combined with role-based access control, such that the role of a user is one of the attributes in rule setting.
Some provisions of access control systems have rule- based policy engines in addition to a role-based policy engine and certain implemented dynamic policies [Des03]. For example, suppose that two of the primary types of software users are product engineers and quality engineers. Both groups usually have access to the same data, but they have different roles to perform in relation to the data and the application's function. In addition, individuals within each group have different job responsibilities that may be identified using several types of attributes such as developing programs and testing areas. Thus, the access decisions can be made in real time by a scripted policy that regulates the access between the groups of product engineers and quality engineers, and each individual within these groups. Rules can either replace or complement role-based access control. However, the creation of rules and security policies is also a complex process, so each organization will need to strike the appropriate balance.

References used for this question:
http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf
and
AIO v3 p162-167 and OIG (2007) p.186-191
also
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION: 356
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)
Section: Security Operation Adimnistration
Explanation/Reference:
Padded cells complement Intrusion Detection Systems (IDSs) and are not related to DBMS security. Padded cells are simulated environments to which IDSs seamlessly transfer detected attackers and are designed to convince an attacker that the attack is going according to the plan. Cell suppression is a technique used against inference attacks by not revealing information in the case where a statistical query produces a very small result set. Perturbation also addresses inference attacks but involves making minor modifications to the results to a query. Partitioning involves splitting a database into two or more physical or logical parts; especially relevant for multilevel secure databases.
Source: LaROSA, Jeanette (domain leader), Application and System Development Security CISSP Open Study Guide, version 3.0, January 2002.

NEW QUESTION: 357
Why is traffic across a packet switched network difficult to monitor?
A. Packets are link encrypted by the carrier
B. Government regulations forbids monitoring
C. Packets can take multiple paths when transmitted
D. The network factor is too high
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
With a packet switched network, packets are difficult to monitor because they can be transmitted using different paths.
A packet-switched network is a digital communications network that groups all transmitted data, irrespective of content, type, or structure into suitably sized blocks, called packets. The network over

which packets are transmitted is a shared network which routes each packet independently from all others and allocates transmission resources as needed.
The principal goals of packet switching are to optimize utilization of available link capacity, minimize response times and increase the robustness of communication. When traversing network adapters, switches and other network nodes, packets are buffered and queued, resulting in variable delay and throughput, depending on the traffic load in the network.
Most modern Wide Area Network (WAN) protocols, including TCP/IP, X.25, and Frame Relay, are based on packet-switching technologies. In contrast, normal telephone service is based on a circuit-switching technology, in which a dedicated line is allocated for transmission between two parties. Circuit-switching is ideal when data must be transmitted quickly and must arrive in the same order in which it's sent. This is the case with most real-time data, such as live audio and video. Packet switching is more efficient and robust for data that can withstand some delays in transmission, such as e-mail messages and Web pages.
All of the other answer are wrong
Reference(s) used for this question:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
and
https://en.wikipedia.org/wiki/Packet-switched_network
and
http://www.webopedia.com/TERM/P/packet_switching.html

NEW QUESTION: 358
An attack initiated by an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization is known as a(n):
A. active attack
B. outside attack
C. inside attack
D. passive attack
Answer: (SHOW ANSWER)
Explanation/Reference:
An inside attack is an attack initiated by an entity inside the security perimeter, an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization whereas an outside attack is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system. An active attack attempts to alter system resources to affect their operation and a passive attack attempts to learn or make use of the information from the system but does not affect system resources.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 359
Preservation of confidentiality within information systems requires that the information is not disclosed to:
A. Authorized person

B. Unauthorized persons or processes.
C. Unauthorized persons.
D. Authorized persons and processes
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
Confidentiality assures that the information is not disclosed to unauthorized persons or processes.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 31.

NEW QUESTION: 360
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: (SHOW ANSWER)
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: 361
This baseline sets certain thresholds for specific errors or mistakes allowed and the amount of these occurrences that can take place before it is considered suspicious?
A. Checkpoint level
B. Ceiling level
C. Clipping level
D. Threshold level
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Organizations usually forgive a particular type, number, or pattern of violations, thus permitting a predetermined number of user errors before gathering this data for analysis. An organization attempting to track all violations, without sophisticated statistical computing ability, would be unable to manage the sheer quantity of such data. To make a violation listing effective, a clipping level must be established. The clipping level establishes a baseline for violation activities that may be normal user errors. Only after this baseline is exceeded is a violation record produced. This solution is particularly effective for small- to medium- sized installations. Organizations with large-scale computing facilities often track all violations and use statistical routines to cull out the minor infractions (e.g., forgetting a password or mistyping it several times).

If the number of violations being tracked becomes unmanageable, the first step in correcting the problems should be to analyze why the condition has occurred. Do users understand how they are to interact with the computer resource? Are the rules too difficult to follow? Violation tracking and analysis can be valuable tools in assisting an organization to develop thorough but useable controls. Once these are in place and records are produced that accurately reflect serious violations, tracking and analysis become the first line of defense. With this procedure, intrusions are discovered before major damage occurs and sometimes early enough to catch the perpetrator. In addition, business protection and preservation are strengthened.
The following answers are incorrect:
All of the other choices presented were simply detractors.
The following reference(s) were used for this question:
Handbook of Information Security Management

NEW QUESTION: 362
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: (SHOW ANSWER)
As protocol was introduced by Visa and Mastercard to allow for more credit card transaction possibilities. It is comprised of three different pieces of software, running on the customer's PC (an electronic wallet), on the merchant's Web server and on the payment server of the merchant's bank. The credit card information is sent by the customer to the merchant's Web server, but it does not open it and instead digitally signs it and sends it to its bank's payment server for processing.
The following answers are incorrect because :
SSH (Secure Shell) is incorrect as it functions as a type of tunneling mechanism that provides terminal like access to remote computers.
S/MIME is incorrect as it is a standard for encrypting and digitally signing electronic mail
and for providing secure data transmissions.
SSL is incorrect as it uses public key encryption and provides data encryption, server

authentication, message integrity, and optional client authentication.
Reference : Shon Harris AIO v3 , Chapter-8: Cryptography , Page : 667-669

NEW QUESTION: 363
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: 364
What is the name of the third party authority that vouches for the binding between the data items in a digital certificate?
A. Registration authority
B. Certification authority
C. Issuing authority
D. Vouching authority
Answer: (SHOW ANSWER)
A certification authority (CA) is a third party entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate. An issuing authority could be considered a correct answer, but not the best answer, since it is too generic.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 365
What is the role of IKE within the IPsec protocol?
A. peer authentication and key exchange
B. data encryption
C. data signature
D. enforcing quality of service
Answer: (SHOW ANSWER)
Explanation/Reference:
Reference: RFC 2409: The Internet Key Exchange (IKE); DORASWAMY, Naganand & HARKINS, Dan, Ipsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, 1999, Prentice Hall PTR; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

NEW QUESTION: 366
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)
Section: Access Control
Explanation/Reference:
Because the optical unit utilizes a camera and infrared light to create the images, sun light can impact the aperture so it must not be positioned in direct light of any type. Because the subject does not need to have direct contact with the optical reader, direct light can impact the reader.
An Iris recognition is a form of biometrics that is based on the uniqueness of a subject's iris. A camera like device records the patterns of the iris creating what is known as Iriscode.
It is the unique patterns of the iris that allow it to be one of the most accurate forms of biometric identification of an individual. Unlike other types of biometics, the iris rarely changes over time. Fingerprints can change over time due to scaring and manual labor, voice patterns can change due to a variety of causes, hand geometry can also change as well. But barring surgery or an accident it is not usual for an iris to change. The subject has a high-resoulution image taken of their iris and this is then converted to Iriscode. The current standard for the Iriscode was developed by John Daugman. When the subject attempts to be authenticated an infrared light is used to capture the iris image and this image is then compared to the Iriscode. If there is a match the subject's identity is confirmed. The subject does not need to have direct contact with the optical reader so it is a less invasive means of authentication then retinal scanning would be.
Reference(s) used for this question:
AIO, 3rd edition, Access Control, p 134.
AIO, 4th edition, Access Control, p 182.
Wikipedia - http://en.wikipedia.org/wiki/Iris_recognition
The following answers are incorrect:
concern that the laser beam may cause eye damage. The optical readers do not use laser so, concern that the laser beam may cause eye damage is not an issue.
the iris pattern changes as a person grows older. The question asked about the physical installation of the scanner, so this was not the best answer. If the question would have been about long term problems then it could have been the best choice. Recent research has shown that Irises actually do change over time: http:// www.nature.com/news/ageing-eyes-hinder-biometric-scans-1.10722 there is a relatively high rate of false accepts. Since the advent of the Iriscode there is a very low rate of false accepts, in fact the algorithm used has never had a false match. This all depends on the quality of the equipment used but because of the uniqueness of the iris even when comparing identical twins, iris patterns are unique.

NEW QUESTION: 367

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: (SHOW ANSWER)
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: 368
Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a
system. It does not permit management to:
A. specify what users can do
B. specify which resources they can access
C. specify how to restrain hackers
D. specify what operations they can perform on a system.
Answer: (SHOW ANSWER)
Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It permits management to specify what users can do, which resources they can access, and what operations they can perform on a system. Specifying HOW to restrain hackers is not directly linked to access control. Source: DUPUIS, Clement, Access Control Systems and Methodology, Version 1, May 2002, CISSP Open Study Group Study Guide for Domain 1, Page 12.

NEW QUESTION: 369
What type of cable is used with 100Base-TX Fast Ethernet?
A. Fiber-optic cable
B. Category 3 or 4 unshielded twisted-pair (UTP).
C. Category 5 unshielded twisted-pair (UTP).
D. RG-58 cable.
Answer: (SHOW ANSWER)
Explanation/Reference:
This is the type of cabling recommended for 100Base-TX networks.

Fiber-optic cable is incorrect. Incorrect media type for 100Base-TX -- 100Base-FX would denote fiber optic cabling.
"Category 3 or 4 unshielded twisted-pair (UTP)" is incorrect. These types are not recommended for 100Mbps operation.
RG-58 cable is incorrect. Incorrect media type for 100Base-TX.
References
CBK, p. 428
AIO3, p. 455

NEW QUESTION: 370

Who should measure the effectiveness of Information System security related controls in an organization?

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

NEW QUESTION: 371
Which of the following type of traffic can easily be filtered with a stateful packet filter by enforcing the context or state of the request?
A. ICMP
B. TCP
C. UDP
D. IP
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
The question is explict in asking *easily*. With TCP connection establishment there is a distinct state or sequence that can be expected. Consult the references for further details.

ICMP, IP and UDP don't have any concept of a session; i.e. each packet or datagram is handled individually, with no reference to the contents of the previous one. With no sessions, these protocols usually cannot be filtered on the state of the session.
Some newer firewalls, however, simulate the concept of state for these protocols, and filter out unexpected packets based upon normal usage. Although these are commonly treated like normal stateful filters, they are more complex to program, and hence more prone to errors.
A stateful packet filter or stateful inspection inspects each packet and only allows known connection states through. So, if a SYN/ACK packet was recieved and there was not a prior SYN packet sent it would filter that packet and not let it in. The correct sequence of steps are known and if the sequence or state is incorrect then it is dropped.
The incorrect answers are:
ICMP. ICMP is basically stateless so you could not easily filter them based on the state or sequence.
UDP. UDP has no real state so you could only partially filter them based on the state or sequence. The question was explicit in asking easily. While it is possible, UDP is not the best answer.
IP. IP would refer to the Internet Protocol and as such is stateless so you would not be able to filter it out easily.
The following reference(s) were used for this question:
http://www.nwo.net/ipf/ipf-howto.pdf

NEW QUESTION: 372
FTP, TFTP, SNMP, and SMTP are provided at what level of the Open Systems Interconnect (OSI) Reference Model?
A. Application
B. Network
C. Presentation
D. Transport
Answer: (SHOW ANSWER)
Explanation/Reference:
Application. The Layer 7 Application Layer of the Open Systems Interconnect (OSI) Reference Model is a service for applications and Operating Systems data transmission, for example FTP, TFTP, SNMP, and SMTP.
The following answers are incorrect:
Network. The Network layer moves information between hosts that are not physically connected. It deals with routing of information. IP is a protocol that is used in Network Layer. FTP, TFTP, SNMP, and SMTP do not reside at the Layer 3 Network Layer in the OSI Reference Model.
Presentation. The Presentation Layer is concerned with the formatting of data into a standard presentation such as
ASCII. FTP, TFTP, SNMP, and SMTP do not reside at the Layer 6 Presentation Layer in the OSI Reference Model.
Transport. The Transport Layer creates an end-to-end transportation between peer hosts. The transmission can be connectionless and unreliable such as UDP, or connection-oriented and ensure

error- free delivery such as TCP. FTP, TFTP, SNMP, and SMTP do not reside at the Layer 4 Transportation Layer in the OSI Reference Model.
The following reference(s) were/was used to create this question: Reference: OSI/ISO.
Shon Harris AIO v.3 p. 420-421
ISC2 OIG, 2997 p.412-413

NEW QUESTION: 373
Which one of the following is usually not a benefit resulting from the use of firewalls?
A. reduces the risks of external threats from malicious hackers.
B. prevents the spread of viruses.
C. reduces the threat level on internal system.
D. allows centralized management and control of services.
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
This is not a benefit of a firewall. Most firewalls are limited when it comes to preventing the spread of viruses.
This question is testing your knowledge of Malware and Firewalls. The keywords within the questions are "usually" and "virus". Once again to come up with the correct answer, you must stay within the context of the question and really ask yourself which of the 4 choices is NOT usually done by a firewall.
Some of the latest Appliances such as Unified Threat Management (UTM) devices does have the ability to do virus scanning but most first and second generation firewalls would not have such ability.
Remember, the questions is not asking about all possible scenarios that could exist but only about which of the 4 choices presented is the BEST.
For the exam you must know your general classes of Malware. There are generally four major classes of malicious code that fall under the general definition of malware:
1. Virus: Parasitic code that requires human action or insertion, or which attaches itself to another program to facilitate replication and distribution. Virus-infected containers can range from e-mail, documents, and data file macros to boot sectors, partitions, and memory fobs. Viruses were the first iteration of malware and were typically transferred by floppy disks (also known as "sneakernet") and injected into memory when the disk was accessed or infected files were transferred from system to system.
2. Worm: Self-propagating code that exploits system or application vulnerabilities to replicate. Once on a system, it may execute embedded routines to alter, destroy, or monitor the system on which it is running, then move on to the next system. A worm is effectively a virus that does not require human interaction or other programs to infect systems.
3. Trojan Horse: Named after the Trojan horse of Greek mythology (and serving a very similar function), a Trojan horse is a general term referring to programs that appear desirable, but actually contain something harmful. A Trojan horse purports to do one thing that the user wants while secretly performing other potentially malicious actions. For example, a user may download a game file, install it, and begin playing the game.

Unbeknownst to the user, the application may also install a virus, launch a worm, or install a utility allowing an attacker to gain unauthorized access to the system remotely, all without the user's knowledge.
4. Spyware: Prior to its use in malicious activity, spyware was typically a hidden application injected through poor browser security by companies seeking to gain more information about a user's Internet activity. Today, those methods are used to deploy other malware, collect private data, send advertising or commercial messages to a system, or monitor system input, such as keystrokes or mouse clicks.
The following answers are incorrect:
reduces the risks of external threats from malicious hackers. This is incorrect because a firewall can reduce the risks of external threats from malicious hackers.
reduces the threat level on internal system. This is incorrect because a firewall can reduce the threat level on internal system.
allows centralized management and control of services. This is incorrect because a firewall can allow centralize management and control of services.
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 3989-4009). Auerbach Publications. Kindle Edition.

NEW QUESTION: 374
What is called the access protection system that limits connections by calling back the number of a previously authorized location?
A. Sendback systems
B. Callback forward systems
C. Callback systems
D. Sendback forward systems
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
The Answer: Call back Systems; Callback systems provide access protection by calling back the number of a previously authorized location, but this control can be compromised by call forwarding.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35.

NEW QUESTION: 375
A prolonged complete loss of electric power is a:
A. brownout
B. blackout
C. surge
D. fault
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery

Explanation/Reference:
A prolonged power outage is a blackout.
From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw-Hill/Osborne, 2005, page 368.

NEW QUESTION: 376
This type of attack is generally most applicable to public-key cryptosystems, what type of attack am I ?
A. Chosen-Ciphertext attack
B. Ciphertext-only attack
C. Plaintext Only Attack
D. Adaptive-Chosen-Plaintext attack
Answer: (SHOW ANSWER)
Explanation/Reference:
A chosen-ciphertext attack is one in which cryptanalyst may choose a piece of ciphertext and attempt to obtain the corresponding decrypted plaintext. This type of attack is generally most applicable to public-key cryptosystems.
A chosen-ciphertext attack (CCA) is an attack model for cryptanalysis in which the cryptanalyst gathers information, at least in part, by choosing a ciphertext and obtaining its decryption under an unknown key. In the attack, an adversary has a chance to enter one or more known ciphertexts into the system and obtain the resulting plaintexts. From these pieces of information the adversary can attempt to recover the hidden secret key used for decryption.
A number of otherwise secure schemes can be defeated under chosen-ciphertext attack. For example, the El Gamal cryptosystem is semantically secure under chosen-plaintext attack, but this semantic security can be trivially defeated under a chosen-ciphertext attack. Early versions of RSA padding used in the SSL protocol were vulnerable to a sophisticated adaptive chosen-ciphertext attack which revealed SSL session keys. Chosen-ciphertext attacks have implications for some self-synchronizing stream ciphers as well.
Designers of tamper-resistant cryptographic smart cards must be particularly cognizant of these attacks, as these devices may be completely under the control of an adversary, who can issue a large number of chosen-ciphertexts in an attempt to recover the hidden secret key.
According to RSA:
Cryptanalytic attacks are generally classified into six categories that distinguish the kind of information the cryptanalyst has available to mount an attack. The categories of attack are listed here roughly in increasing order of the quality of information available to the cryptanalyst, or, equivalently, in decreasing order of the level of difficulty to the cryptanalyst. The objective of the cryptanalyst in all cases is to be able to decrypt new pieces of ciphertext without additional information. The ideal for a cryptanalyst is to extract the secret key.
A ciphertext-only attack is one in which the cryptanalyst obtains a sample of ciphertext, without the plaintext associated with it. This data is relatively easy to obtain in many scenarios, but a successful ciphertext-only attack is generally difficult, and requires a very large ciphertext sample. Such attack was possible on cipher using Code Book Mode where frequency analysis was being used and even thou only

the ciphertext was available, it was still possible to eventually collect enough data and decipher it without having the key.

A known-plaintext attack is one in which the cryptanalyst obtains a sample of ciphertext and the corresponding plaintext as well. The known-plaintext attack (KPA) or crib is an attack model for cryptanalysis where the attacker has samples of both the plaintext and its encrypted version (ciphertext), and is at liberty to make use of them to reveal further secret information such as secret keys and code books.

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

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

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

Two forms of chosen-plaintext attack can be distinguished:

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

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

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

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

An adaptive chosen-ciphertext attack (abbreviated as CCA2) is an interactive form of chosen-ciphertext attack in which an attacker sends a number of ciphertexts to be decrypted, then uses the results of these

decryptions to select subsequent ciphertexts. It is to be distinguished from an indifferent chosen-ciphertext attack (CCA1).
The goal of this attack is to gradually reveal information about an encrypted message, or about the decryption key itself. For public-key systems, adaptive-chosen-ciphertexts are generally applicable only when they have the property of ciphertext malleability - that is, a ciphertext can be modified in specific ways that will have a predictable effect on the decryption of that message.
A Plaintext Only Attack is simply a bogus detractor. If you have the plaintext only then there is no need to perform any attack.
References:
RSA Laboratories FAQs about today's cryptography: What are some of the basic types of cryptanalytic attack?
also see:
http://www.giac.org/resources/whitepaper/cryptography/57.php
and
http://en.wikipedia.org/wiki/Chosen-plaintext_attack

NEW QUESTION: 377
Much like the layers of an onion, _____ is a comprehensive set of security solutions layered to provide the best protection.
A. Defense in Depth
B. Firewall Penetration Testing
C. Risk Assessment
D. Security policy
E. Vulnerability Assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 378
Which of the following statements pertaining to stream ciphers is correct?
A. A stream cipher is a type of asymmetric encryption algorithm.
B. A stream cipher generates what is called a keystream.
C. A stream cipher is slower than a block cipher.
D. A stream cipher is not appropriate for hardware-based encryption.

Answer: (SHOW ANSWER)

Section: Cryptography

Explanation/Reference:

A stream cipher is a type of symmetric encryption algorithm that operates on continuous streams of plain text and is appropriate for hardware-based encryption.

Stream ciphers can be designed to be exceptionally fast, much faster than any block cipher. A stream cipher generates what is called a keystream (a sequence of bits used as a key).

Stream ciphers can be viewed as approximating the action of a proven unbreakable cipher, the one-time pad (OTP), sometimes known as the Vernam cipher. A one-time pad uses a keystream of completely random digits. The keystream is combined with the plaintext digits one at a time to form the ciphertext. This system was proved to be secure by Claude Shannon in 1949. However, the keystream must be (at least) the same length as the plaintext, and generated completely at random. This makes the system very cumbersome to implement in practice, and as a result the one-time pad has not been widely used, except for the most critical applications.

A stream cipher makes use of a much smaller and more convenient key - 128 bits, for example. Based on this key, it generates a pseudorandom keystream which can be combined with the plaintext digits in a similar fashion to the one-time pad. However, this comes at a cost: because the keystream is now pseudorandom, and not truly random, the proof of security associated with the one-time pad no longer holds: it is quite possible for a stream cipher to be completely insecure if it is not implemented properly as we have seen with the Wired Equivalent Privacy (WEP) protocol.

Encryption is accomplished by combining the keystream with the plaintext, usually with the bitwise XOR operation.

Source: DUPUIS, Clement, CISSP Open Study Guide on domain 5, cryptography, April 1999.

More details can be obtained on Stream Ciphers in RSA Security's FAQ on Stream Ciphers.

NEW QUESTION: 379

Sensitivity labels are an example of what application control type?

A. Preventive security controls

B. Detective security controls

C. Compensating administrative controls

D. Preventive accuracy controls

Answer: (SHOW ANSWER)

Sensitivity labels are a preventive security application controls, such as are firewalls, reference monitors, traffic padding, encryption, data classification, one-time passwords, contingency planning, separation of development, application and test environments.

The incorrect answers are:

Detective security controls - Intrusion detection systems (IDS), monitoring activities, and audit trails.

Compensating administrative controls - There no such application control.

Preventive accuracy controls - data checks, forms, custom screens, validity checks, contingency planning, and backups.

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 264). KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Application Controls, Figure 7.1 (page 360).

NEW QUESTION: 380

The high availability of multiple all-inclusive, easy-to-use hacking tools that do NOT require much technical knowledge has brought a growth in the number of which type of attackers?

A. Black hats
B. White hats
C. Script kiddies
D. Phreakers
Answer: (SHOW ANSWER)
As script kiddies are low to moderately skilled hackers using available scripts and tools to easily launch attacks against victims.
The other answers are incorrect because :
Black hats is incorrect as they are malicious , skilled hackers.
White hats is incorrect as they are security professionals.
Phreakers is incorrect as they are telephone/PBX (private branch exchange) hackers.
Reference : Shon Harris AIO v3 , Chapter 12: Operations security , Page : 830

NEW QUESTION: 381
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)
Section: Access Control
Explanation/Reference:
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: 382
What is the MOST critical piece to disaster recovery and continuity planning?
A. Security policy
B. Management support
C. Availability of backup information processing facilities
D. Staff training
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation
Explanation/Reference:
The keyword is ' MOST CRITICAL ' and the correct answer is ' Management Support ' as the management must be convinced of its necessity and that's why a business case must be made. The decision of how a company should recover from any disaster is purely a business decision and should be treated as so.

The other answers are incorrect because :
Security policy is incorrect as it is not the MOST CRITICAL piece.
Availability of backup information processing facilities is incorrect as this comes once the organization has BCP Plans in place and for a BCP Plan , management support must be there.
Staff training comes after the plans are in place with the support from management.
Reference : Shon Harris , AIO v3 , Chapter-9: Business Continuity Planning , Page : 697.

NEW QUESTION: 383
Which of the following are required for Life-Cycle Assurance?
A. System Architecture and Design specification.
B. Security Testing and Covert Channel Analysis.
C. Security Testing and Trusted distribution.
D. Configuration Management and Trusted Facility Management.
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
Security testing and trusted distribution are required for Life-Cycle Assurance.
The following answers are incorrect:
System Architecture and Design specification. Is incorrect because System Architecture is not requried for Life- Cycle Assurance.
Security Testing and Covert Channel Analysis. Is incorrect because Covert Channel Analysis is not requried for Life-Cycle Assurance.
Configuration Management and Trusted Facility Management. Is incorrect because Trusted Facility Management. is not requried for Life-Cycle Assurance.

NEW QUESTION: 384
Which of the following packets should NOT be dropped at a firewall protecting an organization's internal network?
A. Inbound packets with Source Routing option set
B. Router information exchange protocols
C. Inbound packets with an internal address as the source IP address
D. Outbound packets with an external destination IP address
Answer: (SHOW ANSWER)
Normal outbound traffic has an internal source IP address and an external destination IP address.
Traffic with an internal source IP address should only come from an internal interface. Such packets coming from an external interface should be dropped.
Packets with the source-routing option enabled usually indicates a network intrusion attempt.
Router information exchange protocols like RIP and OSPF should be dropped to avoid having internal routing equipment being reconfigured by external agents.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 10: The Perfect Firewall.

NEW QUESTION: 385
Which of the following is NOT a form of detective administrative control?
A. Rotation of duties
B. Required vacations
C. Separation of duties
D. Security reviews and audits
Answer: (SHOW ANSWER)
Explanation/Reference:
Detective administrative controls warn of administrative control violations. Rotation of duties, required vacations and security reviews and audits are forms of detective administrative controls. Separation of duties is the practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process, thus a preventive control rather than a detective control.
Source: DUPUIS, Cl?ment, Access Control Systems and Methodology CISSP Open Study Guide, version
1.0 (march 2002).

NEW QUESTION: 386
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: (SHOW ANSWER)
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: 387
Which of the following is NOT a VPN communications protocol standard?
A. Point-to-point tunnelling protocol (PPTP)
B. Challenge Handshake Authentication Protocol (CHAP)
C. Layer 2 tunnelling protocol (L2TP)
D. IP Security
Answer: (SHOW ANSWER)
CHAP is an authentication mechanism for point-to-point protocol connections that encrypt the user's password. It is a protocol that uses a three-way handshake. The server sends the client a challenge, which includes a random value (a nonce) to thwart replay attacks. The client responds with a MD5 hash of the nonce and the password. The authentication is successful if the client's response is the one that the server expected.
The VPN communication protocol standards listed above are PPTP, L2TP and IPSec.
PPTP and L2TP operate at the data link layer (layer 2) of the OSI model and enable only a single point-to-point connection per session.
The following are incorrect answers:

PPTP uses native PPP authentication and encryption services. Point-to-Point Tunneling Protocol (PPTP) is a VPN protocol that runs over other protocols. PPTP relies on generic routing encapsulation (GRE) to build the tunnel between the endpoints. After the user authenticates, typically with Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2), a Point-to-Point Protocol (PPP) session creates a tunnel using GRE.
L2TP is a combination of PPTP and the earlier Layer 2 Forwarding protocol (L2F). Layer 2 Tunneling Protocol (L2TP) is a hybrid of Cisco's Layer 2 Forwarding (L2F) and Microsoft's PPTP. It allows callers over a serial line using PPP to connect over the Internet to a remote network. A dial-up user connects to his ISP's L2TP access concentrator (LAC) with a PPP connection. The LAC encapsulates the PPP packets into L2TP and forwards it to the remote network's layer 2 network server (LNS). At this point, the LNS authenticates the dial-up user. If authentication is successful, the dial-up user will have access to the remote network.
IPSec operates at the network layer (layer 3) and enables multiple simultaneous tunnels. IP Security (IPSec) is a suite of protocols for communicating securely with IP by providing mechanisms for authenticating and encryption. Implementation of IPSec is mandatory in IPv6, and many organizations are using it over IPv4. Further, IPSec can be implemented in two modes, one that is appropriate for end-to-end protection and one that safeguards traffic between networks.
Reference 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 7067-7071). 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 6987-6990). Auerbach Publications. Kindle Edition.

NEW QUESTION: 388
Which of the following is NOT a correct notation for an IPv6 address?
A. 2001:0db8:0:0:0:0:1428:57ab
B. ABCD:EF01:2345:6789:ABCD:EF01:2345:6789
C. ::1
D. 2001:DB8::8:800::417A
Answer: (SHOW ANSWER)
Explanation/Reference:
This is not a correct notation for an IPv6 address because the the "::" can only appear once in an address.
The use of "::" is a shortcut notation that indicates one or more groups of 16 bits of zeros.
::1 is the loopback address using the special notation
Reference: IP Version 6 Addressing Architecture
http://tools.ietf.org/html/rfc4291#section-2.1

NEW QUESTION: 389
Which of the following is not a component of a Operations Security "triples"?
A. Asset

B. Threat
C. Vulnerability
D. Risk
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation
Explanation/Reference:
The Operations Security domain is concerned with triples - threats, vulnerabilities and assets.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 216.

NEW QUESTION: 390
What does the (star) property mean in the Bell-LaPadula model?
A. No write up
B. No read up
C. No write down
D. No read down
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
The (star) property of the Bell-LaPadula access control model states that writing of information by a subject at a higher level of sensitivity to an object at a lower level of sensitivity is not permitted (no write 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 202).
Also check out: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 5: Security Models and Architecture (page 242, 243).

NEW QUESTION: 391
Who first described the DoD multilevel military security policy in abstract, formal terms?
A. David Bell and Leonard LaPadula
B. Rivest, Shamir and Adleman
C. Whitfield Diffie and Martin Hellman
D. David Clark and David Wilson
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
It was David Bell and Leonard LaPadula who, in 1973, first described the DoD multilevel military security policy in abstract, formal terms. The Bell-LaPadula is a Mandatory Access Control (MAC) model concerned with confidentiality. Rivest, Shamir and Adleman (RSA) developed the RSA encryption algorithm. Whitfield Diffie and Martin Hellman published the Diffie-Hellman key agreement algorithm in

1976. David Clark and David Wilson developed the Clark-Wilson integrity model, more appropriate for security in commercial activities.
Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (pages 78,109).

NEW QUESTION: 392
The session layer provides a logical persistent connection between peer hosts. Which of the following is one of the modes used in the session layer to establish this connection?
A. Full duplex
B. Synchronous
C. Asynchronous
D. Half simplex
Answer: (SHOW ANSWER)
Explanation/Reference:
Layer 5 of the OSI model is the Session Layer. This layer provides a logical persistent connection between peer hosts. A session is analogous to a conversation that is necessary for applications to exchange information.
The session layer is responsible for establishing, managing, and closing end-to-end connections, called sessions, between applications located at different network endpoints. Dialogue control management provided by the session layer includes full-duplex, half-duplex, and simplex communications. Session layer management also helps to ensure that multiple streams of data stay synchronized with each other, as in the case of multimedia applications like video conferencing, and assists with the prevention of application related data errors.
The session layer is responsible for creating, maintaining, and tearing down the session.
Three modes are offered:
(Full) Duplex: Both hosts can exchange information simultaneously, independent of each other.
Half Duplex: Hosts can exchange information, but only one host at a time.
Simplex: Only one host can send information to its peer. Information travels in one direction only.
Another aspect of performance that is worthy of some attention is the mode of operation of the network or connection. Obviously, whenever we connect together device A and device B, there must be some way for A to send to B and B to send to A. Many people don't realize, however, that networking technologies can differ in terms of how these two directions of communication are handled. Depending

on how the network is set up, and the characteristics of the technologies used, performance may be improved through the selection of performance-enhancing modes.

Basic Communication Modes of Operation

Let's begin with a look at the three basic modes of operation that can exist for any network connection, communications channel, or interface.

Simplex Operation

In simplex operation, a network cable or communications channel can only send information in one direction; it's a "one-way street". This may seem counter-intuitive: what's the point of communications that only travel in one direction? In fact, there are at least two different places where simplex operation is encountered in modern networking.

The first is when two distinct channels are used for communication: one transmits from A to B and the other from B to A. This is surprisingly common, even though not always obvious. For example, most if not all fiber optic communication is simplex, using one strand to send data in each direction. But this may not be obvious if the pair of fiber strands are combined into one cable.

Simplex operation is also used in special types of technologies, especially ones that are asymmetric. For example, one type of satellite Internet access sends data over the satellite only for downloads, while a regular dial-up modem is used for upload to the service provider. In this case, both the satellite link and the dial-up connection are operating in a simplex mode.

Half-Duplex Operation

Technologies that employ half-duplex operation are capable of sending information in both directions between two nodes, but only one direction or the other can be utilized at a time. This is a fairly common mode of operation when there is only a single network medium (cable, radio frequency and so forth) between devices.

While this term is often used to describe the behavior of a pair of devices, it can more generally refer to any number of connected devices that take turns transmitting. For example, in conventional Ethernet networks, any device can transmit, but only one may do so at a time. For this reason, regular (unswitched) Ethernet networks are often said to be "half-duplex", even though it may seem strange to describe a LAN that way.

Full-Duplex Operation

In full-duplex operation, a connection between two devices is capable of sending data in both directions simultaneously. Full-duplex channels can be constructed either as a pair of simplex links (as described above) or using one channel designed to permit bidirectional simultaneous transmissions. A full-duplex link can only connect two devices, so many such links are required if multiple devices are to be connected together.

Note that the term "full-duplex" is somewhat redundant; "duplex" would suffice, but everyone still says "full- duplex" (likely, to differentiate this mode from half-duplex).

For a listing of protocols associated with Layer 5 of the OSI model, see below:

ADSP - AppleTalk Data Stream Protocol

ASP - AppleTalk Session Protocol

H.245 - Call Control Protocol for Multimedia Communication

ISO-SP

OSI session-layer protocol (X.225, ISO 8327)
iSNS - Internet Storage Name Service
The following are incorrect answers:
Synchronous and Asynchronous are not session layer modes.
Half simplex does not exist. By definition, simplex means that information travels one way only, so half-simplex is a oxymoron.
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 5603-5636). Auerbach Publications. Kindle Edition.
and
http://www.tcpipguide.com/free/t_SimplexFullDuplexandHalfDuplexOperation.htm and
http://www.wisegeek.com/what-is-a-session-layer.htm

NEW QUESTION: 393
Which of the following are required for Life-Cycle Assurance?
A. System Architecture and Design specification.
B. Security Testing and Covert Channel Analysis.
C. Security Testing and Trusted distribution.
D. Configuration Management and Trusted Facility Management.
Answer: (SHOW ANSWER)
Security testing and trusted distribution are required for Life-Cycle Assurance.
The following answers are incorrect:
System Architecture and Design specification. Is incorrect because System Architecture is not requried for Life-Cycle Assurance.
Security Testing and Covert Channel Analysis. Is incorrect because Covert Channel Analysis is not requried for Life-Cycle Assurance.
Configuration Management and Trusted Facility Management. Is incorrect because Trusted Facility Management. is not requried for Life-Cycle Assurance.

NEW QUESTION: 394
Which of the following best defines add-on security?
A. Physical security complementing logical security measures.
B. Protection mechanisms implemented as an integral part of an information system.
C. Layer security.
D. Protection mechanisms implemented after an information system has become operational.
Answer: D (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
The Internet Security Glossary (RFC2828) defines add-on security as "The retrofitting of protection mechanisms, implemented by hardware or software, after the [automatic data processing] system has become operational." Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 395
In a SSL session between a client and a server, who is responsible for generating the master secret that will be used as a seed to generate the symmetric keys that will be used during the session?
A. Both client and server
B. The client's browser
C. The web server
D. The merchant's Certificate Server
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
Once the merchant server has been authenticated by the browser client, the browser generates a master secret that is to be shared only between the server and client. This secret serves as a seed to generate the session (private) keys. The master secret is then encrypted with the merchant's public key and sent to the server. The fact that the master secret is generated by the client's browser provides the client assurance that the server is not reusing keys that would have been used in a previous session with another client.
Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 6: Cryptography (page 112). Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, page 569.

NEW QUESTION: 396
A momentary high voltage is a:
A. spike
B. blackout
C. surge
D. fault
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
Too much voltage for a short period of time is a spike.
Too much voltage for a long period of time is a surge.
Not enough voltage for a short period of time is a sag or dip
Not enough voltage for a long period of time is brownout
A short power interruption is a fault
A long power interruption is a blackout
You MUST know all of the power issues above for the purpose of the exam.
From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw-Hill/Osborne, 2005, page 368.

NEW QUESTION: 397

The major objective of system configuration management is which of the following?
A. system maintenance.
B. system stability.
C. system operations.
D. system tracking.
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
A major objective with Configuration Management is stability. The changes to the system are controlled so that they don't lead to weaknesses or faults in th system.
The following answers are incorrect:
system maintenance. Is incorrect because it is not the best answer. Configuration Management does control the changes to the system but it is not as important as the overall stability of the system.
system operations. Is incorrect because it is not the best answer, the overall stability of the system is much more important.
system tracking. Is incorrect because while tracking changes is important, it is not the best answer. The overall stability of the system is much more important.

NEW QUESTION: 398
Which of the following statements pertaining to a security policy is incorrect?
A. Its main purpose is to inform the users, administrators and managers of their obligatory requirements for protecting technology and information assets.
B. It specifies how hardware and software should be used throughout the organization.
C. It needs to have the acceptance and support of all levels of employees within the organization in order for it to be appropriate and effective.
D. It must be flexible to the changing environment.
Answer: (SHOW ANSWER)
A security policy would NOT define how hardware and software should be used throughout the organization. A standard or a procedure would provide such details but not a policy. A security policy is a formal statement of the rules that people who are given access to anorganization's technology and information assets must abide. The policy communicates the security goals to all of the users, the administrators, and the managers. The goals will be largely determined by the following key tradeoffs: services offered versus security provided, ease of use versus security, and cost of security versus risk of loss.
The main purpose of a security policy is to inform the users, the administrators and the managers of their obligatory requirements for protecting technology and information assets.
The policy should specify the mechanisms through which these requirements can be met. Another purpose is to provide a baseline from which to acquire, configure and audit computer systems and networks for compliance with the policy. In order for a security policy to be appropriate and effective, it needs to have the acceptance and support of all levels of employees within the organization. A good security policy must:

Be able to be implemented through system administration procedures, publishing of acceptable use guidelines, or other appropriate methods
Be able to be enforced with security tools, where appropriate, and with sanctions, where actual prevention is not technically feasible
Clearly define the areas of responsibility for the users, the administrators, and the managers
Be communicated to all once it is established
Be flexible to the changing environment of a computer network since it is a living document
Reference(s) used for this question:
National Security Agency, Systems and Network Attack Center (SNAC),The 60 Minute Network Security Guide, February 2002, page 7. or A local copy is kept at:
https://www.freepracticetests.org/documents/The%2060%20Minute%20Network%20Security%20Guide.pdf

NEW QUESTION: 399
Which TCSEC class specifies discretionary protection?
A. B2
B. B1
C. C2
D. C1
Answer: (SHOW ANSWER)
C1 involves discretionary protection, C2 involves controlled access protection, B1 involves labeled security protection and B2 involves structured protection. Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 400
The Terminal Access Controller Access Control System (TACACS) employs which of the following?
A. a user ID and static password for network access
B. a user ID and dynamic password for network access
C. a user ID and symmetric password for network access
D. a user ID and asymmetric password for network access
Answer: (SHOW ANSWER)
For networked applications, the Terminal Access Controller Access Control System (TACACS) employs a user ID and a static password for network access.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 44.

NEW QUESTION: 401
Which of the following should NOT be performed by an operator?
A. Implementing the initial program load
B. Monitoring execution of the system
C. Data entry

D. Controlling job flow

E. Explanation:

Under the principle of separation of duties, an operator should not be performing data entry. This should be left to data entry personnel.

System operators represent a class of users typically found in data center environments where mainframe systems are used. They provide day-to-day operations of the mainframe environment, ensuring that scheduled jobs are running effectively and troubleshooting problems that may arise. They also act as the arms and legs of the mainframe environment, load and unloading tape and results of job print runs. Operators have elevated privileges, but less than those of system administrators. If misused, these privileges may be used to circumvent the system's security policy. As such, use of these privileges should be monitored through audit logs.

Some of the privileges and responsibilities assigned to operators include:

Implementing the initial program load: This is used to start the operating system. The boot process or initial program load of a system is a critical time for ensuring system security. Interruptions to this process may reduce the integrity of the system or cause the system to
crash, precluding its availability.

Monitoring execution of the system: Operators respond to various events, to include errors, interruptions, and job completion messages.

Volume mounting: This allows the desired application access to the system and its data.

Controlling job flow: Operators can initiate, pause, or terminate programs. This may allow an operator to affect the scheduling of jobs. Controlling job flow involves the manipulation of configuration information needed by the system. Operators with the ability to control a job or application can cause output to be altered or diverted, which can threaten the confidentiality.

Bypass label processing: This allows the operator to bypass security label information to run foreign tapes (foreign tapes are those from a different data center that would not be using the same label format that the system could run). This privilege should be strictly controlled to prevent unauthorized access.

Renaming and relabeling resources: This is sometimes necessary in the mainframe environment to allow programs to properly execute. Use of this privilege should be monitored, as it can allow the unauthorized viewing of sensitive information.

Reassignment of ports and lines: Operators are allowed to reassign ports or lines. If misused, reassignment can cause program errors, such as sending sensitive output to an unsecured location. Furthermore, an incidental port may be opened, subjecting the system to an attack through the creation of a new entry point into the system.

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 19367-19395). Auerbach Publications. Kindle Edition.

Which of the following should be performed by an operator?

A. Changing profiles

B. Approving changes
C. Adding and removal of users
D. Installing system software
Answer: (SHOW ANSWER)
Of the listed tasks, installing system software is the only task that should normally be performed by an operator in a properly segregated environment. Source: MOSHER, Richard & ROTHKE, Ben, CISSP CBK Review presentation on domain
7.

NEW QUESTION: 402
Which of the following forms of authentication would most likely apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier?
A. Dynamic authentication
B. Continuous authentication
C. Encrypted authentication
D. Robust authentication
Answer: B (LEAVE A REPLY)
Continuous authentication is a type of authentication that provides protection against impostors who can see, alter, and insert information passed between the claimant and verifier even after the claimant/verifier authentication is complete. These are typically referred to as active attacks, since they assume that the imposter can actively influence the connection between claimant and verifier. One way to provide this form of authentication is to apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier. There are other combinations of cryptography that can provide this form of authentication but current strategies rely on applying some type of cryptography to every bit of data sent. Otherwise, any unprotected bit would be suspect. Robust authentication relies on dynamic authentication data that changes with each authenticated session between a claimant and a verifier, but does not provide protection against active attacks. Encrypted authentication is a distracter. Source: GUTTMAN, Barbara & BAGWILL, Robert, NIST Special Publication 800-xx, Internet Security Policy: A Technical Guide, Draft Version, May 25, 2000 (page 34).

NEW QUESTION: 403
A public key algorithm that does both encryption and digital signature is which of the following?
A. RSA
B. DES
C. IDEA
D. Diffie-Hellman
Answer: (SHOW ANSWER)
RSA can be used for encryption, key exchange, and digital signatures. Key Exchange versus key Agreement
KEY EXCHANGE Key exchange (also known as "key establishment") is any method in cryptography by which cryptographic keys are exchanged between users, allowing use of a cryptographic algorithm.

If sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received. The nature of the equipping they require depends on the encryption technique they might use. If they use a code, both will require a copy of the same codebook. If they use a cipher, they will need appropriate keys. If the cipher is a symmetric key cipher, both will need a copy of the same key. If an asymmetric key cipher with the public/private key property, both will need the other's public key.
KEY AGREEMENT Diffie-Hellman is a key agreement algorithm used by two parties to agree on a shared secret. The Diffie Hellman (DH) key agreement algorithm describes a means for two parties to agree upon a shared secret over a public network in such a way that the secret will be unavailable to eavesdroppers. The DH algorithm converts the shared secret into an arbitrary amount of keying material. The resulting keying material is used as a symmetric encryption key.
The other answers are not correct because:
DES and IDEA are both symmetric algorithms.
Diffie-Hellman is a common asymmetric algorithm, but is used only for key agreement. It is not typically used for data encryption and does not have digital signature capability.
References:
http://tools.ietf.org/html/rfc2631
For Diffie-Hellman information: http://www.netip.com/articles/keith/diffie-helman.htm

NEW QUESTION: 404
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: (SHOW ANSWER)
Explanation/Reference:
Controls are implemented to mitigate risk and reduce the potential for loss. Preventive controls are put in place to inhibit harmful occurrences; detective controls are established to discover harmful occurrences; corrective controls are used to restore systems that are victims of harmful attacks.
It is not feasible and possible to eliminate all risks and the potential for loss as risk/threats are constantly changing.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 32.

NEW QUESTION: 405
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)
Section: Access Control
Explanation/Reference:
Radius, TACACS and DIAMETER are classified as authentication, authorization, and accounting (AAA) servers.
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 33.
also see:
The term "AAA" is often used, describing cornerstone concepts [of the AIC triad] Authentication, Authorization, and Accountability. Left out of the AAA acronym is Identification which is required before the three "A's" can follow. Identity is a claim, Authentication proves an identity, Authorization describes the action you can perform on a system once you have been identified and authenticated, and accountability holds users accountable for their actions.
Reference: CISSP Study Guide, Conrad Misenar, Feldman p. 10-11, (c) 2010 Elsevier.

NEW QUESTION: 406
Which of the following is a problem regarding computer investigation issues?
A. Information is tangible.
B. Evidence is easy to gather.
C. Computer-generated records are only considered secondary evidence, thus are not as reliable as best evidence.
D. In many instances, an expert or specialist is not required.
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
Because computer-generated records normally fall under the category of hearsay evidence because they cannot be proven accurate and reliable this can be a problem.
Under the U.S. Federal Rules of Evidence, hearsay evidence is generally not admissible in court. This inadmissibility is known as the hearsay rule, although there are some exceptions for how, when, by whom and in what circumstances data was collected.
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).
IMPORTANT NOTE:
For the purpose of the exam it is very important to remember the Business Record exemption to the Hearsay Rule. For example: if you create log files and review them on a regular basis as part of a business process, such files would be admissable in court and they would not be considered hearsay because they were made in the course of regular business and it is part of regular course of business to create such record.
Here is another quote from the HISM book:
Business Record Exemption to the Hearsay Rule

Federal Rules of Evidence 803(6) allow a court to admit a report or other business document made at or near the time by or from information transmitted by a person with knowledge, if kept in the course of regularly conducted business activity, and if it was the regular practice of that business activity to make the [report or document], all as shown by testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness.
To meet Rule 803(6) the witness must:
* Have custody of the records in question on a regular basis.
* Rely on those records in the regular course of business.
* Know that they were prepared in the regular course of business.
Audit trails meet the criteria if they are produced in the normal course of business. The process to produce the output will have to be proven to be reliable. If computer-generated evidence is used and admissible, the court may order disclosure of the details of the computer, logs, and maintenance records in respect to the system generating the printout, and then the defense may use that material to attack the reliability of the evidence. If the audit trails are not used or reviewed - at least the exceptions (e.g., failed log-on attempts) - in the regular course of business, they do not meet the criteria for admissibility.
Federal Rules of Evidence 1001(3) provide another exception to the hearsay rule. This rule allows a memory or disk dump to be admitted as evidence, even though it is not done in the regular course of business. This dump merely acts as statement of fact. System dumps (in binary or hexadecimal) are not hearsay because they are not being offered to prove the truth of the contents, but only the state of the computer.
BUSINESS RECORDS LAW EXAMPLE:
The business records law was enacted in 1931 (PA No. 56). For a document to be admissible under the statute, the proponent must show: (1) the document was made in the regular course of business; (2) it was the regular course of business to make the record; and (3) the record was made when the act, transaction, or event occurred, or shortly thereafter (State v. Vennard, 159 Conn. 385, 397 (1970); Mucci v. LeMonte, 157 Conn. 566, 570 (1969). The failure to establish any one of these essential elements renders the document inadmissible under the statute (McCahill v. Town and Country Associates, Ltd. , 185 Conn. 37 (1981); State v.
Peary, 176 Conn. 170 (1978); Welles v. Fish Transport Co. , , 123 Conn. 49 (1937).
The statute expressly provides that the person who made the business entry does not have to be unavailable as a witness and the proponent does not have to call as a witness the person who made the record or show the person to be unavailable (State v. Jeustiniano, 172 Conn. 275 (1977).
The person offering the business records as evidence does not have to independently prove the trustworthiness of the record. But, there is no presumption that the record is accurate; the record's accuracy and weight are issues for the trier of fact (State v. Waterman, 7 Conn. App. 326 (1986); Handbook of Connecticut Evidence, Second Edition, s 11. 14. 3).
Reference: http://search.cga.state.ct.us/dtsearch_lpa.asp?cmd=getdoc&DocId=16833&Index=I%3A%5Czindex
%5C1995&HitCount=0&hits=&hc=0&req=&Item=712

NEW QUESTION: 407
Which of the following is true about Kerberos?
A. It utilizes public key cryptography.
B. It encrypts data after a ticket is granted, but passwords are exchanged in plain text.
C. It depends upon symmetric ciphers.
D. It is a second party authentication system.
Answer: (SHOW ANSWER)
Kerberos depends on secret keys (symmetric ciphers). Kerberos is a third party authentication protocol. It was designed and developed in the mid 1980's by MIT. It is considered open source but is copyrighted and owned by MIT. It relies on the user's secret keys. The password is used to encrypt and decrypt the keys.
The following answers are incorrect:
It utilizes public key cryptography. Is incorrect because Kerberos depends on secret keys (symmetric ciphers).
It encrypts data after a ticket is granted, but passwords are exchanged in plain text. Is incorrect because the passwords are not exchanged but used for encryption and decryption of the keys.
It is a second party authentication system. Is incorrect because Kerberos is a third party authentication system, you authenticate to the third party (Kerberos) and not the system you are accessing.
References:
MIT http://web.mit.edu/kerberos/
Wikipedi http://en.wikipedia.org/wiki/Kerberos_%28protocol%29
OIG CBK Access Control (pages 181 - 184)
AIOv3 Access Control (pages 151 - 155)

NEW QUESTION: 408
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: (SHOW 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: 409
What is a packet sniffer?
A. It tracks network connections to off-site locations.
B. It monitors network traffic for illegal packets.
C. It scans network segments for cabling faults.
D. It captures network traffic for later analysis.
Answer: D (LEAVE A REPLY)
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 410
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: (SHOW ANSWER)
Explanation/Reference:
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.