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.leads4pass.com/csslp.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An attacker exploits actual code of an application and uses a security hole to carry out an attack before the application vendor knows about the vulnerability. Which of the following types of attack is this?

A. Replay

B. Zero-day

C. Man-in-the-middle

D. Denial-of-Service

Correct Answer: B

A zero-day attack, also known as zero-hour attack, is a computer threat that tries to exploit computer application vulnerabilities which are unknown to others, undisclosed to the software vendor, or for which no security fix is available. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software vendor knows about the vulnerability. User awareness training is the most effective technique to mitigate such attacks. Answer: A is incorrect. A replay attack is a type of attack in which attackers capture packets containing passwords or digital signatures whenever packets pass between two hosts on a network. In an attempt to obtain an authenticated connection, the attackers then resend the captured packet to the system. In this type of attack, the attacker does not know the actual password, but can simply replay the captured packet. Answer: C is incorrect. Man-in-the-middle attacks occur when an attacker successfully inserts an intermediary software or program between two communicating hosts. The intermediary software or program allows attackers to listen to and modify the communication packets passing between the two hosts. The software intercepts the communication packets and then sends the information to the receiving host. The receiving host responds to the software, presuming it to be the legitimate client. Answer: D is incorrect. A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a computer or network. It is also known as network saturation attack or bandwidth consumption attack. Attackers perform DoS attacks by sending a large number of protocol packets to a network.

QUESTION 2

Which of the following phases of NIST SP 800-37 CandA methodology examines the residual risk for acceptability, and prepares the final security accreditation package?

A. Security Accreditation

B. Initiation

C. Continuous Monitoring

D. Security Certification

Correct Answer: A

The various phases of NIST SP 800-37 CandA 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.

QUESTION 3

Which of the following DoD policies establishes policies and assigns responsibilities to achieve DoD IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network-centric warfare?

A. DoDI 5200.40

B. DoD 8500.1 Information Assurance (IA)

C. DoD 8510.1-M DITSCAP

D. DoD 8500.2 Information Assurance Implementation

Correct Answer: B

DoD 8500.1 Information Assurance (IA) sets up policies and allots responsibilities to achieve DoD IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network-centric warfare. DoD 8500.1 also summarizes the roles and responsibilities for the persons responsible for carrying out the IA policies. Answer: D is incorrect. The DoD 8500.2 Information Assurance Implementation pursues 8500.1. It provides assistance on how to implement policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks. DoD Instruction 8500.2 allots tasks and sets procedures for applying integrated layered protection of the DOD information systems and networks in accordance with the DoD 8500.1 policy. It also provides some important guidelines on how to implement an IA program. Answer: A is incorrect. DoDI 5200.40 executes the policy, assigns responsibilities, and recommends procedures under reference for Certification and Accreditation(CandA) of information technology (IT). Answer: C is incorrect. DoD 8510.1-M DITSCAP provides standardized activities leading to accreditation, and establishes a process and management baseline.

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

Correct Answer: C

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

QUESTION 5

FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAF levels shows that the procedures and controls are

tested and reviewed?

A. Level 4

B. Level 5

C. Level 2

D. Level 3

E. Level 1

Correct Answer: A

The following are the five levels of FITSAF based on SEI\\'s Capability Maturity Model (CMM): Level 1: The first level reflects that an asset has documented a security policy. Level 2:

The second level shows that the asset has documented procedures and controls to implement the policy. Level 3: The third level indicates that these procedures and controls have been implemented. Level 4: The fourth level shows that the

procedures and controls are tested and reviewed. Level 5: The fifth level is the final level and shows that the asset has procedures and controls fully integrated into a comprehensive program.