Free Questions for CSSLP by vceexamstest

Shared by Hall on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

Options:

A- Backup policy

B- User password policy

C- Privacy policy

D- Network security policy

Answer:

C

Explanation:

Monitoring the computer hard disks or e-mails of employees pertains to the privacy policy of an organization.

Answer A is incorrect. The backup policy of a company is related to the backup of its data.

Answer D is incorrect. The network security policy is related to the security of a company's network.

Answer B is incorrect. The user password policy is related to passwords that users provide to log on to the network.

Question 2

Question Type: MultipleChoice

You work as a security engineer for BlueWell Inc. You want to use some techniques and procedures to verify the effectiveness of security controls in Federal Information System. Which of the following NIST documents will guide you?

Options:

A- NIST Special Publication 800-53

B- NIST Special Publication 800-59

C- NIST Special Publication 800-53A

D- NIST Special Publication 800-37

Answer:

C

Explanation:

NIST has developed a suite of documents for conducting Certification & Accreditation (C&A). These documents are as follows:

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

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

3.NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System.

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

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

Question 3

Question Type: MultipleChoice

An authentication method uses smart cards as well as usernames and passwords for authentication. Which of the following authentication methods is being referred to?

Options:

A- Anonymous

B- Mutual

C- Multi-factor

D- Biometrics

Answer:

C

Explanation:

Multi-factor authentication involves a combination of multiple methods of authentication. For example, an authentication method that uses smart cards as well as usernames and passwords can be referred to as multi-factor authentication.

Answer B is incorrect. Mutual authentication is a process in which a client process and server are required to prove their identities to

each other before performing any application function. The client and server identities can be verified through a trusted third party and use

shared secrets as in the case of Kerberos v5. The MS-CHAP v2 and EAP-TLS authentication methods support mutual authentication.

Answer A is incorrect. Anonymous authentication is an authentication method used for Internet communication. It provides limited access to specific public folders and directory information. It is supported by all clients and is used to access unsecured content in public folders. An administrator must create a user account in IIS to enable the user to connect anonymously.

Answer D is incorrect. Biometrics authentication uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical qualities to identify a user.

Question 4

Question Type: **MultipleChoice**

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 We-are-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?

Options:

A- ARIN

B- APNIC

C- RIPE

D- SuperScan

Answer:

D

Explanation:

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.

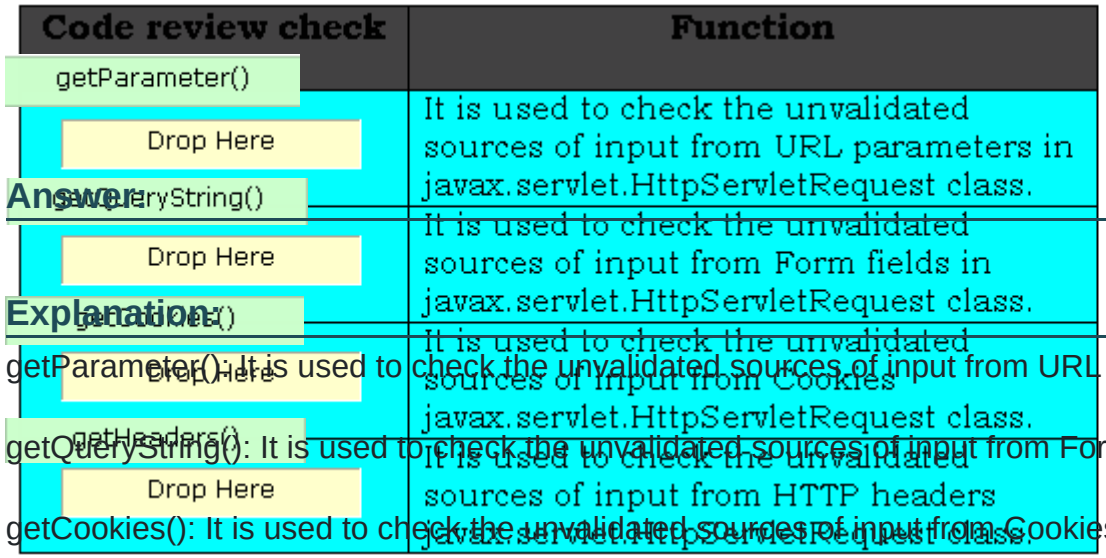
It has the transmission speed control utility.

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 5

Question Type: DragDrop

Security code review identifies the unvalidated input calls made by an attacker and avoids those calls to be processed by the server. It performs various review checks on the stained calls of servlet for identifying unvalidated input from the attacker. Choose the appropriate review checks and drop them in front of their respective functions.



Answer:

Explanation:

getParameter(): It is used to check the unvalidated sources of input from URL parameters in javax.servlet.HttpServletRequest class.

getQueryString(): It is used to check the unvalidated sources of input from Form fields in javax.servlet.HttpServletRequest class.

getCookies(): It is used to check the unvalidated sources of input from Cookies javax.servlet.HttpServletRequest class.

getHeaders(): It is used to check the unvalidated sources of input from HTTP headers javax.servlet.HttpServletRequest class.

Question 6

Question Type: MultipleChoice

Which of the following NIST documents provides a guideline for identifying an information system as a National Security System?

Options:

A- NIST SP 800-37

B- NIST SP 800-59

C- NIST SP 800-53

D- NIST SP 800-60

E- NIST SP 800-53A

Answer:

B

Explanation:

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.

Question 7

Question Type: **MultipleChoice**

In 2003, NIST developed a new Certification & Accreditation (C&A) guideline known as FIPS 199. What levels of potential impact are defined by FIPS 199?

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

Options:

A- Moderate

B- Medium

C- High

D- Low

Answer:

B, C, D

Explanation:

In 2003, NIST developed a new Certification & Accreditation (C&A) guideline known as FIPS 199. FIPS 199 is a standard for security categorization of Federal Information and Information Systems. It defines three levels of potential impact:

Low: It causes a limited adverse effect.

Medium: It causes a serious adverse effect.

High: It causes a severe adverse effect.

Question 8

Question Type: **MultipleChoice**

"Enhancing the Development Life Cycle to Produce Secure Software" summarizes the tools and practices that are helpful in producing secure software. What are these tools and practices?

Each correct answer represents a complete solution. Choose three.

Options:

A- Leverage attack patterns

B- Compiler security checking and enforcement

C- Tools to detect memory violations

D- Safe software libraries

E- Code for reuse and maintainability

Answer:

B, C, D

Explanation:

The tools and practices that are helpful in producing secure software are summarized in the report 'Enhancing the Development Life Cycle to

Produce Secure Software'. The tools and practices are as follows:

Compiler security checking and enforcement

Safe software libraries

Runtime error checking and safety enforcement

Tools to detect memory violations

Code obfuscation

Answer A and E are incorrect. These are secure coding principles and practices of defensive coding.

Question 9

Question Type: MultipleChoice

Which of the following are the basic characteristics of declarative security? Each correct answer represents a complete solution. Choose all that apply.

Options:

A- It is a container-managed security.

B- It has a runtime environment.

C- All security constraints are stated in the configuration files.

D- The security policies are applied at the deployment time.

Answer:

A, B, C

Explanation:

The following are the basic characteristics of declarative security:

In declarative security, programming is not required. All security constraints are stated in the configuration files.

It is a container-managed security. The application server manages the enforcing process of security constraints.

It has a runtime environment. The security policies for runtime environment are represented by the deployment descriptor. It can support different environments, such as development, testing, and production.

Answer D is incorrect. It is the characteristic of programmatic security.

Question 10

Question Type: MultipleChoice

An assistant from the HR Department calls you to ask the Service Hours & Maintenance Slots for your ERP system. In which document will you most probably find this information?

Options:

A- Service Level Agreement

B- Release Policy

C- Service Level Requirements

D- Underpinning Contract

Answer:

A

Explanation:

You will most probably find this information in the Service Level Agreement document. Amongst other information, SLA contains information

about the agreed Service Hours and maintenance slots for any particular Service.

Service Level Agreement (frequently abbreviated as SLA) is a part of a service contract where the level of service is formally defined. In practice, the term SLA is sometimes used to refer to the contracted delivery time (of the service) or performance.

Service Level Agreement (SLA) is a negotiated agreement between two parties where one is the customer and the other is the service provider. This can be a legally binding formal or informal 'contract'. Contracts between the Service Provider and other third parties are often

(incorrectly) called SLAs, as the level of service has been set by the (principal) customer there can be no 'agreement' between third parties

(these agreements are simply a 'contract'). Operating Level Agreements or OLA(s) however, may be used by internal groups to support SLA

(s).

Answer B is incorrect. Release Policy is a set of rules for deploying releases into the live operational environment, defining different approaches for releases depending on their urgency and impact.

Answer C is incorrect. The Service Level Requirements document contains the requirements for a service from the client viewpoint, defining detailed service level targets, mutual responsibilities, and other requirements specific to a certain group of customers.

Answer D is incorrect. Underpinning Contract (UC) is a contract between an IT service provider and a third party. In another way, it is

an agreement between the IT organization and an external provider about the delivery of one or more services. The third party provides

services that support the delivery of a service to a customer. The Underpinning Contract defines targets and responsibilities that are required

to meet agreed Service Level targets in an SLA.

Question 11

Question Type: MultipleChoice

Which of the following plans is documented and organized for emergency response, backup operations, and recovery maintained by an activity as part of its security program that will ensure the availability of critical resources and facilitates the continuity of operations in an emergency situation?

Options:

A- Continuity Of Operations Plan

B- Business Continuity Plan

C- Contingency Plan

D- Disaster Recovery Plan

Answer:

C

Explanation:

Contingency plan is prepared and documented for emergency response, backup operations, and recovery maintained by an activity as the

element of its security program that will ensure the availability of critical resources and facilitates the continuity of operations in an emergency

situation.

A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments

or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies and actions to deal with

specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and

'triggers' for initiating planned actions. They are required to help governments, businesses, or individuals to recover from serious incidents in

the minimum time with minimum cost and disruption.

Answer D is incorrect. A disaster recovery plan should contain data, hardware, and software that can be critical for a business. It

should also include the plan for sudden loss such as hard disc crash. The business should use backup and data recovery utilities to limit the

loss of data.

Answer A is incorrect. The Continuity Of Operation Plan (COOP) refers to the preparations and institutions maintained by the United

States government, providing survival of federal government operations in the case of catastrophic events. It provides procedures and

capabilities to sustain an organization's essential. COOP is the procedure documented to ensure persistent critical operations throughout any

period where normal operations are unattainable.

Answer B is incorrect. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an

organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster

or extended disruption. The logistical plan is called a business continuity plan.

Question 12

Question Type: MultipleChoice

Fill in the blank with an appropriate security type. applies the internal security policies of the software applications when they are deployed.

Options:

A- Programmatic security

Answer:

A

Explanation:

security, the code of the software application controls the security behavior, and authentication decisions are made based on the business

logic, such as the user role or the task performed by the user in a specific security context.