Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

CSSLP MCQs
CSSLP TestPrep
CSSLP Study Guide
CSSLP Practice Test
CSSLP Exam Questions

killexams.com

ISC2

CSSLP

Certified Secure Software Lifecycle Professional

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/CSSLP

Answer option D 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 option B is incorrect. Biometrics authentication uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical qualities to identify a user.

QUESTION: 298
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 option 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 option 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 option 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.

QUESTION: 299

The Phase 2 of DITSCAP C&A is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. What are the process activities of this phase? Each correct answer represents a complete solution. Choose all that apply.

A. Registration
B. System development
C. Certification analysis
D. Assessment of the Analysis Results
E. Configuring refinement of the SSAA

Answer: B,C,D,E

Explanation:
The Phase 2 of DITSCAP C&A is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. This phase takes place between the signing of the initial version of the SSAA and the formal accreditation of the system. This phase verifies security requirements during system development. The process activities of this phase are as follows:
Configuring refinement of the SSAA System development
Certification analysis
Assessment of the Analysis Results
Answer option A is incorrect. Registration is a Phase 1 activity.

QUESTION: 300
Which of the following methods determines the principle name of the current user and returns the java.security.Principal object in the HttpServletRequest interface?

A. getCallerPrincipal()
B. getRemoteUser()
C. isUserInRole()
D. getUserPrincipal()

Answer: D

Explanation:
The getUserPrincipal() method determines the principle name of the current user and returns the java.security.Principal object. The java.security.Principal object contains the remote user name. The value of the getUserPrincipal() method returns null if no user is authenticated.

Answer option B is incorrect. The getRemoteUser() method returns the user name that is used for the client authentication. The value of the getRemoteUser() method returns null if no user is authenticated.
Answer option C is incorrect. The isUserInRole() method determines whether the remote user is granted a specified user role. The value of the isUserInRole() method returns true if the remote user is granted the specified user role; otherwise it returns false.
Answer option A is incorrect. The getCallerPrincipal() method is used to identify a caller using a java.security.Principal object. It is not used in the HttpServletRequest interface.

QUESTION: 301
Which of the following strategies is used to minimize the effects of a disruptive event on a company, and is created to prevent interruptions to normal business activity?

A. Continuity of Operations Plan
B. Disaster Recovery Plan
C. Contingency Plan
D. Business Continuity Plan

Answer: D

Explanation:
BCP is a strategy to minimize the consequence of the instability and to allow for the continuation of business processes. The goal of BCP is to minimize the effects of a disruptive event on a company, and is formed to avoid interruptions to normal business activity.
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 option C 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 option B is incorrect. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking), and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related

aspects such as key personnel, facilities, crisis communication, and reputation protection, and should refer to the disaster recovery plan (DRP) for IT-related infrastructure recovery/continuity.
Answer option A is incorrect. The Continuity Of Operation Plan (COOP) refers to the preparations and institutions maintained by the United States government, providing survival of federal government operations in the case of catastrophic events. It provides procedures and capabilities to sustain an organization's essential. COOP is the procedure documented to ensure persistent critical operations throughout any period where normal operations are unattainable.

QUESTION: 302
Single Loss Expectancy (SLE) represents an organization's loss from a single threat. Which of the following formulas best describes the Single Loss Expectancy (SLE)?

A. SLE = Asset Value (AV) * Exposure Factor (EF)
B. SLE = Annualized Loss Expectancy (ALE) * Exposure Factor (EF)
C. SLE = Annualized Loss Expectancy (ALE) * Annualized Rate of Occurrence (ARO)
D. SLE = Asset Value (AV) * Annualized Rate of Occurrence (ARO)

Answer: A

Explanation:
Single Loss Expectancy is a term related to Risk Management and Risk Assessment. It can be defined as the monetary value expected from the occurrence of a risk on an asset. It is mathematically expressed as follows:
Single Loss Expectancy (SLE) = Asset Value (AV) * Exposure Factor (EF)
where the Exposure Factor is represented in the impact of the risk over the asset, or percentage of asset lost. As an example, if the Asset Value is reduced two thirds, the exposure factor value is .66. If the asset is completely lost, the Exposure Factor is 1.0. The result is a monetary value in the same unit as the Single Loss Expectancy is expressed. Answer options B, D, and C are incorrect. These are not valid formulas of SLE.

QUESTION: 303
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. In order to do so, he performs the following steps of the pre-attack phase successfully:
Information gathering Determination of network range Identification of active systems Location of open ports and applications Now, which of the following tasks should he perform next?

A. Install a backdoor to log in remotely on the We-are-secure server.

B. Fingerprint the services running on the we-are-secure network.
C. Map the network of We-are-secure Inc.
D. Perform OS fingerprinting on the We-are-secure network.

Answer: D

Explanation:
John will perform OS fingerprinting on the We-are-secure network. Fingerprinting is the easiest way to detect the Operating System (OS) of a remote system. OS detection is important because, after knowing the target system's OS, it becomes easier to hack into the system. The comparison of data packets that are sent by the target system is done by fingerprinting. The analysis of data packets gives the attacker a hint as to which operating system is being used by the remote system. There are two types of fingerprinting techniques as follows:
1.Active fingerprinting
2.Passive fingerprinting In active fingerprinting ICMP messages are sent to the target system and the response message of the target system shows which OS is being used by the remote system. In passive fingerprinting the number of hops reveals the OS of the remote system.
Answer options B and C are incorrect. John should perform OS fingerprinting first, after which it will be easy to identify which services are running on the network since there are many services that run only on a specific operating system. After performing OS fingerprinting, John should perform networking mapping.
Answer option A is incorrect. This is a pre-attack phase, and only after gathering all relevant knowledge of a network should John install a backdoor.

QUESTION: 304
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.

Answer:
A technical effo

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.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.