Free Questions for CSSLP by braindumpscollection

Shared by Raymond on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You work as a security manager for BlueWell Inc. You are performing the external vulnerability testing, or penetration testing to get a better snapshot of your organization's security posture. Which of the following penetration testing techniques will you use for searching paper disposal areas for unshredded or otherwise improperly disposed-of reports?

Options:

A- Sniffing

B- Scanning and probing

C- Dumpster diving

D- Demon dialing

Answer:

C

Explanation:

Dumpster diving technique is used for searching paper disposal areas for unshredded or otherwise improperly disposed-of reports.

Answer B is incorrect. In scanning and probing technique, various scanners, like a port scanner, can reveal information about a network's infrastructure and enable an intruder to access the network's unsecured ports.

Answer D is incorrect. Demon dialing technique automatically tests every phone line in an exchange to try to locate modems that are attached to the network.

Answer A is incorrect. In sniffing technique, protocol analyzer can be used to capture data packets that are later decoded to collect information such as passwords or infrastructure configurations.

Question 2

Question Type: MultipleChoice

A part of a project deals with the hardware work. As a project manager, you have decided to hire a company to deal with all hardware work on the project. Which type of risk response is this?

Options:

A- Exploit

B- Mitigation

C- Transference

D- Avoidance

Answer:

C

Explanation:

When you are hiring a third party to own risk, it is known as transference risk response.

Transference is a strategy to mitigate negative risks or threats. In this strategy, consequences and the ownership of a risk is transferred to a

third party. This strategy does not eliminate the risk but transfers responsibility of managing the risk to another party. Insurance is an

example of transference.

Answer B is incorrect. The act of spending money to reduce a risk probability and impact is known as mitigation.

Answer A is incorrect. Exploit is a strategy that may be selected for risks with positive impacts where the organization wishes to ensure

that the opportunity is realized.

Answer D is incorrect. When extra activities are introduced into the project to avoid the risk, this is an example of avoidance.

Question 3

Question Type: MultipleChoice

What are the differences between managed and unmanaged code technologies?

Each correct answer represents a complete solution. Choose two.

Options:

A- Managed code is referred to as Hex code, whereas unmanaged code is referred to as byte code.

B- C and C++ are the examples of managed code, whereas Java EE and Microsoft.NET are the examples of unmanaged code.

C- Managed code executes under management of a runtime environment, whereas unmanaged code is executed by the CPU of a computer system.

D- Managed code is compiled into an intermediate code format, whereas unmanaged code is compiled into machine code.

Answer:

C, D

Explanation:

Programming languages are categorized into two technologies:

1.Managed code: This computer program code is compiled into an intermediate code format. Managed code is referred to as byte code. It

executes under the management of a runtime environment. Java EE and Microsoft.NET are the examples of managed code.

2.Unmanaged code: This computer code is compiled into machine code. Unmanaged code is executed by the CPU of a computer system. C

and C++ are the examples of unmanaged code.

Answer A is incorrect. Managed code is referred to as byte code.

Answer B is incorrect. C and C++ are the examples of unmanaged code, whereas Java EE and Microsoft.NET are the examples of

managed code.

Question 4

Question Type: MultipleChoice

Security Test and Evaluation (ST&E) is a component of risk assessment. It is useful in discovering system vulnerabilities. For what purposes is ST&E used?

Each correct answer represents a complete solution. Choose all that apply.

Options:

A- To implement the design of system architecture

B- To determine the adequacy of security mechanisms, assurances, and other properties to enforce the security policy

C- To assess the degree of consistency between the system documentation and its implementation

D- To uncover design, implementation, and operational flaws that may allow the violation of security policy

Answer:

B, C, D

Explanation:

Security Test and Evaluation (ST&E) is a component of risk assessment. It is useful in discovering system vulnerabilities. According to NIST SP

800-42 (Guideline on Network Security Testing), ST&E is used for the following purposes:

To assess the degree of consistency between the system documentation and its implementation

To determine the adequacy of security mechanisms, assurances, and other properties to enforce the security policy

To uncover design, implementation, and operational flaws that may allow the violation of security policy

Answer A is incorrect. ST&E is not used for the implementation of the system architecture.

Question 5

Question Type: MultipleChoice

Which of the following security objectives are defined for information and information systems by the FISMA? Each correct answer represents a part of the solution. Choose all that apply.

Options:

A- Authenticity

B- Availability

C- Integrity

D- Confidentiality

Answer:

B, C, D

Explanation:

FISMA defines the following three security objectives for information and information systems:

Confidentiality: It means that the data should only be accessible to authorized users. Access includes printing, displaying, and other such forms of disclosure, including simply revealing the existence of an object.

Integrity: It means that only authorized users are able to modify data. Modification admits changing, changing the status, deleting, and creating.

Availability: It means that the data should only be available to authorized users.

Answer A is incorrect. Authenticity is not defined by the FISMA as one of the security objectives for information and information systems.

Question 6

Question Type: MultipleChoice

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?

Options:

A- Assessment, monitoring, and assurance

B- Vulnerability management

C- Risk assessment

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

Answer:

A

Explanation:

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

of risk levels.

Question 7

Question Type: MultipleChoice

A number of security patterns for Web applications under the DARPA contract have been developed by Kienzle, Elder, Tyree, and Edwards-Hewitt. Which of the following patterns are applicable to aspects of authentication in Web applications?b Each correct answer represents a complete solution. Choose all that apply.

Options:

A- Authenticated session

B- Secure assertion

C- Partitioned application

D- Password authentication

E- Account lockout

F- Password propagation

Answer:

A, D, E, F

Explanation:

The various patterns applicable to aspects of authentication in the Web applications are as follows:

Account lockout: It implements a limit on the incorrect password attempts to protect an account from automated password-guessing attacks.

Authenticated session: It allows a user to access more than one access-restricted Web page without re-authenticating every page. It also integrates user authentication into the basic session model.

Password authentication: It provides protection against weak passwords, automated password-guessing attacks, and mishandling of passwords.

Password propagation: It offers a choice by requiring that a user's authentication credentials be verified by the database before providing access to that user's data.

Answer B and C are incorrect. Secure assertion and partitioned application patterns are applicable to software assurance in general.

Question 8

Question Type: MultipleChoice

Which of the following NIST Special Publication documents provides a guideline on questionnaires and checklists through which systems can be evaluated for compliance against specific control objectives?

Options:

A- NIST SP 800-37

B- NIST SP 800-26

C- NIST SP 800-53A

D- NIST SP 800-59

E- NIST SP 800-53

F- NIST SP 800-60

Answer:

B

Explanation:

NIST SP 800-26 (Security Self-Assessment Guide for Information Technology Systems) provides a guideline on questionnaires and checklists

through which systems can be evaluated for compliance against specific control objectives.

Answer A, E, C, D, and F are incorrect. NIST has developed a suite of documents for conducting Certification & Accreditation (C&A).

These documents are as follows:

NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information

Systems.

NIST Special Publication 800-53: This document provides a guideline for security controls for Federal Information Systems.

NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security

controls in Federal Information System.

NIST Special Publication 800-59: This document is a guideline for identifying an information system as a National Security System.

NIST Special Publication 800-60: This document is a guide for mapping types of information and information systems to security objectives and risk levels.