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.pass4itsure.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

Which of the following is a signature-based intrusion detection system (IDS) ?

A. RealSecure

B. StealthWatch

C. Tripwire

D. Snort

Correct Answer: D

Snort is a signature-based intrusion detection system. 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. StealthWatch is a behavior-based intrusion detection system. Answer: A is incorrect. RealSecure is a network-based IDS that monitors TCP, UDP and ICMP traffic and is configured to look for attack patterns. Answer: C is incorrect. Tripwire is a file integrity checker for UNIX/Linux that can be used for host-based intrusion detection.

QUESTION 2

To help review or design security controls, they can be classified by several criteria . One of these criteria is based on their nature. According to this criterion, which of the following controls consists of incident response processes, management oversight, security awareness, and training?

A. Compliance control

B. Physical control

C. Procedural control

D. Technical control

Correct Answer: C

Procedural controls include incident response processes, management oversight, security awareness, and training. Answer: B is incorrect. Physical controls include fences, doors, locks, and fire extinguishers. Answer: D is incorrect. Technical controls include user authentication (login) and logical access controls, antivirus software, and firewalls. Answer: A is incorrect. The legal and regulatory, or compliance controls, include privacy laws, policies, and clauses.

QUESTION 3

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 CandA methodology will define the above task?

A. Initiation

B. Security Certification

C. Continuous Monitoring

D. Security Accreditation

Correct Answer: C

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 4

Which of the following DITSCAP CandA phases takes place between the signing of the initial version of the SSAA and the formal accreditation of the system?

A. Phase 4

B. Phase 3

C. Phase 1

D. Phase 2

Correct Answer: D

The Phase 2 of DITSCAP CandA 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. Answer: C, B, and A are incorrect. These phases do not take place between the signing of the initial version of the SSAA and the formal accreditation of the system.

QUESTION 5

Which of the following phases of the DITSCAP CandA process is used to define the CandA level of effort, to identify the main CandA 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

Correct Answer: A

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