CISSP Q&As

Certified Information Systems Security Professional

Pass ISC CISSP Exam with 100% Guarantee

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

https://www.lead4pass.com/CISSP.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

How do covert timing channels convey information?

A. By generating noise and traffic with the data

B. By modifying the timing of a system resource in some measurable way

C. By changing a system\\'s stored data characteristics

D. By performing a covert channel analysis

Correct Answer: B

The correct answer is "By modifying the timing of a system resource in some measurable way". A covert timing channel alters the timing of parts of the system to enable it to be used to communicate information covertly (outside the normal security function).

*

Answer "By changing a system\\'s stored data characteristics" is the description of the use of a covert storage channel.

*

"By generating noise and traffic with the data" is a technique to combat the use of covert channels.

*

Answer "By performing a covert channel analysis" is the Orange Book requirement for B3, B2, and A1 evaluated systems.

QUESTION 2

What does CSMAstand for?

A. Common Systems Methodology Applications

B. Carrier Sense Multiple Access

C. Carrier Sense Multiple Attenuation

D. CarrierStation Multi-port Actuator

Correct Answer: B

The correct answer is "Carrier Sense Multiple Access". The other acronyms do not exist.

QUESTION 3

Which of the following types of business continuity tests includes assessment of resilience to internal and external risks without endangering live operations?

A. Walkthrough

B. Simulation

C. Parallel

D. White box

Correct Answer: B

QUESTION 4

In a relational database system, a primary key is chosen from a set of:

A. Candidate keys.

B. Foreign keys.

C. Secondary keys.

D. Cryptographic keys.

Correct Answer: A

The correct answer is candidate keys by definition. Answer Foreign keys is incorrect because a foreign key in one table refers to a primary key in another. Answer Secondary keys is a made-up distracter, and answer Cryptographic key refers to keys used in encipherment and decipherment.

QUESTION 5

What would BEST define risk management?

A. The process of eliminating the risk

B. The process of assessing the risks

C. The process of reducing risk to an acceptable level

D. The process of transferring risk

Correct Answer: C

Explanation: This is the basic process of risk management.

Risk is the possibility of damage happening and the ramifications of such damage should it occur. Information risk management (IRM) is the process of identifying and assessing risk, reducing it to an acceptable level, and implementing the

right mechanisms to maintain that level. There is no such thing as a 100 percent secure environment. Every environment has vulnerabilities and threats to a certain degree.

The skill is in identifying these threats, assessing the probability of them actually occurring and the damage they could cause, and then taking the right steps to reduce the overall level of risk in the environment to what the organization

identifies as acceptable. Proper risk management requires a strong commitment from senior management, a documented process that supports the organization\\'s mission, an information risk management (IRM) policy and a delegated IRM

team. Once you\\'ve identified your company\\'s acceptable level of risk, you need to develop an information risk management policy.

The IRM policy should be a subset of the organization\\'s overall risk management policy (risks to a company include more than just information security issues) and should be mapped to the organizational security policies, which lay out the

acceptable risk and the role of security as a whole in the organization. The IRM policy is focused on risk management while the security policy is very high-level and addresses all aspects of security. The IRM policy should address the

following items:

Objectives of IRM team

Level of risk the company will accept and what is considered an acceptable risk (as defined in the previous article)

Formal processes of risk identification

Connection between the IRM policy and the organization\\'s strategic planning processes Responsibilities that fall under IRM and the roles that are to fulfill them Mapping of risk to internal controls

Approach for changing staff behaviors and resource allocation in response to risk analysis Mapping of risks to performance targets and budgets Key indicators to monitor the effectiveness of controls

Shon Harris provides a 10,000-foot view of the risk management process below:

A big question that companies have to deal with is, "What is enough security?" This can be restated as, "What is our acceptable risk level?" These two questions have an inverse relationship. You can\\'t know what constitutes enough security

unless you know your necessary baseline risk level.

To set an enterprise-wide acceptable risk level for a company, a few things need to be investigated and understood. A company must understand its federal and state legal requirements, its regulatory requirements, its business drivers and

objectives, and it must carry out a risk and threat analysis. (I will dig deeper into formalized risk analysis processes in a later article, but for now we will take a broad approach.) The result of these findings is then used to define the company\\'s

acceptable risk level, which is then outlined in security policies, standards, guidelines and procedures.

Although there are different methodologies for enterprise risk management, the core components of any risk analysis is made up of the following:

Identify company assets

Assign a value to each asset

Identify each asset\\'s vulnerabilities and associated threats Calculate the risk for the identified assets

Once these steps are finished, then the risk analysis team can identify the necessary countermeasures to mitigate the calculated risks, carry out cost/benefit analysis for these countermeasures and report to senior management their findings.

When we look at information security, there are several types of risk a corporation needs to be aware of and address properly. The following items touch on the major categories:

?Physical damage Fire, water, vandalism, power loss, and natural disasters ?Human interaction Accidental or intentional action or inaction that can disrupt productivity ?Equipment malfunction Failure of systems and peripheral devices ?

Inside and outside attacks Hacking, cracking, and attacking ?Misuse of data Sharing trade secrets, fraud, espionage, and theft ?Loss of data Intentional or unintentional loss of information through destructive means ?Application error

Computation errors, input errors, and buffer overflows

The following answers are incorrect:

The process of eliminating the risk is not the best answer as risk cannot be totally eliminated.

The process of assessing the risks is also not the best answer. The process of transferring risk is also not the best answer and is one of the ways of handling a risk after a risk analysis has been performed. Shon Harris , AIO v3 , Chapter 3:

Security Management Practices , Page: 66-68 and

http://searchsecurity.techtarget.com/tip/Understanding-risk

QUESTION 6

Which of the following BEST describes Recovery Time Objective (RTO)?

A. Time of application resumption after disaster

B. Time of application verification after disaster.

C. Time of data validation after disaster.

D. Time of data restoration from backup after disaster.

Correct Answer: A

QUESTION 7

Another type of artificial intelligence technology involves genetic algorithms. Genetic algorithms are part of the general class known as:

A. Suboptimal computing

B. Biological computing

C. Evolutionary computing

D. Neural networks

Correct Answer: C

Evolutionary computing uses the Darwinian principles of survival of the fittest, mutation, and the adaptation of successive generations of populations to their environment. The genetic algorithm implements this process through iteration of generations of a constant-size population of items or individuals. Each individual is characterized by a finite string of symbols called genomes. The genomes are used to represent possible solutions to a problem in a fixed search space. For example, if the fixed population of the first generation of individuals consists of random binary numbers, and the problem is to find the minimum binary number that can be represented by an individual, each binary number is assigned a fitness value based on the individuals binary number value. The smaller the binary number represented by a parent individual, the higher level of fitness that is assigned to it. Through cross breeding among the numbers (known as crossover), mutations of the numbers, and pairing of numbers with high fitness ratings, the smallest value that can be represented by the number of bits in the binary number will emerge in later generations.

*Answer neural networks, is incorrect and has been discussed extensively in previous questions in this chapter.
*Answer Suboptimal computing is a distracter and answer biological computing, refers to computation performed by using certain characteristics of living organisms.

QUESTION 8

Which is NOT an element of two-factor authentication?

A. Something you are

B. Something you have

C. Something you know

D. Something you ate

Correct Answer: D

QUESTION 9

A security evaluation report and an accreditation statement are produced in which of the following phases of the system development life cycle?

A. project initiation and planning phase

B. system design specification phase

C. development and documentation phase

D. acceptance phase

Correct Answer: D

Explanation: The Answer: "acceptance phase". Note the question asks about an "evaluation report" - which details how the system evaluated, and an "accreditation statement" which describes the level the system is allowed to operate at.

Because those two activities are a part of testing and testing is a part of the acceptance phase, the only answer above that can be correct is "acceptance phase".

The other answers are not correct because:

The "project initiation and planning phase" is just the idea phase. Nothing has been developed yet to be evaluated,

tested, accredited, etc.

The "system design specification phase" is essentially where the initiation and planning phase is fleshed out. For example, in the initiation and planning phase, we might decide we want the system to have authentication. In the design

specification phase, we decide that that authentication will be accomplished via username/password. But there is still nothing actually developed at this point to evaluate or accredit.

The "development and documentation phase" is where the system is created and documented. Part of the documentation includes specific evaluation and accreditation criteria. That is the criteria that will be used to evaluate and accredit the

system during the "acceptance phase".

In other words - you cannot evaluate or accredit a system that has not been created yet. Of the four answers listed, only the acceptance phase is dealing with an existing system. The others deal with planning and creating the system, but the

actual system isn\\'t there yet.

Reference:

Official ISC2 Guide Page: 558 - 559

All in One Third Edition page: 832 - 833 (recommended reading)

QUESTION 10

During which phase of an IT system life cycle are security requirements developed?

A. Operation

B. Initiation

C. Functional design analysis and Planning

D. Implementation

Correct Answer: C

Explanation: The software development life cycle (SDLC) (sometimes referred to as the System Development Life Cycle) is the process of creating or altering software systems, and the models and methodologies that people use to develop

these systems.

The NIST SP 800-64 revision 2 has within the description section of para 3.2.1:

This section addresses security considerations unique to the second SDLC phase. Key security activities for this phase include:

?Conduct the risk assessment and use the results to supplement the baseline security controls;

?Analyze security requirements;

?Perform functional and security testing;

?Prepare initial documents for system certification and accreditation; and ?Design security architecture.

Reviewing this publication you may want to pick development/acquisition. Although initiation would be a decent choice, it is correct to say during this phase you would only brainstorm the idea of security requirements. Once you start to

develop and acquire hardware/software components then you would also develop the security controls for these. The Shon Harris reference below is correct as well.

Shon Harris\\' Book (All-in-One CISSP Certification Exam Guide) divides the SDLC differently:

-Project initiation

-Functional design analysis and planning

-System design specifications

-Software development

-Installation

-Maintenance support

-Revision and replacement

According to the author (Shon Harris), security requirements should be developed during the functional design analysis and planning phase.

SDLC POSITIONING FROM NIST 800-64

SDLC Positioning in the enterprise

Information system security processes and activities provide valuable input into managing IT systems and their development, enabling risk identification, planning and mitigation. A risk management approach involves continually balancing the

protection of agency information and assets with the cost of security controls and mitigation strategies throughout the complete information system development life cycle (see Figure 2-1 above). The most effective way to implement risk

management is to identify critical assets and operations, as well as systemic vulnerabilities across the agency. Risks are shared and not bound by organization, revenue source, or topologies. Identification and verification of critical assets and

operations and their interconnections can be achieved through the system security planning process, as well as through the compilation of information from the Capital Planning and Investment Control (CPIC) and Enterprise Architecture (EA)

processes to establish insight into the agency\\'s vital business operations, their supporting assets, and existing interdependencies and relationships.

With critical assets and operations identified, the organization can and should perform a business impact analysis (BIA). The purpose of the BIA is to relate systems and assets with the critical services they provide and assess the

consequences of their disruption. By identifying these systems, an agency can manage security effectively by establishing priorities. This positions the security office to facilitate the IT program\\'s cost-effective performance as well as articulate

its business impact and value to the agency.

SDLC OVERVIEW FROM NIST 800-64

SDLC Overview from NIST 800-64 Revision 2

NIST 800-64 Revision 2 is one publication within the NISTstandards that I would recommend you look at for more details about the SDLC. It describe in great details what activities would take place and they have a nice diagram for each of

the phases of the SDLC. You will find a copy at:

http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf

DISCUSSION:

Different sources present slightly different info as far as the phases names are concerned.

People sometimes gets confused with some of the NIST standards. For example NIST 800-64 Security Considerations in the Information System Development Life Cycle has slightly different names, the activities mostly remains the same.

NIST clearly specifies that Security requirements would be considered throughout ALL of the phases. The keyword here is considered, if a question is about which phase they would be developed than Functional Design Analysis would be the

correct choice. Within the NIST standard they use different phase, howeverr under the second phase you will see that they talk specifically about Security Functional requirements analysis which confirms it is not at the initiation stage so it

become easier to come out with the answer to this question. Here is what is stated:

The security functional requirements analysis considers the system security environment, including the enterprise information security policy and the enterprise security architecture. The analysis should address all requirements for

confidentiality, integrity, and availability of information, and should include a review of all legal, functional, and other security requirements contained in applicable laws, regulations, and guidance.

At the initiation step you would NOT have enough detailed yet to produce the Security Requirements. You are mostly brainstorming on all of the issues listed but you do not develop them all at that stage.

By considering security early in the information system development life cycle (SDLC), you may be able to avoid higher costs later on and develop a more secure system from the start.

NIST says:

NIST`s Information Technology Laboratory recently issued Special Publication (SP) 800- 64, Security Considerations in the Information System Development Life Cycle, by Tim Grance, Joan Hash, and Marc Stevens, to help organizations

include security requirements in their planning for every phase of the system life cycle, and to select, acquire, and use appropriate and cost-effective security controls.

I must admit this is all very tricky but reading skills and paying attention to KEY WORDS is a must for this exam.

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, Fifth Edition, Page 956

and

NIST S-64 Revision 2 at http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64- Revision2.pdf

and

http://www.mks.com/resources/resource-pages/software-development-life-cycle-sdlc- system-development

QUESTION 11

Ding Ltd. is a firm specialized in intellectual property business. A new video streaming application needs to be installed for the purpose of conducting the annual awareness program as per the firm security program. The application will stream internally copyrighted computer based training videos. The requirements for the application installation are to use a single server, low cost technologies, high performance and no high availability capacities.

In regards to storage technology, what is the most suitable configuration for the server hard drives?

A. Single hard disk (no RAID)

B. RAID 0

C. RAID 1

D. RAID 10

Correct Answer: A

Explanation: Single hard disk does provide low cost requirement and no high availability but doesn\\'t provide high performance

RAID 1 (mirroring) provides the exact opposite of the needs : low performance, high cost and high availability RAID 10 provides performance but it is an expensive solution with high availability capacities

The following reference(s) were/was used to create this question: Shon Harris, AIO 5th, Operations Security, Page 1086

QUESTION 12

Complete the blanks. When using PKI, I digitally sign a message using my _____ key. The recipient verifies my signature using my _____ key.

A. Private / Public

B. Public / Private

C. Symmetric / Asymmetric

D. Private / Symmetric

Correct Answer: A

Explanation: When we encrypt messages using our private keys which are only available to us. The person who wants to read and decrypt the message need only have our public keys to do so.

The whole point to PKI is to assure message integrity, authentication of the source, and to provide secrecy with the digital encryption.

See below a nice walktrough of Digital Signature creation and verification from the Comodo web site:

Digital Signatures apply the same functionality to an e-mail message or data file that a handwritten signature does for a paper-based document. The Digital Signature vouches for the origin and integrity of a message, document or other data

file.

How do we create a Digital Signature?

The creation of a Digital Signature is a complex mathematical process. However as the complexities of the process are computed by the computer, applying a Digital Signature is no more difficult that creating a handwritten one!

The following text illustrates in general terms the processes behind the generation of a Digital Signature:

1.

Alice clicks \\'sign\\' in her email application or selects which file is to be signed.

2.

Alice\\'s computer calculates the \\'hash\\' (the message is applied to a publicly known mathematical hashing function that coverts the message into a long number referred to as the hash).

3.

The hash is encrypted with Alice\\'s Private Key (in this case it is known as the Signing Key) to create the Digital Signature.

4.

The original message and its Digital Signature are transmitted to Bob.

5.

Bob receives the signed message. It is identified as being signed, so his email application knows which actions need to be performed to verify it.

6.

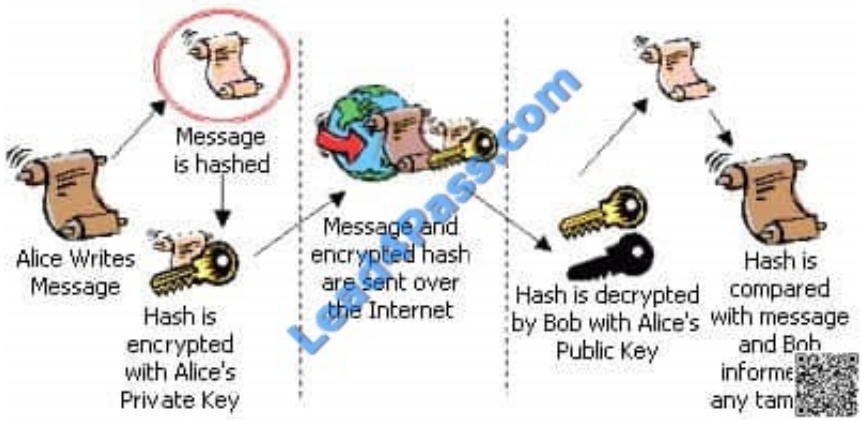
Bob\\'s computer decrypts the Digital Signature using Alice\\'s Public Key.

7.

Bob\\'s computer also calculates the hash of the original message (remember - the mathematical function used by Alice to do this is publicly known).

8.

Bob\\'s computer compares the hashes it has computed from the received message with the now decrypted hash received with Alice\\'s message.



digital signature creation and verification

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

However, if the two hashes differ when compared then the integrity of the original message has been compromised. If the original message is tampered with it will result in Bob\\'s computer calculating a different hash value. If a different hash value is created, then the original message will have been altered. As a result the verification of the Digital Signature will fail and Bob will be informed. Origin, Integrity, Non-Repudiation, and Preventing Men-In-The-Middle (MITM) attacks

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

Creating and validating a digital signature

Due to the recent Global adoption of Digital Signature law, Alice may now sign a transaction, message or piece of digital data, and so long as it is verified successfully it is a legally permissible means of proof that Alice has made the

transaction or written the message.

The following answers are incorrect:

-Public / Private: This is the opposite of the right answer.

-

Symmetric / Asymmetric: Not quite. Sorry. This form of crypto is asymmetric so you were almost on target.

-

Private / Symmetric: Well, you got half of it right but Symmetric is wrong.

The following reference(s) was used to create this question: http://www.comodo.com/resources/small-business/digital-certificates3.php

QUESTION 13

Which of the following are suitable protocols for securing VPN connections at the lower layers of the OSI model?

A. S/MIME and SSH

B. TLS and SSL

C. IPsec and L2TP D. PKCS#10 and X.509

Correct Answer: C

Reference: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw- Hill/Osborne, page 467; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

QUESTION 14

Imprisonment is a possible sentence under:

A. Neither civil nor criminal law

B. Both civil and criminal law

C. Civil (tort) law

D. Criminal law

Correct Answer: D

The correct answer is Criminal law. It is the only one of the choices where imprisonment is possible.

QUESTION 15

What does the * (star) integrity axiom mean in the Biba model?

A. No read up

B. No write down

C. No read down

D. No write up

Correct Answer: D

Explanation: The *- (star) integrity axiom of the Biba access control model states that an object at one level of integrity is not permitted to modify an object of a higher level of integrity (no write up).

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 Architectures and Models (page 205).

QUESTION 16

Which statement is true regarding company/employee relations during and after a disaster?

A. Senior-level executives are the only employees who should receive continuing salaries during the disruptive event.

B. The organizations responsibility to the employees families ends when the disaster stops the business from functioning.

C. The organization has a responsibility to continue salaries or other funding to the employees and/or families affected by the disaster.

D. Employees should seek any means of obtaining compensation after a disaster, including fraudulent ones.

Correct Answer: C

The organization has an inherent responsibility to its employees and their families during and after a disaster or other disruptive event. The company must be insured to the extent it can properly compensate its employees and families. Alternatively, employees do not have the right to obtain compensatory damages fraudulently if the organization cannot compensate.

QUESTION 17

Which one of the following is not a primary component or aspect of firewall systems?

A. Protocol filtering

B. Packet switching

C. Rule enforcement engine

D. Extended logging capability

Correct Answer: B

Explanation: This is not a main function of a firewall, packet switching is a main feature of a Switch (working only in the layer 2 of the OSI model). Firewall are network security devices that can function through layer 2 to layer 7 of the OSI model. They usually include rule engine that enforce the enterprise security policy of the company. They provide protocol filtering to enforce our requirements through the forwarded or deny of traffic. They also provide logging capabilities so we can analyze what is happening in a very low level in our network.

QUESTION 18

Which of the following is the BIGGEST weakness when using native Lightweight Directory Access Protocol (LDAP) for authentication?

A. Authorizations are not included in the server response

B. Unsalted hashes are passed over the network

C. The authentication session can be replayed

D. Passwords are passed in cleartext

Correct Answer: D

QUESTION 19

What is called the number of columns in a table?

A. Schema

B. Relation

C. Degree

D. Cardinality

Correct Answer: C

Explanation: The number of columns in a relation (a table) is the degree whereas the cardinality is the number of rows. The schema is the description of the database. 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 2: Access control systems (page 45).

QUESTION 20

Two companies wish to share electronic inventory and purchase orders in a supplier and client relationship. What is the BEST security solution for them?

A. Write a Service Level Agreement (SLA) for the two companies.

B. Set up a Virtual Private Network (VPN) between the two companies.

C. Configure a firewall at the perimeter of each of the two companies.

D. Establish a File Transfer Protocol (FTP) connection between the two companies.

Correct Answer: B

QUESTION 21

Rewritable and erasable (CDR/W) optical disk are sometimes used for backups that require short time storage for changeable data, but require?

A. Faster file access than tape.

B. Slower file access than tape.

C. Slower file access than drive.

D. Slower file access than scale.

Correct Answer: A

Explanation: This is true, when we use optical media like CD? to make our backups we need a constant throughput on the file access and data transfer inside the disk because of the risk to get a buffer overrun error in the CD writer. If the buffer user by the CD burner is empty and the Hard disk does not provide data for that time, the Backup will be unsuccessful. This can be solved with a Technology known as "Burn Proof".

QUESTION 22

Which of the following can be used as a covert channel?

A. Storage and timing.

B. Storage and low bits.

C. Storage and permissions.

D. Storage and classification.

Correct Answer: A

Explanation: The Orange book requires protection against two types of covert channels, Timing and Storage.

The following answers are incorrect:

Storage and low bits. Is incorrect because, low bits would not be considered a covert channel.

Storage and permissions. Is incorrect because, permissions would not be considered a covert channel.

Storage and classification. Is incorrect because, classification would not be considered a covert channel.

QUESTION 23

The organization that establishes a collaborative partnership of computer incident response, security and law enforcement professionals who work together to handle computer security incidents and to provide both proactive and reactive security services for the

A. Federal CIO Council

B. FederalComputer Incident Response Center

C. CERT/CC

D. Center for Infrastructure Protection

Correct Answer: B

To again quote the FedCIRC charter, FedCIRC provides assistance and guidance in incident response and provides a centralized approach to incident handling across agency boundaries. Specifically, the mission of FedCIRC is to: Provide civil agencies with technical information, tools, methods, assistance, and guidance Be proactive and provide liaison activities and analytical support Encourage the development of quality products and services through collaborative relationships with Federal civil agencies, the Department of Defense, academia, and private industry Promote the highest security profile for government information technology (IT) resources Promote incident response and handling procedural awareness with the federal government

*

Answer CERT Coordination Center (CERT/CC), is a unit of the Carnegie Mellon University Software Engineering Institute (SEI). SEI is a Federally funded RandD Center . CERT\\'s mission is to alert the Internet community to vulnerabilities and attacks and to conduct research and training in the areas of computer security, including incident response.

*

Answer "Center for Infrastructure Protection" is a distracter and answer "Federal CIO Council", the Federal Chief Information Officers\\' Council, is the sponsor of FedCIRC.

QUESTION 24

Which choice below would NOT be considered a benefit of employing incident-handling capability?

A. An individual acting alone would not be able to subvert a security process or control.

B. It enhances internal communications and the readiness of the organization to respond to incidents.

C. Security training personnel would have a better understanding of users knowledge of security issues.

D. It assists an organization in preventing damage from future incidents.

Correct Answer: A

The primary benefits of employing an incident-handling capability are containing and repairing damage from incidents and preventing future damagE. Additional benefits related to establishing an incidenthandling capability are:

Enhancement of the risk assessment process. An incidenthandling capability will allow organizations to collect threat data that may be useful in their risk assessment and safeguard selection processes (e.g., in designing new systems).

Statistics on the numbers and types of incidents in the organization can be used in the risk-assessment process as an indication of vulnerabilities and threats.

Enhancement of internal communications and the readiness of the organization to respond to any type of incident, not just computer security incidents. Internal communications will be improved, management will be better organized to receive

communications, and contacts within public affairs, legal staff, law enforcement, and other groups will have been preestablished. Security training personnel will have a better understanding of users knowledge of security issues. Trainers can

use actual incidents to vividly illustrate the importance of computer security. Training that is based on current threats and controls recommended by incident-handling staff provides users with information more specifically directed to their

current needs, thereby reducing the risks to the organization from incidents. *Answer "An individual acting alone would not be able to subvert a security process or control" is a benefit of employing separation of duties controls. Source:

National Institute of Standards and Technology, An Introduction to Computer Security: The NIST Handbook Special Publication 800-12.

QUESTION 25

Which type of attack involves the altering of a systems Address Resolution Protocol (ARP) table so that it contains incorrect IP to MAC address mappings?

A. Reverse ARP

B. Poisoning ARP cache

C. ARP table poisoning

D. Reverse ARP table poisoning

Correct Answer: C

Explanation: ARP table poisoning, also referred to as ARP cache poisoning, is the process of altering a system\\'s ARP table so that it contains incorrect IP to MAC address mappings. This allows requests to be sent to a different device instead

of the one it is actually intended for. It is an excellent way to fool systems into thinking that a certain device has a certain address so that information can be sent to and captured on an attacker\\'s computer.

The following answers are incorrect:

"Reverse ARP" is the process of determining what an IP address is from a known MAC address

"Poisoning ARP cache" This is not the correct term.

"Reverse ARP table poisoning" There is no attack that goes by that name.

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

TestPrep Certified Information Systems Security Professional (CISSP) Skillsoft Course

QUESTION 26

Which of the following would best describe the difference between white-box testing and black-box testing?

A. White-box testing is performed by an independent programmer team.

B. Black-box testing uses the bottom-up approach.

C. White-box testing examines the program internal logical structure.

D. Black-box testing involves the business units

Correct Answer: C

Explanation: Black-box testing observes the system external behavior, while white-box testing is a detailed exam of a logical path, checking the possible conditions. Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 299).

QUESTION 27

_____ are added to Linux passwords to increase their randomness.

A. Salts

B. Pepper

C. Grains

D. MD5 hashes

E. Asymmetric algorithms

Correct Answer: A

Explanation: Salts are added to Linux passwords to increase their randomness. They are used to help insure that no two users have the same, hashed password.

QUESTION 28

What can be defined as: It confirms that users\\' needs have been met by the supplied solution?

A. Accreditation

B. Certification

C. Assurance

D. Acceptance

Correct Answer: D

Explanation: Acceptance confirms that users\\' needs have been met by the supplied solution. Verification and Validation informs Acceptance by establishing the evidence ?set against acceptance criteria - to determine if the solution meets the users\\' needs. Acceptance should also explicitly address any integration or interoperability requirements involving other equipment or systems. To enable acceptance every user and system requirement must have a \\'testable\\' characteristic.

Accreditation is the formal acceptance of security, adequacy, authorization for operation and acceptance of existing risk. Accreditation is the formal declaration by a Designated Approving Authority (DAA) that an IS is approved to operate in a particular security mode using a prescribed set of safeguards to an acceptable level of risk.

Certification is the formal testing of security safeguards and assurance is the degree of confidence that the implemented security measures work as intended. The certification is a Comprehensive evaluation of the technical and nontechnical security features of an IS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified ecurity requirements.

Assurance is the descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality. For example, an evaluation may require that all source code is kept in a change management system, or that full functional testing is performed. The Common Criteria provides a catalogue of these, and the requirements may vary from one evaluation to the next. The requirements for particular targets or types of products are documented in the Security Targets (ST) and Protection Profiles (PP), respectively. Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 4, August 1999. and Official ISC2 Guide to the CISSP CBK, Second Edition, on page 211. and http://www.aof.mod.uk/aofcontent/tactical/randa/content/randaintroduction.htm

QUESTION 29

What is the role of IKE within the IPsec protocol?

A. peer authentication and key exchange

B. data encryption

C. data signature

D. enforcing quality of service

Correct Answer: A

Reference: RFC 2409: The Internet Key Exchange (IKE); DORASWAMY, Naganand and HARKINS, Dan, Ipsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, 1999, Prentice Hall PTR; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

QUESTION 30

Communications devices must operate:

A. at different speeds to communicate.

B. at the same speed to communicate.

C. at varying speeds to interact.

D. at high speed to interact.

Correct Answer: B

Explanation: Communications devices must operate at the same speed to communicate. 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 100.

QUESTION 31

Which of the following is a function of Security Assertion Markup Language (SAML)?

A. File allocation

B. Redundancy check

C. Extended validation

D. Policy enforcement

Correct Answer: D

QUESTION 32

Which of the following choices describe a condition when RAM and Secondary storage are used together?

A. Primary storage

B. Secondary storage

C. Virtual storage

D. Real storage

Correct Answer: C

Explanation: Virtual storage a service provided by the operating system where it uses a combination of RAM and disk storage to simulate a much larger address space than is actually present. Infrequently used portions of memory are paged

out by being written to secondary storage and paged back in when required by a running program.

Most OS\\'s have the ability to simulate having more main memory than is physically available in the system. This is done by storing part of the data on secondary storage, such as a disk. This can be considered a virtual page. If the data

requested by the system is not currently in main memory, a page fault is taken. This condition triggers the OS handler. If the virtual address is a valid one, the OS will locate the physical page, put the right information in that page, update the

translation table, and then try the request again. Some other page might be swapped out to make room. Each process may have its own separate virtual address space along with its own mappings and protections.

The following are incorrect answers:

Primary storage is incorrect. Primary storage refers to the combination of RAM, cache and the processor registers. Primary Storage The data waits for processing by the processors, it sits in a staging area called primary storage. Whether

implemented as memory, cache, or registers (part of the CPU), and regardless of its location, primary storage stores data that has a high probability of being requested by the CPU, so it is usually faster than long-term, secondary storage. The

location where data is stored is denoted by its physical memory address. This memory register identifier remains constant and is independent of the value stored there. Some examples of primary storage devices include random-access

memory (RAM), synchronous dynamic random-access memory (SDRAM), and read-only memory (ROM). RAM is volatile, that is, when the system shuts down, it flushes the data in RAM although recent research has shown that data may still

be retrievable. Contrast this

Secondary storage is incorrect. Secondary storage holds data not currently being used by the CPU and is used when data must be stored for an extended period of time using high- capacity, nonvolatile storage. Secondary storage includes

disk, floppies, CD\\'s, tape, etc. While secondary storage includes basically anything different from primary storage, virtual memory\\'s use of secondary storage is usually confined to high-speed disk storage.

Real storage is incorrect. Real storage is another word for primary storage and distinguishes physical memory from virtual memory.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17164-17171). Auerbach Publications. Kindle Edition.

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17196-17201). Auerbach Publications. Kindle Edition.

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17186-17187). Auerbach Publications. Kindle Edition.

QUESTION 33

The use of proximity card to gain access to a building is an example of what type of security control?

A. Legal

B. Logical

C. Physical

D. Procedural

Correct Answer: C

QUESTION 34

Which TCSEC (Orange Book) rating or level requires the system to clearly identify functions of the security administrator to perform security-related functions?

A. C2

B. B1

C. B2

D. B3

Correct Answer: D

Explanation: The Security Administrator role is define only at level B3 (and A1). It requires the system to clearly identify functions of security administrator to perform security-related functions.

TCSEC B2 level specifies that the system must support separation of operator and administrator roles.

TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation. U.S. Department of Defense, Trusted Computer System Evaluation Criteria (Orange Book), DOD 5200.28-STD. December 1985 (also available here). The CISSP?Prep

Guide, Second Edition: Mastering the CISSP and ISSEPTM Exams By Ronald L. Krutz and Russell Dean Vines on Page 308

QUESTION 35

In regards to information classification what is the main responsibility of information (data) owner?

A. determining the data sensitivity or classification level

B. running regular data backups

C. audit the data users

D. periodically check the validity and accuracy of the data

Correct Answer: A

Explanation: Making the determination to decide what level of classification the information requires is the main responsibility of the data owner.

The data owner within classification is a person from Management who has been entrusted with a data set that belong to the company. It could be for example the Chief Financial Officer (CFO) who has been entrusted with all financial date or

it could be the Human Resource Director who has been entrusted with all Human Resource data. The information owner will decide what classification will be applied to the data based on Confidentiality, Integrity, Availability, Criticality, and

Sensitivity of the data.

The Custodian is the technical person who will implement the proper classification on objects in accordance with the Data Owner. The custodian DOES NOT decide what classification to apply, it is the Data Owner who will dictate to the

Custodian what is the classification to apply.

NOTE:

The term Data Owner is also used within Discretionary Access Control (DAC). Within DAC it means the person who has created an object. For example, if I create a file on my system then I am the owner of the file and I can decide who else

could get access to the file. It is left to my discretion. Within DAC access is granted based solely on the Identity of the subject, this is why sometimes DAC is referred to as Identity Based Access Control.

The other choices were not the best answer

Running regular backups is the responsibility of custodian. Audit the data users is the responsibility of the auditors Periodically check the validity and accuracy of the data is not one of the data owner responsibility

Reference(s) used for this question:

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

John Wiley and Sons, 2001, Page 14, Chapter 1: Security Management Practices.

QUESTION 36

Which one of the following is NOT a typical bus designation in a digital computer?

A. Control

B. Address

C. Data

D. Secondary

Correct Answer: D

The correct answer is Secondary, a distracter.

QUESTION 37

The "vulnerability of a facility" to damage or attack may be assessed by all of the following except:

A. Inspection

B. History of losses

C. Security controls

D. security budget

Correct Answer: D

Explanation: Source: The CISSP Examination Textbook- Volume 2: Practice by S. Rao Vallabhaneni.

QUESTION 38

Which of the following is most concerned with personnel security?

A. Management controls

B. Operational controls

C. Technical controls

D. Human resources controls

Correct Answer: B

Explanation: Many important issues in computer security involve human users, designers, implementers, and managers.

A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs. Since operational controls address security methods focusing on mechanisms primarily

implemented and executed by people (as opposed to systems), personnel security is considered a form of operational control.

Operational controls are put in place to improve security of a particular system (or group of systems). They often require specialized expertise and often rely upon management activities as well as technical controls. Implementing dual control

and making sure that you have more than one person that can perform a task would fall into this category as well. Management controls focus on the management of the IT security system and the management of risk for a system. They are

techniques and concerns that are normally addressed by management.

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access of misuse, facilitate detection of security violations, and support security requirements

for applications and data.

Reference use for this question:

NIST SP 800-53 Revision 4 http://dx.doi.org/106028/NIST.SP.800-53r4 You can get it as a word document by clicking HERE NIST SP 800-53 Revision 4 has superseded the document below:

SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Page A-18).

QUESTION 39

When implementing controls in a heterogeneous end-point network for an organization, it is critical that

A. hosts are able to establish network communications.

B. users can make modifications to their security software configurations.

C. common software security components be implemented across all hosts.

D. firewalls running on each host are fully customizable by the user.

Correct Answer: C

QUESTION 40

Which of the following control helps to identify an incident\\'s activities and potentially an intruder?

A. Deterrent

B. Preventive

C. Detective

D. Compensating

Correct Answer: C

Explanation: Detective control helps identify an incident\\'s activities and potentially an intruder

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

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to

circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught)

outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an

attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process.

This oversight acts as a deterrent, curbing an attacker\\'s appetite in the face of probable repercussions. The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized

functions, leading to unwanted events. When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many

threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs. It is this fundamental reason why access controls are the key target of circumvention by

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

determine most employees from installing wireless access points.

Preventative Controls

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

cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker).

Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control\\'s implementation.

Compensating Controls

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

required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk. For example, the access control policy may

state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption

protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes,

such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of

least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk. As mentioned previously, strongly

managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise\\'s assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user

can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will

offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system. This can be used to detect the occurrence of errors, the

attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by

authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the

environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls

must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may

affect access controls, their applicability, status, or management.

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls

placed on system files or even have default administrative accounts unknowingly implemented upon install. Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation

of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation

must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:

Deterrent - Deterrent controls are intended to discourage a potential attacker Preventive - Preventive controls are intended to avoid an incident from occurring Compensating - Compensating Controls provide an alternative measure of control

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

CISA Review Manual 2014 Page number 44 and

Official ISC2 CISSP guide 3rd edition Page number 50 and 51

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.lead4pass.com/allproducts

Need Help

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