Free Questions for CISSP

Shared by Hansen on 03-03-2025

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following is an open standard for exchanging authentication and authorization data between parties?

Options:

A- Wired markup language
B- Hypertext Markup Language (HTML)
C- Extensible Markup Language (XML)
D- Security Assertion Markup Language (SAML)

Answer:

D

Explanation:

Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties, such as a service provider and an identity provider. SAML is based on Extensible Markup Language (XML), which is a markup language that defines a set of rules for encoding and structuring data in a human-readable and machine-readable format. SAML enables single sign-on (SSO), which is a system that allows a user to log in and access multiple related servers and applications with a single authentication process. SAML uses assertions, which are statements that contain information about the user, such as their identity, attributes, or privileges, to communicate between the parties. SAML also uses protocols, which are sets of rules and messages that define how the parties request and respond to the assertions, to establish the trust and security of the communication. Wired markup language is not a term used in information security, but it could refer to a markup language that is used for creating web pages or applications that run on a wired network. Hypertext Markup Language (HTML) is a markup language that is used for creating and displaying web pages or applications that run on a web browser. HTML is not an open standard for exchanging authentication and authorization data between parties, but rather a standard for defining the structure and content of web pages or applications.

Question 2

Question Type: MultipleChoice

The security organization is loading for a solution that could help them determine with a strong level of confident that attackers have breached their network. Which solution is MOST effective at discovering successful network breach?

Options:

A- Installing an intrusion prevention system (IPS)
B- Deploying a honeypot
C- Installing an intrusion detection system (IDS)
D- Developing a sandbox

Answer:

B

Explanation:

A honeypot is a decoy system that is designed to attract and trap attackers, while diverting them from the real network assets. A honeypot can help detect successful network breaches by monitoring the attacker's activities and collecting forensic evidence. An intrusion prevention system (IPS) and an intrusion detection system (IDS) are both proactive measures that aim to prevent or detect network attacks, but they cannot confirm if a breach has occurred. A sandbox is an isolated environment that is used to test or run untrusted code or applications, but it is not a tool for discovering network breaches.Reference:1,2,3

Question 3

Question Type: MultipleChoice

Computer forensics require which of the following are MAIN steps?

Options:

A- Announce the incident to responsible sections, analyze the data, and assimilate the data for correlation
B- Take action to contain the damage, announce the incident to responsible sections, and analyze the data
C- Acquire the data without altering, authenticate the recovered data, and analyze the data
D- Access the data before destruction, assimilate the data for correlation, and take action to

contain the damage

Answer:

C

Explanation:

The main steps that computer forensics requires are to acquire the data without altering, authenticate the recovered data, and analyze the data. Computer forensics is the process of collecting, preserving, and examining digital evidence from computers or other electronic devices, such as smartphones, tablets, or cameras. Computer forensics follows a standard methodology that consists of the following steps:

Acquire the data without altering: This step involves creating a bit-by-bit copy or image of the original data source, such as a hard disk, a memory card, or a network packet, without modifying or damaging the original data. This ensures the integrity and the admissibility of the digital evidence in a court of law.

Authenticate the recovered data: This step involves verifying that the copied or imaged data is identical to the original data, and that it has not been tampered with or corrupted during the acquisition process. This can be done by using cryptographic hash functions, such as MD5 or SHA-1, that generate a unique and fixed-length value for the data, and comparing the hash values of the original and the copied data.

Analyze the data: This step involves examining the data for any relevant information or clues that can help to answer the questions or solve the problems related to the investigation. This can involve various techniques, such as keyword searching, file carving, timeline analysis, or malware analysis, depending on the type and the purpose of the data.

The other options are not the main steps that computer forensics requires. Announce the incident to responsible sections, take action to contain the damage, and assimilate the data for correlation are steps that are more related to incident response or security operations, not computer forensics. Access the data before destruction is not a step that computer forensics requires, as it implies that the data is already compromised or lost, which may prevent the acquisition or the authentication of the data.Reference:CISSP All-in-One Exam Guide, Eighth Edition, Chapter 8: Security Operations, page 1070.Official (ISC)2 CISSP CBK Reference, Fifth Edition, Chapter 7: Security Operations, page 1071.

Question 4

Question Type: MultipleChoice

When auditing the Software Development Life Cycle (SDLC) which of the following is one of the high-level audit phases?

Options:

A- Requirements
B- Risk assessment
C- Due diligence
D- Planning

Answer:

D

Explanation:

The high-level audit phase that is represented by the option D is planning. An audit is a systematic and independent examination and evaluation of the evidence, records, or activities of an entity, such as a process, a system, or an organization, to determine the compliance, effectiveness, or efficiency of the entity, and to provide assurance, recommendations, or improvements for the entity. The audit process consists of several phases, such as planning, execution, reporting, and follow-up. The planning phase is the first and the most important phase of the audit process, as it involves defining the objectives, scope, and criteria of the audit, and determining the roles, responsibilities, and resources of the audit team. The planning phase also involves conducting the preliminary risk assessment, the background research, and the stakeholder analysis of the audit entity, and developing the audit plan, the audit checklist, and the audit schedule .Reference: [CISSP CBK, Fifth Edition, Chapter 6, page 572]; [100 CISSP Questions, Answers and Explanations, Question 19].

Question 5

Question Type: MultipleChoice

Which of the following is a unique feature of attribute-based access control (ABAC)?

Options:

A- A user is granted access to a system based on group affinity.
B- A user is granted access to a system with biometric authentication.

C- A user is granted access to a system at a particular time of day.
D- A user is granted access to a system based on username and password.

Answer:

C

Explanation:

The unique feature of attribute-based access control (ABAC) that is represented by the option C is that a user is granted access to a system at a particular time of day. ABAC is a type of access control model that uses attributes as the basis for granting or denying access to resources or actions. Attributes are properties or characteristics of entities, such as users, devices, resources, or actions, that can be used to describe or identify them. Attributes can be static or dynamic, and can be derived from various sources, such as identity, environment, location, or time. ABAC can use any combination of attributes to define the access policies and rules, and to evaluate the access requests. ABAC is more flexible and granular than other access control models, such as Mandatory Access Control (MAC), Discretionary Access Control (DAC), or Role Based Access Control (RBAC), which use labels, owners, or roles as the basis for access control.A unique feature of ABAC is that it can use the time attribute to grant or deny access to a system, based on the particular time of day, such as the working hours, the holidays, or the weekends56.Reference:CISSP CBK, Fifth Edition, Chapter 5, page 443;CISSP Practice Exam -- FREE 20 Questions and Answers, Question 18.

Question 6

Question Type: MultipleChoice

Which change management role is responsible for the overall success of the project and supporting the change throughout the organization?

Options:

A- Change driver
B- Change implementer
C- Program sponsor
D- Project manager

Answer:

C

Explanation:

The change management role that is responsible for the overall success of the project and supporting the change throughout the organization is the program sponsor. The program sponsor is the senior executive or stakeholder who provides the vision, direction, and support for the change management project, and who ensures the alignment and integration of the change management project with the business goals and strategy of the organization.The program sponsor is responsible for the overall success of the project and supporting the change throughout the organization, as they can provide the leadership, guidance, and resources for the change management project, and communicate and advocate the benefits and value of the change management project to the other stakeholders, such as the management, the employees, or the customers34.Reference:CISSP CBK, Fifth Edition, Chapter 6, page 554;2024 Pass4itsure CISSP Dumps, Question 20.

Question 7

Question Type: MultipleChoice

Which of the following is a covert channel type?

Options:

A- Storage
B- Pipe
C- Memory
D- Monitoring

Answer:

A

Explanation:

The covert channel type that is represented by the option A is storage. A covert channel is a type of communication channel that allows the unauthorized or hidden transfer of information or data between two entities, such as processes, users, or systems, that are not supposed to communicate with each other, and that bypasses the security policies and mechanisms of the system. A storage covert channel is a type of covert channel that uses the shared storage

resources, such as memory, disk, or cache, to communicate the information or data, by modifying or reading the storage contents, such as the values, the locations, or the states, of the storage resources.A storage covert channel can compromise the confidentiality and integrity of the information or data, and violate the security principles of the system, such as the least privilege or the separation of duties12.Reference:CISSP CBK, Fifth Edition, Chapter 5, page 449;CISSP Practice Exam -- FREE 20 Questions and Answers, Question 19.

Question 8

Question Type: MultipleChoice

When reviewing vendor certifications for handling and processing of company data, which of the following is the BEST Service Organization Controls (SOC) certification for the vendor to possess?

Options:

A- SOC 1 Type 1
B- SOC 2 Type 1
C- SOC 2 Type 2
D- SOC 3

Answer:

C

Explanation:

The best Service Organization Controls (SOC) certification for the vendor to possess for handling and processing of company data is SOC 2 Type 2. SOC is a framework that defines the standards and criteria for the reporting and auditing of the internal controls and processes of a service organization, such as a cloud service provider, that affect the security, availability, processing integrity, confidentiality, or privacy of the information and systems of the user entities, such as the customers or clients of the service organization. SOC 2 Type 2 is a certification that indicates that the service organization has undergone an independent audit that evaluates and verifies the design and operating effectiveness of the internal controls and processes of the service organization, based on the Trust Services Criteria (TSC) of security, availability, processing integrity, confidentiality, or privacy, over a period of time, usually six to twelve months. SOC 2 Type 2 is the best SOC certification for the vendor to possess for handling and processing of company data, as it can provide the highest level of assurance and transparency for the security, reliability, and compliance of the vendor's services .Reference: [CISSP CBK, Fifth Edition, Chapter 2, page 90]; [CISSP Practice Exam -- FREE 20 Questions and Answers, Question 20].