

CSSLP^{Q&As}

Certified Secure Software Lifecycle Professional Practice Test

Pass ISC CSSLP Exam with 100% Guarantee

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

<https://www.pass2lead.com/csslp.html>

100% Passing Guarantee
100% Money Back Assurance

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

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



QUESTION 1

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 Weare-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

Correct Answer: D

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.

QUESTION 2

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

Correct Answer: C

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 (DoD8510.1- 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.

QUESTION 3

Certification and Accreditation (CandA or CnA) is a process for implementing information security. Which of the following is the correct order of CandA phases in a DITSCAP assessment?

- A. Verification, Definition, Validation, and Post Accreditation
- B. Definition, Validation, Verification, and Post Accreditation
- C. Definition, Verification, Validation, and Post Accreditation
- D. Verification, Validation, Definition, and Post Accreditation

Correct Answer: C

CandA consists of four phases in a DITSCAP assessment. These phases are the same as NIACAP phases. The order of these phases is as follows: 1. Definition: The definition phase is focused on understanding the IS business case, the mission, environment, and architecture. This phase determines the security requirements and level of effort necessary to achieve Certification and Accreditation (CandA). 2. Verification: The second phase confirms the evolving or modified system's compliance with the information. The verification phase ensures that the fully integrated system will be ready for certification testing. 3. Validation: The third phase confirms abidance of the fully integrated system with the security policy. This phase follows the requirements slated in the SSAA. The objective of the validation phase is to show the required evidence to support the DAA in accreditation process. 4. Post Accreditation: The Post Accreditation is the final phase of DITSCAP assessment and it starts after the system has been certified and accredited for operations. This phase ensures secure system management, operation, and maintenance to save an acceptable level of residual risk.

QUESTION 4

You work as a Security Manager for Tech Perfect Inc. You find that some applications have failed to encrypt network traffic while ensuring secure communications in the organization. Which of the following will you use to resolve the issue?

- A. SCP
- B. TLS
- C. IPSec

D. HTTPS

Correct Answer: B

In order to resolve the issue, you should use TLS (Transport Layer Security). Transport Layer Security (TLS) is a cryptographic protocol that provides security and data integrity for communications over networks such as the Internet. TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end. Several versions of the protocols are in wide-spread use in applications like web browsing, electronic mail, Internet faxing, instant messaging, and voiceover-IP (VoIP). The TLS protocol, an application layer protocol, allows client/server applications to communicate across a network in a way designed to prevent eavesdropping, tampering, and message forgery. TLS provides endpoint authentication and communications confidentiality over the Internet using cryptography. Answer: C is incorrect. Internet Protocol Security (IPSec) is a method of securing data. It secures traffic by using encryption and digital signing. It enhances the security of data as if an IPSec packet is captured, its contents cannot be read. IPSec also provides sender verification that ensures the certainty of the datagram's origin to the receiver. Answer: D is incorrect. Hypertext Transfer Protocol Secure (HTTPS) protocol is a protocol used in the Universal Resource Locator (URL) address line to connect to a secure site. If a site has been made secure by using the Secure Sockets Layer (SSL) then HTTPS, instead of HTTP protocol, should be used as a protocol type in the URL. Answer: A is incorrect. The SCP (secure copy) protocol is a network protocol that supports file transfers. The SCP protocol, which runs on port 22, is based on the BSD RCP protocol which is tunneled through the Secure Shell (SSH) protocol to provide encryption and authentication. SCP might not even be considered a protocol itself, but merely a combination of RCP and SSH. The RCP protocol performs the file transfer and the SSH protocol performs authentication and encryption. SCP protects the authenticity and confidentiality of the data in transit. It hinders the ability for packet sniffers to extract usable information from the data packets.

QUESTION 5

You are the project manager for your organization. You are preparing for the quantitative risk analysis. Mark, a project team member, wants to know why you need to do quantitative risk analysis when you just completed qualitative risk analysis. Which one of the following statements best defines what quantitative risk analysis is?

- A. Quantitative risk analysis is the process of prioritizing risks for further analysis or action by assessing and combining their probability of occurrence and impact.
- B. Quantitative risk analysis is the review of the risk events with the high probability and the highest impact on the project objectives.
- C. Quantitative risk analysis is the planning and quantification of risk responses based on probability and impact of each risk event.
- D. Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives.

Correct Answer: D

Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives. It is performed on risk that have been prioritized through the qualitative risk analysis process. Answer: A is incorrect. This is actually the definition of qualitative risk analysis. Answer: B is incorrect. While somewhat true, this statement does not completely define the quantitative risk analysis process. Answer: C is incorrect. This is not a valid statement about the quantitative risk analysis process. Risk response planning is a separate project management process.