



ISC2

Exam Questions CSSLP

Certified Information Systems Security Professional

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

You and your project team have identified the project risks and now are analyzing the probability and impact of the risks. What type of analysis of the risks provides a quick and high-level review of each identified risk event?

- A. Quantitative risk analysis
- B. Qualitative risk analysis
- C. Seven risk responses
- D. A risk probability-impact matrix

Answer: B

Explanation:

Qualitative risk analysis is a high-level, fast review of the risk event. Qualitative risk analysis qualifies the risk events for additional analysis.

NEW QUESTION 2

You work as a project manager for BlueWell Inc. You are working on a project and the management wants a rapid and cost-effective means for establishing priorities for planning risk responses in your project. Which risk management process can satisfy management's objective for your project?

- A. Qualitative risk analysis
- B. Historical information
- C. Rolling wave planning
- D. Quantitative analysis

Answer: A

Explanation:

Qualitative risk analysis is the best answer as it is a fast and low-cost approach to analyze the risk impact and its effect. It can promote certain risks onto risk response planning. Qualitative Risk Analysis uses the likelihood and impact of the identified risks in a fast and cost-effective manner. Qualitative Risk Analysis establishes a basis for a focused quantitative analysis or Risk Response Plan by evaluating the precedence of risks with a concern to impact on the project's scope, cost, schedule, and quality objectives. The qualitative risk analysis is conducted at any point in a project life cycle. The primary goal of qualitative risk analysis is to determine proportion of effect and theoretical response. The inputs to the Qualitative Risk Analysis process are: Organizational process assets Project Scope Statement Risk Management Plan Risk Register Answer B is incorrect. Historical information can be helpful in the qualitative risk analysis, but it is not the best answer for the question as historical information is not always available (consider new projects). Answer D is incorrect. Quantitative risk analysis is in-depth and often requires a schedule and budget for the analysis. Answer C is incorrect. Rolling wave planning is not a valid answer for risk analysis processes.

NEW QUESTION 3

Which of the following roles is also known as the accreditor?

- A. Data owner
- B. Chief Risk Officer
- C. Chief Information Officer
- D. Designated Approving Authority

Answer: D

Explanation:

Designated Approving Authority (DAA) is also known as the accreditor. Answer A is incorrect. The data owner (information owner) is usually a member of management, in charge of a specific business unit, and is ultimately responsible for the protection and use of a specific subset of information. Answer B is incorrect. A Chief Risk Officer (CRO) is also known as Chief Risk Management Officer (CRMO). The Chief Risk Officer or Chief Risk Management Officer of a corporation is the executive accountable for enabling the efficient and effective governance of significant risks, and related opportunities, to a business and its various segments. Risks are commonly categorized as strategic, reputational, operational, financial, or compliance-related. CRO's are accountable to the Executive Committee and The Board for enabling the business to balance risk and reward. In more complex organizations, they are generally responsible for coordinating the organization's Enterprise Risk Management (ERM) approach. Answer C is incorrect. The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise responsible for the information technology and computer systems that support enterprise goals. The CIO plays the role of a leader and reports to the chief executive officer, chief operations officer, or chief financial officer. In military organizations, they report to the commanding officer.

NEW QUESTION 4

In which of the following cryptographic attacking techniques does an attacker obtain encrypted messages that have been encrypted using the same encryption algorithm?

- A. Chosen plaintext attack
- B. Chosen ciphertext attack
- C. Ciphertext only attack
- D. Known plaintext attack

Answer: C

Explanation:

In a ciphertext only attack, an attacker obtains encrypted messages that have been encrypted using the same encryption algorithm.

NEW QUESTION 5

Which of the following testing methods verifies the interfaces between components against a software design?

- A. Regression testing
- B. Integration testing

- C. Black-box testing
- D. Unit testing

Answer: B

Explanation:

Integration testing is a software testing that seeks to verify the interfaces between components against a software design. Software components may be integrated in an iterative way or all together ("big bang"). Normally the former is considered a better practice since it allows interface issues to be localized more quickly and fixed. Integration testing works to expose defects in the interfaces and interaction between the integrated components (modules). Progressively larger groups of tested software components corresponding to elements of the architectural design are integrated and tested until the software works as a system. Answer A is incorrect. Regression testing focuses on finding defects after a major code change has occurred. Specifically, it seeks to uncover software regressions, or old bugs that have come back. Such regressions occur whenever software functionality that was previously working correctly stops working as intended. Typically, regressions occur as an unintended consequence of program changes, when the newly developed part of the software collides with the previously existing code. Answer D is incorrect. Unit testing refers to tests that verify the functionality of a specific section of code, usually at the function level. In an object-oriented environment, this is usually at the class level, and the minimal unit tests include the constructors and destructors. These types of tests are usually written by developers as they work on code (white-box style), to ensure that the specific function is working as expected. One function might have multiple tests, to catch corner cases or other branches in the code. Unit testing alone cannot verify the functionality of a piece of software, but rather is used to assure that the building blocks the software uses work independently of each other. Answer C is incorrect. The black-box testing uses external descriptions of the software, including specifications, requirements, and design to derive test cases. These tests can be functional or non-functional, though usually functional. The test designer selects valid and invalid inputs and determines the correct output. There is no knowledge of the test object's internal structure. This method of test design is applicable to all levels of software testing: unit, integration, functional testing, system and acceptance. The higher the level, and hence the bigger and more complex the box, the more one is forced to use black box testing to simplify. While this method can uncover unimplemented parts of the specification, one cannot be sure that all existent paths are tested.

NEW QUESTION 6

An asset with a value of \$600,000 is subject to a successful malicious attack threat twice a year. The asset has an exposure of 30 percent to the threat. What will be the annualized loss expectancy?

- A. \$360,000
- B. \$180,000
- C. \$280,000
- D. \$540,000

Answer: A

Explanation:

The annualized loss expectancy will be \$360,000. Annualized loss expectancy (ALE) is the annually expected financial loss to an organization from a threat. The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as follows:

ALE = Single Loss Expectancy (SLE) * Annualized Rate of Occurrence (ARO) Here, it is as follows:

SLE = Asset value * EF (Exposure factor)

= 600,000 * (30/100)

= 600,000 * 0.30

= 180,000

ALE = SLE * ARO

= 180,000 * 2

= 360,000

Answer C, B, and D are incorrect. These are not valid answers.

NEW QUESTION 7

What are the subordinate tasks of the Initiate and Plan IA C&A phase of the DIACAP process? Each correct answer represents a complete solution. Choose all that apply.

- A. Initiate IA implementation plan
- B. Develop DIACAP strategy
- C. Assign IA controls.
- D. Assemble DIACAP team
- E. Register system with DoD Component IA Program.
- F. Conduct validation activity.

Answer: ABCDE

Explanation:

The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk.

The subordinate tasks of the Initiate and Plan IA C&A phase are as follows: Register system with DoD Component IA Program. Assign IA controls. Assemble DIACAP team. Develop DIACAP strategy. Initiate IA implementation plan. Answer F is incorrect. Validation activities are conducted in the second phase of the DIACAP process, i.e., Implement and Validate Assigned IA Controls.

NEW QUESTION 8

You work as a project manager for a company. The company has started a new security software project. The software configuration management will be used throughout the lifecycle of the project. You are tasked to modify the functional features and the basic logic of the software and then make them compatible to the initial design of the project. Which of the following procedures of the configuration management will you follow to accomplish the task?

- A. Configuration status accounting
- B. Configuration control
- C. Configuration audits
- D. Configuration identification

Answer: B

Explanation:

Configuration control is a procedure of the Configuration management. Configuration control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them. It supports the change of the functional and physical attributes of software at various points in time, and performs systematic control of changes to the identified attributes. Answer C is incorrect. Configuration audits confirm that the configuration identification for a configured item is accurate, complete, and will meet specified program needs. Configuration audits are broken into functional and physical configuration audits. They occur either at delivery or at the moment of effecting the change. A functional configuration audit ensures that functional and performance attributes of a configuration item are achieved, while a physical configuration audit ensures that a configuration item is installed in accordance with the requirements of its detailed design documentation. Answer D is incorrect. Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baselined. Baselining an attribute forces formal configuration change control processes to be effected in the event that these attributes are changed. Answer A is incorrect. The configuration status accounting procedure is the ability to record and report on the configuration baselines associated with each configuration item at any moment of time. It supports the functional and physical attributes of software at various points in time, and performs systematic control of accounting to the identified attributes for the purpose of maintaining software integrity and traceability throughout the software development life cycle.

NEW QUESTION 9

The NIST Information Security and Privacy Advisory Board (ISPAB) paper "Perspectives on Cloud Computing and Standards" specifies potential advantages and disadvantages of virtualization. Which of the following disadvantages does it include? Each correct answer represents a complete solution. Choose all that apply.

- A. It increases capabilities for fault tolerant computing using rollback and snapshot features.
- B. It increases intrusion detection through introspection.
- C. It initiates the risk that malicious software is targeting the VM environment.
- D. It increases overall security risk shared resources.
- E. It creates the possibility that remote attestation may not work.
- F. It involves new protection mechanisms for preventing VM escape, VM detection, and VM-VM interference.
- G. It increases configuration effort because of complexity and composite system.

Answer: CDEFG

Explanation:

The potential security disadvantages of virtualization are as follows: It increases configuration effort because of complexity and composite system. It initiates the problem of how to prevent overlap while mapping VM storage onto host files. It introduces the problem of virtualizing the TPM. It creates the possibility that remote attestation may not work. It initiates the problem of detecting VM covert channels. It involves new protection mechanisms for preventing VM escape, VM detection, and VM-VM interference. It initiates the possibility of virtual networking configuration errors. It initiates the risk that malicious software is targeting the VM environment.

It increases overall security risk shared resources, such as networks, clipboards, clocks, printers, desktop management, and folders. Answer A and B are incorrect. These are not the disadvantages of virtualization, as described in the NIST Information Security and Privacy Advisory Board (ISPAB) paper "Perspectives on Cloud Computing and Standards".

NEW QUESTION 10

Adam works as a Computer Hacking Forensic Investigator for a garment company in the United States. A project has been assigned to him to investigate a case of a disloyal employee who is suspected of stealing design of the garments, which belongs to the company and selling those garments of the same design under different brand name. Adam investigated that the company does not have any policy related to the copy of design of the garments. He also investigated that the trademark under which the employee is selling the garments is almost identical to the original trademark of the company. On the grounds of which of the following laws can the employee be prosecuted?

- A. Espionage law
- B. Trademark law
- C. Cyber law
- D. Copyright law

Answer: B

Explanation:

The Trademark law is a piece of legislation that contains the federal statutes of trademark law in the United States. The Act prohibits a number of activities, including trademark infringement, trademark dilution, and false advertising. Trademarks were traditionally protected in the United States only under State common law, growing out of the tort of unfair competition. Trademark law in the United States is almost entirely enforced through private lawsuits. The exception is in the case of criminal counterfeiting of goods. Otherwise, the responsibility is entirely on the mark owner to file suit in either state or federal civil court in order to restrict an infringing use. Failure to "police" a mark by stopping infringing uses can result in the loss of protection. Answer D is incorrect. Copyright law of the United States governs the legally enforceable rights of creative and artistic works under the laws of the United States. Copyright law in the United States is part of federal law, and is authorized by the U.S. Constitution. The power to enact copyright law is granted in Article I, Section 8, Clause 8, also known as the Copyright Clause. This clause forms the basis for U.S. copyright law ("Science", "Authors", "Writings") and patent law ("useful Arts", "Inventors", "Discoveries"), and includes the limited terms (or durations) allowed for copyrights and patents ("limited Times"), as well as the items they may protect. In the U.S., registrations of claims of copyright, recordation of copyright transfers, and other administrative aspects of copyright are the responsibility of the United States Copyright Office, a part of the Library of Congress. Answer A is incorrect. The Espionage Act of 1917 was a United States federal law passed shortly after entering World War I, on June 15, 1917, which made it a crime for a person: To convey information with intent to interfere with the operation or success of the armed forces of the United States or to promote the success of its enemies. This was punishable by death or by imprisonment for not more than 30 years. To convey false reports or false statements with intent to interfere with the operation or success of the military or naval forces of the United States or to promote the success of its enemies and whoever when the United States is at war, to cause or attempt to cause insubordination, disloyalty, mutiny, refusal of duty, in the military or naval forces of the United States, or to willfully obstruct the recruiting or enlistment service of the United States. Answer C is incorrect. Cyber law is a very wide term, which wraps up the legal issue related to the use of communicative, transactional and distributive aspect of networked information device and technologies. It is commonly known as INTERNET LAW. These Laws are important to apply as Internet does not tend to make any geographical and jurisdictional boundaries clear; this is the reason why Cyber law is not very efficient. A single transaction may involve the laws of at least three jurisdictions, which are as follows: 1.The laws of the state/nation in which the user resides 2.The laws of the state/nation that apply where the server hosting the transaction is located 3.The laws of the state/nation, which apply to the person or business with whom the transaction takes place

NEW QUESTION 10

DoD 8500.2 establishes IA controls for information systems according to the Mission Assurance Categories (MAC) and confidentiality levels. Which of the following MAC levels requires high integrity and medium availability?

- A. MAC III
- B. MAC IV
- C. MAC I
- D. MAC II

Answer: D

Explanation:

The various MAC levels are as follows: MAC I: It states that the systems have high availability and high integrity. MAC II: It states that the systems have high integrity and medium availability. MAC III: It states that the systems have basic integrity and availability.

NEW QUESTION 15

The Phase 4 of DITSCAP C&A is known as Post Accreditation. This phase starts after the system has been accredited in Phase 3. What are the process activities of this phase? Each correct answer represents a complete solution. Choose all that apply.

- A. Security operations
- B. Maintenance of the SSAA
- C. Compliance validation
- D. Change management
- E. System operations
- F. Continue to review and refine the SSAA

Answer: ABCDE

Explanation:

The Phase 4 of DITSCAP C&A is known as Post Accreditation. This phase starts after the system has been accredited in the Phase 3. The goal of this phase is to continue to operate and manage the system and to ensure that it will maintain an acceptable level of residual risk. The process activities of this phase are as follows: System operations Security operations Maintenance of the SSAA Change management Compliance validation Answer F is incorrect. It is a Phase 3 activity.

NEW QUESTION 19

Which of the following statements about the availability concept of Information security management is true?

- A. It ensures that modifications are not made to data by unauthorized personnel or processes.
- B. It determines actions and behaviors of a single individual within a system.
- C. It ensures reliable and timely access to resources.
- D. It ensures that unauthorized modifications are not made to data by authorized personnel or processes.

Answer: C

Explanation:

The concept of availability ensures reliable and timely access to data or resources. In other words, availability ensures that the systems are up and running when needed. The availability concept also ensures that the security services are in working order. Answer A and D are incorrect. The concept of integrity ensures that modifications are not made to data by unauthorized personnel or processes. It also ensures that unauthorized modifications are not made to data by authorized personnel or processes. Answer B is incorrect. Accountability determines the actions and behaviors of an individual within a system, and identifies that particular individual. Audit trails and logs support accountability.

NEW QUESTION 20

Martha registers a domain named Microsoft.in. She tries to sell it to Microsoft Corporation. The infringement of which of the following has she made?

- A. Copyright
- B. Trademark
- C. Patent
- D. Intellectual property

Answer: B

Explanation:

According to the Lanham Act, domain names fall under trademarks law. A new section 43(d) of the Trademark Act (Lanham Act) states that anyone who in bad faith registers, traffics in, or uses a domain name that infringes or dilutes another's trademark has committed trademark infringement. Factors involved in assessing bad faith focus on activities typically associated with cyberpiracy or cybersquatting, such as whether the registrant has offered to sell the domain name to the trademark holder for financial gain without having used or intended to use it for a bona fide business; whether the domain- name registrant registered multiple domain names that are confusingly similar to the trademarks of others; and whether the trademark incorporated in the domain name is distinctive and famous. Other factors are whether the domain name consists of the legal name or common handle of the domain-name registrant and whether the domain-name registrant previously used the mark in connection with a bona fide business.

NEW QUESTION 22

You work as a systems engineer for BlueWell Inc. Which of the following tools will you use to look outside your own organization to examine how others achieve their performance levels, and what processes they use to reach those levels?

- A. Benchmarking
- B. Six Sigma
- C. ISO 9001:2000
- D. SEI-CMM

Answer: A

Explanation:

Benchmarking is the tool used by system assessment process to provide a point of reference by which performance measurements can be reviewed with respect to other organizations. Benchmarking is also recognized as Best Practice Benchmarking or Process Benchmarking. It is a process used in management and mostly useful for strategic management. It is the process of comparing the business processes and performance metrics including cost, cycle time, productivity, or quality to another that is widely considered to be an industry standard benchmark or best practice. It allows organizations to develop plans on how to implement best practice with the aim of increasing some aspect of performance. Benchmarking might be a one-time event, although it is frequently treated as a continual process in which organizations continually seek out to challenge their practices. It allows organizations to develop plans on how to make improvements or adapt specific best practices, usually with the aim of increasing some aspect of performance. Answer C is incorrect. The ISO 9001:2000 standard combines the three standards 9001, 9002, and 9003 into one, called 9001. Design and development procedures are required only if a company does in fact engage in the creation of new products. The 2000 version sought to make a radical change in thinking by actually placing the concept of process management front and center ("Process management" was the monitoring and optimizing of a company's tasks and activities, instead of just inspecting the final product). The ISO 9001:2000 version also demands involvement by upper executives, in order to integrate quality into the business system and avoid delegation of quality functions to junior administrators. Another goal is to improve effectiveness via process performance metrics numerical measurement of the effectiveness of tasks and activities. Expectations of continual process improvement and tracking customer satisfaction were made explicit. Answer B is incorrect. Six Sigma is a business management strategy, initially implemented by Motorola. As of 2009 it enjoys widespread application in many sectors of industry, although its application is not without controversy. Six Sigma seeks to improve the quality of process outputs by identifying and removing the causes of defects and variability in manufacturing and business processes. It uses a set of quality management methods, including statistical methods, and creates a special infrastructure of people within the organization ("Black Belts", "Green Belts", etc.) who are experts in these methods. Each Six Sigma project carried out within an organization follows a defined sequence of steps and has quantified financial targets (cost reduction or profit increase). The often used Six Sigma symbol is as follows:



Answer D is incorrect. Capability Maturity Model Integration (CMMI) was created by Software Engineering Institute (SEI). CMMI in software engineering and organizational development is a process improvement approach that provides organizations with the essential elements for effective process improvement. It can be used to guide process improvement across a project, a division, or an entire organization. CMMI can help integrate traditionally separate organizational functions, set process improvement goals and priorities, provide guidance for quality processes, and provide a point of reference for appraising current processes. CMMI is now the de facto standard for measuring the maturity of any process. Organizations can be assessed against the CMMI model using Standard CMMI Appraisal Method for Process Improvement (SCAMPI).

NEW QUESTION 26

Della works as a security engineer for BlueWell Inc. She wants to establish configuration management and control procedures that will document proposed or actual changes to the information system. Which of the following phases of NIST SP 800-37 C&A methodology will define the above task?

- A. Initiation
- B. Security Certification
- C. Continuous Monitoring
- D. Security Accreditation

Answer: C

Explanation:

The various phases of NIST SP 800-37 C&A are as follows:

Phase 1: Initiation- This phase includes preparation, notification and resource identification. It performs the security plan analysis, update, and acceptance. Phase 2: Security Certification- The Security certification phase evaluates the controls and documentation. Phase 3: Security Accreditation- The security accreditation phase examines the residual risk for acceptability, and prepares the final security accreditation package. Phase 4: Continuous Monitoring-This phase monitors the configuration management and control, ongoing security control verification, and status reporting and documentation.

NEW QUESTION 28

Which of the following tools is used to attack the Digital Watermarking?

- A. Steg-Only Attack
- B. Active Attacks
- C. 2Mosaic
- D. Gifshuffle

Answer: C

Explanation:

2Mosaic is a tool used for watermark breaking. It is an attack against a digital watermarking system. In this type of attack, an image is chopped into small pieces and then placed together. When this image is embedded into a web page, the web browser renders the small pieces into one image. This image looks like a real image with no watermark in it. This attack is successful, as it is impossible to read watermark in very small pieces. Answer D is incorrect. Gifshuffle is used to hide message or information inside GIF images. It is done by shuffling the colormap. This tool also provides compression and encryption. Answer B and A are incorrect. Active Attacks and Steg-Only Attacks are used to attack Steganography.

NEW QUESTION 29

CORRECT TEXT

Fill in the blank with an appropriate phrase. models address specifications, requirements, design, verification and validation, and maintenance activities.

- A. Life cycle

Answer: A

Explanation:

A life cycle model helps to provide an insight into the development process and emphasizes on the relationships among the different activities in this process. This model describes a structured approach to the development and adjustment process involved in producing and maintaining systems. The life cycle model

addresses specifications, design, requirements, verification and validation, and maintenance activities.

NEW QUESTION 31

Which of the following penetration testing techniques automatically tests every phone line in an exchange and tries to locate modems that are attached to the network?

- A. Demon dialing
- B. Sniffing
- C. Social engineering
- D. Dumpster diving

Answer: A

Explanation:

The demon dialing technique automatically tests every phone line in an exchange and tries to locate modems that are attached to the network. Information about these modems can then be used to attempt external unauthorized access. Answer B is incorrect. In sniffing, a protocol analyzer is used to capture data packets that are later decoded to collect information such as passwords or infrastructure configurations. Answer D is incorrect. Dumpster diving technique is used for searching paper disposal areas for unshredded or otherwise improperly disposed-of reports. Answer C is incorrect. Social engineering is the most commonly used technique of all, getting information (like passwords) just by asking for them.

NEW QUESTION 32

Which of the following actions does the Data Loss Prevention (DLP) technology take when an agent detects a policy violation for data of all states? Each correct answer represents a complete solution. Choose all that apply.

- A. It creates an alert.
- B. It quarantines the file to a secure location.
- C. It reconstructs the session.
- D. It blocks the transmission of content.

Answer: ABD

Explanation:

When an agent detects a policy violation for data of all states, the Data Loss prevention (DLP) technology takes one of the following actions: It creates an alert. It notifies an administrator of a violation. It quarantines the file to a secure location. It encrypts the file. It blocks the transmission of content. Answer C is incorrect. Data Loss Prevention (DLP) reconstructs the session when data is in motion.

NEW QUESTION 34

Which of the following statements best describes the difference between the role of a data owner and the role of a data custodian?

- A. The custodian makes the initial information classification assignments, and the operations manager implements the scheme.
- B. The data owner implements the information classification scheme after the initial assignment by the custodian.
- C. The custodian implements the information classification scheme after the initial assignment by the operations manager.
- D. The data custodian implements the information classification scheme after the initial assignment by the data owner.

Answer: D

Explanation:

The data owner is responsible for ensuring that the appropriate security controls are in place, for assigning the initial classification to the data to be protected, for approving access requests from other parts of the organization, and for periodically reviewing the data classifications and access rights. Data owners are primarily responsible for determining the data's sensitivity or classification levels, whereas the data custodian has the responsibility for backup, retention, and recovery of data. The data owner delegates these responsibilities to the custodian. Answer B, A, and C are incorrect. These are not the valid answers.

NEW QUESTION 35

Penetration testing (also called pen testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker could exploit. Which of the following areas can be exploited in a penetration test? Each correct answer represents a complete solution. Choose all that apply.

- A. Kernel flaws
- B. Information system architectures
- C. Race conditions
- D. File and directory permissions
- E. Buffer overflows
- F. Trojan horses
- G. Social engineering

Answer: ACDEFG

Explanation:

Penetration testing (also called pen testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker could exploit. Following are the areas that can be exploited in a penetration test: Kernel flaws: Kernel flaws refer to the exploitation of kernel code flaws in the operating system. Buffer overflows: Buffer overflows refer to the exploitation of a software failure to properly check for the length of input data. This overflow can cause malicious behavior on the system. Race conditions: A race condition is a situation in which an attacker can gain access to a system as a privileged user. File and directory permissions: In this area, an attacker exploits weak permissions restrictions to gain unauthorized access of documents. Trojan horses: These are malicious programs that can exploit an information system by attaching themselves in valid programs and files. Social engineering: In this technique, an attacker uses his social skills and persuasion to acquire valuable information that can be used to conduct an attack against a system.

NEW QUESTION 40

Which of the following security controls works as the totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy?

- A. Common data security architecture (CDSA)
- B. Application program interface (API)
- C. Trusted computing base (TCB)
- D. Internet Protocol Security (IPSec)

Answer: C

Explanation:

Trusted computing base (TCB) refers to hardware, software, controls, and processes that cause a computer system or network to be devoid of malicious software or hardware. Maintaining the trusted computing base (TCB) is essential for security policy to be implemented successfully. Answer D is incorrect. Internet Protocol Security (IPSec) is a standard-based protocol that provides the highest level of VPN security. IPSec can encrypt virtually everything above the networking layer. It is used for VPN connections that use the L2TP protocol. It secures both data and password. IPSec cannot be used with Point-to-Point Tunneling Protocol (PPTP). Answer A is incorrect. The Common data security architecture (CDSA) is a set of layered security services and cryptographic framework. It deals with the communications and data security problems in the emerging Internet and intranet application space. It presents an infrastructure for building cross-platform, interoperable, security-enabled applications for client-server environments. Answer B is incorrect. An application programming interface (API) is an interface implemented by a software program which enables it to interact with other software. It facilitates interaction between different software programs similar to the way the user interface facilitates interaction between humans and computers. An API is implemented by applications, libraries, and operating systems to determine their vocabularies and calling conventions, and is used to access their services. It may include specifications for routines, data structures, object classes, and protocols used to communicate between the consumer and the implementer of the API.

NEW QUESTION 45

Which of the following is a malicious exploit of a website, whereby unauthorized commands are transmitted from a user trusted by the website?

- A. Cross-Site Scripting
- B. Injection flaw
- C. Side channel attack
- D. Cross-Site Request Forgery

Answer: D

Explanation:

CSRF (Cross-Site Request Forgery) is a malicious exploit of a website, whereby unauthorized commands are transmitted from a user trusted by the website. It is also known as a one-click attack or session riding. CSRF occurs when a user is tricked by an attacker into activating a request in order to perform some unauthorized action. It increases data loss and malicious code execution. Answer A is incorrect. Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications which enable malicious attackers to inject client-side script into web pages viewed by other users. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls, such as the same origin policy. Cross-site scripting carried out on websites were roughly 80% of all security vulnerabilities documented by Symantec as of 2007. Their impact may range from a petty nuisance to a significant security risk, depending on the sensitivity of the data handled by the vulnerable site, and the nature of any security mitigations implemented by the site owner. Answer C is incorrect. A side channel attack is based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms (compare cryptanalysis). For example, timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information which can be exploited to break the system. Many side-channel attacks require considerable technical knowledge of the internal operation of the system on which the cryptography is implemented. Answer B is incorrect. Injection flaws are the vulnerabilities where a foreign agent illegally uses a sub-system. They are the vulnerability holes that can be used to attack a database of Web applications. It is the most common technique of attacking a database. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing involuntary commands or changing data. Injection flaws include XSS (HTML Injection) and SQL Injection.

NEW QUESTION 50

Which of the following activities are performed by the 'Do' cycle component of PDCA (plan- do-check-act)? Each correct answer represents a complete solution. Choose all that apply.

- A. It detects and responds to incidents properly.
- B. It determines controls and their objectives.
- C. It manages resources that are required to achieve a goal.
- D. It performs security awareness training.
- E. It operates the selected controls.

Answer: ACDE

Explanation:

The 'Do' cycle component performs the following activities: It operates the selected controls. It detects and responds to incidents properly. It performs security awareness training. It manages resources that are required to achieve a goal. Answer B is incorrect. This activity is performed by the 'Plan' cycle component of PDCA.

NEW QUESTION 53

Which of the following techniques is used to identify attacks originating from a botnet?

- A. Passive OS fingerprinting
- B. Recipient filtering
- C. IFilter
- D. BPF-based filter

Answer: A

Explanation:

Passive OS fingerprinting can identify attacks originating from a botnet. Network Administrators can configure the firewall to take action on a botnet attack by using information obtained from passive OS fingerprinting. Passive OS fingerprinting (POSFP) allows the sensor to determine the operating system used by the hosts. The sensor examines the traffic flow between two hosts and then stores the operating system of those two hosts along with their IP addresses. In order to determine the type of operating system, the sensor analyzes TCP SYN and SYN ACK packets that are traveled on the network. The sensor computes the attack relevance rating to determine the relevancy of victim attack using the target host OS. After it, the sensor modifies the alert's risk rating or filters the alert for the attack. Passive OS fingerprinting is also used to improve the alert output by reporting some information, such as victim OS, relevancy to the victim in the alert, and

source of the OS identification. Answer D is incorrect. A BPF-based filter is used to limit the number of packets seen by tcpdump; this renders the output more usable on networks with a high volume of traffic. Answer B is incorrect. Recipient filtering is used to block messages on the basis of whom they are sent to. Answer C is incorrect. IFilters are used to extract contents from files that are crawled. IFilters also remove application-specific formatting before the content of a document is indexed by the search engine.

NEW QUESTION 56

Which of the following are included in Technical Controls? Each correct answer represents a complete solution. Choose all that apply.

- A. Identification and authentication methods
- B. Configuration of the infrastructure
- C. Password and resource management
- D. Implementing and maintaining access control mechanisms
- E. Security devices
- F. Conducting security-awareness training

Answer: ABCDE

Explanation:

Technical Controls are also known as Logical Controls. These controls include the following: Implementing and maintaining access control mechanisms Password and resource management Identification and authentication methods Security devices Configuration of the infrastructure Answer F is incorrect. It is a part of Administrative Controls.

NEW QUESTION 58

Which of the following agencies is responsible for funding the development of many technologies such as computer networking, as well as NLS?

- A. DIAP
- B. DTIC
- C. DARPA
- D. DISA

Answer: C

Explanation:

The Defense Advanced Research Projects Agency (DARPA) is an agency of the United States Department of Defense responsible for the development of new technology for use by the military. DARPA has been responsible for funding the development of many technologies which have had a major effect on the world, including computer networking, as well as NLS, which was both the first hypertext system, and an important precursor to the contemporary ubiquitous graphical user interface. DARPA supplies technological options for the entire Department, and is designed to be the "technological engine" for transforming DoD. Answer D is incorrect. The Defense Information Systems Agency is a United States Department of Defense combat support agency with the goal of providing real-time information technology (IT) and communications support to the President, Vice President, Secretary of Defense, the military Services, and the Combatant Commands. DISA, a Combat Support Agency, engineers and provides command and control capabilities and enterprise infrastructure to continuously operate and assure a global net-centric enterprise in direct support to joint warfighters, National level leaders, and other mission and coalition partners across the full spectrum of operations.

Answer B is incorrect. The Defense Technical Information Center (DTIC) is a repository of scientific and technical documents for the United States Department of Defense. DTIC serves the DoD community as the largest central resource for DoD and government-funded scientific, technical, engineering, and business related information available today. DTIC's documents are available to DoD personnel and defense contractors, with unclassified documents also available to the public. DTIC's aim is to serve a vital link in the transfer of information among DoD personnel, DoD contractors, and potential contractors and other U.S. Government agency personnel and their contractors. Answer A is incorrect. The Defense-wide Information Assurance Program (DIAP) protects and supports DoD information, information systems, and information networks, which is important to the Department and the armed forces throughout the day-to-day operations, and in the time of crisis. The DIAP uses the OSD method to plan, observe, organize, and incorporate IA activities. The role of DIAP is to act as a facilitator for program execution by the combatant commanders, Military Services, and Defense Agencies. The DIAP staff combines functional and programmatic skills for a comprehensive Defense-wide approach to IA. The DIAP's main objective is to ensure that the DoD's vital information resources are secured and protected by incorporating IA activities to get a secure net-centric GIG operation enablement and information supremacy by applying a Defense-in-Depth methodology that integrates the capabilities of people, operations, and technology to establish a multi-layer, multidimensional protection.

NEW QUESTION 60

Which of the following is an open source network intrusion detection system?

- A. NETSH
- B. Macof
- C. Sourcefire
- D. Snort

Answer: D

Explanation:

Snort is an open source network intrusion prevention and detection system that operates as a network sniffer. It logs activities of the network that is matched with the predefined signatures. Signatures can be designed for a wide range of traffic, including Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP). The three main modes in which Snort can be configured are as follows: Sniffer mode: It reads the packets of the network and displays them in a continuous stream on the console. Packet logger mode: It logs the packets to the disk. Network intrusion detection mode: It is the most complex and configurable configuration, allowing Snort to analyze network traffic for matches against a user-defined rule set. Answer B is incorrect. Macof is a tool of the dsniiff tool set and used to flood the local network with random MAC addresses. It causes some switches to fail open in repeating mode, and facilitates sniffing. Answer C is incorrect. Sourcefire is the company that owns and maintains Snort. Answer A is incorrect. NETSH is not a network intrusion detection system. NETSH is a command line tool to configure TCP/IP settings such as the IP address, Subnet Mask, Default Gateway, DNS, WINS addresses, etc.

NEW QUESTION 65

You work as a security manager for BlueWell Inc. You are going through the NIST SP 800- 37 C&A methodology, which is based on four well defined phases. In which of the following phases of NIST SP 800-37 C&A methodology does the security categorization occur?

- A. Security Accreditation
- B. Security Certification
- C. Continuous Monitoring
- D. Initiation

Answer: D

Explanation:

The various phases of NIST SP 800-37 C&A are as follows: Phase 1: Initiation- This phase includes preparation, notification and resource identification. It performs the security plan analysis, update, and acceptance. Phase 2: Security Certification- The Security certification phase evaluates the controls and documentation. Phase 3: Security Accreditation- The security accreditation phase examines the residual risk for acceptability, and prepares the final security accreditation package. Phase 4: Continuous Monitoring-This phase monitors the configuration management and control, ongoing security control verification, and status reporting and documentation.

NEW QUESTION 69

Fill in the blank with the appropriate security mechanism. is a computer hardware mechanism or programming language construct which handles the occurrence of exceptional events.

- A. Exception handling

Answer: A

Explanation:

Exception handling is a computer hardware mechanism or programming language construct that handles the occurrence of events. These events occur during the software execution process and interrupt the instruction flow. Exception handling performs the specific activities for managing the exceptional events.

NEW QUESTION 71

Which of the following plans is designed to protect critical business processes from natural or man-made failures or disasters and the resultant loss of capital due to the unavailability of normal business processes?

- A. Contingency plan
- B. Business continuity plan
- C. Crisis communication plan
- D. Disaster recovery plan

Answer: B

Explanation:

The business continuity plan is designed to protect critical business processes from natural or man-made failures or disasters and the resultant loss of capital due to the unavailability of normal business processes. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan. Answer C is incorrect. The crisis communication plan can be broadly defined as the plan for the exchange of information before, during, or after a crisis event. It is considered as a sub-specialty of the public relations profession that is designed to protect and defend an individual, company, or organization facing a public challenge to its reputation. The aim of crisis communication plan is to assist organizations to achieve continuity of critical business processes and information flows under crisis, disaster or event driven circumstances. Answer A is incorrect. A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and "triggers" for initiating planned actions. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption. Answer D is incorrect. A disaster recovery plan should contain data, hardware, and software that can be critical for a business. It should also include the plan for sudden loss such as hard disc crash. The business should use backup and data recovery utilities to limit the loss of data.

NEW QUESTION 75

Martha works as a Project Leader for BlueWell Inc. She and her team have developed accounting software. The software was performing well. Recently, the software has been modified. The users of this software are now complaining about the software not working properly. Which of the following actions will she take to test the software?

- A. Perform integration testing
- B. Perform regression testing
- C. Perform unit testing
- D. Perform acceptance testing

Answer: B

Explanation:

Regression testing can be performed any time when a program needs to be modified either to add a feature or to fix an error. It is a process of repeating Unit testing and Integration testing whenever existing tests need to be performed again along with the new tests. Regression testing is performed to ensure that no existing errors reappear, and no new errors are introduced. Answer D is incorrect. The acceptance testing is performed on the application before its implementation into the production environment. It is done either by a client or an application specialist to ensure that the software meets the requirement for which it was made. Answer A is incorrect. Integration testing is a logical extension of unit testing. It is performed to identify the problems that occur when two or more units are combined into a component. During integration testing, a developer combines two units that have already been tested into a component, and tests the interface between the two units. Although integration testing can be performed in various ways, the following three approaches are generally used: The top-down approach The bottom-up approach The umbrella approach Answer B is incorrect. Unit testing is a type of testing in which each independent unit of an application is tested separately. During unit testing, a developer takes the smallest unit of an application, isolates it from the rest of the application code, and tests it to determine whether it works as expected. Unit testing is performed before integrating these independent units into modules. The most common approach to unit testing requires drivers and stubs to be written. Drivers and stubs are programs. A driver simulates a calling unit, and a stub simulates a called unit.

NEW QUESTION 78

Which of the following terms ensures that no intentional or unintentional unauthorized modification is made to data?

- A. Non-repudiation
- B. Integrity
- C. Authentication
- D. Confidentiality

Answer: B

Explanation:

Integrity ensures that no intentional or unintentional unauthorized modification is made to data. Answer D is incorrect. Confidentiality refers to the protection of data against unauthorized access. Administrators can provide confidentiality by encrypting data. Answer A is incorrect. Non-repudiation is a mechanism to prove that the sender really sent this message. Answer B is incorrect. Authentication is the process of verifying the identity of a person or network host.

NEW QUESTION 83

The Web resource collection is a security constraint element summarized in the Java Servlet Specification v2.4. Which of the following elements does it include? Each correct answer represents a complete solution. Choose two.

- A. HTTP methods
- B. Role names
- C. Transport guarantees
- D. URL patterns

Answer: AD

Explanation:

Web resource collection is a set of URL patterns and HTTP operations that define all resources required to be protected. It is a security constraint element summarized in the Java Servlet Specification v2.4. The Web resource collection includes the following elements: URL patterns HTTP methods. Answer B is incorrect. An authorization constraint includes role names. Answer C is incorrect. A user data constraint includes transport guarantees.

NEW QUESTION 85

Which of the following authentication methods is used to access public areas of a Web site?

- A. Anonymous authentication
- B. Biometrics authentication
- C. Mutual authentication
- D. Multi-factor authentication

Answer: A

Explanation:

Anonymous authentication is an authentication method used for Internet communication. It provides limited access to specific public folders and directory information or public areas of a Web site. It is supported by all clients and is used to access unsecured content in public folders. An administrator must create a user account in IIS to enable the user to connect anonymously. Answer D is incorrect. Multi-factor authentication involves a combination of multiple methods of authentication. For example, an authentication method that uses smart cards as well as usernames and passwords can be referred to as multi-factor authentication. Answer B is incorrect. Mutual authentication is a process in which a client process and server are required to prove their identities to each other before performing any application function. The client and server identities can be verified through a trusted third party and use shared secrets as in the case of Kerberos v5.

The MS-CHAP v2 and EAP-TLS authentication methods support mutual authentication. Answer C is incorrect. Biometrics authentication uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical qualities to identify a user.

NEW QUESTION 86

Which of the following statements are true about declarative security? Each correct answer represents a complete solution. Choose all that apply.

- A. It is employed in a layer that relies outside of the software code or uses attributes of the code.
- B. It applies the security policies on the software applications at their runtime.
- C. In this security, authentication decisions are made based on the business logic.
- D. In this security, the security decisions are based on explicit statements.

Answer: ABD

Explanation:

Declarative security applies the security policies on the software applications at their runtime. In this type of security, the security decisions are based on explicit statements that confine security behavior. Declarative security applies security permissions that are required for the software application to access the local resources and provides role-based access control to an individual software component and software application. It is employed in a layer that relies outside of the software code or uses attributes of the code. Answer C is incorrect. In declarative security, authentication decisions are coarse-grained in nature from an operational or external security perspective.

NEW QUESTION 91

You work as a Security Manager for Tech Perfect Inc. The company has a Windows based network. It is required to determine compatibility of the systems with custom applications. Which of the following techniques will you use to accomplish the task?

- A. Safe software storage
- B. Antivirus management
- C. Backup control
- D. Software testing

Answer: D

Explanation:

In order to accomplish the task, you should use the software testing technique. By using this technique you can determine compatibility of systems with custom applications or you can identify other unforeseen interactions. You can also use the software testing technique while you are upgrading software. Answer B is incorrect. You can use the antivirus management to save the systems from viruses, unexpected software interactions, and the subversion of security controls. Answer A is incorrect. You can use the safe software storage technique to ensure that the software and backup copies have not been modified without authorization. Answer B is incorrect. You can use the backup control to perform back up of software and data.

NEW QUESTION 96

Which of the following types of obfuscation transformation increases the difficulty for a de-obfuscation tool so that it cannot extract the true application from the obfuscated version?

- A. Preventive transformation
- B. Data obfuscation
- C. Control obfuscation
- D. Layout obfuscation

Answer: A

Explanation:

Preventive transformation increases the difficulty for a de-obfuscation tool so that it cannot extract the true application from the obfuscated version.

NEW QUESTION 99

Which of the following programming languages are compiled into machine code and directly executed by the CPU of a computer system? Each correct answer represents a complete solution. Choose two.

- A. C
- B. Microosft.NET
- C. Java EE
- D. C++

Answer: AD

Explanation:

C and C++ programming languages are unmanaged code. Unmanaged code is compiled into machine code and directly executed by the CPU of a computer system. Answer C and B are incorrect. Java EE and Microsoft.Net are compiled into an intermediate code format.

NEW QUESTION 104

Which of the following requires all general support systems and major applications to be fully certified and accredited before these systems and applications are put into production? Each correct answer represents a part of the solution. Choose all that apply.

- A. NIST
- B. Office of Management and Budget (OMB)
- C. FIPS
- D. FISMA

Answer: BD

Explanation:

FISMA and Office of Management and Budget (OMB) require all general support systems and major applications to be fully certified and accredited before they are put into production. General support systems and major applications are also referred to as information systems and are required to be reaccredited every three years. Answer A is incorrect. The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce. The institute's official mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. Answer B is incorrect. The Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States federal government for use by all non-military government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community (ANSI, IEEE, ISO, etc.). Some FIPS standards were originally developed by the U.S. government. For instance, standards for encoding data (e.g., country codes), but more significantly some encryption standards, such as the Data Encryption Standard (FIPS 46-3) and the Advanced Encryption Standard (FIPS 197). In 1994, NOAA (Noaa) began broadcasting coded signals called FIPS (Federal Information Processing System) codes along with their standard weather broadcasts from local stations. These codes identify the type of emergency and the specific geographic area (such as a county) affected by the emergency.

NEW QUESTION 105

Which of the following is a standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system?

- A. FITSAF
- B. FIPS
- C. TCSEC
- D. SSAA

Answer: C

Explanation:

Trusted Computer System Evaluation Criteria (TCSEC) is a United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. TCSEC was used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information. It was replaced with the development of the Common Criteria international standard originally published in 2005. The TCSEC, frequently referred to as the Orange Book, is the centerpiece of the DoD Rainbow Series publications. Answer D is incorrect. System Security Authorization Agreement (SSAA) is an information security document used in the United States Department of Defense (DoD) to describe and accredit networks and systems. The SSAA is part of the Department of Defense Information Technology Security Certification and Accreditation Process, or DITSCAP (superseded by DIACAP). The DoD instruction (issues in December 1997, that describes DITSCAP and provides an outline for the SSAA document is DODI 5200.40. The DITSCAP application manual (DoD 8510.1- M), published in July 2000, provides additional

details. Answer A is incorrect. FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. It provides an approach for federal agencies. It determines how federal agencies are meeting existing policy and establish goals. The main advantage of FITSAF is that it addresses the requirements of Office of Management and Budget (OMB). It also addresses the guidelines provided by the National Institute of Standards and Technology (NIST). Answer B is incorrect. The Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States federal government for use by all non-military government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community (ANSI, IEEE, ISO, etc.). Some FIPS standards were originally developed by the U.S. government. For instance, standards for encoding data (e.g., country codes), but more significantly some encryption standards, such as the Data Encryption Standard (FIPS 46-3) and the Advanced Encryption Standard (FIPS 197). In 1994, NOAA (Noaa) began broadcasting coded signals called FIPS (Federal Information Processing System) codes along with their standard weather broadcasts from local stations. These codes identify the type of emergency and the specific geographic area (such as a county) affected by the emergency.

NEW QUESTION 109

Which of the following phases of the DITSCAP C&A process is used to define the C&A level of effort, to identify the main C&A roles and responsibilities, and to create an agreement on the method for implementing the security requirements?

- A. Phase 1
- B. Phase 4
- C. Phase 2
- D. Phase 3

Answer: A

Explanation:

The Phase 1 of the DITSCAP C&A process is known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements. Answer B is incorrect. The Phase 2 of the DITSCAP C&A process is known as Verification. Answer D is incorrect. The Phase 3 of the DITSCAP C&A process is known as Validation. Answer B is incorrect. The Phase 4 of the DITSCAP C&A process is known as Post Accreditation.

NEW QUESTION 113

What are the security advantages of virtualization, as described in the NIST Information Security and Privacy Advisory Board (ISPAB) paper "Perspectives on Cloud Computing and Standards"? Each correct answer represents a complete solution. Choose three.

- A. It increases capabilities for fault tolerant computing.
- B. It adds a layer of security for defense-in-depth.
- C. It decreases exposure of weak software.
- D. It decreases configuration effort.

Answer: ABC

Explanation:

The security advantages of virtualization are as follows: It adds a layer of security for defense-in-depth. It provides strong encapsulation of errors. It increases intrusion detection through introspection. It decreases exposure of weak software. It increases the flexibility for discovery. It increases capabilities for fault tolerant computing using rollback and snapshot features. Answer D is incorrect. Virtualization increases configuration effort because of complexity of the virtualization layer and composite system.

NEW QUESTION 115

Which of the following are the principle duties performed by the BIOS during POST (power- on-self-test)? Each correct answer represents a part of the solution. Choose all that apply.

- A. It provides a user interface for system's configuration.
- B. It identifies, organizes, and selects boot devices.
- C. It delegates control to other BIOS, if it is required.
- D. It discovers size and verifies system memory.
- E. It verifies the integrity of the BIOS code itself.
- F. It interrupts the execution of all running programs.

Answer: ABCDE

Explanation:

The principle duties performed by the BIOS during POST (power-on-self- test) are as follows: It verifies the integrity of the BIOS code itself. It discovers size and verifies system memory. It discovers, initializes, and catalogs all system hardware. It delegates control to other BIOS if it is required. It provides a user interface for system's configuration. It identifies, organizes, and selects boot devices. It executes the bootstrap program. Answer F is incorrect. The BIOS does not interrupt the execution of all running programs.

NEW QUESTION 116

Which of the following are the goals of risk management? Each correct answer represents a complete solution. Choose three.

- A. Identifying the risk
- B. Assessing the impact of potential threats
- C. Identifying the accused
- D. Finding an economic balance between the impact of the risk and the cost of the countermeasure

Answer: ABD

Explanation:

There are three goals of risk management as follows: Identifying the risk Assessing the impact of potential threats Finding an economic balance between the impact of the risk and the cost of the countermeasure Answer B is incorrect. Identifying the accused does not come under the scope of risk management.

NEW QUESTION 121

DRAG DROP

Drag and drop the correct DoD Policy Series at their appropriate places.

Policy Subject Area	DoD Policy Series	
General	Drop Here	8540
IA Certification and Accreditation	Drop Here	8570
Security Management	Drop Here	8530
Computer Network Defense	Drop Here	8520
IA Education, Training, and Awareness	Drop Here	8510
Interconnectivity	Drop Here	8500

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The various DoD policy series are as follows:

DoD Policy Series	Policy Subject Area
8500	General
8510	IA Certification and Accreditation
8520	Security Management
8530	Computer Network Defense
8540	Interconnectivity
8550	Network and Web
8560	IA Monitoring
8570	IA Education, Training, and Awareness
8580	Other (Integration)

NEW QUESTION 122

Which of the following are examples of passive attacks? Each correct answer represents a complete solution. Choose all that apply.

- A. Dumpster diving
- B. Placing a backdoor
- C. Eavesdropping
- D. Shoulder surfing

Answer: ACD

Explanation:

In eavesdropping, dumpster diving, and shoulder surfing, the attacker violates the confidentiality of a system without affecting its state. Hence, they are considered passive attacks.

NEW QUESTION 123

DRAG DROP

Auditing is used to track user accounts for file and object access, logon attempts, system shutdown, and many more vulnerabilities to enhance the security of the network. It encompasses a wide variety of activities. Place the different auditing activities in front of their descriptions.

Command	Description	
Place Here	It is the activity of recording information to a log file or database about events or occurrences.	Log Analysis
Place Here	It is the activity of manually or programmatically reviewing logged information.	Intrusion Detection
Place Here	These are the notifications that are sent to an administrator whenever a specific event occurs.	Alarm Triggers
Place Here	It is a process to detect unwanted system access by monitoring both recorded information and real time events.	Monitoring
Place Here	It is a systematic form of monitoring where the logged information is analyzed in detail. It is done to find out the trends and patterns as well as abnormal, unauthorized, illegal, and policy-violating activities.	Logging

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Auditing encompasses a wide variety of activities as follows: Logging: It is the activity of recording information to a log file or database about events or occurrences. Log Analysis: It is a systematic form of monitoring where the logged information is analyzed in detail. It is done to find out the trends and patterns as well as abnormal, unauthorized, illegal, and policy-violating activities. Intrusion Detection: It is a process to detect unwanted system access by monitoring both recorded information and real time events. Alarm Triggers: These are the notifications that are sent to an administrator whenever a specific event occurs. Monitoring: It is the activity of manually or programmatically reviewing logged information.

NEW QUESTION 125

Which of the following elements of the BCP process emphasizes on creating the scope and the additional elements required to define the parameters of the plan?

- A. Business continuity plan development
 B. Plan approval and implementation
 C. Business impact analysis
 D. Scope and plan initiation

Answer: D

Explanation:

The scope and plan initiation process in BCP symbolizes the beginning of the BCP process. It emphasizes on creating the scope and the additional elements required to define the parameters of the plan. The scope and plan initiation phase embodies a check of the company's operations and support services. The scope activities include creating a detailed account of the work required, listing the resources to be used, and defining the management practices to be employed. Answer B is incorrect. The business impact assessment is a method used to facilitate business units to understand the impact of a disruptive event. This phase includes the execution of a vulnerability assessment. This process makes out the mission-critical areas and business processes that are important for the survival of business. It is similar to the risk assessment process. The function of a business impact assessment process is to create a document, which is used to help and understand what impact a disruptive event would have on the business. Answer A is incorrect. The business continuity plan development refers to the utilization of the information collected in the Business Impact Analysis (BIA) for the creation of the recovery strategy plan to support the critical business functions. The information gathered from the BIA is mapped out to make a strategy for creating a continuity plan. The business continuity plan development process includes the areas of plan implementation, plan testing, and ongoing plan maintenance. This phase also consists of defining and documenting the continuity strategy. Answer B is incorrect. The plan approval and implementation process involves creating enterprise-wide awareness of the plan, getting the final senior management signoff, and implementing a maintenance procedure for updating the plan as required.

NEW QUESTION 130

Fill in the blank with an appropriate phrase. A is defined as any activity that has an effect on defining, designing, building, or executing a task, requirement, or procedure.

- A. technical effort

Answer: A

Explanation:

A technical effort is described as any activity, which has an effect on defining, designing, building, or implementing a task, requirement, or procedure. The technical effort is an element of technical management that is required to progress efficiently and effectively from a business need to the deployment and operation

of the system.

NEW QUESTION 134

Which of the following specifies the behaviors of the DRM implementation and any applications that are accessing the implementation?

- A. OS fingerprinting
- B. OTA provisioning
- C. Access control
- D. Compliance rule

Answer: D

Explanation:

The Compliance rule specifies the behaviors of the DRM implementation and any applications that are accessing the implementation. The compliance rule specifies the following elements: Definition of specific license rights Device requirements Revocation of license path or penalties when the implementation is not robust enough or noncompliant Answer B is incorrect. Over-the-air provisioning is a mechanism to deploy MIDlet suites over a network. It is a method of distributing MIDlet suites. MIDlet suite providers install their MIDlet suites on Web servers and provide a hypertext link for downloading. A user can use this link to download the MIDlet suite either through the Internet microbrowser or through WAP on his device. Answer B is incorrect. An access control is a system, which enables an authority to control access to areas and resources in a given physical facility, or computer-based information system. Access control system, within the field of physical security, is generally seen as the second layer in the security of a physical structure. It refers to all mechanisms that control visibility of screens, views, and data within Siebel Business Applications. Answer A is incorrect. OS fingerprinting is a process in which an external host sends special traffic on the external network interface of a computer to determine the computer's operating system. It is one of the primary steps taken by hackers in preparing an attack.

NEW QUESTION 139

An authentication method uses smart cards as well as usernames and passwords for authentication. Which of the following authentication methods is being referred to?

- A. Anonymous
- B. Mutual
- C. Multi-factor
- D. Biometrics

Answer: C

Explanation:

Multi-factor authentication involves a combination of multiple methods of authentication. For example, an authentication method that uses smart cards as well as usernames and passwords can be referred to as multi-factor authentication. Answer B is incorrect. Mutual authentication is a process in which a client process and server are required to prove their identities to each other before performing any application function. The client and server identities can be verified through a trusted third party and use shared secrets as in the case of Kerberos v5. The MS-CHAP v2 and EAP-TLS authentication methods support mutual authentication. Answer A is incorrect. Anonymous authentication is an authentication method used for Internet communication. It provides limited access to specific public folders and directory information. It is supported by all clients and is used to access unsecured content in public folders. An administrator must create a user account in IIS to enable the user to connect anonymously. Answer D is incorrect. Biometrics authentication uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical qualities to identify a user.

NEW QUESTION 140

Which of the following is the most secure method of authentication?

- A. Biometrics
- B. Username and password
- C. Anonymous
- D. Smart card

Answer: A

Explanation:

Biometrics is a method of authentication that uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical qualities to identify a user. Nowadays, the usage of biometric devices such as hand scanners and retinal scanners is becoming more common in the business environment. It is the most secure method of authentication. Answer B is incorrect. Username and password is the least secure method of authentication in comparison of smart card and biometrics authentication. Username and password can be intercepted. Answer D is incorrect. Smart card authentication is not as reliable as biometrics authentication. Answer B is incorrect. Anonymous authentication does not provide security as a user can log on to the system anonymously and he is not prompted for credentials.

NEW QUESTION 144

DRAG DROP Security code review identifies the unvalidated input calls made by an attacker and avoids those calls to be processed by the server. It performs various review checks on the stained calls of servlet for identifying unvalidated input from the attacker. Choose the appropriate review checks and drop them in front of their respective functions.

Code review check	Function
Drop Here	It is used to check the unvalidated sources of input from URL parameters in <code>javax.servlet.HttpServletRequest</code> class.
Drop Here	It is used to check the unvalidated sources of input from Form fields in <code>javax.servlet.HttpServletRequest</code> class.
Drop Here	It is used to check the unvalidated sources of input from Cookies <code>javax.servlet.HttpServletRequest</code> class.
Drop Here	It is used to check the unvalidated sources of input from HTTP headers <code>javax.servlet.HttpServletRequest</code> class.

getParameter()

getQueryString()

getCookies()

getHeaders()

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

The various security code review checks performed on the stained calls of servlet are as follows: `getParameter()`: It is used to check the unvalidated sources of input from URL parameters in `javax.servlet.HttpServletRequest` class. `getQueryString()`: It is used to check the unvalidated sources of input from Form fields in `javax.servlet.HttpServletRequest` class. `getCookies()`: It is used to check the unvalidated sources of input from Cookies `javax.servlet.HttpServletRequest` class. `getHeaders()`: It is used to check the unvalidated sources of input from HTTP headers `javax.servlet.HttpServletRequest` class.

NEW QUESTION 145

Which of the following are the responsibilities of a custodian with regard to data in an information classification program? Each correct answer represents a complete solution. Choose three.

- A. Performing data restoration from the backups when necessary
 B. Running regular backups and routinely testing the validity of the backup data
 C. Determining what level of classification the information requires
 D. Controlling access, adding and removing privileges for individual users

Answer: ABD

Explanation:

The owner of information delegates the responsibility of protecting that information to a custodian. The following are the responsibilities of a custodian with regard to data in an information classification program: Running regular backups and routinely testing the validity of the backup data Performing data restoration from the backups when necessary Controlling access, adding and removing privileges for individual users Answer B is incorrect. Determining what level of classification the information requires is the responsibility of the owner.

NEW QUESTION 146

Which of the following security objectives are defined for information and information systems by the FISMA? Each correct answer represents a part of the solution. Choose all that apply.

- A. Authenticity
 B. Availability
 C. Integrity
 D. Confidentiality

Answer: BCD

Explanation:

FISMA defines the following three security objectives for information and information systems: Confidentiality: It means that the data should only be accessible to authorized users. Access includes printing, displaying, and other such forms of disclosure, including simply revealing the existence of an object. Integrity: It means that only authorized users are able to modify data. Modification admits changing, changing the status, deleting, and creating. Availability: It means that the data should only be available to authorized users. Answer A is incorrect. Authenticity is not defined by the FISMA as one of the security objectives for information and information systems.

NEW QUESTION 147

What are the differences between managed and unmanaged code technologies? Each correct answer represents a complete solution. Choose two.

- A. Managed code is referred to as Hex code, whereas unmanaged code is referred to as byte code.
 B. C and C++ are the examples of managed code, whereas Java EE and Microsoft.NET are the examples of unmanaged code.
 C. Managed code executes under management of a runtime environment, whereas unmanaged code is executed by the CPU of a computer system.
 D. Managed code is compiled into an intermediate code format, whereas unmanaged code is compiled into machine code.

Answer: CD

Explanation:

Programming languages are categorized into two technologies: 1.Managed code: This computer program code is compiled into an intermediate code format. Managed code is referred to as byte code. It executes under the management of a runtime environment. Java EE and Microsoft.NET are the examples of managed code. 2.Unmanaged code: This computer code is compiled into machine code. Unmanaged code is executed by the CPU of a computer system. C and C++ are the examples of unmanaged code. Answer A is incorrect. Managed code is referred to as byte code. Answer B is incorrect. C and C++ are the examples of unmanaged code, whereas Java EE and Microsoft.NET are the examples of managed code.

NEW QUESTION 149

Which of the following can be used to accomplish authentication? Each correct answer represents a complete solution. Choose all that apply.

- A. Encryption
- B. Biometrics
- C. Token
- D. Password

Answer: BCD

Explanation:

The following can be used to accomplish authentication: 1.Password 2.Biometrics 3.Token A password is a secret word or string of characters that is used for authentication, to prove identity, or gain access to a resource.

NEW QUESTION 154

Samantha works as an Ethical Hacker for we-are-secure Inc. She wants to test the security of the we-are-secure server for DoS attacks. She sends large number of ICMP ECHO packets to the target computer. Which of the following DoS attacking techniques will she use to accomplish the task?

- A. Smurf dos attack
- B. Land attack
- C. Ping flood attack
- D. Teardrop attack

Answer: C

Explanation:

According to the scenario, Samantha is using the ping flood attack. In a ping flood attack, an attacker sends a large number of ICMP packets to the target computer using the ping command, i.e., ping -f target_IP_address. When the target computer receives these packets in large quantities, it does not respond and hangs. However, for such an attack to take place, the attacker must have sufficient Internet bandwidth, because if the target responds with an "ECHO reply ICMP packet" message, the attacker must have both the incoming and outgoing bandwidths available for communication. Answer A is incorrect. In a smurf DoS attack, an attacker sends a large amount of ICMP echo request traffic to the IP broadcast addresses. These ICMP requests have a spoofed source address of the intended victim. If the routing device delivering traffic to those broadcast addresses delivers the IP broadcast to all the hosts, most of the IP addresses send an ECHO reply message. However, on a multi- access broadcast network, hundreds of computers might reply to each packet when the target network is overwhelmed by all the messages sent simultaneously. Due to this, the network becomes unable to provide services to all the messages and crashes. Answer D is incorrect. In a teardrop attack, a series of data packets are sent to the target computer with overlapping offset field values. As a result, the target computer is unable to reassemble these packets and is forced to crash, hang, or reboot. Answer B is incorrect. In a land attack, the attacker sends a spoofed TCP SYN packet in which the IP address of the target is filled in both the source and destination fields. On receiving the spoofed packet, the target system becomes confused and goes into a frozen state. Now-a-days, antivirus can easily detect such an attack.

NEW QUESTION 156

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully performed the following steps of the pre-attack phase to check the security of the We-are-secure network: Gathering information Determining the network range Identifying active systems Now, he wants to find the open ports and applications running on the network. Which of the following tools will he use to accomplish his task?

- A. ARIN
- B. APNIC
- C. RIPE
- D. SuperScan

Answer: D

Explanation:

In such a situation, John will use the SuperScan tool to find the open ports and applications on the We-are-secure network. SuperScan is a TCP/UDP port scanner. It also works as a ping sweeper and hostname resolver. It can ping a given range of IP addresses and resolve the host name of the remote system. The features of SuperScan are as follows: It scans any port range from a built-in list or any given range. It performs ping scans and port scans using any IP range. It modifies the port list and port descriptions using the built in editor. It connects to any discovered open port using user-specified "helper" applications. It has the transmission speed control utility. Answer C, A, and B are incorrect. RIPE, ARIN, and APNIC are the Regional Internet Registries (RIR) that manage, distribute, and register public IP addresses within their respective regions. These can be used as passive tools by an attacker to determine the network range.

NEW QUESTION 157

Security Test and Evaluation (ST&E) is a component of risk assessment. It is useful in discovering system vulnerabilities. For what purposes is ST&E used? Each correct answer represents a complete solution. Choose all that apply.

- A. To implement the design of system architecture
- B. To determine the adequacy of security mechanisms, assurances, and other properties to enforce the security policy
- C. To assess the degree of consistency between the system documentation and its implementation
- D. To uncover design, implementation, and operational flaws that may allow the violation of security policy

Answer: BCD

Explanation:

Security Test and Evaluation (ST&E) is a component of risk assessment. It is useful in discovering system vulnerabilities. According to NIST SP 800-42 (Guideline on Network Security Testing), ST&E is used for the following purposes: To assess the degree of consistency between the system documentation and its implementation To determine the adequacy of security mechanisms, assurances, and other properties to enforce the security policy To uncover design, implementation, and operational flaws that may allow the violation of security policy Answer A is incorrect. ST&E is not used for the implementation of the system architecture.

NEW QUESTION 160

Which of the following documents is defined as a source document, which is most useful for the ISSE when classifying the needed security functionality?

- A. Information Protection Policy (IPP)
- B. IMM
- C. System Security Context
- D. CONOPS

Answer: A

Explanation:

The Information Protection Policy (IPP) is defined as a source document, which is most useful for the ISSE when classifying the needed security functionality. The IPP document consists of the threats to the information management and the security services and controls needed to respond to those threats. Answer B is incorrect. The IMM is the source document describing the customer's needs based on identifying users, processes, and information. Answer B is incorrect. The System Security Context is the output of SE and ISSEP. It is the translation of the requirements into system parameters and possible measurement concepts that meet the defined requirements. Answer D is incorrect. The Concept of Operations (CONOPS) is a document describing the characteristics of a proposed system from the viewpoint of an individual who will use that system. It is used to communicate the quantitative and qualitative system characteristics to all stakeholders. CONOPS are widely used in the military or in government services, as well as other fields. A CONOPS generally evolves from a concept and is a description of how a set of capabilities may be employed to achieve desired objectives or a particular end state for a specific scenario.

NEW QUESTION 161

Which of the following governance bodies provides management, operational and technical controls to satisfy security requirements?

- A. Senior Management
- B. Business Unit Manager
- C. Information Security Steering Committee
- D. Chief Information Security Officer

Answer: A

Explanation:

Senior management provides management, operational and technical controls to satisfy security requirements. The governance roles and responsibilities are mentioned below in the table:

Governance Body	Membership	Responsibilities
Information Security Steering Committee	CFO, CEO, COO, CTO, VP Business units chaired by CISO	It establishes and supports security programs
Senior Management	C-level, unit VPs and senior VPs	It provides management, operational and technical controls to satisfy security requirements.
Chief Information Security Officer	CISO and staff	It directs and coordinates implementations of information security program.
Business Unit Managers	Department heads and supervisors	They Classify and establish requirements for safeguarding information assets.

NEW QUESTION 162

Audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function. Under which of the following controls does audit control come?

- A. Reactive controls
- B. Detective controls
- C. Protective controls
- D. Preventive controls

Answer: B

Explanation:

Audit trail or audit log comes under detective controls. Detective controls are the audit controls that are not needed to be restricted. Any control that performs a monitoring activity can likely be defined as a Detective Control. For example, it is possible that mistakes, either intentional or unintentional, can be made. Therefore, an additional Protective control is that these companies must have their financial results audited by an independent Certified Public Accountant. The role of this accountant is to act as an auditor. In fact, any auditor acts as a Detective control. If the organization in question has not properly followed the rules, a diligent auditor should be able to detect the deficiency which indicates that some control somewhere has failed. Answer A is incorrect. Reactive or corrective controls typically work in response to a detective control, responding in such a way as to alert or otherwise correct an unacceptable condition. Using the example of account rules, either the internal Audit Committee or the SEC itself, based on the report generated by the external auditor, will take some corrective action. In this way, they are acting as a Corrective or Reactive control. Answer C and D are incorrect. Protective or preventative controls serve to proactively define and possibly enforce acceptable behaviors. As an example, a set of common accounting rules are defined and must be followed by any publicly traded company. Each quarter, any particular company must publicly state its current financial standing and accounting as reflected by an application of these rules. These accounting rules and the SEC requirements serve as protective or preventative controls.

NEW QUESTION 165

Which of the following terms refers to the protection of data against unauthorized access?

- A. Integrity
- B. Recovery

- C. Auditing
- D. Confidentiality

Answer: D

Explanation:

Confidentiality is a term that refers to the protection of data against unauthorized access. Administrators can provide confidentiality by encrypting data. Symmetric encryption is a relatively fast encryption method. Hence, this method of encryption is best suited for encrypting large amounts of data such as files on a computer. Answer A is incorrect. Integrity ensures that no intentional or unintentional unauthorized modification is made to data. Answer B is incorrect. Auditing is used to track user accounts for file and object access, logon attempts, system shutdown etc. This enhances the security of the network. Before enabling auditing, the type of event to be audited should be specified in the Audit Policy in User Manager for Domains.

NEW QUESTION 170

In which of the following phases of the SDLC does the software and other components of the system faithfully incorporate the design specifications and provide proper documentation and training?

- A. Design
- B. Evaluation and acceptance
- C. Programming and training
- D. Initiation

Answer: C

Explanation:

In the programming and training phase of the SDLC, the software and other components of the system faithfully incorporate the design specifications, and proper documentation and training are provided. Answer D is incorrect. During the initiation phase, the need for a system is expressed and the purpose of the system is documented. Answer A is incorrect. During the design phase, systems requirements are incorporated into design. This phase specifies to include controls that support the auditing of the system. Answer B is incorrect. During the evaluation and acceptance phase, the system and data are validated, all the control requirements and the user requirements are met by the system.

NEW QUESTION 173

Which of the following characteristics are described by the DIAP Information Readiness Assessment function? Each correct answer represents a complete solution. Choose all that apply.

- A. It provides for entry and storage of individual system data.
- B. It performs vulnerability/threat analysis assessment.
- C. It provides data needed to accurately assess IA readiness.
- D. It identifies and generates IA requirements.

Answer: BCD

Explanation:

The characteristics of the DIAP Information Readiness Assessment function are as follows: It provides data needed to accurately assess IA readiness. It identifies and generates IA requirements. It performs vulnerability/threat analysis assessment. Answer A is incorrect. It is a function performed by the ASSET system.

NEW QUESTION 178

In digital rights management, the level of robustness depends on the various types of tools and attacks to which they must be resistant or immune. Which of the following types of tools are expensive, require skill, and are not easily available?

- A. Hand tools
- B. Widely available tools
- C. Specialized tools
- D. Professional tools

Answer: D

Explanation:

The tools used in DRM to define the level of robustness are as follows: 1. Widely available tools: These tools are easy to use and are available to everyone. For example, screw-drivers and file editors. 2. Specialized tools: These tools require skill and are available at reasonable prices. For example, debuggers, decompilers, and memory scanners. 3. Professional tools: These tools are expensive, require skill, and are not easily available. For example, logic analyzers, circuit emulators, and chip disassembly systems.

NEW QUESTION 180

Harry is the project manager of the MMQ Construction Project. In this project, Harry has identified a supplier who can create stained glass windows for 1,000 window units in the construction project. The supplier is an artist who works by himself, but creates windows for several companies throughout the United States. Management reviews the proposal to use this supplier and while they agree that the supplier is talented, they do not think the artist can fulfill the 1,000 window units in time for the project's deadline. Management asked Harry to find a supplier who can fulfill the completion of the windows by the needed date in the schedule. What risk response has management asked Harry to implement?

- A. Transference
- B. Avoidance
- C. Mitigation
- D. Acceptance

Answer: C

Explanation:

This is an example of mitigation. By changing to a more reliable supplier, Harry is reducing the probability the supplier will be late. It's still possible that the vendor

may not be able to deliver the stained glass windows, but the more reputable supplier reduces the probability of the lateness. Mitigation is a risk response planning technique associated with threats that seeks to reduce the probability of occurrence or impact of a risk to below an acceptable threshold. Risk mitigation involves taking early action to reduce the probability and impact of a risk occurring on the project. Adopting less complex processes, conducting more tests, or choosing a more stable supplier are examples of mitigation actions. Answer A is incorrect. Transference is when the risk is transferred to a third party, usually for a fee. While this question does include a contractual relationship, the risk is the lateness of the windows. Transference focuses on transferring the risk to a third party to manage the risk event. In this instance, the management of the risk is owned by a third party; the third party actually creates the risk event because of the possibility of the lateness of the windows. Answer B is incorrect. Avoidance changes the project plan to avoid the risk. If the project manager and management changed the window-type to a standard window in the project requirements, then this would be avoidance. Risk avoidance is a technique used for threats. It creates changes to the project management plan that are meant to either eliminate the risk completely or to protect the project objectives from its impact. Risk avoidance removes the risk event entirely either by adding additional steps to avoid the event or reducing the project scope requirements. It may seem the answer to all possible risks, but avoiding risks also means losing out on the potential gains that accepting (retaining) the risk might have allowed. Answer D is incorrect. Acceptance accepts the risk that the windows could be late and offers no response.

NEW QUESTION 182

John works as a systems engineer for BlueWell Inc. He has modified the software, and wants to retest the application to ensure that bugs have been fixed or not. Which of the following tests should John use to accomplish the task?

- A. Reliability test
- B. Functional test
- C. Performance test
- D. Regression test

Answer: D

Explanation:

John should use the regression tests to retest the application to guarantee that bugs have been fixed. This test will help him to check that the earlier working functions have not failed as a result of the changes, and newly added features have not created problems with the previous versions. The various types of internal tests performed on builds are as follows: Regression tests: It is also known as the verification testing. These tests are developed to confirm that capabilities in earlier builds continue to work correctly in the subsequent builds. Functional test: These tests emphasizes on verifying that the build meets its functional and data requirements and correctly generates each expected display and report. Performance tests: These tests are used to identify the performance thresholds of each build. Reliability tests: These tests are used to identify the reliability thresholds of each build.

NEW QUESTION 187

Which of the following statements about a host-based intrusion prevention system (HIPS) are true? Each correct answer represents a complete solution. Choose two.

- A. It can detect events scattered over the network.
- B. It is a technique that allows multiple computers to share one or more IP addresses.
- C. It can handle encrypted and unencrypted traffic equally.
- D. It cannot detect events scattered over the network.

Answer: CD

Explanation:

A host-based intrusion prevention system (HIPS) is an application usually employed on a single computer. It complements traditional finger- print-based and heuristic antivirus detection methods, since it does not need continuous updates to stay ahead of new malware. When a malicious code needs to modify the system or other software residing on the machine, a HIPS system will notice some of the resulting changes and prevent the action by default or notify the user for permission. It can handle encrypted and unencrypted traffic equally and cannot detect events scattered over the network. Answer B is incorrect. Network address translation (NAT) is a technique that allows multiple computers to share one or more IP addresses. NAT is configured at the server between a private network and the Internet. It allows the computers in a private network to share a global, ISP assigned address. NAT modifies the headers of packets traversing the server. For packets outbound to the Internet, it translates the source addresses from private to public, whereas for packets inbound from the Internet, it translates the destination addresses from public to private. Answer A is incorrect. Network intrusion prevention system (NIPS) is a hardware/software platform that is designed to analyze, detect, and report on security related events. NIPS is designed to inspect traffic and based on its configuration or security policy, it can drop malicious traffic. NIPS is able to detect events scattered over the network and can react.

NEW QUESTION 190

Which of the following processes will you involve to perform the active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures?

- A. Penetration testing
- B. Baselineing
- C. Risk analysis
- D. Compliance checking

Answer: A

Explanation:

A penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The intent of a penetration test is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered. It is a component of a full security audit. Answer B is incorrect. Risk analysis is the science of risks and their probability and evaluation in a business or a process. It is an important factor in security enhancement and prevention in a system. Risk analysis should be performed as part of the risk management process for each project. The outcome of the risk analysis would be the creation or review of the risk register to identify and quantify risk elements to the project and their potential impact. Answer D is incorrect. Compliance checking performs the reviews for safeguards and controls to verify whether the entity is complying with particular procedures, rules or not. It includes the inspection of operational systems to guarantee that hardware and software controls have been correctly implemented and maintained. Compliance checking covers the activities such as penetration testing and vulnerability assessments. Compliance checking must be performed by skilled persons, or by an automated software package. Answer B is incorrect. Baselineing is a method for analyzing the performance of computer networks. The method is marked by comparing the current performance to a historical metric, or "baseline". For

example, if a user measured the performance of a network switch over a period of time, he could use that performance figure as a comparative baseline if he made a configuration change to the switch.

NEW QUESTION 195

Fill in the blank with an appropriate phrase The is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity.

A. Biba model

Answer: A

Explanation:

The Biba model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject.

NEW QUESTION 200

Maria has been recently appointed as a Network Administrator in Gentech Inc. She has been tasked to perform network security testing to find out the vulnerabilities and shortcomings of the present network infrastructure. Which of the following testing approaches will she apply to accomplish this task?

- A. Gray-box testing
- B. White-box testing
- C. Black-box testing
- D. Unit testing

Answer: C

Explanation:

Maria is new for this organization and she does not have any idea regarding the present infrastructure. Therefore, black box testing is best suited for her. Blackbox testing is a technique in which the testing team has no knowledge about the infrastructure of the organization. The testers must first determine the location and extent of the systems before commencing their analysis. This testing technique is costly and time consuming. Answer B is incorrect. White box testing, also known as Clear box or Glass box testing, takes into account the internal mechanism of a system or application. The connotations of "Clear box" and "Glass box" indicate that a tester has full visibility of the internal workings of the system. It uses knowledge of the internal structure of an application. It is applicable at the unit, integration, and system levels of the software testing process. It consists of the following testing methods: Control flow-based testing Create a graph from source code. Describe the flow of control through the control flow graph. Design test cases to cover certain elements of the graph. Data flow-based testing Test connections between variable definitions. Check variation of the control flow graph. Set DEF (n) contains variables that are defined at node n. Set USE (n) are variables that are read. Answer A is incorrect. Graybox testing is a combination of whitebox testing and blackbox testing. In graybox testing, the test engineer is equipped with the knowledge of system and designs test cases or test data based on system knowledge. The security tester typically performs graybox testing to find vulnerabilities in software and network system. Answer D is incorrect. Unit testing is a type of testing in which each independent unit of an application is tested separately. During unit testing, a developer takes the smallest unit of an application, isolates it from the rest of the application code, and tests it to determine whether it works as expected. Unit testing is performed before integrating these independent units into modules. The most common approach to unit testing requires drivers and stubs to be written. Drivers and stubs are programs. A driver simulates a calling unit, and a stub simulates a called unit.

NEW QUESTION 201

Which of the following are the types of intellectual property? Each correct answer represents a complete solution. Choose all that apply.

- A. Patent
- B. Copyright
- C. Standard
- D. Trademark

Answer: ABD

Explanation:

Common types of intellectual property include copyrights, trademarks, patents, industrial design rights, and trade secrets. A copyright is a form of intellectual property, which secures to its holder the exclusive right to produce copies of his or her works of original expression, such as a literary work, movie, musical work or sound recording, painting, photograph, computer program, or industrial design, for a defined, yet extendable, period of time. It does not cover ideas or facts. Copyright laws protect intellectual property from misuse by other individuals. A trademark is a distinctive sign used by an individual, business organization, or other legal entity to identify that the products or services to consumers with which the trademark appears originate from a unique source, and to distinguish its products or services from those of other entities. A trademark is designated by the following symbols: : It is for an unregistered trade mark and it is used to promote or brand goods. : It is for an unregistered service mark and it is used to promote or brand services. : It is for a registered trademark. A patent is a set of exclusive rights granted by a state to an inventor or their assignee for a limited period of time in exchange for a public disclosure of an invention. Answer B is incorrect. It is not a type of intellectual property.

NEW QUESTION 206

Which of the following methods is a means of ensuring that system changes are approved before being implemented, only the proposed and approved changes are implemented, and the implementation is complete and accurate?

- A. Configuration control
- B. Documentation control
- C. Configuration identification
- D. Configuration auditing

Answer: B

Explanation:

Documentation control is a method of ensuring that system changes should be agreed upon before being implemented, only the proposed and approved changes are implemented, and the implementation is complete and accurate. Documentation control is involved in the strict events for proposing, monitoring, and approving system changes and their implementation. It helps the change process by supporting the person who synchronizes the analytical task, approves system changes,

reviews the implementation of changes, and oversees other tasks such as documenting the controls. Answer D is incorrect. Configuration auditing is the quality assurance element of configuration management. It is occupied in the process of periodic checks to establish the consistency and completeness of accounting information and to validate that all configuration management policies are being followed. Configuration audits are broken into functional and physical configuration audits. They occur either at delivery or at the moment of effecting the change. A functional configuration audit ensures that functional and performance attributes of a configuration item are achieved, while a physical configuration audit ensures that a configuration item is installed in accordance with the requirements of its detailed design documentation. Answer A is incorrect. Configuration control is a procedure of the Configuration management. Configuration control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them. It supports the change of the functional and physical attributes of software at various points in time, and performs systematic control of changes to the identified attributes. Answer B is incorrect. Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baselined. Baselining an attribute forces formal configuration change control processes to be effected in the event that these attributes are changed.

NEW QUESTION 207

.....

Relate Links

100% Pass Your CSSLP Exam with Exam Bible Prep Materials

<https://www.exambible.com/CSSLP-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>