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.leads4pass.com/sscp.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

What is the key size of the International Data Encryption Algorithm (IDEA)?

A. 64 bits

B. 128 bits

C. 160 bits

D. 192 bits

Correct Answer: B

The International Data Encryption Algorithm (IDEA) is a block cipher that operates on 64 bit blocks of data with a 128-bit key. The data blocks are divided into 16 smaller blocks and each has eight rounds of mathematical functions performed on it. It is used in the PGP encryption software.

Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 3).

QUESTION 2

The primary service provided by Kerberos is which of the following?

A. non-repudiation

B. confidentiality

C. authentication

D. authorization

Correct Answer: C

The Answer: authentication. Kerberos is an authentication service. It can use single-factor or multi-factor authentication methods.

The following answers are incorrect:

non-repudiation. Since Kerberos deals primarily with symmetric cryptography, it does not help with non-repudiation. confidentiality. Once the client is authenticated by Kerberos and obtains its session key and ticket, it may use them to assure confidentiality of its communication with a server; however, that is not a Kerberos service as such. authorization. Although Kerberos tickets may include some authorization information, the meaning of the authorization fields is not standardized in the Kerberos specifications, and authorization is not a primary Kerberos service.

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

ISC2 OIG,2007 p. 179-184 Shon Harris AIO v.3 152-155

QUESTION 3

Which of the following server contingency solutions offers the highest availability?

A. System backups

B. Electronic vaulting/remote journaling

C. Redundant arrays of independent disks (RAID)

D. Load balancing/disk replication

Correct Answer: D

Of the offered technologies, load balancing/disk replication offers the highest availability, measured in terms of minutes of lost data or server downtime. A Network-Attached Storage (NAS) or a Storage Area Network (SAN) solution combined with virtualization would offer an even higher availability.

Source: SWANSON, Marianne, and al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 49).

QUESTION 4

What is called the percentage at which the False Rejection Rate equals the False Acceptance Rate?

A. False Rejection Rate (FRR) or Type I Error

B. False Acceptance Rate (FAR) or Type II Error

C. Crossover Error Rate (CER)

D. Failure to enroll rate (FTE or FER)

Correct Answer: C

The percentage at which the False Rejection Rate equals the False Acceptance Rate is called the Crossover Error Rate (CER). Another name for the CER is the Equal Error Rate (EER), any of the two terms could be used.

Equal error rate or crossover error rate (EER or CER) It is the rate at which both accept and reject errors are equal. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate.

The other choices were all wrong answers:

The following are used as performance metrics for biometric systems:

false accept rate or false match rate (FAR or FMR): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted. This is when an impostor would be accepted by the system.

False reject rate or false non-match rate (FRR or FNMR): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected. This is when a valid company employee would be rejected by the system.

Failure to enroll rate (FTE or FER): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.

Reference(s) used for this question:

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.

and

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

QUESTION 5

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

Correct Answer: A

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 knownplaintext 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 chosenplaintext 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

QUESTION 6

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.

Correct Answer: C

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 uide, 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

QUESTION 7

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 uide, McGraw-Hill/Osborne, 2002, chapter

8: Cryptography (page 581).

QUESTION 8

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

Correct Answer: C

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

QUESTION 9

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.

Correct Answer: C

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.

QUESTION 10

Encapsulating Security Payload (ESP) provides some of the services of Authentication Headers (AH), but it is primarily designed to provide:

A. Confidentiality

B. Cryptography

C. Digital signatures

D. Access Control

Correct Answer: A

Source: TIPTON, Harold F. and KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, page 164.

QUESTION 11

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

Correct Answer: D

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

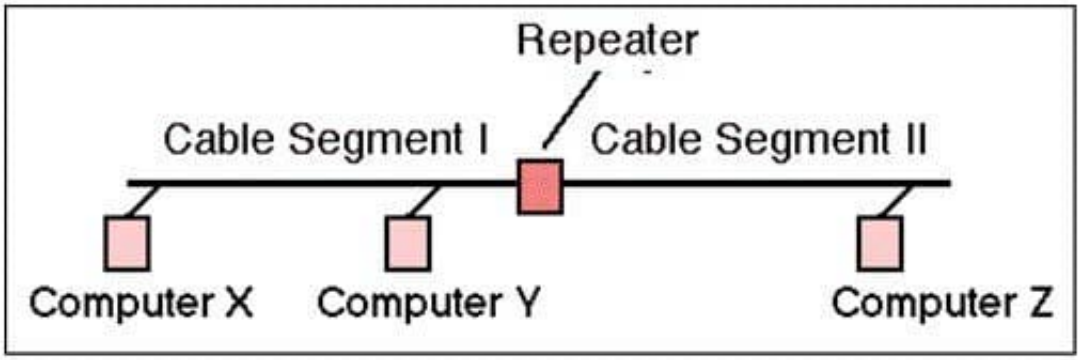
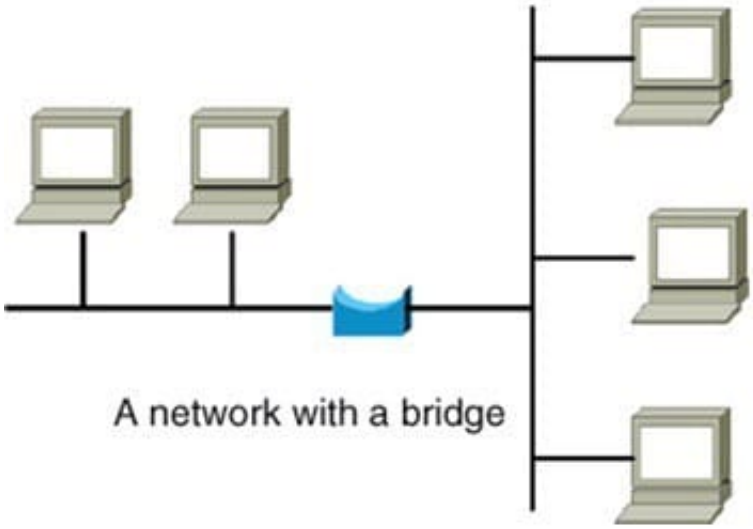


Image Reference- http://www.erg.abdn.ac.uk/~gorry/course/images/repeater.gif

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 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

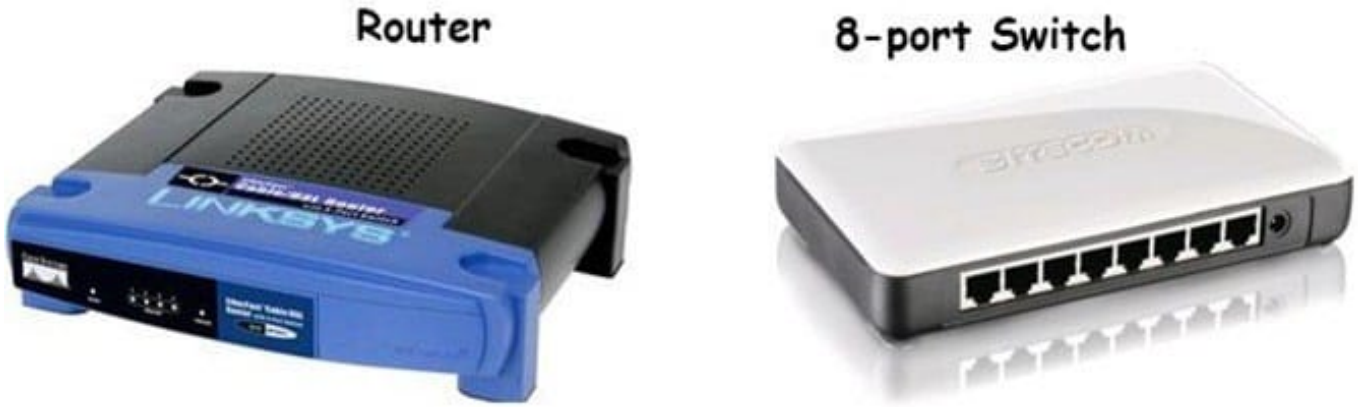


Image Reference- http://www.computer-networking-success.com/images/router-switch.jpg

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

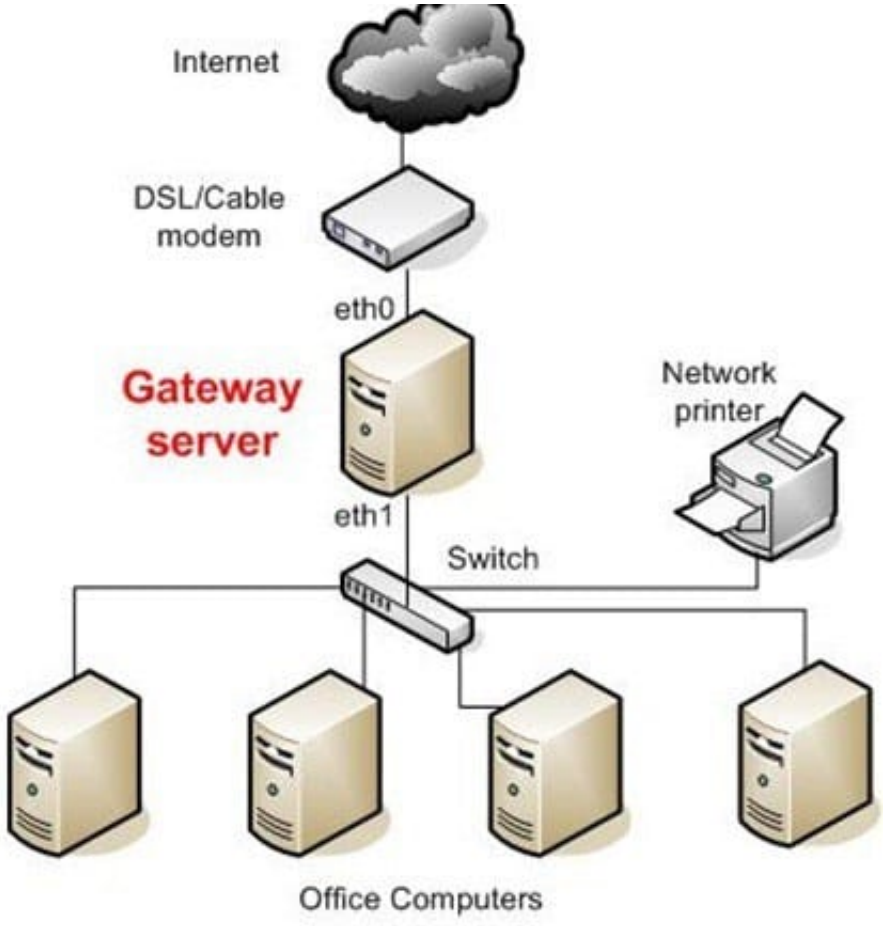


Image Referencehttp://static.howtoforge.com/images/screenshots/556af08d5e43aa768260f9e589dc547f- 3024.jpg

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

QUESTION 12

In the UTP category rating, the tighter the wind:

A. the higher the rating and its resistance against interference and crosstalk.

B. the slower the rating and its resistance against interference and attenuation.

C. the shorter the rating and its resistance against interference and attenuation.

D. the longer the rating and its resistance against interference and attenuation.

Correct Answer: A

The category rating is based on how tightly the copper cable is wound within the shielding: The tighter the wind, the higher the rating and its resistance against interference and crosstalk. Twisted pair copper cabling is a form of wiring in which two conductors are wound together for the purposes of canceling out electromagnetic interference (EMI) from external sources and crosstalk from neighboring wires. Twisting wires decreases interference because the loop area between the wires (which determines the magnetic coupling into the signal) is reduced. In balanced pair operation, the two wires typically carry equal and opposite signals (differential mode) which are combined by subtraction at the destination. The noise from the two wires cancel each other in this subtraction because the two wires have been exposed to similar EMI.

The twist rate (usually defined in twists per metre) makes up part of the specification for a given type of cable. The greater the number of twists, the greater the attenuation of crosstalk. Where pairs are not twisted, as in most residential interior telephone wiring, one member of the pair may be closer to the source than the other, and thus exposed to slightly different induced EMF.

Reference:

KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley and Sons, Page 101.

and

http://www.consultants-online.co.za/pub/itap_101/html/ch04s05.html

QUESTION 13

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 14

Which of the following is used in database information security to hide information?

A. Inheritance

B. Polyinstantiation

C. Polymorphism

D. Delegation

Correct Answer: B

Polyinstantiation enables a relation to contain multiple tuples with the same primary keys with each instance distinguished by a security level. When this information is inserted into a database, lower-level subjects need to be restricted from this information. Instead of just restricting access, another set of data is created to fool the lower-level subjects into thinking that the information actually means something else.

Source: HARRIS, Shon, All-In-One CISSP Certification uide, McGraw-Hill/Osborne, 2002, chapter 11: Application and System Development (page 727).

QUESTION 15

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

A. 81

B. 80

C. 8080

D. 8180

Correct Answer: B

HTTP is Port 80.

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