Vendor:ISC

Exam Code:CSSLP

Exam Name: Certified Secure Software Lifecycle Professional Practice Test

Version: Demo

QUESTION 1

Which of the following is designed to detect unwanted attempts at accessing, manipulating, and disabling of computer systems through the Internet?

A. DAS

B. IPsec

C. IDS

D. ACL

Correct Answer: C

An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers, malware and/or disgruntled employees. An IDS cannot directly detect attacks within properly encrypted traffic. An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, trojan horses, and worms). Answer: D is incorrect. Access Control List (ACL) is the most commonly used object in Cisco IOS. It filters packets or network traffic by controlling whether routed packets are forwarded or blocked at the router\\'s interfaces. According to the criteria specified within the access lists, router determines whether the packets to be forwarded or dropped. Access control list criteria could be the source or destination address of the traffic or other information. The types of Cisco ACLs are Standard IP, Extended IP, IPX, Appletalk, etc. Answer: B is incorrect. Internet Protocol Security (IPSec) is a method of securing data. It secures traffic by using encryption and digital signing. It enhances the security of data as if an IPSec packet is captured, its contents cannot be read. IPSec also provides sender verification that ensures the certainty of the datagram\\'s origin to the receiver. Answer: A is incorrect. Direct- attached storage (DAS) is a digital storage system that is directly attached to a server or workstation, without using a storage network.

QUESTION 2

You are the project manager of QSL project for your organization. You are working with your project team and several key stakeholders to create a diagram that shows how various elements of a system interrelate and the mechanism of causation within the system. What diagramming technique are you using as a part of the risk identification process?

A. Cause and effect diagrams

B. Influence diagrams

C. Predecessor and successor diagramming

D. System or process flowcharts

Correct Answer: D

In this example you are using a system or process flowchart. These can help identify risks within the process flow, such as bottlenecks or redundancy. Answer: A is incorrect. A cause and effect diagram, also known as an Ishikawa or fishbone diagram, can reveal causal factors to the effect to be solved. Answer: B is incorrect. An influence diagram shows causal influences, time ordering of events and relationships among variables and outcomes. Answer: C is incorrect. Predecessor and successor diagramming is not a valid risk identification term.

QUESTION 3

Which of the following coding practices are helpful in simplifying code? Each correct answer represents a complete solution. Choose all that apply.

A. Programmers should use multiple small and simple functions rather than a single complex function.

B. Software should avoid ambiguities and hidden assumptions, recursions, and GoTo statements.

C. Programmers should implement high-consequence functions in minimum required lines of code and follow proper coding standards.

D. Processes should have multiple entry and exit points.

Correct Answer: ABC

The various coding practices that are helpful in simplifying the code are as follows: Programmers should implement high-consequence functions in minimum required lines of code and follow the proper coding standards. Software should implement the functions that are defined in the software specification. Software should avoid ambiguities and hidden assumptions, recursion, and GoTo statements. Programmers should use multiple small and simple functions rather than a complex function. The processes should have only one entry point and minimum exit points. Interdependencies should be minimum so that a process module or component can be disabled when it is not needed, or replaced when it is found insecure or a better alternative is available, without disturbing the software operations. Programmers should use object-oriented techniques to keep the code simple and small. Some of the object-oriented techniques are object inheritance, encapsulation, and polymorphism. Answer: D is incorrect. Processes should have only one entry point and the minimum number of exit points.

QUESTION 4

Which of the following is an example of over-the-air (OTA) provisioning in digital rights management?

A. Use of shared secrets to initiate or rebuild trust.

B. Use of software to meet the deployment goals.

C. Use of concealment to avoid tampering attacks.

D. Use of device properties for unique identification.

Correct Answer: A

Over- the- air provisioning is a mechanism to deploy MIDlet suites over a network. It is a method of distributing MIDlet suites. MIDlet suite providers install their MIDlet suites on Web servers and provide a hypertext link for downloading. A user can use this link to download the MIDlet suite either through the Internet microbrowser or through WAP on his device. Over-the-air provisioning is required for end-to-end encryption or other security purposes in order to deliver copyrighted software to a mobile device. For example, use of shared secrets to initiate or rebuild trust. Answer: D and C are incorrect. The use of device properties for unique identification and the use of concealment to avoid tampering attacks are the security challenges in digital rights management (DRM). Answer: B is incorrect. The use of software and hardware to meet the deployment goals is a distracter.

QUESTION 5

Which of the following types of attacks occurs when an attacker successfully inserts an intermediary software or program between two communicating hosts?

A. Denial-of-service attack

B. Dictionary attack

C. Man-in-the-middle attack

D. Password guessing attack

Correct Answer: C

When an attacker successfully inserts an intermediary software or program between two

---

QUESTION 6

Mark works as a Network Administrator for NetTech Inc. He wants users to access only those resources that are required for them. Which of the following access control models will he use?

A. Discretionary Access Control

B. Mandatory Access Control

C. Policy Access Control

D. Role-Based Access Control

Correct Answer: D

Role-based access control (RBAC) is an access control model. In this model, a user can access resources according to his role in the organization. For example, a backup administrator is responsible for taking backups of important data. Therefore, he is only authorized to access this data for backing it up. However, sometimes users with different roles need to access the same resources. This situation can also be handled using the RBAC model. Answer: B is incorrect. Mandatory Access Control (MAC) is a model that uses a predefined set of access privileges for an object of the system. Access to an object is restricted on the basis of the sensitivity of the object and granted through authorization. Sensitivity of an object is defined by the label assigned to it. For example, if a user receives a copy of an object that is marked as "secret", he cannot grant permission to other users to see this object unless they have the appropriate permission. Answer: A is incorrect. DAC is an access control model. In this model, the data owner has the right to decide who can access the data. This model is commonly used in PC environment. The basis of this model is the use of Access Control List (ACL). Answer: C is incorrect. There is no such access control model as Policy Access Control.

QUESTION 7

Which of the following tiers addresses risks from an information system perspective?

A. Tier 0

B. Tier 3

C. Tier 2

D. Tier 1

Correct Answer: B

The information system level is the tier 3. It addresses risks from an information system perspective, and is guided by the risk decisions at tiers 1 and 2. Risk decisions at tiers 1 and 2 impact the ultimate selection and deployment of requisite safeguards. This also has an impact on the countermeasures at the information system level. The RMF primarily operates at tier3 but it can also have interactions at tiers 1 and 2. Answer: A is incorrect. It is an invalid Tier description. Answer: D is incorrect. The Organization Level is the Tier 1, and it addresses risks from an organizational perspective. Answer: C is incorrect. The mission and business process level is the Tier 2, and it addresses risks from the mission and business process perspective.

QUESTION 8

The National Information Assurance Certification and Accreditation Process (NIACAP) is the minimum standard process for the certification and accreditation of computer and telecommunications systems that handle U.S. national security information. What are the different types of NIACAP accreditation? Each correct answer represents a complete solution. Choose all that apply.

A. Site accreditation

B. Type accreditation

C. Secure accreditation

D. System accreditation

Correct Answer: ABD

NIACAP accreditation is of three types depending on what is being certified. They are as follows: 1.Site accreditation: This type of accreditation evaluates the applications and systems at a specific, self contained location. 2.Type accreditation:

This type of accreditation evaluates an application or system that is distributed to a number of different locations. 3.System accreditation: This accreditation evaluates a major application or general support system. Answer:

C is incorrect. No such type of NIACAP accreditation exists.

QUESTION 9

Which of the following security controls will you use for the deployment phase of the SDLC to build secure software? Each correct answer represents a complete solution. Choose all that apply.

A. Change and Configuration Control

B. Security Certification and Accreditation (CandA)

C. Vulnerability Assessment and Penetration Testing

D. Risk Adjustments

Correct Answer: BCD

The various security controls in the SDLC deployment phase are as follows: Secure Installation: While performing any software installation, it should kept in mind that the security configuration of the environment should never be reduced. If

it is reduced then security issues and overall risks can affect the environment. Vulnerability Assessment and Penetration Testing: Vulnerability assessments (VA) and penetration testing (PT) is used to determine the risk and attest to the strength of the software after it has been deployed. Security Certification and Accreditation (CandA): Security certification is the process used to ensure controls which are effectively implemented through established verification techniques and procedures, giving organization officials confidence that the appropriate safeguards and countermeasures are in place as means of protection. Accreditation is the provisioning of the necessary security authorization by a senior organization official to process, store, or transmit information. Risk Adjustments: Contingency plans and exceptions should be generated so that the residual risk be above the acceptable threshold.

QUESTION 10

Which of the following are the types of access controls? Each correct answer represents a complete solution. Choose three.

A. Physical

B. Technical

C. Administrative

D. Automatic

Correct Answer: ABC

Security guards, locks on the gates, and alarms come under physical access control. Policies and procedures implemented by an organization come under administrative access control. IDS systems, encryption, network segmentation, and antivirus controls come under technical access control. Answer: D is incorrect. There is no such type of access control as automatic control.

QUESTION 11

Which of the following acts is used to recognize the importance of information security to the economic and national security interests of the United States?

A. Computer Misuse Act

B. Lanham Act

C. Computer Fraud and Abuse Act

D. FISMA

Correct Answer: D

The Federal Information Security Management Act of 2002 is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002. The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency- wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA has brought attention within the federal government to cybersecurity and explicitly emphasized a \\'risk-based policy for cost-effective security\\'. FISMA requires agency program officials, chief information officers, and Inspectors Generals (IGs) to conduct annual reviews of the agency\\'s information security program and report the results to Office of Management and Budget (OMB). OMB uses this data to assist in its oversight responsibilities and to

prepare this annual report to Congress on agency compliance with the act. Answer: B is incorrect. The Lanham Act is a piece of legislation that contains the federal statutes of trademark law in the United States. The Act prohibits a number of activities, including trademark infringement, trademark dilution, and false advertising. It is also called Lanham Trademark Act. Answer: A is incorrect. The Computer Misuse Act 1990 is an act of the UK Parliament which states the following statement: Unauthorized access to the computer material is punishable by 6 months imprisonment or a fine "not exceeding level 5 on the standard scale" (currently 5000). Unauthorized access with the intent to commit or facilitate commission of further offences is punishable by 6 months/maximum fine on summary conviction or 5 years/fine on indictment. Unauthorized modification of computer material is subject to the same sentences as section 2 offences. Answer: C is incorrect. The Computer Fraud and Abuse Act is a law passed by the United States Congress in 1984 intended to reduce cracking of computer systems and to address federal computer-related offenses. The Computer Fraud and Abuse Act (codified as 18 U.S.C. 1030) governs cases with a compelling federal interest, where computers of the federal government or certain financial institutions are involved, where the crime itself is interstate in nature, or computers used in interstate and foreign commerce. It was amended in 1986, 1994, 1996, in 2001 by the USA PATRIOT Act, and in 2008 by the Identity Theft Enforcement and Restitution Act. Section (b) of the act punishes anyone who not just commits or attempts to commit an offense under the Computer Fraud and Abuse Act but also those who conspire to do so.

QUESTION 12

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we-are-secure.com. You have searched all open ports of the we-are-secure server. Now, you want to perform the next information-gathering step, i.e., passive OS fingerprinting. Which of the following tools can you use to accomplish the task?

A. Superscan

B. NBTscan

C. Nmap

D. P0f

Correct Answer: D

According to the scenario, you have searched all open ports of the we-are-secure server. Now you want to perform the next information-gathering step, i.e., passive OS fingerprinting. For this, you will use the P0f tool to accomplish the task. P0f is a passive OS fingerprinting tool that is used to identify the operating system of a target host simply by examining captured packets even when the device is behind a packet firewall. It does not generate any additional direct or indirect network traffic. P0f can also be used to gather various information, such as firewall presence, NAT use (for policy enforcement), existence of a load balancer setup, the distance to the remote system and its uptime, etc. Answer: C is incorrect. Nmap is used for active OS fingerprinting. Nmap is a free open-source utility for network exploration and security auditing. It is used to discover computers and services on a computer network, thus creating a "map" of the network. Just like many simple port scanners, Nmap is capable of discovering passive services. In addition, Nmap may be able to determine various details about the remote computers. These include operating system, device type, uptime, software product used to run a service, exact version number of that product, presence of some firewall techniques and, on a local area network, even vendor of the remote network card. Nmap runs on Linux, Microsoft Windows etc.Answer: A is incorrect. 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: B is incorrect. NBTscan is a scanner that scans IP networks for NetBIOS name information. It sends a NetBIOS status query to each address in a supplied range and lists received information in human readable form. It displays IP address, NetBIOS computer name, logged-in user name and MAC address of each responded host. NBTscan works in the same manner as nbtstat, but it operates on a range of addresses instead of just one.