SSCP Q&As

System Security Certified Practitioner (SSCP)

Pass ISC SSCP Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/SSCP.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by ISC Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

Correct Answer: D

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.

QUESTION 2

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.

Correct Answer: B

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

QUESTION 3

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

Correct Answer: A

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. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Chapter 7: Applications and Systems Development (page 264).

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

QUESTION 4

What algorithm was DES derived from?

A. Twofish.

B. Skipjack.

C. Brooks-Aldeman.

D. Lucifer.

Correct Answer: D

NSA took the 128-bit algorithm Lucifer that IBM developed, reduced the key size to 64 bits and with that developed DES.

The following answers are incorrect:

Twofish. This is incorrect because Twofish is related to Blowfish as a possible replacement for DES.

Skipjack. This is incorrect, Skipjack was developed after DES by the NSA .

Brooks-Aldeman. This is incorrect because this is a distractor, no algorithm exists with this name.

QUESTION 5

Which of the following is not a logical control when implementing logical access security?

A. access profiles.

B. userids.

C. employee badges.

D. passwords.

Correct Answer: C

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.

QUESTION 6

Which of the following statements is NOT true of IPSec Transport mode?

A. It is required for gateways providing access to internal systems

B. Set-up when end-point is host or communications terminates at end-points

C. If used in gateway-to-host communication, gateway must act as host

D. When ESP is used for the security protocol, the hash is only applied to the upper layer protocols contained in the packet

Correct Answer: A

Source: TIPTON, Harold F. and KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Pages 166-167.

QUESTION 7

A periodic review of user account management should not determine:

A. Conformity with the concept of least privilege.

B. Whether active accounts are still being used.

C. Strength of user-chosen passwords.

D. Whether management authorizations are up-to-date.

Correct Answer: C

Organizations should have a process for (1) requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.

Reviews should examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up- to-date, whether required training has been completed, and so forth. These reviews can be conducted on at least two levels: (1) on an application-by-application basis, or (2) on a system wide basis. The strength of user passwords is beyond the scope of a simple user account management review, since it requires specific tools to try and crack the password file/database through either a dictionary or brute-force attack in order to check

the strength of passwords.

Reference(s) used for this question:

SWANSON, Marianne and 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 28).

QUESTION 8

Which of the following would constitute the best example of a password to use for access to a system by a network administrator?

A. holiday

B. Christmas12

C. Jenny

D. GyN19Za!

Correct Answer: D

GyN19Za! would be the the best answer because it contains a mixture of upper and lower case characters, alphabetic and numeric characters, and a special character making it less vulnerable to password attacks.

All of the other answers are incorrect because they are vulnerable to brute force or dictionary attacks. Passwords should not be common words or names. The addition of a number to the end of a common word only marginally strengthens it because a common password attack would also check combinations of words:

Christmas23 Christmas123 etc...

QUESTION 9

Which of the following access control models is based on sensitivity labels?

A. Discretionary access control

B. Mandatory access control

C. Rule-based access control

D. Role-based access control

Correct Answer: B

Access decisions are made based on the clearance of the subject and the sensitivity label of the object.

Example: Eve has a "Secret" security clearance and is able to access the "Mugwump Missile Design Profile" because its sensitivity label is "Secret." She is denied access to the "Presidential Toilet Tissue Formula" because its sensitivity label

is "Top Secret."

The other answers are not correct because:

Discretionary Access Control is incorrect because in DAC access to data is determined by the data owner. For example, Joe owns the "Secret Chili Recipe" and grants read access to Charles.

Role Based Access Control is incorrect because in RBAC access decsions are made based on the role held by the user. For example, Jane has the role "Auditor" and that role includes read permission on the "System Audit Log."

Rule Based Access Control is incorrect because it is a form of MAC. A good example would be a Firewall where rules are defined and apply to anyone connecting through the firewall.

References:

All in One third edition, page 164.

Official ISC2 Guide page 187.

QUESTION 10

A prolonged power supply that is below normal voltage is a:

A. brownout

B. blackout

C. surge

D. fault

Correct Answer: A

A prolonged power supply that is below normal voltage is a brownout.

From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw- Hill/Osborne, 2005, page 368.

QUESTION 11

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.

Correct Answer: B

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).

QUESTION 12

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.

Correct Answer: A

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)

QUESTION 13

Which of the following statements pertaining to a Criticality Survey is incorrect?

A. It is implemented to gather input from all personnel that is going to be part of the recovery teams.

B. The purpose of the survey must be clearly stated.

C. Management\\'s approval should be obtained before distributing the survey.

D. Its intent is to find out what services and systems are critical to keeping the organization in business.

Correct Answer: A

The Criticality Survey is implemented through a standard questionnaire to gather input from the most knowledgeable people. Not all personnel that is going to be part of recovery teams is necessarily able to help in identifying critical functions

of the organization. The intent of such a survey is to identify the services and systems that are critical to the organization.

Having a clearly stated purpose for the survey helps in avoiding misinterpretations.

Management\\'s approval of the survey should be obtained before distributing it.

Source: HARE, Chris, CISSP Study Guide: Business Continuity Planning Domain,

QUESTION 14

A common way to create fault tolerance with leased lines is to group several T1s together with an inverse multiplexer placed:

A. at one end of the connection.

B. at both ends of the connection.

C. somewhere between both end points.

D. in the middle of the connection.

Correct Answer: B

A common way to create fault tolerance with leased lines is to group several T1s together with an inverse multiplexer placed at both ends of the connection.

In fact it would be a Multiplexer at one end and DeMultiplexer at other end or vice versa. Inverse Multiplexer at both end.

In electronics, a multiplexer (or mux) is a device that selects one of several analog or digital input signals and forwards the selected input into a single line. A multiplexer of 2n inputs has n select lines, which are used to select which input line

to send to the output. Multiplexers are mainly used to increase the amount of data that can be sent over the network within a certain amount of time and bandwidth. A multiplexer is also called a data selector.

An electronic multiplexer makes it possible for several signals to share one device or resource, for example one A/D converter or one communication line, instead of having one device per input signal.

On the other hand, a demultiplexer (or demux) is a device taking a single input signal and selecting one of many data-output-lines, which is connected to the single input. A multiplexer is often used with a complementary demultiplexer on the

receiving end.

An electronic multiplexer can be considered as a multiple-input, single-output switch, and a demultiplexer as a single-input, multiple-output switch References:

KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley and Sons, Page 72.

and

https://secure.wikimedia.org/wikipedia/en/wiki/Multiplexer

QUESTION 15

Which of the following backup methods is most appropriate for off-site archiving?

A. Incremental backup method

B. Off-site backup method

C. Full backup method

D. Differential backup method

Correct Answer: C

The full backup makes a complete backup of every file on the system every time it is run. Since a single backup set is needed to perform a full restore, it is appropriate for off-site archiving.

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Chapter 3: Telecommunications and Network Security (page 69).

QUESTION 16

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

Correct Answer: D

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).

QUESTION 17

What is called the use of technologies such as fingerprint, retina, and iris scans to authenticate the individuals requesting access to resources?

A. Micrometrics

B. Macrometrics

C. Biometrics

D. MicroBiometrics

Correct Answer: C

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley and Sons, Page 35.

QUESTION 18

What does it mean to say that sensitivity labels are "incomparable"?

A. The number of classification in the two labels is different.

B. Neither label contains all the classifications of the other.

C. the number of categories in the two labels are different.

D. Neither label contains all the categories of the other.

Correct Answer: D

If a category does not exist then you cannot compare it. Incomparable is when you have two disjointed sensitivity labels, that is a category in one of the labels is not in the other label. "Because neither label contains all the categories of the

other, the labels can\\'t be compared.

They\\'re said to be incomparable"

COMPARABILITY:

The label:

TOP SECRET [VENUS ALPHA]

is "higher" than either of the labels:

SECRET [VENUS ALPHA] TOP SECRET [VENUS]

But you can\\'t really say that the label:

TOP SECRET [VENUS]

is higher than the label:

SECRET [ALPHA]

Because neither label contains all the categories of the other, the labels can\\'t be compared. They\\'re said to be incomparable. In a mandatory access control system, you won\\'t be allowed access to a file whose label is incomparable to your

clearance.

The Multilevel Security policy uses an ordering relationship between labels known as the dominance relationship. Intuitively, we think of a label that dominates another as being "higher" than the other. Similarly, we think of a label that is

dominated by another as being "lower" than the other. The dominance relationship is used to determine permitted operations and information flows.

DOMINANCE

The dominance relationship is determined by the ordering of the Sensitivity/Clearance component of the label and the intersection of the set of Compartments.

Sample Sensitivity/Clearance ordering are:

Top Secret > Secret > Confidential > Unclassified

s3 > s2 > s1 > s0

Formally, for label one to dominate label 2 both of the following must be true:

The sensitivity/clearance of label one must be greater than or equal to the sensitivity/clearance of label two.

The intersection of the compartments of label one and label two must equal the compartments of label two.

Additionally:

Two labels are said to be equal if their sensitivity/clearance and set of compartments are exactly equal. Note that dominance includes equality. One label is said to strictly dominate the other if it dominates the other but is not equal to the

other.

Two labels are said to be incomparable if each label has at least one compartment that is not included in the other\\'s set of compartments.

The dominance relationship will produce a partial ordering over all possible MLS labels, resulting in what is known as the MLS Security Lattice.

The following answers are incorrect:

The number of classification in the two labels is different. Is incorrect because the categories are what is being compared, not the classifications.

Neither label contains all the classifications of the other. Is incorrect because the categories are what is being compared, not the classifications.

the number of categories in the two labels is different. Is incorrect because it is possibe a category exists more than once in one sensitivity label and does exist in the other so they would be comparable.

Reference(s) used for this question:

OReilly - Computer Systems and Access Control (Chapter 3) http://www.oreilly.com/catalog/csb/chapter/ ch03.html and

http://rubix.com/cms/mls_dom

QUESTION 19

What is the maximum number of different keys that can be used when encrypting with Triple DES?

A. 1

B. 2

C. 3

D. 4

Correct Answer: C

Triple DES encrypts a message three times. This encryption can be accomplished in several ways. The most secure form of triple DES is when the three encryptions are performed with three different keys. Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Chapter 4: Cryptography (page 152).

QUESTION 20

Which backup method only copies files that have been recently added or changed and also leaves the archive bit unchanged?

A. Full backup method

B. Incremental backup method

C. Fast backup method

D. Differential backup method

Correct Answer: D

A differential backup is a partial backup that copies a selected file to tape only if the archive bit for that file is turned on, indicating that it has changed since the last full backup. A differential backup leaves the archive bits unchanged on the files it copies.

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Chapter 3: Telecommunications and Network Security (page 69).

Also see: http://e-articles.info/e/a/title/Backup-Types/

Backup software can use or ignore the archive bit in determining which files to back up, and can either turn the archive bit off or leave it unchanged when the backup is complete. How the archive bit is used and manipulated determines what type of backup is done, as follows

Full backup

A full backup, which Microsoft calls a normal backup, backs up every selected file, regardless of the status of the archive bit. When the backup completes, the backup software turns off the archive bit for every file that was backed up. Note that "full" is a misnomer because a full backup backs up only the files you have selected, which may be as little as one directory or even a single file, so in that sense Microsoft\\'s terminology is actually more accurate. Given the choice, full backup is the method to use because all files are on one tape, which makes it much easier to retrieve files from tape when necessary. Relative to partial backups, full backups also increase redundancy because all files are on all tapes. That means that if one tape fails, you may still be able to retrieve a given file from another tape.

Differential backup

A differential backup is a partial backup that copies a selected file to tape only if the archive bit for that file is turned on, indicating that it has changed since the last full backup. A differential backup leaves the archive bits unchanged on the files it copies. Accordingly, any differential backup set contains all files that have changed since the last full backup. A differential backup set run soon after a full backup will contain relatively few files. One run soon before the next full backup is due will contain many files, including those contained on all previous differential backup sets since the last full backup. When you use differential backup, a complete backup set comprises only two tapes or tape sets: the tape that contains the last full backup and the tape that contains the most recent differential backup.

Incremental backup

An incremental backup is another form of partial backup. Like differential backups, Incremental Backups copy a selected file to tape only if the archive bit for that file is turned on. Unlike the differential backup, however, the incremental backup clears the archive bits for the files it backs up. An incremental backup set therefore contains only files that have changed since the last full backup or the last incremental backup. If you run an incremental backup daily, files changed on Monday are on the Monday tape, files changed on Tuesday are on the Tuesday tape, and so forth. When you use an incremental backup scheme, a complete backup set comprises the tape that contains the last full backup and all of the tapes that contain every incremental backup done since the last normal backup. The only advantages of incremental backups are that they minimize backup time and keep multiple versions of files that change frequently. The disadvantages are that backed-up files are scattered across multiple tapes, making it difficult to locate any particular file you need to restore, and that there is no redundancy. That is, each file is stored only on one tape.

Full copy backup

A full copy backup (which Microsoft calls a copy backup) is identical to a full backup except for the last step. The full backup finishes by turning off the archive bit on all files that have been backed up. The full copy backup instead leaves the archive bits unchanged. The full copy backup is useful only if you are using a combination of full backups and incremental or differential partial backups. The full copy backup allows you to make a duplicate "full" backup--e.g., for storage offsite, without altering the state of the hard drive you are backing up, which would destroy the integrity of the partial backup rotation.

Some Microsoft backup software provides a bizarre backup method Microsoft calls a daily copy backup. This method ignores the archive bit entirely and instead depends on the date- and timestamp of files to determine which files should be backed up. The problem is, it\\'s quite possible for software to change a file without changing the date- and timestamp, or to change the date- and timestamp without changing the contents of the file. For this reason, we regard the daily copy backup as entirely unreliable and recommend you avoid using it.

QUESTION 21

Related to information security, the prevention of the intentional or unintentional unauthorized disclosure of contents is which of the following?

A. Confidentiality

B. Integrity

C. Availability

D. capability

Correct Answer: A

Confidentiality is the prevention of the intentional or unintentional unauthorized disclosure of contents.

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley and Sons, Page 60.

QUESTION 22

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.

Correct Answer: C

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. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley and Sons, Page 38.

QUESTION 23

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

Correct Answer: C

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. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Chapter 5: Security Architecture and Models (page 205).

QUESTION 24

Which of the following is NOT a type of motion detector?

A. Photoelectric sensor

B. Passive infrared sensors

C. Microwave Sensor.

D. Ultrasonic Sensor.

Correct Answer: A

A photoelectric sensor does not "directly" sense motion there is a narrow beam that won\\'t set off the sensor unless the beam is broken. Photoelectric sensors, along with dry contact switches, are a type of perimeter intrusion detector.

All of the other answers are valid types of motion detectors types. The content below on the different types of sensors is from Wikepedia: Indoor Sensors These types of sensors are designed for indoor use. Outdoor use would not be advised due to false alarm vulnerability and weather durability.Passive infrared detectors

Passive Infrared Sensor

The passive infrared detector (PIR) is one of the most common detectors found in household and small business environments because it offers affordable and reliable functionality. The term passive means the detector is able to function without the need to generate and radiate its own energy (unlike ultrasonic and microwave volumetric intrusion detectors that are "active" in operation). PIRs are able to distinguish if an infrared emitting object is present by first learning the ambient temperature of the monitored space and then detecting a change in the temperature caused by the presence of an object. Using the principle of differentiation, which is a check of presence or nonpresence, PIRs verify if an intruder or object is actually there. Creating individual zones of detection where each zone comprises one or more layers can achieve differentiation. Between the zones there are areas of no sensitivity (dead zones) that are used by the sensor for comparison.

Ultrasonic detectors

Using frequencies between 15 kHz and 75 kHz, these active detectors transmit ultrasonic sound waves that are inaudible to humans. The Doppler shift principle is the underlying method of operation, in which a change in frequency is detected due to object motion. This is caused when a moving object changes the frequency of sound waves around it. Two conditions must occur to successfully detect a Doppler shift event:

There must be motion of an object either towards or away from the receiver. The motion of the object must cause a

change in the ultrasonic frequency to the receiver relative to the transmitting frequency.

The ultrasonic detector operates by the transmitter emitting an ultrasonic signal into the area to be protected. The sound waves are reflected by solid objects (such as the surrounding floor, walls and ceiling) and then detected by the receiver. Because ultrasonic waves are transmitted through air, then hard- surfaced objects tend to reflect most of the ultrasonic energy, while soft surfaces tend to absorb most energy.

When the surfaces are stationary, the frequency of the waves detected by the receiver will be equal to the transmitted frequency. However, a change in frequency will occur as a result of the Doppler principle, when a person or object is moving towards or away from the detector. Such an event initiates an alarm signal. This technology is considered obsolete by many alarm professionals, and is not actively installed.

Microwave detectors

This device emits microwaves from a transmitter and detects any reflected microwaves or reduction in beam intensity using a receiver. The transmitter and receiver are usually combined inside a single housing (monostatic) for indoor applications, and separate housings (bistatic) for outdoor applications. To reduce false alarms this type of detector is usually combined with a passive infrared detector or "Dualtec" alarm.

Microwave detectors respond to a Doppler shift in the frequency of the reflected energy, by a phase shift, or by a sudden reduction of the level of received energy. Any of these effects may indicate motion of an intruder.

Photo-electric beams

Photoelectric beam systems detect the presence of an intruder by transmitting visible or infrared light beams across an area, where these beams may be obstructed. To improve the detection surface area, the beams are often employed in stacks of two or more. However, if an intruder is aware of the technology\\'s presence, it can be avoided. The technology can be an effective long- range detection system, if installed in stacks of three or more where the transmitters and receivers are staggered to create a fence-like barrier. Systems are available for both internal and external applications. To prevent a clandestine attack using a secondary light source being used to hold the detector in a \\'sealed\\' condition whilst an intruder passes through, most systems use and detect a modulated light source. Glass break detectors

The glass break detector may be used for internal perimeter building protection. When glass breaks it generates sound in a wide band of frequencies. These can range from infrasonic, which is below 20 hertz (Hz) and can not be heard by the human ear, through the audio band from 20 Hz to 20 kHz which humans can hear, right up to ultrasonic, which is above 20 kHz and again cannot be heard. Glass break acoustic detectors are mounted in close proximity to the glass panes and listen for sound frequencies associated with glass breaking. Seismic glass break detectors are different in that they are installed on the glass pane. When glass breaks it produces specific shock frequencies which travel through the glass and often through the window frame and the surrounding walls and ceiling. Typically, the most intense frequencies generated are between 3 and 5 kHz, depending on the type of glass and the presence of a plastic interlayer. Seismic glass break detectors "feel" these shock frequencies and in turn generate an alarm condition.

The more primitive detection method involves gluing a thin strip of conducting foil on the inside of the glass and putting low-power electrical current through it. Breaking the glass is practically guaranteed to tear the foil and break the circuit.

Smoke, heat, and carbon monoxide detectors

Heat Detection System

Most systems may also be equipped with smoke, heat, and/or carbon monoxide detectors. These are also known as 24 hour zones (which are on at all times). Smoke detectors and heat detectors protect from the risk of fire and carbon

monoxide detectors protect from the risk of carbon monoxide. Although an intruder alarm panel may also have these detectors connected, it may not meet all the local fire code requirements of a fire alarm system.

Other types of volumetric sensors could be:

Active Infrared Passive Infrared/Microware combined Radar Accoustical Sensor/Audio Vibration Sensor (seismic) Air Turbulence

QUESTION 25

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

A. The Waterfall model

B. The modified Waterfall model

C. The Spiral model

D. The Critical Path Model (CPM)

Correct Answer: C

The spiral model is actually a meta-model that incorporates a number of the software development models. This model depicts a spiral that incorporates the various phases of software development. The model states that each cycle of the spiral involves the same series of steps for each part of the project. CPM refers to the Critical Path Methodology.

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Chapter 7: Applications and Systems Development (page 246).

QUESTION 26

Knowledge-based Intrusion Detection Systems (IDS) are more common than:

A. Network-based IDS

B. Host-based IDS

C. Behavior-based IDS

D. Application-Based IDS

Correct Answer: C

Knowledge-based IDS are more common than behavior-based ID systems.

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley and Sons, Page 63.

Application-Based IDS - "a subset of HIDS that analyze what\\'s going on in an application using the transaction log files of the application." Source: Official ISC2 CISSP CBK Review Seminar Student Manual Version 7.0 p. 87

Host-Based IDS - "an implementation of IDS capabilities at the host level. Its most significant difference from NIDS is intrusion detection analysis, and related processes are limited to the boundaries of the host." Source: Official ISC2 Guide to

the CISSP CBK - p. 197

Network-Based IDS - "a network device, or dedicated system attached to the network, that monitors traffic traversing the network segment for which it is integrated." Source: Official ISC2 Guide to the CISSP CBK - p. 196

CISSP for dummies a book that we recommend for a quick overview of the 10 domains has nice and concise coverage of the subject:

Intrusion detection is defined as real-time monitoring and analysis of network activity and data for potential vulnerabilities and attacks in progress. One major limitation of current intrusion detection system (IDS) technologies is the requirement

to filter false alarms lest the operator (system or security administrator) be overwhelmed with data. IDSes are classified in many different ways, including active and passive, network- based and host-based, and knowledge- based and behavior-based:

Active and passive IDS An active IDS (now more commonly known as an intrusion prevention system -- IPS) is a system that\\'s configured to automatically block suspected attacks in progress without any intervention required by an operator. IPS has the advantage of providing real-time corrective action in response to an attack but has many disadvantages as well. An IPS must be placed in- line along a network boundary; thus, the IPS itself is susceptible to attack. Also, if false alarms and legitimate traffic haven\\'t been properly identified and filtered, authorized users and applications may be improperly denied access. Finally, the IPS itself may be used to effect a Denial of Service (DoS) attack by intentionally flooding the system with alarms that cause it to block connections until no connections or bandwidth are available.

A passive IDS is a system that\\'s configured only to monitor and analyze network traffic activity and alert an operator to potential vulnerabilities and attacks. It isn\\'t capable of performing any protective or corrective functions on its own. The major advantages of passive IDSes are that these systems can be easily and rapidly deployed and are not normally susceptible to attack themselves.

Network-based and host-based IDS

A network-based IDS usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous mode and a separate management interface. The IDS is placed along a network segment or boundary

and monitors all traffic on that segment.

A host-based IDS requires small programs (or agents) to be installed on individual systems to be monitored. The agents monitor the operating system and write data to log files and/or trigger alarms. A host-based IDS can only monitor the

individual host systems on which the agents are installed; it doesn\\'t monitor the entire network.

Knowledge-based and behavior-based IDS

A knowledge-based (or signature-based) IDS references a database of previous attack profiles and known system vulnerabilities to identify active intrusion attempts. Knowledge-based IDS is currently more common than behavior-based IDS.

Advantages of knowledge-based systems include the following:

It has lower false alarm rates than behavior-based IDS.

Alarms are more standardized and more easily understood than behavior-based IDS.

Disadvantages of knowledge-based systems include these:

Signature database must be continually updated and maintained.

New, unique, or original attacks may not be detected or may be improperly classified.

A behavior-based (or statistical anomalybased) IDS references a baseline or learned pattern of normal system activity to identify active intrusion attempts. Deviations from this baseline or pattern cause an alarm to be triggered.

Advantages of behavior-based systems include that they

Dynamically adapt to new, unique, or original attacks.

Are less dependent on identifying specific operating system vulnerabilities.

Disadvantages of behavior-based systems include

Higher false alarm rates than knowledge-based IDSes.

Usage patterns that may change often and may not be static enough to implement an effective behavior- based IDS.

QUESTION 27

Which of the following is the most critical item from a disaster recovery point of view?

A. Data

B. Hardware/Software

C. Communication Links

D. Software Applications

Correct Answer: A

The most important point is ALWAYS the data. Everything else can be replaced or repaired.

Data MUST be backed up, backups must be regularly tested, because once it is truly lost, it is lost forever.

The goal of disaster recovery is to minimize the effects of a disaster or disruption. It means taking the necessary steps to ensure that the resources, personnel, and business processes are able to resume operation in a timely manner . This is

different from continuity planning, which provides methods and procedures for dealing with longer-term outages and disasters.

The goal of a disaster recovery plan is to handle the disaster and its ramifications right after the disaster hits; the disaster recovery plan is usually very information technology (IT) focused. A disaster recovery plan (DRP) is carried out when

everything is still in emergency mode, and everyone is scrambling to get all critical systems back online.

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 887). McGraw-Hill.

Kindle Edition.

and

Veritas eLearning CD - Introducing Disaster Recovery Planning, Chapter 1.

QUESTION 28

Which of the following protects Kerberos against replay attacks?

A. Tokens

B. Passwords

C. Cryptography

D. Time stamps

Correct Answer: D

A replay attack refers to the recording and retransmission of packets on the network. Kerberos uses time stamps, which protect against this type of attack. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter

8: Cryptography (page 581).

QUESTION 29

What is used to bind a document to its creation at a particular time?

A. Network Time Protocol (NTP)

B. Digital Signature

C. Digital Timestamp

D. Certification Authority (CA)

Correct Answer: C

While a digital signature binds a document to the possessor of a particular key, a digital timestamp binds a document to its creation at a particular time.

Trusted timestamping is the process of securely keeping track of the creation and modification time of a document. Security here means that no one -- not even the owner of the document -- should be able to change it once it has been

recorded provided that the timestamper\\'s integrity is never compromised.

The administrative aspect involves setting up a publicly available, trusted timestamp management infrastructure to collect, process and renew timestamps or to make use of a commercially available time stamping service.

A modern example of using a Digital Timestamp is the case of an industrial research organization that may later need to prove, for patent purposes, that they made a particular discovery on a particular date; since magnetic media can be

altered easily, this may be a nontrivial issue. One possible solution is for a researcher to compute and record in a hardcopy laboratory notebook a cryptographic hash of the relevant data file. In the future, should there be a need to prove the

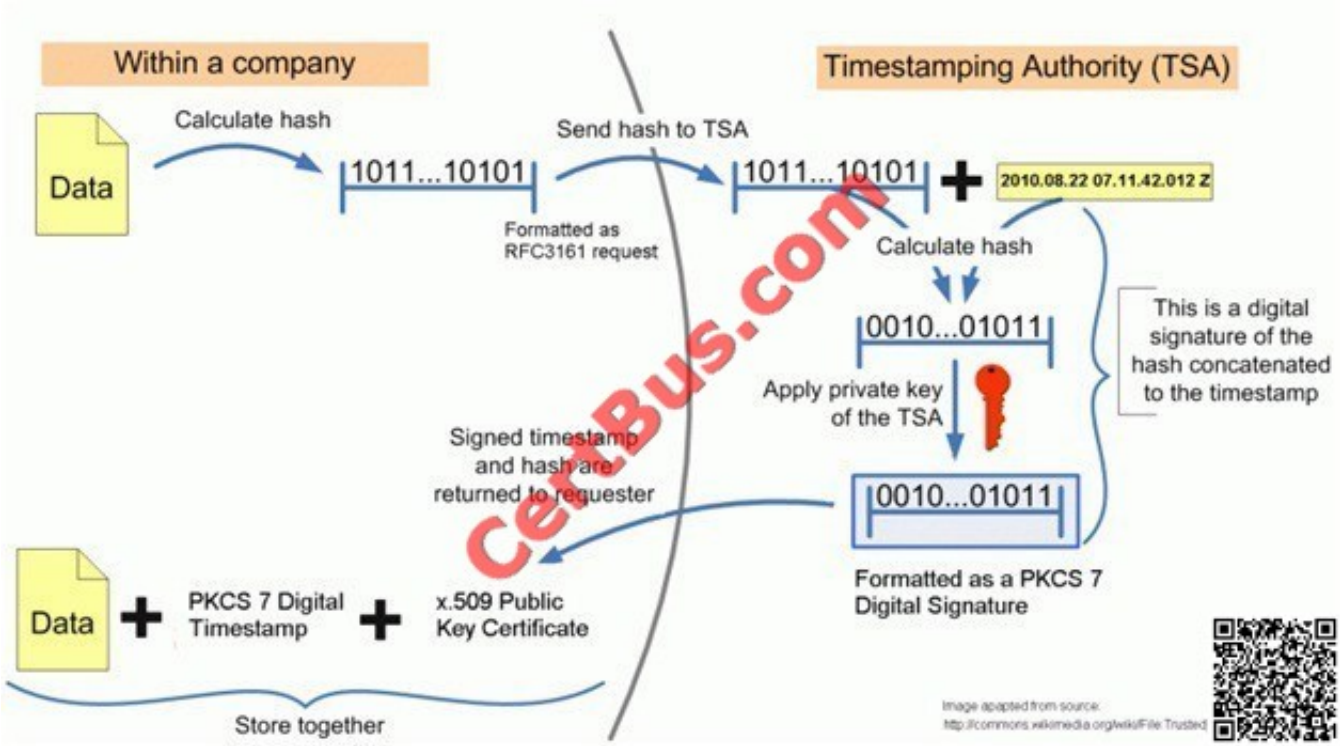
version of this file retrieved from a backup tape has not been altered, the hash function could be recomputed and compared with the hash value recorded in that paper notebook.

According to the RFC 3161 standard, a trusted timestamp is a timestamp issued by a trusted third party (TTP) acting as a Time Stamping Authority (TSA). It is used to prove the existence of certain data before a certain point (e.g. contracts,

research data, medical records,...) without the possibility that the owner can backdate the timestamps. Multiple TSAs can be used to increase reliability and reduce vulnerability.

The newer ANSI ASC X9.95 Standard for trusted timestamps augments the RFC 3161 standard with data- level security requirements to ensure data integrity against a reliable time source that is provable to any third party. This standard has

been applied to authenticating digitally signed data for regulatory compliance, financial transactions, and legal evidence.



Digital TimeStamp

The following are incorrect answers:

Network Time Protocol (NTP) is used to achieve high accuracy time synchronization for computers across a network.

A Certification Authority (CA) is the entity responsible for the issuance of digital certificates.

A Digital Signature provides integrity and authentication but does not bind a document to a specific time it was created.

Reference used for this question:

http://en.m.wikipedia.org/wiki/File:Trusted_timestamping.gif

and http://en.wikipedia.org/wiki/Trusted_timestamping

QUESTION 30

A proxy is considered a:

A. first generation firewall.

B. third generation firewall.

C. second generation firewall.

D. fourth generation firewall.

Correct Answer: C

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.

QUESTION 31

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

Correct Answer: C

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.

QUESTION 32

What would BEST define a covert channel?

A. An undocumented backdoor that has been left by a programmer in an operating system

B. An open system port that should be closed.

C. A communication channel that allows transfer of information in a manner that violates the system\\'s security policy.

D. A trojan horse.

Correct Answer: C

The Answer: A communication channel that allows transfer of information in a manner that violates the system\\'s security policy.

A covert channel is a way for an entity to receive information in an unauthorized manner. It is an information flow that is not controlled by a security mechanism. This type of information path was not developed for communication; thus, the system does not properly protect this path, because the developers never envisioned information being passed in this way. Receiving information in this manner clearly violates the system\\'s security policy. The channel to transfer this unauthorized data is the result of one of the following conditions:?Oversight in the development of the product Improper implementation of access controls

Existence of a shared resource between the two entities

Installation of a Trojan horse

The following answers are incorrect:

An undocumented backdoor that has been left by a programmer in an operating system is incorrect because it is not a means by which unauthorized transfer of information takes place. Such backdoor is usually referred to as a Maintenance

Hook. An open system port that should be closed is incorrect as it does not define a covert channel.

A trojan horse is incorrect because it is a program that looks like a useful program but when you install it it would include a bonus such as a Worm, Backdoor, or some other malware without the installer knowing about it.

Reference(s) used for this question:

Shon Harris AIO v3 , Chapter-5 : Security Models and Architecture

AIOv4 Security Architecture and Design (pages 343 - 344)

AIOv5 Security Architecture and Design (pages 345 - 346)

QUESTION 33

Which of the following classes is the first level (lower) defined in the TCSEC (Orange Book) as mandatory protection?

A. B

B. A

C. C

D. D

Correct Answer: A

B level is the first Mandatory Access Control Level. First published in 1983 and updated in 1985, the TCSEC, frequently referred to as the Orange Book, was a United States Government Department of Defense (DoD) standard that sets basic standards for the implementation of security protections in computing systems. Primarily intended to help the DoD find products that met those basic standards, TCSEC was used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information on military and government systems. As such, it was strongly focused on enforcing confidentiality with no focus on other aspects of security such as integrity or availability. Although it has since been superseded by the common criteria, it influenced the development of other product evaluation criteria, and some of its basic approach and terminology continues to be used.

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 17920-17926). Auerbach Publications. Kindle Edition.

and

THE source for all TCSEC "level" questions:

http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt (paragraph 3 for this one)

QUESTION 34

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

Correct Answer: B

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. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley and Sons, Page 34.

QUESTION 35

Which of the following should NOT normally be allowed through a firewall?

A. SNMP

B. SMTP

C. HTTP

D. SSH

Correct Answer: A

The Simple Network Management Protocol (SNMP) is a useful tool for remotely managing network devices.

Since it can be used to reconfigure devices, SNMP traffic should be blocked at the organization\\'s firewall. Using a VPN with encryption or some type of Tunneling software would be highly recommended in this case.

Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 4:

Sockets and Services from a Security Viewpoint.

QUESTION 36

The RSA algorithm is an example of what type of cryptography?

A. Asymmetric Key.

B. Symmetric Key.

C. Secret Key.

D. Private Key.

Correct Answer: A

The following answers are incorrect.

Symmetric Key. Is incorrect because RSA is a Public Key or a Asymmetric Key cryptographic system and not a Symmetric Key or a Secret Key cryptographic system.

Secret Key. Is incorrect because RSA is a Public Key or a Asymmetric Key cryptographic system and not a Secret Key or a Symmetric Key cryptographic system.

Private Key. Is incorrect because Private Key is just one part if an Asymmetric Key cryptographic system, a Private Key used alone is also called a Symmetric Key cryptographic system.

QUESTION 37

If an employee\\'s computer has been used by a fraudulent employee to commit a crime, the hard disk may be seized as evidence and once the investigation is complete it would follow the normal steps of the Evidence Life Cycle. In such case, the Evidence life cycle would not include which of the following steps listed below?

A. Acquisition collection and identification

B. Analysis

C. Storage, preservation, and transportation

D. Destruction

Correct Answer: D

Unless the evidence is illegal then it should be returned to owner, not destroyed.

The Evidence Life Cycle starts with the discovery and collection of the evidence. It progresses through the following series of states until it is finally returned to the victim or owner:

Acquisition collection and identification

Analysis

Storage, preservation, and transportation

Presented in court

Returned to victim (owner)

The Second edition of the ISC2 book says on page 529-530:

Identifying evidence: Correctly identifying the crime scene, evidence, and potential containers of evidence.

Collecting or acquiring evidence: Adhering to the criminalistic principles and ensuring that the contamination and the destruction of the scene are kept to a minimum. Using sound, repeatable, collection techniques that allow for the

demonstration of the accuracy and integrity of evidence, or copies of evidence.

Examining or analyzing the evidence: Using sound scientific methods to determine the characteristics of the evidence, conducting comparison for individuation of evidence, and conducting event reconstruction.

Presentation of findings: Interpreting the output from the examination and analysis based on findings of fact and articulating these in a format appropriate for the intended audience (e.g., court brief, executive memo, report).

Note on returning the evidence to the Owner/Victim

The final destination of most types of evidence is back with its original owner. Some types of evidence, such as

drugs or drug paraphernalia (i.e., contraband), are destroyed after the trial.

Any evidence gathered during a search, although maintained by law enforcement, is legally under the control of the courts. And although a seized item may be yours and may even have your name on it, it might not be returned to you unless

the suspect signs a release or after a hearing by the court. Unfortunately, many victims do not want to go to trial; they just want to get their property back. Many investigations merely need the information on a disk to prove or disprove a fact in question; thus, there is no need to seize the entire system. Once a schematic of the system is drawn or photographed, the hard disk can be removed and then transported to a forensic lab for copying.

Mirror copies of the suspect disk are obtained using forensic software and then one of those copies can be returned to the victim so that business operations can resume.

Reference(s) used for this question:

KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Chapter 9: Law, Investigation, and Ethics (page 309).

and

The Official Study Book, Second Edition, Page 529-230

QUESTION 38

Which of the following cryptographic attacks describes when the attacker has a copy of the plaintext and the corresponding ciphertext?

A. known plaintext

B. brute force

C. ciphertext only

D. chosen plaintext

Correct Answer: A

The goal to this type of attack is to find the cryptographic key that was used to encrypt the message. Once the key has been found, the attacker would then be able to decrypt all messages that had been encrypted using that key. 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. The term "crib" originated at Bletchley Park, the British World War II decryption operation

In cryptography, a brute force attack or exhaustive key search is a strategy that can in theory be used against any encrypted data by an attacker who is unable to take advantage of any weakness in an encryption system that would otherwise make his task easier. It involves systematically checking all possible keys until the correct key is found. In the worst case, this would involve traversing the entire key space, also called search space.

In cryptography, a ciphertext-only attack (COA) or known ciphertext attack is an attack model for cryptanalysis where the attacker is assumed to have access only to a set of ciphertexts.

The attack is completely successful if the corresponding plaintexts can be deduced, or even better, the key. The ability to obtain any information at all about the underlying plaintext is still considered a success. For example, if an adversary is

sending ciphertext continuously to maintain traffic-flow security, it would be very useful to be able to distinguish real messages from nulls. Even making an informed guess of the existence of real messages would facilitate traffic analysis.

In the history of cryptography, early ciphers, implemented using pen-and-paper, were routinely broken using ciphertexts alone. Cryptographers developed statistical techniques for attacking ciphertext, such as frequency analysis. Mechanical

encryption devices such as Enigma made these attacks much more difficult (although, historically, Polish cryptographers were able to mount a successful ciphertext-only cryptanalysis of the Enigma by exploiting an insecure protocol for

indicating the message settings).

Every modern cipher attempts to provide protection against ciphertext-only attacks. The vetting process for a new cipher design standard usually takes many years and includes exhaustive testing of large quantities of ciphertext for any

statistical departure from random noise. See:

Advanced Encryption Standard process. Also, the field of steganography evolved, in part, to develop methods like mimic functions that allow one piece of data to adopt the statistical profile of another. Nonetheless poor cipher usage or

reliance on home-grown proprietary algorithms that have not been subject to thorough scrutiny has resulted in many computer-age encryption systems that are still subject to ciphertext-only attack. Examples include:

Early versions of Microsoft\\'s PPTP virtual private network software used the same RC4 key for the sender and the receiver (later versions had other problems). In any case where a stream cipher like RC4 is used twice with the same key it is

open to ciphertext-only attack. See: stream cipher attack

Wired Equivalent Privacy (WEP), the first security protocol for Wi-Fi, proved vulnerable to several attacks, most of them ciphertext-only.

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, where the cryptanalyst makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions.

References:

Source: TIPTON, Harold, Official (ISC)2 Guide to the CISSP CBK (2007), page 271.

and

Wikipedia at the following links:

http://en.wikipedia.org/wiki/Chosen-plaintext_attack

http://en.wikipedia.org/wiki/Known-plaintext_attack

http://en.wikipedia.org/wiki/Ciphertext-only_attack

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

QUESTION 39

Which of the following services is NOT provided by the digital signature standard (DSS)?

A. Encryption

B. Integrity

C. Digital signature

D. Authentication

Correct Answer: A

DSS provides Integrity, digital signature and Authentication, but does not provide Encryption.

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Chapter 4: Cryptography (page 160).

QUESTION 40

One of the following assertions is NOT a characteristic of Internet Protocol Security (IPsec)

A. Data cannot be read by unauthorized parties

B. The identity of all IPsec endpoints are confirmed by other endpoints

C. Data is delivered in the exact order in which it is sent

D. The number of packets being exchanged can be counted.

Correct Answer: C

IPSec provide replay protection that ensures data is not delivered multiple times, however IPsec does not ensure that data is delivered in the exact order in which it is sent. IPSEC uses TCP and packets may be delivered out of order to the receiving side depending which route was taken by the packet.

Internet Protocol Security (IPsec) has emerged as the most commonly used network layer security control for protecting communications. IPsec is a framework of open standards for ensuring private communications over IP networks. Depending on how IPsec is implemented and configured, it can provide any combination of the following types of protection:

Confidentiality. IPsec can ensure that data cannot be read by unauthorized parties. This is accomplished by encrypting data using a cryptographic algorithm and a secret key a value known only to the two parties exchanging data. The data can only be decrypted by someone who has the secret key.

Integrity. IPsec can determine if data has been changed (intentionally or unintentionally) during transit. The integrity of data can be assured by generating a message authentication code (MAC) value, which is a cryptographic checksum of the data. If the data is altered and the MAC is recalculated, the old and new MACs will differ.

Peer Authentication. Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from the expected host.

Replay Protection. The same data is not delivered multiple times, and data is not delivered grossly out of order. However, IPsec does not ensure that data is delivered in the exact order in which it is sent.

Traffic Analysis Protection. A person monitoring network traffic does not know which parties are communicating, how often communications are occurring, or how much data is being exchanged. However, the number of packets being

exchanged can be counted.

Access Control. IPsec endpoints can perform filtering to ensure that only authorized IPsec users can access particular network resources. IPsec endpoints can also allow or block certain types of network traffic, such as allowing Web server

access but denying file sharing.

The following are incorrect answers because they are all features provided by IPSEC:

"Data cannot be read by unauthorized parties" is wrong because IPsec provides confidentiality through the usage of the Encapsulating Security Protocol (ESP), once encrypted the data cannot be read by unauthorized parties because they

have access only to the ciphertext. This is accomplished by encrypting data using a cryptographic algorithm and a session key, a value known only to the two parties exchanging data. The data can only be decrypted by someone who has a

copy of the session key.

"The identity of all IPsec endpoints are confirmed by other endpoints" is wrong because IPsec provides peer authentication: Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate, ensuring

that the network traffic and data is being sent from the expected host.

"The number of packets being exchanged can be counted" is wrong because although IPsec provides traffic protection where a person monitoring network traffic does not know which parties are communicating, how often communications are

occurring, or how much data is being exchanged, the number of packets being exchanged still can be counted.

Reference(s) used for this question:

NIST 800-77 Guide to IPsec VPNs . Pages 2-3 to 2-4

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.certbus.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: