

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

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



QUESTION 1

You are responsible for network and information security at a large hospital. It is a significant concern that any change to any patient record can be easily traced back to the person who made that change. What is this called?

- A. Availability
- B. Confidentiality
- C. Non repudiation
- D. Data Protection

Correct Answer: C

Non repudiation refers to mechanisms that prevent a party from falsely denying involvement in some data transaction.

QUESTION 2

Which of the following is generally used in packages in order to determine the package or product tampering?

- A. Tamper resistance
- B. Tamper evident
- C. Tamper data
- D. Tamper proof

Correct Answer: A

Tamper resistance is resistance tampered by the users of a product, package, or system, or the users who can physically access it. It includes simple as well as complex devices. The complex device encrypts all the information between individual chips, or renders itself inoperable. Tamper resistance is generally used in packages in order to determine package or product tampering. Answer: B is incorrect. Tamper evident specifies a process or device that makes unauthorized access to the protected object easily detected. Answer: D is incorrect. Tamper proofing makes computers resistant to interference. Tamper proofing measures include automatic removal of sensitive information, automatic shutdown, and automatic physical locking. Answer: C is incorrect. Tamper data is used to view and modify the HTTP or HTTPS headers and post parameters.

QUESTION 3

Which of the following steps of the LeGrand Vulnerability-Oriented Risk Management method determines the necessary compliance offered by risk management practices and assessment of risk levels?

- A. Assessment, monitoring, and assurance
- B. Vulnerability management
- C. Risk assessment

D. Adherence to security standards and policies for development and deployment

Correct Answer: A

Assessment, monitoring, and assurance determines the necessary compliance that are offered by risk management practices and assessment of risk levels.

QUESTION 4

The rights of an author or a corporation to make profit from the creation of their products (such as software, music, etc.) are protected by the Intellectual Property law. Which of the following are the components of the Intellectual Property law? Each correct answer represents a part of the solution. Choose two.

- A. Trademark law
- B. Industrial Property law
- C. Copyright law
- D. Patent law

Correct Answer: BC

The Industrial Property law and the Copyright law are the components of the Intellectual Property law.

QUESTION 5

Which of the following are the scanning methods used in penetration testing? Each correct answer represents a complete solution. Choose all that apply.

- A. Vulnerability
- B. Port
- C. Services
- D. Network

Correct Answer: ABD

The vulnerability, port, and network scanning tools are used in penetration testing. Vulnerability scanning is a process in which a Penetration Tester uses various tools to assess computers, computer systems, networks or applications for weaknesses. There are a number of types of vulnerability scanners available today, distinguished from one another by a focus on particular targets. While functionality varies between different types of vulnerability scanners, they share a common, core purpose of enumerating the vulnerabilities present in one or more targets. Vulnerability scanners are a core technology component of Vulnerability management. Port scanning is the first basic step to get the details of open ports on the target system. Port scanning is used to find a hackable server with a hole or vulnerability. A port is a medium of communication between two computers. Every service on a host is identified by a unique 16-bit number called a port. A port scanner is a piece of software designed to search a network host for open ports. This is often used by administrators to check the security of their networks and by hackers to identify running services on a host with the view to compromising it. Port scanning is used to find the open ports, so that it is possible to search exploits related to that service and application. Network scanning is a penetration testing activity in which a penetration tester or an attacker identifies active hosts on a network, either to attack them or to perform security assessment. A penetration

tester uses various tools to identify all the live or responding hosts on the network and their corresponding IP addresses.
Answer: C is incorrect. This option comes under vulnerability scanning.

[Latest CSSLP Dumps](#)

[CSSLP VCE Dumps](#)

[CSSLP Study Guide](#)