



CertsMania

Free Questions for **CISSP**

Shared by **Dev** on **Sep 10, 2025**

For More Free Questions and Preparation Resources

Check the Links on Last Page



CertsMania

Questions # 1:

Which of the following is a characteristic of the independent testing of a program?

Options:

A.

Independent testing increases the likelihood that a test will expose the effect of a hidden feature.

B.

Independent testing decreases the likelihood that a test will expose the effect of a hidden feature.

C.

Independent testing teams help decrease the cost of creating test data and system design specification.

D.

Independent testing teams help identify functional requirements and Service Level Agreements (SLA)

Answer

A

Explanation

Independent testing is a type of testing that is performed by a third-party or external entity that is not involved in the development or operation of the program. Independent testing has several advantages, such as reducing bias, increasing objectivity, and improving quality. One of the characteristics of independent testing is that it increases the likelihood that a test will expose the effect of a hidden feature. A hidden feature is a functionality or behavior of the program that is not documented or specified, and may be intentional or unintentional. Independent testing can reveal the effect of a hidden feature by using different test cases, techniques, or perspectives than the ones used by the developers or operators of the program. **References:** CISSP All-in-One Exam Guide, Eighth Edition, Chapter 21: Software Development Security, page 1169; CISSP Official (ISC)2 Practice Tests, Third Edition, Domain 8: Software Development Security, Question 8.17, page 308.

Questions # 2:

Which of the following would be the BEST mitigation practice for man-in-the-middle (MITM) Voice over Internet Protocol (VoIP) attacks?

Options:

A.

Use Media Gateway Control Protocol (MGCP)

B.

Use Transport Layer Security (TLS) protocol

C.

Use File Transfer Protocol (FTP)

D.

Use Secure Shell (SSH) protocol

Answer

B

Explanation

The best mitigation practice for man-in-the-middle (MITM) Voice over Internet Protocol (VoIP) attacks is to use Transport Layer Security (TLS) protocol. TLS is a protocol that provides secure and encrypted communication and connection between two systems or devices over an unsecured or public network, such as the internet. TLS can mitigate MITM VoIP attacks, because it can:

Verify and authenticate the identity and the validity of the systems or devices that are involved in the VoIP communication or connection, by using the digital certificates and the public keys, and prevent any impersonation, spoofing, or repudiation of the VoIP communication or connection.

Encrypt and decrypt the data or the information that are exchanged in the VoIP communication or connection, by using the public keys and the private keys, and prevent any interception, modification, or eavesdropping of the VoIP communication or connection.

Sign and verify the data or the information that are exchanged in the VoIP communication or connection, by using the digital signatures and the public keys,

and ensure that the VoIP communication or connection are not altered, corrupted, or tampered with.

The other options are not the best mitigation practices for MITM VoIP attacks. Media Gateway Control Protocol (MGCP) is a protocol that provides the control and the management of the media gateways or the devices that convert the voice or the audio signals from one format or network to another format or network, such as from analog to digital, or from circuit-switched to packet-switched. MGCP does not mitigate MITM VoIP attacks, but rather facilitates the VoIP communication or connection, and it does not provide any security or encryption features or mechanisms. File Transfer Protocol (FTP) is a protocol that provides the transfer or the exchange of the files or the data between two systems or devices over a network, such as the internet. FTP does not mitigate MITM VoIP attacks, but rather supports the VoIP communication or connection, and it does not provide any security or encryption features or mechanisms. Secure Shell (SSH) is a protocol that provides secure and encrypted communication and connection between two systems or devices over an unsecured or public network, such as the internet. SSH can mitigate MITM VoIP attacks, but it is not the best option, because it is not designed or optimized for the VoIP communication or connection, and it may have some limitations or challenges, such as the bandwidth, the latency, or the compatibility of the protocol. **References:** CISSP All-in-One Exam Guide, Eighth Edition, Chapter 5: Communication and Network Security, page 589. Official (ISC)2 CISSP CBK Reference, Fifth Edition, Chapter 5: Communication and Network Security, page 590.

Questions # 3:

Which of the following BEST provides for non-repudiation of user account actions?

Options:

- A.
Centralized authentication system
- B.
File auditing system
- C.
Managed Intrusion Detection System (IDS)
- D.
Centralized logging system



CertsMania

Answer

D

Explanation

A centralized logging system is the best option for providing non-repudiation of user account actions. Non-repudiation is the ability to prove that a certain action or event occurred and who was responsible for it, without the possibility of denial or dispute. A centralized logging system is a system that collects, stores, and analyzes the log records generated by various sources, such as applications, servers, devices, or users. A centralized logging system can provide non-repudiation by capturing and preserving the evidence of the user account actions, such as the timestamp, the username, the IP address, the action performed, and the outcome. A centralized logging system can also prevent the tampering or deletion of the log records by using encryption, hashing, digital signatures, or write-once media. **References:** CISSP All-in-One Exam Guide, Eighth Edition, Chapter 7: Security Operations, page 382. CISSP Practice Exam | Boson, Question 10.

Questions # 4:

The threat modeling identifies a man-in-the-middle (MITM) exposure. Which countermeasure should the information system security officer (ISSO) select to mitigate the risk of a protected Health information (PHI) data leak?

Options:

A.

Auditing

B.

Anonymization

C.

Privacy monitoring

D.

Data retention



CertsMania

Answer

B

Explanation

The countermeasure that the information system security officer (ISSO) should select to mitigate the risk of a protected health information (PHI) data leak due to a man-in-the-middle (MITM) exposure is anonymization. A MITM exposure is a type of network attack where an attacker intercepts, modifies, or relays the communication between two parties, such as a client and a server, without their knowledge or consent. A MITM exposure can compromise the confidentiality, integrity, and availability of the data and the network, and can lead to data theft, fraud, or sabotage. A PHI data leak is a type of data breach where the sensitive and personal information of patients or health care providers, such as medical records, diagnoses, treatments, or insurance details, are exposed or disclosed to unauthorized parties, such as hackers, competitors, or media. A PHI data leak can violate the privacy and security of the data and the individuals, and can result in legal or regulatory penalties, reputational damage, or financial losses. Anonymization is a technique that removes or masks the identifying or personal information from the data, such as names, addresses, or social security numbers, and replaces them with pseudonyms, codes, or random values. Anonymization can prevent or reduce the risk of a PHI data leak due to a MITM exposure, as it makes the data untraceable and unlinkable to the individuals, and protects the data from being accessed or misused by unauthorized parties. Auditing, privacy monitoring, and data retention are not countermeasures that the ISSO should select to mitigate the risk of a PHI data leak due to a MITM exposure, as they are either not effective or not relevant for preventing or reducing the data exposure or disclosure, or they may have other purposes or functions than data protection. **References:**

MITM Exposure

PHI Data Leak

Anonymization

Questions # 5:

A recent information security risk assessment identified weak system access controls on mobile devices as a high me In order to address this risk and ensure only authorized staff access company information, which of the following should the organization implement?

Options:

A.

Intrusion prevention system (IPS)

B.

Multi-factor authentication (MFA)

C.

Data loss protection (DLP)

D.

Data at rest encryption



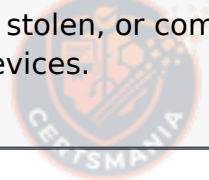
CertsMania

Answer

B

Explanation

Multi-factor authentication (MFA) is a method of authentication that requires two or more independent factors to verify the identity of a user, such as something you know, something you have, or something you are. MFA can help address the risk of weak system access controls on mobile devices, as it provides a higher level of security than a single factor, such as a password. MFA can prevent unauthorized access to company information, even if the mobile device is lost, stolen, or compromised. An intrusion prevention system (IPS) is a device or software that monitors and blocks network traffic based on predefined rules or signatures. An IPS can help protect the network from external attacks, but it does not address the system access controls on mobile devices. Data loss protection (DLP) is a system or tool that prevents the unauthorized disclosure, transfer, or leakage of sensitive data. DLP can help protect the company information from being exposed, but it does not address the system access controls on mobile devices. Data at rest encryption is a technique that encrypts the data that is stored on a device or a media. Data at rest encryption can help protect the company information from being accessed, even if the mobile device is lost, stolen, or compromised, but it does not address the system access controls on mobile devices.



CertsMania

Questions # 6:

Directive controls are a form of change management policy and procedures. Which of the following subsections are recommended as part of the change management process?

Options:

A.

Build and test

B.

Implement security controls

C.

Categorize Information System (IS)

D.

Select security controls



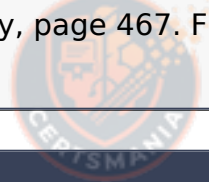
CertsMania

Answer

A

Explanation

Build and test is a subsection that is recommended as part of the change management process. Change management is a process that ensures that any changes to the organization's information systems and assets are controlled, documented, and approved, and that they do not adversely affect the security and the performance of the systems and the assets. Change management is based on the principles of directive controls, which are the policies and the procedures that guide and regulate the change management process. One of the subsections of the change management process is build and test, which involves developing and verifying the proposed changes before implementing them in the production environment. Build and test can help ensure that the changes are consistent with the design specifications, that they meet the security and the functional requirements, and that they do not introduce any errors, flaws, or vulnerabilities. Build and test can also help evaluate the impact and the benefits of the changes, and identify and resolve any issues or conflicts that may arise during the change process. **References:** CISSP All-in-One Exam Guide, Eighth Edition, Chapter 8: Software Development Security, page 467. Free daily CISSP practice questions, Question



CertsMania

Questions # 7:

Which of the following is the GREATEST risk of relying only on Capability Maturity Models (CMM) for software to guide process improvement and assess capabilities of acquired software?

Options:

A.

Organizations can only reach a maturity level 3 when using CMMs

B.

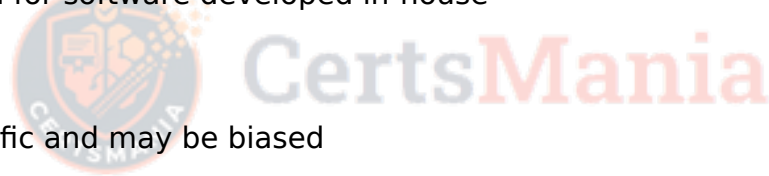
CMMs do not explicitly address safety and security

C.

CMMs can only be used for software developed in-house

D.

CMMs are vendor specific and may be biased



Answer

B

Explanation

The greatest risk of relying only on Capability Maturity Models (CMMs) for software to guide process improvement and assess capabilities of acquired software is that CMMs do not explicitly address safety and security. CMMs are frameworks that measure and improve the maturity and quality of the software development processes and products. CMMs define different levels of maturity, from initial to optimized, based on the presence and effectiveness of the key process areas, such as requirements management, project planning, configuration management, quality assurance, or risk management. CMMs can help to evaluate and improve the software development processes and products, but they do not explicitly address the safety and security aspects of the software. Safety and security are important attributes of the software, especially for critical or sensitive applications, such as medical, military, or financial applications. Safety and security require specific processes and practices, such as threat modeling, secure coding, vulnerability testing, or incident response, that are not covered by the CMMs. Therefore, relying only on CMMs for software may result in overlooking or neglecting the safety and security issues of the software, which may lead to serious consequences, such as harm, loss, or breach. Organizations can only reach a maturity level 3 when using CMMs, CMMs can only be used for software developed in-house, and CMMs are vendor specific and may be biased are not the greatest risks of relying only on CMMs for software. These are some of the limitations or challenges of using CMMs for software, but they are not as significant or critical as the lack of safety and security. Organizations can reach higher maturity levels than level 3 when using CMMs, depending on the implementation and assessment of the CMMs. CMMs can be used for software developed in-house or outsourced, depending on the scope and criteria of the CMMs. CMMs are not vendor specific and may not be biased, as they are based on industry standards and best practices, such as ISO/IEC 15504 or ISO/IEC 33001. **References:** Official (ISC)2 CISSP CBK Reference, Fifth Edition, Domain 8, Software Development Security, page 831. CISSP All-in-One Exam Guide, Eighth Edition, Chapter 8, Software Development Security, page 767.

Questions # 8:

In Federated Identity Management (FIM), which of the following represents the concept of federation?

Options:

A.

Collection of information logically grouped into a single entity

B.

Collection, maintenance, and deactivation of user objects and attributes in one or more systems, directories or applications

C.

Collection of information for common identities in a system

D.

Collection of domains that have established trust among themselves

Answer

D

Explanation

The concept of federation in Federated Identity Management (FIM) is the collection of domains that have established trust among themselves. A domain is a logical or administrative boundary that defines the scope and authority of an identity provider (IdP) or a service provider (SP). An IdP is an entity that creates, maintains, and verifies the identities and attributes of the users. An SP is an entity that provides services or resources to the users, and relies on the IdP for the authentication and authorization of the users. A federation is a group of domains that have agreed to share and accept the identities and attributes of the users across the domains, based on a common set of policies, standards, and protocols. A federation enables the users to access multiple services or resources from different domains, using a single or federated identity, without having to create or manage multiple accounts or credentials. A federation also enhances the security, privacy, and convenience of the users and the domains, by reducing the identity management overhead and complexity, and by enabling the users to control the disclosure and use of their identity information. References: [CISSP CBK, Fifth Edition, Chapter 5, page 449]; [CISSP Practice Exam - FREE 20 Questions and Answers, Question 18].

Questions # 9:

Which of the following threats would be MOST likely mitigated by monitoring assets containing open source libraries for vulnerabilities?

Options:

A.

Distributed denial-of-service (DDoS) attack

B.

Zero-day attack

C.

Phishing attempt

D.

Advanced persistent threat (APT) attempt

Answer

B

Explanation

The threat that would be most likely mitigated by monitoring assets containing open source libraries for vulnerabilities is a zero-day attack. A zero-day attack is a type of attack that exploits a previously unknown or undisclosed vulnerability in a system or application, before the vendor or developer can release a patch or a fix for the vulnerability. A zero-day attack can cause severe damage or compromise to the system or application, as there is no available defense or protection against the attack. A zero-day attack can target any system or application, but it can be more prevalent or effective against those that contain open source libraries, as the open source libraries are publicly available and accessible, and can be analyzed or reverse-engineered by the attackers to discover and exploit the vulnerabilities. Monitoring assets containing open source libraries for vulnerabilities can help to mitigate a zero-day attack, as it can help to identify and report the vulnerabilities in the open source libraries, and to apply the patches or fixes as soon as they are available. References: [CISSP CBK, Fifth Edition, Chapter 3, page 239]; [100 CISSP Questions, Answers and Explanations, Question 18].

Questions # 10:

What determines the level of security of a combination lock?

Options:

A.

Complexity of combination required to open the lock

B.

Amount of time it takes to brute force the combination

C.

The number of barrels associated with the internal mechanism

D.

The hardness score of the metal lock material

Answer

B

Explanation

The amount of time it takes to brute force the combination determines the level of security of a combination lock. A combination lock is a type of physical lock that requires a sequence of numbers or symbols to open it. A combination lock can be used to protect a door, a safe, a locker, or a bike. The level of security of a combination lock depends on how difficult or easy it is to guess or crack the combination. One way to measure the difficulty or ease of cracking the combination is by calculating the amount of time it takes to brute force the combination, which is a method of trying all possible combinations until finding the correct one. The amount of time it takes to brute force the combination depends on various factors, such as the number of possible combinations, the speed of the brute force tool, and the resistance of the lock. The longer it takes to brute force the combination, the higher the level of security of the combination lock. **References:** CISSP All-in-One Exam Guide, Eighth Edition, Chapter 3: Security Engineering, page 130. Free daily CISSP practice questions, Question 5.

Questions # 11:

Which of the following is MOST appropriate to collect evidence of a zero-day attack?

Options:

A.

Firewall

B.

Honeypot

C.

Antispam

D.

Antivirus



CertsMania

Answer

B

Explanation

A honeypot is a decoy system that is designed to attract and trap attackers. A honeypot can be used to collect evidence of a zero-day attack, which is an attack that exploits a previously unknown vulnerability. A honeypot can capture the attacker's actions, tools, and techniques, and provide valuable information for analysis and mitigation. A honeypot can also divert the attacker's attention from the real targets and waste their time and resources. A firewall, an antispam, and an antivirus are not effective in detecting or preventing zero-day attacks, as they rely on known signatures or rules that may not match the new attack. **References:** CISSP Official Study Guide, 9th Edition, page 1010; CISSP All-in-One Exam Guide, 8th Edition, page 1089

Questions # 12:

What type of attack sends Internet Control Message Protocol (ICMP) echo requests to the target machine with a larger payload than the target can handle?

Options:

A.

Man-in-the-Middle (MITM)

B.

Denial of Service (DoS)

C.

Domain Name Server (DNS) poisoning

D.

Buffer overflow



CertsMania

Answer

B

Explanation

The type of attack that sends Internet Control Message Protocol (ICMP) echo requests to the target machine with a larger payload than the target can handle is the Denial of Service (DoS) attack. A DoS attack is a type of attack that aims to disrupt or degrade the normal functioning or availability of a system or network, by consuming or exhausting its resources, such as bandwidth, memory, or processing power. A DoS attack can prevent or delay the legitimate or authorized users or processes from accessing or using the system or network, and compromise the availability and reliability of the system or network. A DoS attack can be performed by using various methods or techniques, such as flooding, amplification, or synchronization. One of the methods or techniques of a DoS attack is to send ICMP echo requests to the target machine with a larger payload than the target can handle. ICMP is a network protocol that is used to send control or error messages between the hosts or routers in a network, such as ping or traceroute. An ICMP echo request is a type of ICMP message that is used to test the connectivity or reachability of a host or router in a network, by requesting a reply from the destination host or router. An ICMP echo request can also carry a payload, which is a data or information that is attached to the ICMP message. A DoS attack can send ICMP echo requests to the target machine with a larger payload than the target can handle, by using a tool or technique that can generate or spoof the ICMP echo requests with a large or arbitrary payload size, such as ping of death or jolt. This can cause the target machine to receive more ICMP echo requests than it can process or respond, and overload or crash the target machine, resulting in a denial of service. Man-in-the-Middle (MITM), Domain Name Server (DNS) poisoning, or buffer overflow are not the types of attacks that send ICMP echo requests to the target machine with a larger payload than the target can handle, as they are either more related to the interception, manipulation, or corruption of the network traffic or data, rather than the consumption or exhaustion of the network resources. **References:** CISSP All-in-One Exam Guide, Eighth Edition, Chapter 6: Secure Network Architecture and Securing Network Components, page 377; CISSP Official (ISC)2 Practice Tests, Third Edition, Domain 4: Communication and Network Security, Question 4.9, page 187.

Which of the following is the FIRST step for defining Service Level Requirements (SLR)?

Options:

A.

Creating a prototype to confirm or refine the customer requirements

B.

Drafting requirements for the service level agreement (SLA)

C.

Discussing technology and solution requirements with the customer

D.

Capturing and documenting the requirements of the customer

Answer

D

Explanation

Service Level Requirements (SLR) are the expectations and needs of the customer for a particular service, such as availability, performance, security, or reliability. The first step for defining SLR is to capture and document the requirements of the customer, which involves identifying the stakeholders, understanding their business objectives, and eliciting their functional and non-functional requirements. This step ensures that the service provider and the customer have a clear and common understanding of what the service should deliver and how it will be measured. **References:** CISSP All-in-One Exam Guide, Eighth Edition, Chapter 8: Security Operations, page 507. Official (ISC)² CISSP CBK Reference, Fifth Edition, Domain 7: Security Operations, page 853.

Questions # 14:

Which of the following should be included in a hardware retention policy?

Which of the following should be included in a hardware retention policy?

Options:

A.

The use of encryption technology to encrypt sensitive data prior to retention

B.

Retention of data for only one week and outsourcing the retention to a third-party vendor

C.

Retention of all sensitive data on media and hardware

D.

A plan to retain data required only for business purposes and a retention schedule

Answer

D

Explanation

A hardware retention policy is a set of guidelines that defines how long hardware and data should be kept and how they should be disposed of when they are no longer needed. A hardware retention policy should include a plan to retain data required only for business purposes and a retention schedule that specifies the duration and frequency of data retention. This can help to reduce the risk of data breaches, comply with legal and regulatory requirements, optimize storage space and costs, and support business continuity and disaster recovery. A hardware retention policy should also include procedures for secure data erasure and hardware disposal to prevent unauthorized access to sensitive data. References:

Hardware Retention Policy

Disposal of IT Equipment Policy

Data Retention Policy

Questions # 15:

Which security evaluation model assesses a product's Security Assurance Level (SAL) in comparison to similar solutions?

Options:

A.

Payment Card Industry Data Security Standard (PCI-DSS)

B.

International Organization for Standardization (ISO) 27001

C.

Common criteria (CC)

D.

Control Objectives for Information and Related Technology (COBIT)



Answer

C

Explanation

Common criteria (CC) is an international standard (ISO/IEC 15408) for evaluating the security properties and capabilities of information technology (IT) products and systems. CC defines a common framework and methodology for expressing security requirements, conducting security evaluations, and certifying security assurance levels. CC allows vendors, customers, and evaluators to compare and contrast the security features and functions of different IT products and systems based on their security assurance levels (SALs). SALs range from EAL1 (functionally tested) to EAL7 (formally verified design and tested). **References:** Official (ISC)2 CISSP CBK Reference, Chapter 3: Security Architecture and Engineering, Section: Security Evaluation Models, pp. 331-334.

Questions # 16:

A network administrator is configuring a database server and would like to ensure the database engine is listening on a certain port. Which of the following commands should the administrator use to accomplish this goal?

Options:

A.

nslookup

B.

netstat -a

C.

ipconfig /a

D.

arp -a



CertsMania

Answer

B

Explanation

The “netstat -a” command is a command-line tool that can be used to display the status of all the network connections and listening ports on a server. The “netstat -a” command can show the protocol, local address, foreign address, and state of each connection or port. The network administrator can use this command to ensure the database engine is listening on a certain port by looking for the port number in the local address column and the “LISTENING” state in the state column. The other options are not commands that can be used to accomplish this goal, as they either do not display the listening ports, do not work on a server, or do not relate to the network. **References:** CISSP - Certified Information Systems Security Professional, Domain 4. Communication and Network Security, 4.2 Secure network components, 4.2.2 Prevent or mitigate network attacks, 4.2.2.1 Network discovery and mapping; CISSP Exam Outline, Domain 4. Communication and Network Security, 4.2 Secure network components, 4.2.2 Prevent or mitigate network attacks, 4.2.2.1 Network discovery and mapping

Questions # 17:

To monitor the security of buried data lines inside the perimeter of a facility, which of the following is the MOST effective control?

Options:

A.

Fencing around the facility with closed-circuit television (CCTV) cameras at all entry points

B.

Ground sensors installed and reporting to a security event management (SEM) system

C.

Steel casing around the facility ingress points

D.

regular sweeps of the perimeter, including manual inspection of the cable ingress points

Answer

B

Explanation

The most effective control to monitor the security of buried data lines inside the perimeter of a facility is to use ground sensors installed and reporting to a security event management (SEM) system. Ground sensors are devices that detect and measure the physical changes or disturbances in the ground, such as vibration, pressure, or sound, caused by any movement or activity near the buried data lines. Ground sensors can report the detected signals to a security event management system, which is a system that collects, analyzes, and correlates the security events and alerts from various sources, such as sensors, cameras, or logs. A security event management system can help to identify and respond to any unauthorized or malicious attempts to access, tamper, or damage the buried data lines, and to alert the security personnel or authorities³⁴. **References:** CISSP CBK, Fifth Edition, Chapter 5, page 435; 2024 Pass4itsure CISSP Dumps, Question 14.

Questions # 18:

Which of the following BEST ensures the integrity of transactions to intended recipients?

Options:

A.

Public key infrastructure (PKI)

B.

Blockchain technology

C.

Pre-shared key (PSK)

D.

Answer

A

Explanation

The best option that ensures the integrity of transactions to intended recipients is public key infrastructure (PKI). PKI is a system that provides the services and the mechanisms for creating, managing, distributing, using, storing, and revoking the digital certificates and the public keys that are used for securing the communication and the transactions between the systems or the entities. PKI ensures the integrity of transactions to intended recipients, because it can:

Verify and authenticate the identity and the validity of the systems or the entities that are involved in the transactions, by using the digital certificates and the public keys, and prevent any impersonation, spoofing, or repudiation of the transactions.

Encrypt and decrypt the data or the information that are exchanged in the transactions, by using the public keys and the private keys, and prevent any interception, modification, or eavesdropping of the transactions.

Sign and verify the data or the information that are exchanged in the transactions, by using the digital signatures and the public keys, and ensure that the transactions are not altered, corrupted, or tampered with.

The other options are not the best options that ensure the integrity of transactions to intended recipients. Blockchain technology is a system that provides a distributed and decentralized ledger or database that records and validates the transactions or the events that are shared and agreed upon by the participants or the nodes in the network, by using the cryptographic hashes and the consensus mechanisms. Blockchain technology can ensure the integrity of transactions to intended recipients, but it is not the best option, because it may not provide the same level of verification, authentication, encryption, decryption, signing, and verification as PKI, and it may have some limitations or challenges, such as the scalability, the performance, or the interoperability of the system. Pre-shared key (PSK) is a system that provides a symmetric encryption or decryption key that is shared or agreed upon by the systems or the entities that are involved in the communication or the transactions, and that is used for securing the communication or the transactions. PSK can ensure the integrity of transactions to intended recipients, but it is not the best option, because it may not provide the same level of verification, authentication, encryption, decryption, signing, and verification as PKI, and it may have some risks or drawbacks, such as the key distribution, the key management, or the key compromise of the system. Web of trust is a system that provides a decentralized and distributed trust model that relies on the users or the entities to create, validate, and exchange the digital certificates and the public keys that are used for securing the communication or the transactions, by using the endorsements or the ratings of the other

users or the entities. Web of trust can ensure the integrity of transactions to intended recipients, but it is not the best option, because it may not provide the same level of verification, authentication, encryption, decryption, signing, and verification as PKI, and it may have some issues or problems, such as the quality, the reliability, or the consistency of the system. **References:** CISSP All-in-One Exam Guide, Eighth Edition, Chapter 5: Communication and Network Security, page 633. Official (ISC)2 CISSP CBK Reference, Fifth Edition, Chapter 5: Communication and Network Security, page 634.

Questions # 19:

A security professional was tasked with rebuilding a company's wireless infrastructure. Which of the following are the MOST important factors to consider while making a decision on which wireless spectrum to deploy?

Options:

A.

Hybrid frequency band, service set identifier (SSID), and interpolation

B.

Performance, geographic location, and radio signal interference

C.

Facility size, intermodulation, and direct satellite service

D.

Existing client devices, manufacturer reputation, and electrical interference

Answer

B

Explanation

The wireless spectrum is the range of frequencies that can be used for wireless communication. Different wireless standards use different frequency bands, such as 2.4 GHz, 5 GHz, or 6 GHz. The choice of the wireless spectrum depends on several factors, such as the performance, geographic location, and radio signal interference of the wireless network. Performance refers to the data rate, bandwidth, and latency of the wireless network. Geographic location refers to the regulatory and legal restrictions on the use of certain frequency bands in different countries or regions. Radio signal interference refers

to the noise and distortion caused by other wireless devices or sources that share the same frequency band. Hybrid frequency band, SSID, and interpolation are not relevant factors for choosing the wireless spectrum. **References:** CISSP CBK Reference, 5th Edition, Chapter 4, page 211; CISSP All-in-One Exam Guide, 8th Edition, Chapter 4, page 173

Questions # 20:

Which of the following is used to ensure that data mining activities Will NOT reveal sensitive data?

Options:

A.

Implement two-factor authentication on the underlying infrastructure.

B.

Encrypt data at the field level and tightly control encryption keys.

C.

Preprocess the databases to see if inn can be disclosed from the learned patterns.

D.

Implement the principle of least privilege on data elements so a reduced number of users can access the database.

Answer

B

Explanation

Encrypting data at the field level ensures that sensitive information remains confidential and secure even during data mining activities. Tight control over encryption keys further ensures that only authorized personnel can access and decrypt sensitive data. References: Unable to provide specific references due to browsing limitations.

Questions # 21:

What is the MAIN objective of risk analysis in Disaster Recovery (DR) planning?

Options:

A.

Establish Maximum Tolerable Downtime (MTD) Information Systems (IS).

B.

Define the variable cost for extended downtime scenarios.

C.

Identify potential threats to business availability.

D.

Establish personnel requirements for various downtime scenarios.

Answer

C

Explanation

Risk analysis is the process of identifying, assessing, and prioritizing the risks that could affect an organization's assets, operations, or objectives. Risk analysis is an essential component of Disaster Recovery (DR) planning, as it helps to determine the likelihood and impact of various disaster scenarios, and to develop appropriate mitigation and recovery strategies. The main objective of risk analysis in DR planning is to identify potential threats to business availability, which is the ability of an organization to continue its critical business functions and processes in the event of a disaster. Business availability depends on the availability of the information systems (IS) that support the business functions and processes, such as hardware, software, data, network, and personnel. Risk analysis helps to identify the vulnerabilities and threats that could compromise the availability of the IS, and to estimate the potential losses and damages that could result from a disaster. Risk analysis also helps to establish the recovery point objective (RPO), which is the maximum acceptable amount of data loss after a disaster, and the recovery time objective (RTO), which is the maximum acceptable time to restore the normal operations after a disaster. **References:** Official (ISC)2 Guide to the CISSP CBK, Fifth Edition, Chapter 7: Security Operations, page 330. [CISSP All-in-One Exam Guide, Eighth Edition], Chapter 8: Business Continuity and Disaster Recovery Planning, page 461.

Which of the following factors is a PRIMARY reason to drive changes in an Information Security Continuous Monitoring (ISCM) strategy?

Options:

A.

Testing and Evaluation (TE) personnel changes

B.

Changes to core missions or business processes

C.

Increased Cross-Site Request Forgery (CSRF) attacks

D.

Changes in Service Organization Control (SOC) 2 reporting requirements

Answer

B

Explanation

The factor that is a primary reason to drive changes in an Information Security Continuous Monitoring (ISCM) strategy is changes to core missions or business processes. ISCM is a process that provides ongoing and real-time observation, assessment, and reporting of the security posture and performance of an organization, system, or network, against a set of predefined criteria, standards, or regulations. ISCM can help to provide timely and accurate information and feedback on the security status and risks of the organization, system, or network, as well as to support the security decision making and actions of the organization and the stakeholders. ISCM should follow a well-defined strategy that specifies the scope, objectives, methodology, tools, techniques, roles, and responsibilities for the ISCM process, as well as the frequency, format, and distribution of the ISCM reports. The ISCM strategy should be aligned with the security goals and strategies of the organization, system, or network, and it should be reviewed and updated regularly to ensure its relevance and effectiveness. The factor that is a primary reason to drive changes in the ISCM strategy is changes to core missions or business processes. The core missions or business processes are the essential and fundamental activities or functions that the organization, system, or network performs or supports to achieve its vision, mission, values, and strategies. The core missions or business processes can affect the ISCM strategy, as they can determine the scope, direction, and priority of the ISCM process, as well as the security risks and opportunities that the organization, system, or network faces. Changes to core missions or business processes can have a significant

impact on the ISCM strategy, as they can create a gap or a misalignment between the ISCM strategy and the core missions or business processes, and expose the organization, system, or network to new or increased security threats or vulnerabilities. Therefore, changes to core missions or business processes would require a review and possible change to the ISCM strategy, to ensure that the ISCM strategy is consistent and compatible with the core missions or business processes, and that the ISCM strategy supports and enables the organization, system, or network to achieve its core missions or business processes. Testing and Evaluation (TE) personnel changes, increased Cross-Site Request Forgery (CSRF) attacks, or changes in Service Organization Control (SOC) 2 reporting requirements are not the factors that are primary reasons to drive changes in the ISCM strategy, as they are more related to the operational, technical, or compliance aspects of the ISCM process, rather than the strategic or business aspects of the ISCM process. **References:** CISSP All-in-One Exam Guide, Eighth Edition, Chapter 18: Security Assessment and Testing, page 1015; CISSP Official (ISC)2 Practice Tests, Third Edition, Domain 6: Security Assessment and Testing, Question 6.9, page 246.

Questions # 23:

Which of the following would be the BEST guideline to follow when attempting to avoid the exposure of sensitive data?

Options:

A.

Store sensitive data only when necessary.

B.

Educate end-users on methods of attacks on sensitive data.

C.

Establish report parameters for sensitive data.

D.

Monitor mail servers for sensitive data being exfiltrated.

Answer

A

Explanation

The best guideline to follow when attempting to avoid the exposure of sensitive data is to store sensitive data only when necessary. Sensitive data is a type of data or information that is considered or classified as confidential, private, or secret, and that can cause harm or damage to the data owner or the data subject, or to the organization or the business, if it is accessed or disclosed by unauthorized parties, such as hackers, insiders, or competitors. Sensitive data can include various types or categories, such as personal data, financial data, health data, or intellectual property data. Sensitive data can be exposed or revealed by various methods, such as a breach, which is a type of incident or event that occurs on a system or a network, and that results in the unauthorized access or disclosure of the sensitive data, and that compromises the confidentiality, integrity, or availability of the sensitive data. Sensitive data can be protected or secured by various methods, such as a guideline, which is a type of rule or principle that provides the direction, instruction, or recommendation for handling or managing the sensitive data, and that can be used as a reference or a standard for measuring or evaluating the compliance or alignment with the security requirements or regulations. Storing sensitive data only when necessary is a guideline that can be followed when attempting to avoid the exposure of sensitive data, as it can provide the benefits of both minimizing and securing the sensitive data, such as reducing the attack surface and exposure of the sensitive data, and enhancing the performance and security of the system or the network . References: [CISSP CBK, Fifth Edition, Chapter 3, page 230]; [CISSP Practice Exam - FREE 20 Questions and Answers, Question 17].

Questions # 24:

What would be the MOST cost effective solution for a Disaster Recovery (DR) site given that the organization's systems cannot be unavailable for more than 24 hours?

Options:

A.

Warm site

B.

Hot site

C.

Mirror site

D.

Cold site



CertsMania

Answer

A

Explanation

A warm site is the most cost effective solution for a disaster recovery (DR) site given that the organization's systems cannot be unavailable for more than 24 hours. A DR site is a backup facility that can be used to restore the normal operation of the organization's IT systems and infrastructure after a disruption or disaster. A DR site can have different levels of readiness and functionality, depending on the organization's recovery objectives and budget. The main types of DR sites are:

Hot site: a DR site that is fully operational and equipped with the necessary hardware, software, telecommunication lines, and network connectivity to allow the organization to be up and running almost immediately. A hot site has all the required servers, workstations, and communications links, and can function as a branch office or data center that is online and connected to the production network. A hot site also has a backup of the data from the systems at the primary site, which may be replicated in real time or near real time. A hot site greatly reduces or eliminates downtime for the organization, but it is also very expensive to maintain and operate.

Warm site: a DR site that is partially operational and equipped with some of the hardware, software, telecommunication lines, and network connectivity to allow the organization to be up and running within a short time. A warm site has some of the required servers, workstations, and communications links, and can function as a temporary office or data center that is offline or partially connected to the production network. A warm site may have a backup of the data from the systems at the primary site, but it is not updated or synchronized as frequently as a hot site. A warm site reduces downtime for the organization, but it is also less expensive than a hot site.

Cold site: a DR site that is not operational and equipped with only the basic infrastructure and environmental support systems to allow the organization to be up and running within a long time. A cold site has none of the required servers, workstations, and communications links, and cannot function as an office or data center until they are installed and configured. A cold site does not have a backup of the data from the systems at the primary site, and it has to be restored from other sources, such as tapes or disks. A cold site increases downtime for the organization, but it is also the cheapest option among the DR sites.

Mirror site: a DR site that is an exact replica of the primary site, with the same hardware, software, telecommunication lines, and network connectivity, and with the same data and applications. A mirror site is always online and synchronized with the primary site, and can take over the operation of the organization seamlessly in the event of a disruption or disaster. A mirror site eliminates downtime for the organization, but it is also the most expensive option among the DR sites.

A warm site is the most cost effective solution for a disaster recovery (DR) site given that the organization's systems cannot be unavailable for more than 24 hours, because it can provide a balance between the recovery time and the recovery cost. A warm site can enable the organization to resume its critical functions and operations within a reasonable time frame, without spending too much on the DR site maintenance and operation. A warm site can also provide some flexibility and scalability for the organization to adjust its recovery strategies and resources according to its needs and priorities.

The other options are not the most cost effective solutions for a disaster recovery (DR) site given that the organization's systems cannot be unavailable for more than 24 hours, but rather solutions that are either too costly or too slow for the organization's recovery objectives and budget. A hot site is a solution that is too costly for a disaster recovery (DR) site given that the organization's systems cannot be unavailable for more than 24 hours, because it requires the organization to invest a lot of money on the DR site equipment, software, and services, and to pay for the ongoing operational and maintenance costs. A hot site may be more suitable for the organization's systems that cannot be unavailable for more than a few hours or minutes, or that have very high availability and performance requirements. A mirror site is a solution that is too costly for a disaster recovery (DR) site given that the organization's systems cannot be unavailable for more than 24 hours, because it requires the organization to duplicate its entire primary site, with the same hardware, software, data, and applications, and to keep them online and synchronized at all times. A mirror site may be more suitable for the organization's systems that cannot afford any downtime or data loss, or that have very strict compliance and regulatory requirements. A cold site is a solution that is too slow for a disaster recovery (DR) site given that the organization's systems cannot be unavailable for more than 24 hours, because it requires the organization to spend a lot of time and effort on the DR site installation, configuration, and restoration, and to rely on other sources of backup data and applications. A cold site may be more suitable for the organization's systems that can be unavailable for more than a few days or weeks, or that have very low criticality and priority.

Questions # 25:

Recovery strategies of a Disaster Recovery planning (DRIP) MUST be aligned with which of the following?

Options:

A.

Hardware and software compatibility issues

B.

Applications' critically and downtime tolerance

○ C.

Budget constraints and requirements

○ D.

Cost/benefit analysis and business objectives

Answer

D

Explanation

Recovery strategies of a Disaster Recovery planning (DRP) must be aligned with the cost/benefit analysis and business objectives. A DRP is a part of a BCP/DRP that focuses on restoring the normal operation of the organization's IT systems and infrastructure after a disruption or disaster. A DRP should include various components, such as:

Risk assessment: a process that identifies and evaluates the potential threats and vulnerabilities that might affect the IT systems and infrastructure, and estimates the likelihood and impact of a disruption or disaster

Recovery objectives: a process that defines and quantifies the acceptable levels of recovery for the IT systems and infrastructure, such as the recovery point objective (RPO), which is the maximum amount of data loss that can be tolerated, and the recovery time objective (RTO), which is the maximum amount of downtime that can be tolerated

Recovery strategies: a process that selects and implements the appropriate methods and resources to recover the IT systems and infrastructure, such as backup, replication, redundancy, or failover

DRP document: a document that outlines and details the scope, purpose, and features of the DRP, such as the roles and responsibilities, the recovery procedures, and the contact information

Testing, training, and exercises: a process that evaluates and validates the effectiveness and readiness of the DRP, and educates and trains the relevant stakeholders, such as the IT staff, the management, and the users, on the DRP and their roles and responsibilities

Maintenance and review: a process that monitors and updates the DRP, and addresses any changes or issues that might affect the DRP, such as the IT requirements, the threat landscape, or the feedback and lessons learned

Recovery strategies of a DRP must be aligned with the cost/benefit analysis and business objectives, because it can ensure that the DRP is feasible and suitable, and that it can

achieve the desired outcomes and objectives in a cost-effective and efficient manner. A cost/benefit analysis is a technique that compares the costs and benefits of different recovery strategies, and determines the optimal one that provides the best value for money. A business objective is a goal or a target that the organization wants to achieve through its IT systems and infrastructure, such as increasing the productivity, profitability, or customer satisfaction. A recovery strategy that is aligned with the cost/benefit analysis and business objectives can help to:

Optimize the use and allocation of the IT resources and funds for the recovery

Minimize the negative impacts and risks of a disruption or disaster on the IT systems and infrastructure

Maximize the positive outcomes and benefits of the recovery for the IT systems and infrastructure

Support and enable the achievement of the organizational goals and targets through the IT systems and infrastructure

The other options are not the factors that the recovery strategies of a DRP must be aligned with, but rather factors that should be considered or addressed when developing or implementing the recovery strategies of a DRP. Hardware and software compatibility issues are factors that should be considered when developing the recovery strategies of a DRP, because they can affect the functionality and interoperability of the IT systems and infrastructure, and may require additional resources or adjustments to resolve them. Applications' criticality and downtime tolerance are factors that should be addressed when implementing the recovery strategies of a DRP, because they can determine the priority and urgency of the recovery for different applications, and may require different levels of recovery objectives and resources. Budget constraints and requirements are factors that should be considered when developing the recovery strategies of a DRP, because they can limit the availability and affordability of the IT resources and funds for the recovery, and may require trade-offs or compromises to balance them.

Questions # 26:

What is the MOST important step during forensic analysis when trying to learn the purpose of an unknown application?

Options:

A.

Disable all unnecessary services

B.

Ensure chain of custody

C.

Prepare another backup of the system

D.

Isolate the system from the network

Answer

D

Explanation

Isolating the system from the network is the most important step during forensic analysis when trying to learn the purpose of an unknown application. An unknown application is an application that is not recognized or authorized by the system or network administrator, and that may have been installed or executed without the user's knowledge or consent. An unknown application may have various purposes, such as:

Providing a legitimate or useful function or service for the user, such as a utility or a tool

Providing an illegitimate or malicious function or service for the attacker, such as a malware or a backdoor

Providing a neutral or benign function or service for the developer, such as a trial or a demo

Forensic analysis is a process that involves examining and investigating the system or network for any evidence or traces of the unknown application, such as its origin, nature, behavior, and impact. Forensic analysis can provide several benefits, such as:

Identifying and classifying the unknown application as legitimate, malicious, or neutral

Determining and assessing the purpose and function of the unknown application

Detecting and resolving any issues or risks caused by the unknown application

Preventing and mitigating any future incidents or attacks involving the unknown application

Isolating the system from the network is the most important step during forensic analysis when trying to learn the purpose of an unknown application, because it can ensure that

the system is isolated and protected from any external or internal influences or interferences, and that the forensic analysis is conducted in a safe and controlled environment. Isolating the system from the network can also help to:

Prevent the unknown application from communicating or connecting with any other system or network, and potentially spreading or escalating the attack

Prevent the unknown application from receiving or sending any commands or data, and potentially altering or deleting the evidence

Prevent the unknown application from detecting or evading the forensic analysis, and potentially hiding or destroying itself

The other options are not the most important steps during forensic analysis when trying to learn the purpose of an unknown application, but rather steps that should be done after or along with isolating the system from the network. Disabling all unnecessary services is a step that should be done after isolating the system from the network, because it can ensure that the system is optimized and simplified for the forensic analysis, and that the system resources and functions are not consumed or affected by any irrelevant or redundant services. Ensuring chain of custody is a step that should be done along with isolating the system from the network, because it can ensure that the integrity and authenticity of the evidence are maintained and documented throughout the forensic process, and that the evidence can be traced and verified. Preparing another backup of the system is a step that should be done after isolating the system from the network, because it can ensure that the system data and configuration are preserved and replicated for the forensic analysis, and that the system can be restored and recovered in case of any damage or loss.

Questions # 27:

An organization is found lacking the ability to properly establish performance indicators for its Web hosting solution during an audit. What would be the MOST probable cause?

Options:

A.

Absence of a Business Intelligence (BI) solution

B.

Inadequate cost modeling

C.

Improper deployment of the Service-Oriented Architecture (SOA)

D.

Insufficient Service Level Agreement (SLA)

Answer

D

Explanation



CertsMania

Insufficient Service Level Agreement (SLA) would be the most probable cause for an organization to lack the ability to properly establish performance indicators for its Web hosting solution during an audit. A Web hosting solution is a service that provides the infrastructure, resources, and tools for hosting and maintaining a website or a web application on the internet. A Web hosting solution can offer various benefits, such as:

Improving the availability and accessibility of the website or web application by ensuring that it is online and reachable at all times

Enhancing the performance and scalability of the website or web application by optimizing the speed, load, and capacity of the web server

Increasing the security and reliability of the website or web application by providing the backup, recovery, and protection of the web data and content

Reducing the cost and complexity of the website or web application by outsourcing the web hosting and management to a third-party provider

A Service Level Agreement (SLA) is a contract or an agreement that defines the expectations, responsibilities, and obligations of the parties involved in a service, such as the service provider and the service consumer. An SLA can include various components, such as:

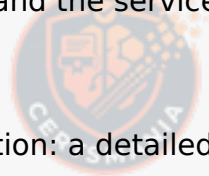
Service description: a detailed explanation of the scope, purpose, and features of the service

Service level objectives: a set of measurable and quantifiable goals or targets for the service quality, performance, and availability

Service level indicators: a set of metrics or parameters that are used to monitor and evaluate the service level objectives

Service level reporting: a process that involves collecting, analyzing, and communicating the service level indicators and objectives

Service level penalties: a set of consequences or actions that are applied when the



CertsMania

service level objectives are not met or violated

Insufficient SLA would be the most probable cause for an organization to lack the ability to properly establish performance indicators for its Web hosting solution during an audit, because it could mean that the SLA does not include or specify the appropriate service level indicators or objectives for the Web hosting solution, or that the SLA does not provide or enforce the adequate service level reporting or penalties for the Web hosting solution. This could affect the ability of the organization to measure and assess the Web hosting solution quality, performance, and availability, and to identify and address any issues or risks in the Web hosting solution.

The other options are not the most probable causes for an organization to lack the ability to properly establish performance indicators for its Web hosting solution during an audit, but rather the factors that could affect or improve the Web hosting solution in other ways. Absence of a Business Intelligence (BI) solution is a factor that could affect the ability of the organization to analyze and utilize the data and information from the Web hosting solution, such as the web traffic, behavior, or conversion. A BI solution is a system that involves the collection, integration, processing, and presentation of the data and information from various sources, such as the Web hosting solution, to support the decision making and planning of the organization. However, absence of a BI solution is not the most probable cause for an organization to lack the ability to properly establish performance indicators for its Web hosting solution during an audit, because it does not affect the definition or specification of the performance indicators for the Web hosting solution, but rather the analysis or usage of the performance indicators for the Web hosting solution. Inadequate cost modeling is a factor that could affect the ability of the organization to estimate and optimize the cost and value of the Web hosting solution, such as the web hosting fees, maintenance costs, or return on investment. A cost model is a tool or a method that helps the organization to calculate and compare the cost and value of the Web hosting solution, and to identify and implement the best or most efficient Web hosting solution. However, inadequate cost modeling is not the most probable cause for an organization to lack the ability to properly establish performance indicators for its Web hosting solution during an audit, because it does not affect the definition or specification of the performance indicators for the Web hosting solution, but rather the estimation or optimization of the cost and value of the Web hosting solution. Improper deployment of the Service-Oriented Architecture (SOA) is a factor that could affect the ability of the organization to design and develop the Web hosting solution, such as the web services, components, or interfaces. A SOA is a software architecture that involves the modularization, standardization, and integration of the software components or services that provide the functionality or logic of the Web hosting solution. A SOA can offer various benefits, such as:

Improving the flexibility and scalability of the Web hosting solution by allowing the addition, modification, or removal of the software components or services without affecting the whole Web hosting solution

Enhancing the interoperability and compatibility of the Web hosting solution by enabling the communication and interaction of the software components or services across different platforms and technologies

Increasing the reusability and maintainability of the Web hosting solution by reducing the duplication and complexity of the software components or services

However, improper deployment of the SOA is not the most probable cause for an organization to lack the ability to properly establish performance indicators for its Web hosting solution during an audit, because it does not affect the definition or specification of the performance indicators for the Web hosting solution, but rather the design or development of the Web hosting solution.

Questions # 28:

When is a Business Continuity Plan (BCP) considered to be valid?

Options:

A.

When it has been validated by the Business Continuity (BC) manager

B.

When it has been validated by the board of directors

C.

When it has been validated by all threat scenarios

D.

When it has been validated by realistic exercises

Answer

D

Explanation

A Business Continuity Plan (BCP) is considered to be valid when it has been validated by realistic exercises. A BCP is a part of a BCP/DRP that focuses on ensuring the continuous operation of the organization's critical business functions and processes during and after a disruption or disaster. A BCP should include various components, such as:

Business impact analysis: a process that identifies and prioritizes the critical business functions and processes, and assesses the potential impacts and risks of a disruption

or disaster on them

Recovery strategies: a process that defines and selects the appropriate methods and resources to recover the critical business functions and processes, such as alternate sites, backup systems, or recovery teams

BCP document: a document that outlines and details the scope, purpose, and features of the BCP, such as the roles and responsibilities, the recovery procedures, and the contact information

Testing, training, and exercises: a process that evaluates and validates the effectiveness and readiness of the BCP, and educates and trains the relevant stakeholders, such as the staff, the management, and the customers, on the BCP and their roles and responsibilities

Maintenance and review: a process that monitors and updates the BCP, and addresses any changes or issues that might affect the BCP, such as the business requirements, the threat landscape, or the feedback and lessons learned

A BCP is considered to be valid when it has been validated by realistic exercises, because it can ensure that the BCP is practical and applicable, and that it can achieve the desired outcomes and objectives in a real-life scenario. Realistic exercises are a type of testing, training, and exercises that involve performing and practicing the BCP with the relevant stakeholders, using simulated or hypothetical scenarios, such as a fire drill, a power outage, or a cyberattack. Realistic exercises can provide several benefits, such as:

Improving the confidence and competence of the organization and its staff in handling a disruption or disaster

Enhancing the performance and efficiency of the organization and its systems in recovering from a disruption or disaster

Increasing the compliance and alignment of the organization and its plans with the internal or external requirements and standards

Facilitating the monitoring and improvement of the organization and its plans by identifying and addressing any gaps, issues, or risks

The other options are not the criteria for considering a BCP to be valid, but rather the steps or parties that are involved in developing or approving a BCP. When it has been validated by the Business Continuity (BC) manager is not a criterion for considering a BCP to be valid, but rather a step that is involved in developing a BCP. The BC manager is the person who is responsible for overseeing and coordinating the BCP activities and processes, such as the business impact analysis, the recovery strategies, the BCP document, the testing, training, and exercises, and the maintenance and review. The BC manager can validate the BCP by reviewing and verifying the BCP components and outcomes, and ensuring that they meet the BCP standards and objectives. However, the validation by the BC manager is not enough to consider the BCP to be valid, as it does not

test or demonstrate the BCP in a realistic scenario. When it has been validated by the board of directors is not a criterion for considering a BCP to be valid, but rather a party that is involved in approving a BCP. The board of directors is the group of people who are elected by the shareholders to represent their interests and to oversee the strategic direction and governance of the organization. The board of directors can approve the BCP by endorsing and supporting the BCP components and outcomes, and allocating the necessary resources and funds for the BCP. However, the approval by the board of directors is not enough to consider the BCP to be valid, as it does not test or demonstrate the BCP in a realistic scenario. When it has been validated by all threat scenarios is not a criterion for considering a BCP to be valid, but rather an unrealistic or impossible expectation for validating a BCP. A threat scenario is a description or a simulation of a possible or potential disruption or disaster that might affect the organization's critical business functions and processes, such as a natural hazard, a human error, or a technical failure. A threat scenario can be used to test and validate the BCP by measuring and evaluating the BCP's performance and effectiveness in responding and recovering from the disruption or disaster. However, it is not possible or feasible to validate the BCP by all threat scenarios, as there are too many or unknown threat scenarios that might occur, and some threat scenarios might be too severe or complex to simulate or test. Therefore, the BCP should be validated by the most likely or relevant threat scenarios, and not by all threat scenarios.

Questions # 29:

Which of the following is the FIRST step in the incident response process?

Options:

A.

Determine the cause of the incident

B.

Disconnect the system involved from the network

C.

Isolate and contain the system involved

D.

Investigate all symptoms to confirm the incident

Answer

D

Explanation

Investigating all symptoms to confirm the incident is the first step in the incident response process. An incident is an event that violates or threatens the security, availability, integrity, or confidentiality of the IT systems or data. An incident response is a process that involves detecting, analyzing, containing, eradicating, recovering, and learning from an incident, using various methods and tools. An incident response can provide several benefits, such as:

Improving the security and risk management of the IT systems and data by identifying and addressing the security weaknesses and gaps

Enhancing the security and decision making of the IT systems and data by providing the evidence and information for the security analysis, evaluation, and reporting

Increasing the security and improvement of the IT systems and data by providing the feedback and input for the security response, remediation, and optimization

Facilitating the compliance and alignment of the IT systems and data with the internal or external requirements and standards

Investigating all symptoms to confirm the incident is the first step in the incident response process, because it can ensure that the incident is verified and validated, and that the incident response is initiated and escalated. A symptom is a sign or an indication that an incident may have occurred or is occurring, such as an alert, a log, or a report.

Investigating all symptoms to confirm the incident involves collecting and analyzing the relevant data and information from various sources, such as the IT systems, the network, the users, or the external parties, and determining whether an incident has actually happened or is happening, and how serious or urgent it is. Investigating all symptoms to confirm the incident can also help to:

Prevent the false positives or negatives that might cause the incident response to be delayed or unnecessary

Identify the scope and impact of the incident on the IT systems and data

Notify and inform the appropriate stakeholders and authorities about the incident

Activate and coordinate the incident response team and resources

The other options are not the first steps in the incident response process, but rather steps that should be done after or along with investigating all symptoms to confirm the incident. Determining the cause of the incident is a step that should be done after investigating all symptoms to confirm the incident, because it can ensure that the root cause and source of

the incident are identified and analyzed, and that the incident response is directed and focused. Determining the cause of the incident involves examining and testing the affected IT systems and data, and tracing and tracking the origin and path of the incident, using various techniques and tools, such as forensics, malware analysis, or reverse engineering. Determining the cause of the incident can also help to:

- Understand the nature and behavior of the incident and the attacker

- Detect and resolve any issues or risks caused by the incident

- Prevent and mitigate any future incidents or attacks involving the same or similar cause

- Support and enable the legal or regulatory actions or investigations against the incident or the attacker

Disconnecting the system involved from the network is a step that should be done along with investigating all symptoms to confirm the incident, because it can ensure that the system is isolated and protected from any external or internal influences or interferences, and that the incident response is conducted in a safe and controlled environment.

Disconnecting the system involved from the network can also help to:

- Prevent the incident from communicating or connecting with any other system or network, and potentially spreading or escalating the attack

- Prevent the incident from receiving or sending any commands or data, and potentially altering or deleting the evidence

- Prevent the incident from detecting or evading the incident response, and potentially hiding or destroying itself

Isolating and containing the system involved is a step that should be done after investigating all symptoms to confirm the incident, because it can ensure that the incident is confined and restricted, and that the incident response is continued and maintained.

Isolating and containing the system involved involves applying and enforcing the appropriate security measures and controls to limit or stop the activity and impact of the incident on the IT systems and data, such as firewall rules, access policies, or encryption keys. Isolating and containing the system involved can also help to:

- Minimize the damage and loss caused by the incident on the IT systems and data

- Maximize the recovery and restoration of the IT systems and data

- Support and enable the eradication and removal of the incident from the IT systems and data

- Facilitate the learning and improvement of the IT systems and data from the incident

Questions # 30:

With what frequency should monitoring of a control occur when implementing Information Security Continuous Monitoring (ISCM) solutions?

Options:

A.

Continuously without exception for all security controls

B.

Before and after each change of the control

C.

At a rate concurrent with the volatility of the security control

D.

Only during system implementation and decommissioning

Answer

C

Explanation

Monitoring of a control should occur at a rate concurrent with the volatility of the security control when implementing Information Security Continuous Monitoring (ISCM) solutions. ISCM is a process that involves maintaining the ongoing awareness of the security status, events, and activities of a system or network, by collecting, analyzing, and reporting the security data and information, using various methods and tools. ISCM can provide several benefits, such as:

Improving the security and risk management of the system or network by identifying and addressing the security weaknesses and gaps

Enhancing the security and decision making of the system or network by providing the evidence and information for the security analysis, evaluation, and reporting

Increasing the security and improvement of the system or network by providing the feedback and input for the security response, remediation, and optimization

Facilitating the compliance and alignment of the system or network with the internal or external requirements and standards

A security control is a measure or mechanism that is implemented to protect the system or network from the security threats or risks, by preventing, detecting, or correcting the security incidents or impacts. A security control can have various types, such as administrative, technical, or physical, and various attributes, such as preventive, detective, or corrective. A security control can also have different levels of volatility, which is the degree or frequency of change or variation of the security control, due to various factors, such as the security requirements, the threat landscape, or the system or network environment.

Monitoring of a control should occur at a rate concurrent with the volatility of the security control when implementing ISCM solutions, because it can ensure that the ISCM solutions can capture and reflect the current and accurate state and performance of the security control, and can identify and report any issues or risks that might affect the security control. Monitoring of a control at a rate concurrent with the volatility of the security control can also help to optimize the ISCM resources and efforts, by allocating them according to the priority and urgency of the security control.

The other options are not the correct frequencies for monitoring of a control when implementing ISCM solutions, but rather incorrect or unrealistic frequencies that might cause problems or inefficiencies for the ISCM solutions. Continuously without exception for all security controls is an incorrect frequency for monitoring of a control when implementing ISCM solutions, because it is not feasible or necessary to monitor all security controls at the same and constant rate, regardless of their volatility or importance. Continuously monitoring all security controls without exception might cause the ISCM solutions to consume excessive or wasteful resources and efforts, and might overwhelm or overload the ISCM solutions with too much or irrelevant data and information. Before and after each change of the control is an incorrect frequency for monitoring of a control when implementing ISCM solutions, because it is not sufficient or timely to monitor the security control only when there is a change of the security control, and not during the normal operation of the security control. Monitoring the security control only before and after each change might cause the ISCM solutions to miss or ignore the security status, events, and activities that occur between the changes of the security control, and might delay or hinder the ISCM solutions from detecting and responding to the security issues or incidents that affect the security control. Only during system implementation and decommissioning is an incorrect frequency for monitoring of a control when implementing ISCM solutions, because it is not appropriate or effective to monitor the security control only during the initial or final stages of the system or network lifecycle, and not during the operational or maintenance stages of the system or network lifecycle. Monitoring the security control only during system implementation and decommissioning might cause the ISCM solutions to neglect or overlook the security status, events, and activities that occur during the regular or ongoing operation of the system or network, and might prevent or limit the ISCM solutions from improving and optimizing the security control.

What is the PRIMARY reason for implementing change management?

Options:

A.

Certify and approve releases to the environment

B.

Provide version rollbacks for system changes

C.

Ensure that all applications are approved

D.

Ensure accountability for changes to the environment

Answer

D

Explanation

Ensuring accountability for changes to the environment is the primary reason for implementing change management. Change management is a process that ensures that any changes to the system or network environment, such as the hardware, software, configuration, or documentation, are planned, approved, implemented, and documented in a controlled and consistent manner. Change management can provide several benefits, such as:

Improving the security and reliability of the system or network environment by preventing or reducing the errors, conflicts, or disruptions that might occur due to the changes

Enhancing the performance and efficiency of the system or network environment by optimizing the resources and functions

Increasing the compliance and alignment of the system or network environment with the internal or external requirements and standards

Facilitating the monitoring and improvement of the system or network environment by tracking and logging the changes and their outcomes

Ensuring accountability for changes to the environment is the primary reason for implementing change management, because it can ensure that the changes are authorized, justified, and traceable, and that the parties involved in the changes are responsible and accountable for their actions and results. Accountability can also help to deter or detect any unauthorized or malicious changes that might compromise the system or network environment.

The other options are not the primary reasons for implementing change management, but rather secondary or specific reasons for different aspects or phases of change management. Certifying and approving releases to the environment is a reason for implementing change management, but it is more relevant for the approval phase of change management, which is the phase that involves reviewing and validating the changes and their impacts, and granting or denying the permission to proceed with the changes. Providing version rollbacks for system changes is a reason for implementing change management, but it is more relevant for the implementation phase of change management, which is the phase that involves executing and monitoring the changes and their effects, and providing the backup and recovery options for the changes. Ensuring that all applications are approved is a reason for implementing change management, but it is more relevant for the application changes, which are the changes that affect the software components or services that provide the functionality or logic of the system or network environment.

Questions # 32:

Which of the following types of business continuity tests includes assessment of resilience to internal and external risks without endangering live operations?

Options:

A.

Walkthrough

B.

Simulation

C.

Parallel

D.

White box



CertsMania

Answer

B

Explanation

Simulation is the type of business continuity test that includes assessment of resilience to internal and external risks without endangering live operations. Business continuity is the ability of an organization to maintain or resume its critical functions and operations in the event of a disruption or disaster. Business continuity testing is the process of evaluating and validating the effectiveness and readiness of the business continuity plan (BCP) and the disaster recovery plan (DRP) through various methods and scenarios. Business continuity testing can provide several benefits, such as:

Improving the confidence and competence of the organization and its staff in handling a disruption or disaster

Enhancing the performance and efficiency of the organization and its systems in recovering from a disruption or disaster

Increasing the compliance and alignment of the organization and its plans with the internal or external requirements and standards

Facilitating the monitoring and improvement of the organization and its plans by identifying and addressing any gaps, issues, or risks

There are different types of business continuity tests, depending on the scope, purpose, and complexity of the test. Some of the common types are:

Walkthrough: a type of business continuity test that involves reviewing and discussing the BCP and DRP with the relevant stakeholders, such as the business continuity team, the management, and the staff. A walkthrough can provide a basic and qualitative assessment of the BCP and DRP, and can help to familiarize and educate the stakeholders with the plans and their roles and responsibilities.

Simulation: a type of business continuity test that involves performing and practicing the BCP and DRP with the relevant stakeholders, using simulated or hypothetical scenarios, such as a fire drill, a power outage, or a cyberattack. A simulation can provide a realistic and quantitative assessment of the BCP and DRP, and can help to test and train the stakeholders with the plans and their actions and reactions.

Parallel: a type of business continuity test that involves activating and operating the alternate site or system, while maintaining the normal operations at the primary site or system. A parallel test can provide a comprehensive and comparative assessment of the BCP and DRP, and can help to verify and validate the functionality and compatibility of the alternate site or system.

Full interruption: a type of business continuity test that involves shutting down and

transferring the normal operations from the primary site or system to the alternate site or system. A full interruption test can provide a conclusive and definitive assessment of the BCP and DRP, and can help to evaluate and measure the impact and effectiveness of the plans.

Simulation is the type of business continuity test that includes assessment of resilience to internal and external risks without endangering live operations, because it can simulate various types of risks, such as natural, human, or technical, and assess how the organization and its systems can cope and recover from them, without actually causing any harm or disruption to the live operations. Simulation can also help to identify and mitigate any potential risks that might affect the live operations, and to improve the resilience and preparedness of the organization and its systems.

The other options are not the types of business continuity tests that include assessment of resilience to internal and external risks without endangering live operations, but rather types that have other objectives or effects. Walkthrough is a type of business continuity test that does not include assessment of resilience to internal and external risks, but rather a review and discussion of the BCP and DRP, without any actual testing or practice. Parallel is a type of business continuity test that does not endanger live operations, but rather maintains them, while activating and operating the alternate site or system. Full interruption is a type of business continuity test that does endanger live operations, by shutting them down and transferring them to the alternate site or system.

Questions # 33:

Which of the following is a PRIMARY advantage of using a third-party identity service?

Options:

A.

Consolidation of multiple providers

B.

Directory synchronization

C.

Web based logon

D.

Automated account management



CertsMania

Answer

D

Explanation

Consolidation of multiple providers is the primary advantage of using a third-party identity service. A third-party identity service is a service that provides identity and access management (IAM) functions, such as authentication, authorization, and federation, for multiple applications or systems, using a single identity provider (IdP). A third-party identity service can offer various benefits, such as:

Improving the user experience and convenience by allowing the users to access multiple applications or systems with a single sign-on (SSO) or a federated identity

Enhancing the security and compliance by applying the consistent and standardized IAM policies and controls across multiple applications or systems

Increasing the scalability and flexibility by enabling the integration and interoperability of multiple applications or systems with different platforms and technologies

Reducing the cost and complexity by outsourcing the IAM functions to a third-party provider, and avoiding the duplication and maintenance of multiple IAM systems

Consolidation of multiple providers is the primary advantage of using a third-party identity service, because it can simplify and streamline the IAM architecture and processes, by reducing the number of IdPs and IAM systems that are involved in managing the identities and access for multiple applications or systems. Consolidation of multiple providers can also help to avoid the issues or risks that might arise from having multiple IdPs and IAM systems, such as the inconsistency, redundancy, or conflict of the IAM policies and controls, or the inefficiency, vulnerability, or disruption of the IAM functions.

The other options are not the primary advantages of using a third-party identity service, but rather secondary or specific advantages for different aspects or scenarios of using a third-party identity service. Directory synchronization is an advantage of using a third-party identity service, but it is more relevant for the scenario where the organization has an existing directory service, such as LDAP or Active Directory, that stores and manages the user accounts and attributes, and wants to synchronize them with the third-party identity service, to enable the SSO or federation for the users. Web based logon is an advantage of using a third-party identity service, but it is more relevant for the aspect where the third-party identity service uses a web-based protocol, such as SAML or OAuth, to facilitate the SSO or federation for the users, by redirecting them to a web-based logon page, where they can enter their credentials or consent. Automated account management is an advantage of using a third-party identity service, but it is more relevant for the aspect where the third-party identity service provides the IAM functions, such as provisioning, deprovisioning, or updating, for the user accounts and access rights, using an automated or self-service mechanism, such as SCIM or JIT.

Questions # 34:

A continuous information security-monitoring program can BEST reduce risk through which of the following?

Options:

A.

Collecting security events and correlating them to identify anomalies

B.

Facilitating system-wide visibility into the activities of critical user accounts

C.

Encompassing people, process, and technology

D.

Logging both scheduled and unscheduled system changes

Answer

C

Explanation

A continuous information security monitoring program can best reduce risk through encompassing people, process, and technology. A continuous information security monitoring program is a process that involves maintaining the ongoing awareness of the security status, events, and activities of a system or network, by collecting, analyzing, and reporting the security data and information, using various methods and tools. A continuous information security monitoring program can provide several benefits, such as:

Improving the security and risk management of the system or network by identifying and addressing the security weaknesses and gaps

Enhancing the security and decision making of the system or network by providing the evidence and information for the security analysis, evaluation, and reporting

Increasing the security and improvement of the system or network by providing the feedback and input for the security response, remediation, and optimization

Facilitating the compliance and alignment of the system or network with the internal or external requirements and standards

A continuous information security monitoring program can best reduce risk through encompassing people, process, and technology, because it can ensure that the continuous information security monitoring program is holistic and comprehensive, and that it covers all the aspects and elements of the system or network security. People, process, and technology are the three pillars of a continuous information security monitoring program, and they represent the following:

People: the human resources that are involved in the continuous information security monitoring program, such as the security analysts, the system administrators, the management, and the users. People are responsible for defining the security objectives and requirements, implementing and operating the security tools and controls, and monitoring and responding to the security events and incidents.

Process: the procedures and policies that are followed in the continuous information security monitoring program, such as the security standards and guidelines, the security roles and responsibilities, the security workflows and tasks, and the security metrics and indicators. Process is responsible for establishing and maintaining the security governance and compliance, ensuring the security consistency and efficiency, and measuring and evaluating the security performance and effectiveness.

Technology: the tools and systems that are used in the continuous information security monitoring program, such as the security sensors and agents, the security loggers and collectors, the security analyzers and correlators, and the security dashboards and reports. Technology is responsible for supporting and enabling the security functions and capabilities, providing the security visibility and awareness, and delivering the security data and information.

The other options are not the best ways to reduce risk through a continuous information security monitoring program, but rather specific or partial ways that can contribute to the risk reduction. Collecting security events and correlating them to identify anomalies is a specific way to reduce risk through a continuous information security monitoring program, but it is not the best way, because it only focuses on one aspect of the security data and information, and it does not address the other aspects, such as the security objectives and requirements, the security controls and measures, and the security feedback and improvement. Facilitating system-wide visibility into the activities of critical user accounts is a partial way to reduce risk through a continuous information security monitoring program, but it is not the best way, because it only covers one element of the system or network security, and it does not cover the other elements, such as the security threats and vulnerabilities, the security incidents and impacts, and the security response and remediation. Logging both scheduled and unscheduled system changes is a specific way to reduce risk through a continuous information security monitoring program, but it is not the best way, because it only focuses on one type of the security events and activities, and it does not focus on the other types, such as the security alerts and notifications, the security analysis and correlation, and the security reporting and documentation.

Questions # 35:

A Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) will provide which of the following?

Options:

A.

Guaranteed recovery of all business functions

B.

Minimization of the need decision making during a crisis

C.

Insurance against litigation following a disaster

D.

Protection from loss of organization resources

Answer

B

Explanation

Minimization of the need for decision making during a crisis is the main benefit that a Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) will provide. A BCP/DRP is a set of policies, procedures, and resources that enable an organization to continue or resume its critical functions and operations in the event of a disruption or disaster. A BCP/DRP can provide several benefits, such as:

Improving the resilience and preparedness of the organization and its staff in handling a disruption or disaster

Enhancing the performance and efficiency of the organization and its systems in recovering from a disruption or disaster

Increasing the compliance and alignment of the organization and its plans with the internal or external requirements and standards

Facilitating the monitoring and improvement of the organization and its plans by identifying and addressing any gaps, issues, or risks

Minimization of the need for decision making during a crisis is the main benefit that a BCP/DRP will provide, because it can ensure that the organization and its staff have a clear and consistent guidance and direction on how to respond and act during a disruption or disaster, and avoid any confusion, uncertainty, or inconsistency that might worsen the situation or impact. A BCP/DRP can also help to reduce the stress and pressure on the organization and its staff during a crisis, and increase their confidence and competence in executing the plans.

The other options are not the benefits that a BCP/DRP will provide, but rather unrealistic or incorrect expectations or outcomes of a BCP/DRP. Guaranteed recovery of all business functions is not a benefit that a BCP/DRP will provide, because it is not possible or feasible to recover all business functions after a disruption or disaster, especially if the disruption or disaster is severe or prolonged. A BCP/DRP can only prioritize and recover the most critical or essential business functions, and may have to suspend or terminate the less critical or non-essential business functions. Insurance against litigation following a disaster is not a benefit that a BCP/DRP will provide, because it is not a guarantee or protection that the organization will not face any legal or regulatory consequences or liabilities after a disruption or disaster, especially if the disruption or disaster is caused by the organization's negligence or misconduct. A BCP/DRP can only help to mitigate or reduce the legal or regulatory risks, and may have to comply with or report to the relevant authorities or parties. Protection from loss of organization resources is not a benefit that a BCP/DRP will provide, because it is not a prevention or avoidance of any damage or destruction of the organization's assets or resources during a disruption or disaster, especially if the disruption or disaster is physical or natural. A BCP/DRP can only help to restore or replace the lost or damaged assets or resources, and may have to incur some costs or losses.

Questions # 36:

What should be the FIRST action to protect the chain of evidence when a desktop computer is involved?

Options:

A.

Take the computer to a forensic lab

B.

Make a copy of the hard drive

C.

Start documenting

D.



CertsMania

Turn off the computer

Answer

B

Explanation

Making a copy of the hard drive should be the first action to protect the chain of evidence when a desktop computer is involved. A chain of evidence, also known as a chain of custody, is a process that documents and preserves the integrity and authenticity of the evidence collected from a crime scene, such as a desktop computer. A chain of evidence should include information such as:

The identity and role of the person who collected, handled, or transferred the evidence

The date and time of the collection, handling, or transfer of the evidence

The location and condition of the evidence

The method and tool used to collect, handle, or transfer the evidence

The signature or seal of the person who collected, handled, or transferred the evidence

Making a copy of the hard drive should be the first action to protect the chain of evidence when a desktop computer is involved, because it can ensure that the original hard drive is not altered, damaged, or destroyed during the forensic analysis, and that the copy can be used as a reliable and admissible source of evidence. Making a copy of the hard drive should also involve using a write blocker, which is a device or a software that prevents any modification or deletion of the data on the hard drive, and generating a hash value, which is a unique and fixed identifier that can verify the integrity and consistency of the data on the hard drive.

The other options are not the first actions to protect the chain of evidence when a desktop computer is involved, but rather actions that should be done after or along with making a copy of the hard drive. Taking the computer to a forensic lab is an action that should be done after making a copy of the hard drive, because it can ensure that the computer is transported and stored in a secure and controlled environment, and that the forensic analysis is conducted by qualified and authorized personnel. Starting documenting is an action that should be done along with making a copy of the hard drive, because it can ensure that the chain of evidence is maintained and recorded throughout the forensic process, and that the evidence can be traced and verified. Turning off the computer is an action that should be done after making a copy of the hard drive, because it can ensure that the computer is powered down and disconnected from any network or device, and that the computer is protected from any further damage or tampering.

Questions # 37:

What is the BEST approach to addressing security issues in legacy web applications?

Options:

A.

Debug the security issues

B.

Migrate to newer, supported applications where possible

C.

Conduct a security assessment

D.

Protect the legacy application with a web application firewall

Answer

B

Explanation

Migrating to newer, supported applications where possible is the best approach to addressing security issues in legacy web applications. Legacy web applications are web applications that are outdated, unsupported, or incompatible with the current technologies and standards. Legacy web applications may have various security issues, such as:

Vulnerabilities and bugs that are not fixed or patched by the developers or vendors

Weak or obsolete encryption and authentication mechanisms that are easily broken or bypassed by attackers

Lack of compliance with the security policies and regulations that are applicable to the web applications

Incompatibility or interoperability issues with the newer web browsers, operating systems, or platforms that are used by the users or clients

Migrating to newer, supported applications where possible is the best approach to addressing security issues in legacy web applications, because it can provide several benefits, such as:

Enhancing the security and performance of the web applications by using the latest technologies and standards that are more secure and efficient

Reducing the risk and impact of the web application attacks by eliminating or minimizing the vulnerabilities and bugs that are present in the legacy web applications

Increasing the compliance and alignment of the web applications with the security policies and regulations that are applicable to the web applications

Improving the compatibility and interoperability of the web applications with the newer web browsers, operating systems, or platforms that are used by the users or clients

The other options are not the best approaches to addressing security issues in legacy web applications, but rather approaches that can mitigate or remediate the security issues, but not eliminate or prevent them. Debugging the security issues is an approach that can mitigate the security issues in legacy web applications, but not the best approach, because it involves identifying and fixing the errors or defects in the code or logic of the web applications, which may be difficult or impossible to do for the legacy web applications that are outdated or unsupported. Conducting a security assessment is an approach that can remediate the security issues in legacy web applications, but not the best approach, because it involves evaluating and testing the security effectiveness and compliance of the web applications, using various techniques and tools, such as audits, reviews, scans, or penetration tests, and identifying and reporting any security weaknesses or gaps, which may not be sufficient or feasible to do for the legacy web applications that are incompatible or obsolete. Protecting the legacy application with a web application firewall is an approach that can mitigate the security issues in legacy web applications, but not the best approach, because it involves deploying and configuring a web application firewall, which is a security device or software that monitors and filters the web traffic between the web applications and the users or clients, and blocks or allows the web requests or responses based on the predefined rules or policies, which may not be effective or efficient to do for the legacy web applications that have weak or outdated encryption or authentication mechanisms.

Questions # 38:

Which of the following is the BEST method to prevent malware from being introduced into a production environment?

Options:

A.

Purchase software from a limited list of retailers

B.

Verify the hash key or certificate key of all updates

C.

Do not permit programs, patches, or updates from the Internet

D.

Test all new software in a segregated environment

Answer

D

Explanation

Testing all new software in a segregated environment is the best method to prevent malware from being introduced into a production environment. Malware is any malicious software that can harm or compromise the security, availability, integrity, or confidentiality of a system or data. Malware can be introduced into a production environment through various sources, such as software downloads, updates, patches, or installations. Testing all new software in a segregated environment involves verifying and validating the functionality and security of the software before deploying it to the production environment, using a separate system or network that is isolated and protected from the production environment. Testing all new software in a segregated environment can provide several benefits, such as:

Preventing the infection or propagation of malware to the production environment

Detecting and resolving any issues or risks caused by the software

Ensuring the compatibility and interoperability of the software with the production environment

Supporting and enabling the quality assurance and improvement of the software

The other options are not the best methods to prevent malware from being introduced into a production environment, but rather methods that can reduce or mitigate the risk of malware, but not eliminate it. Purchasing software from a limited list of retailers is a method that can reduce the risk of malware from being introduced into a production environment, but not prevent it. This method involves obtaining software only from

trusted and reputable sources, such as official vendors or distributors, that can provide some assurance of the quality and security of the software. However, this method does not guarantee that the software is free of malware, as it may still contain hidden or embedded malware, or it may be tampered with or compromised during the delivery or installation process. Verifying the hash key or certificate key of all updates is a method that can reduce the risk of malware from being introduced into a production environment, but not prevent it. This method involves checking the authenticity and integrity of the software updates, patches, or installations, by comparing the hash key or certificate key of the software with the expected or published value, using cryptographic techniques and tools. However, this method does not guarantee that the software is free of malware, as it may still contain malware that is not detected or altered by the hash key or certificate key, or it may be subject to a man-in-the-middle attack or a replay attack that can intercept or modify the software or the key. Not permitting programs, patches, or updates from the Internet is a method that can reduce the risk of malware from being introduced into a production environment, but not prevent it. This method involves restricting or blocking the access or download of software from the Internet, which is a common and convenient source of malware, by applying and enforcing the appropriate security policies and controls, such as firewall rules, antivirus software, or web filters. However, this method does not guarantee that the software is free of malware, as it may still be obtained or infected from other sources, such as removable media, email attachments, or network shares.

Questions # 39:

The configuration management and control task of the certification and accreditation process is incorporated in which phase of the System Development Life Cycle (SDLC)?

Options:

A.

System acquisition and development

B.

System operations and maintenance

C.

System initiation

D.

System implementation

Answer

A

Explanation

The configuration management and control task of the certification and accreditation process is incorporated in the system acquisition and development phase of the System Development Life Cycle (SDLC). The SDLC is a process that involves planning, designing, developing, testing, deploying, operating, and maintaining a system, using various models and methodologies, such as waterfall, spiral, agile, or DevSecOps. The SDLC can be divided into several phases, each with its own objectives and activities, such as:

System initiation: This phase involves defining the scope, purpose, and objectives of the system, identifying the stakeholders and their needs and expectations, and establishing the project plan and budget.

System acquisition and development: This phase involves designing the architecture and components of the system, selecting and procuring the hardware and software resources, developing and coding the system functionality and features, and integrating and testing the system modules and interfaces.

System implementation: This phase involves deploying and installing the system to the production environment, migrating and converting the data and applications from the legacy system, training and educating the users and staff on the system operation and maintenance, and evaluating and validating the system performance and effectiveness.

System operations and maintenance: This phase involves operating and monitoring the system functionality and availability, maintaining and updating the system hardware and software, resolving and troubleshooting any issues or problems, and enhancing and optimizing the system features and capabilities.

The certification and accreditation process is a process that involves assessing and verifying the security and compliance of a system, and authorizing and approving the system operation and maintenance, using various standards and frameworks, such as NIST SP 800-37 or ISO/IEC 27001. The certification and accreditation process can be divided into several tasks, each with its own objectives and activities, such as:

Security categorization: This task involves determining the security level and impact of the system and its data, based on the confidentiality, integrity, and availability criteria, and applying the appropriate security controls and measures.

Security planning: This task involves defining the security objectives and requirements of the system, identifying the roles and responsibilities of the security stakeholders, and developing and documenting the security plan and policy.

Security implementation: This task involves implementing and enforcing the security

controls and measures for the system, according to the security plan and policy, and ensuring the security functionality and compatibility of the system.

Security assessment: This task involves evaluating and testing the security effectiveness and compliance of the system, using various techniques and tools, such as audits, reviews, scans, or penetration tests, and identifying and reporting any security weaknesses or gaps.

Security authorization: This task involves reviewing and approving the security assessment results and recommendations, and granting or denying the authorization for the system operation and maintenance, based on the risk and impact analysis and the security objectives and requirements.

Security monitoring: This task involves monitoring and updating the security status and activities of the system, using various methods and tools, such as logs, alerts, or reports, and addressing and resolving any security issues or changes.

The configuration management and control task of the certification and accreditation process is incorporated in the system acquisition and development phase of the SDLC, because it can ensure that the system design and development are consistent and compliant with the security objectives and requirements, and that the system changes are controlled and documented. Configuration management and control is a process that involves establishing and maintaining the baseline and the inventory of the system components and resources, such as hardware, software, data, or documentation, and tracking and recording any modifications or updates to the system components and resources, using various techniques and tools, such as version control, change control, or configuration audits. Configuration management and control can provide several benefits, such as:

- Improving the quality and security of the system design and development by identifying and addressing any errors or inconsistencies

- Enhancing the performance and efficiency of the system design and development by optimizing the use and allocation of the system components and resources

- Increasing the compliance and alignment of the system design and development with the security objectives and requirements by applying and enforcing the security controls and measures

- Facilitating the monitoring and improvement of the system design and development by providing the evidence and information for the security assessment and authorization

The other options are not the phases of the SDLC that incorporate the configuration management and control task of the certification and accreditation process, but rather phases that involve other tasks of the certification and accreditation process. System operations and maintenance is a phase of the SDLC that incorporates the security monitoring task of the certification and accreditation process, because it can ensure that

the system operation and maintenance are consistent and compliant with the security objectives and requirements, and that the system security is updated and improved. System initiation is a phase of the SDLC that incorporates the security categorization and security planning tasks of the certification and accreditation process, because it can ensure that the system scope and objectives are defined and aligned with the security objectives and requirements, and that the security plan and policy are developed and documented. System implementation is a phase of the SDLC that incorporates the security assessment and security authorization tasks of the certification and accreditation process, because it can ensure that the system deployment and installation are evaluated and verified for the security effectiveness and compliance, and that the system operation and maintenance are authorized and approved based on the risk and impact analysis and the security objectives and requirements.

Questions # 40:

A Java program is being developed to read a file from computer A and write it to computer B, using a third computer C. The program is not working as expected. What is the MOST probable security feature of Java preventing the program from operating as intended?

Options:

A.

Least privilege

B.

Privilege escalation

C.

Defense in depth

D.

Privilege bracketing



CertsMania

Answer

A

Explanation

The most probable security feature of Java preventing the program from operating as intended is least privilege. Least privilege is a principle that states that a subject (such as

a user, a process, or a program) should only have the minimum amount of access or permissions that are necessary to perform its function or task. Least privilege can help to reduce the attack surface and the potential damage of a system or network, by limiting the exposure and impact of a subject in case of a compromise or misuse.

Java implements the principle of least privilege through its security model, which consists of several components, such as:

The Java Virtual Machine (JVM): a software layer that executes the Java bytecode and provides an abstraction from the underlying hardware and operating system. The JVM enforces the security rules and restrictions on the Java programs, such as the memory protection, the bytecode verification, and the exception handling.

The Java Security Manager: a class that defines and controls the security policy and permissions for the Java programs. The Java Security Manager can be configured and customized by the system administrator or the user, and can grant or deny the access or actions of the Java programs, such as the file I/O, the network communication, or the system properties.

The Java Security Policy: a file that specifies the security permissions for the Java programs, based on the code source and the code signer. The Java Security Policy can be defined and modified by the system administrator or the user, and can assign different levels of permissions to different Java programs, such as the trusted or the untrusted ones.

The Java Security Sandbox: a mechanism that isolates and restricts the Java programs that are downloaded or executed from untrusted sources, such as the web or the network. The Java Security Sandbox applies the default or the minimal security permissions to the untrusted Java programs, and prevents them from accessing or modifying the local resources or data, such as the files, the databases, or the registry.

In this question, the Java program is being developed to read a file from computer A and write it to computer B, using a third computer C. This means that the Java program needs to have the permissions to perform the file I/O and the network communication operations, which are considered as sensitive or risky actions by the Java security model. However, if the Java program is running on computer C with the default or the minimal security permissions, such as in the Java Security Sandbox, then it will not be able to perform these operations, and the program will not work as expected. Therefore, the most probable security feature of Java preventing the program from operating as intended is least privilege, which limits the access or permissions of the Java program based on its source, signer, or policy.

The other options are not the security features of Java preventing the program from operating as intended, but rather concepts or techniques that are related to security in general or in other contexts. Privilege escalation is a technique that allows a subject to gain higher or unauthorized access or permissions than what it is supposed to have, by exploiting a vulnerability or a flaw in a system or network. Privilege escalation can help an attacker to perform malicious actions or to access sensitive resources or data, by

bypassing the security controls or restrictions. Defense in depth is a concept that states that a system or network should have multiple layers or levels of security, to provide redundancy and resilience in case of a breach or an attack. Defense in depth can help to protect a system or network from various threats and risks, by using different types of security measures and controls, such as the physical, the technical, or the administrative ones. Privilege bracketing is a technique that allows a subject to temporarily elevate or lower its access or permissions, to perform a specific function or task, and then return to its original or normal level. Privilege bracketing can help to reduce the exposure and impact of a subject, by minimizing the time and scope of its higher or lower access or permissions.



Questions # 41:

Which of the following is the PRIMARY risk with using open source software in a commercial software construction?

Options:

A.

Lack of software documentation

B.

License agreements requiring release of modified code

C.

Expiration of the license agreement

D.

Costs associated with support of the software



Answer

B

Explanation

The primary risk with using open source software in a commercial software construction is license agreements requiring release of modified code. Open source software is software that uses publicly available source code, which can be seen, modified, and distributed by anyone. Open source software has some advantages, such as being affordable and flexible, but it also has some disadvantages, such as being potentially insecure or

unsupported.

One of the main disadvantages of using open source software in a commercial software construction is the license agreements that govern the use and distribution of the open source software. License agreements are legal contracts that specify the rights and obligations of the parties involved in the software, such as the original authors, the developers, and the users. License agreements can vary in terms of their terms and conditions, such as the scope, the duration, or the fees of the software.

Some of the common types of license agreements for open source software are:

Permissive licenses: license agreements that allow the developers and users to freely use, modify, and distribute the open source software, with minimal or no restrictions. Examples of permissive licenses are the MIT License, the Apache License, or the BSD License.

Copyleft licenses: license agreements that require the developers and users to share and distribute the open source software and any modifications or derivatives of it, under the same or compatible license terms and conditions. Examples of copyleft licenses are the GNU General Public License (GPL), the GNU Lesser General Public License (LGPL), or the Mozilla Public License (MPL).

Mixed licenses: license agreements that combine the elements of permissive and copyleft licenses, and may apply different license terms and conditions to different parts or components of the open source software. Examples of mixed licenses are the Eclipse Public License (EPL), the Common Development and Distribution License (CDDL), or the GNU Affero General Public License (AGPL).

The primary risk with using open source software in a commercial software construction is license agreements requiring release of modified code, which are usually associated with copyleft licenses. This means that if a commercial software construction uses or incorporates open source software that is licensed under a copyleft license, then it must also release its own source code and any modifications or derivatives of it, under the same or compatible copyleft license. This can pose a significant risk for the commercial software construction, as it may lose its competitive advantage, intellectual property, or revenue, by disclosing its source code and allowing others to use, modify, or distribute it.

The other options are not the primary risks with using open source software in a commercial software construction, but rather secondary or minor risks that may or may not apply to the open source software. Lack of software documentation is a secondary risk with using open source software in a commercial software construction, as it may affect the quality, usability, or maintainability of the open source software, but it does not necessarily affect the rights or obligations of the commercial software construction. Expiration of the license agreement is a minor risk with using open source software in a commercial software construction, as it may affect the availability or continuity of the open source software, but it is unlikely to happen, as most open source software licenses are perpetual or indefinite. Costs associated with support of the software is a secondary risk with using open source software in a commercial software construction, as it may affect the reliability, security, or performance of the open source software, but it can be

mitigated or avoided by choosing the open source software that has adequate or alternative support options.

Questions # 42:

When in the Software Development Life Cycle (SDLC) MUST software security functional requirements be defined?

Options:

A.

After the system preliminary design has been developed and the data security categorization has been performed

B.

After the vulnerability analysis has been performed and before the system detailed design begins

C.

After the system preliminary design has been developed and before the data security categorization begins

D.

After the business functional analysis and the data security categorization have been performed

Answer

D

Explanation

Software security functional requirements must be defined after the business functional analysis and the data security categorization have been performed in the Software Development Life Cycle (SDLC). The SDLC is a process that involves planning, designing, developing, testing, deploying, operating, and maintaining a system, using various models and methodologies, such as waterfall, spiral, agile, or DevSecOps. The SDLC can be divided into several phases, each with its own objectives and activities, such as:

System initiation: This phase involves defining the scope, purpose, and objectives of the system, identifying the stakeholders and their needs and expectations, and

establishing the project plan and budget.

System acquisition and development: This phase involves designing the architecture and components of the system, selecting and procuring the hardware and software resources, developing and coding the system functionality and features, and integrating and testing the system modules and interfaces.

System implementation: This phase involves deploying and installing the system to the production environment, migrating and converting the data and applications from the legacy system, training and educating the users and staff on the system operation and maintenance, and evaluating and validating the system performance and effectiveness.

System operations and maintenance: This phase involves operating and monitoring the system functionality and availability, maintaining and updating the system hardware and software, resolving and troubleshooting any issues or problems, and enhancing and optimizing the system features and capabilities.

Software security functional requirements are the specific and measurable security features and capabilities that the system must provide to meet the security objectives and requirements. Software security functional requirements are derived from the business functional analysis and the data security categorization, which are two tasks that are performed in the system initiation phase of the SDLC. The business functional analysis is the process of identifying and documenting the business functions and processes that the system must support and enable, such as the inputs, outputs, workflows, and tasks. The data security categorization is the process of determining the security level and impact of the system and its data, based on the confidentiality, integrity, and availability criteria, and applying the appropriate security controls and measures. Software security functional requirements must be defined after the business functional analysis and the data security categorization have been performed, because they can ensure that the system design and development are consistent and compliant with the security objectives and requirements, and that the system security is aligned and integrated with the business functions and processes.

The other options are not the phases of the SDLC when the software security functional requirements must be defined, but rather phases that involve other tasks or activities related to the system design and development. After the system preliminary design has been developed and the data security categorization has been performed is not the phase when the software security functional requirements must be defined, but rather the phase when the system architecture and components are designed, based on the system scope and objectives, and the data security categorization is verified and validated. After the vulnerability analysis has been performed and before the system detailed design begins is not the phase when the software security functional requirements must be defined, but rather the phase when the system design and components are evaluated and tested for the security effectiveness and compliance, and the system detailed design is developed, based on the system architecture and components. After the system preliminary design has been developed and before the data security categorization begins is not the phase when the software security functional requirements must be defined, but rather the phase when the system architecture and components are designed, based on the system scope

and objectives, and the data security categorization is initiated and planned.

Questions # 43:

Which of the following is a web application control that should be put into place to prevent exploitation of Operating System (OS) bugs?

Options:

- A.
Check arguments in function calls
- B.
Test for the security patch level of the environment
- C.
Include logging functions
- D.
Digitally sign each application module

Answer

B

Explanation

Testing for the security patch level of the environment is the web application control that should be put into place to prevent exploitation of Operating System (OS) bugs. OS bugs are errors or defects in the code or logic of the OS that can cause the OS to malfunction or behave unexpectedly. OS bugs can be exploited by attackers to gain unauthorized access, disrupt business operations, or steal or leak sensitive data. Testing for the security patch level of the environment is the web application control that should be put into place to prevent exploitation of OS bugs, because it can provide several benefits, such as:

Detecting and resolving any vulnerabilities or issues caused by the OS bugs by applying the latest security patches or updates from the OS developers or vendors

Enhancing the security and performance of the web applications by using the most secure and efficient version of the OS that supports the web applications

Increasing the compliance and alignment of the web applications with the security policies and regulations that are applicable to the web applications

Improving the compatibility and interoperability of the web applications with the other systems or platforms that interact with the web applications

The other options are not the web application controls that should be put into place to prevent exploitation of OS bugs, but rather web application controls that can prevent or mitigate other types of web application attacks or issues. Checking arguments in function calls is a web application control that can prevent or mitigate buffer overflow attacks, which are attacks that exploit the vulnerability of the web application code that does not properly check the size or length of the input data that is passed to a function or a variable, and overwrite the adjacent memory locations with malicious code or data. Including logging functions is a web application control that can prevent or mitigate unauthorized access or modification attacks, which are attacks that exploit the lack of or weak authentication or authorization mechanisms of the web applications, and access or modify the web application data or functionality without proper permission or verification. Digitally signing each application module is a web application control that can prevent or mitigate code injection or tampering attacks, which are attacks that exploit the vulnerability of the web application code that does not properly validate or sanitize the input data that is executed or interpreted by the web application, and inject or modify the web application code with malicious code or data.

Questions # 44:

Which of the following is used by the Point-to-Point Protocol (PPP) to determine packet formats?

Options:

A.

Layer 2 Tunneling Protocol (L2TP)

B.

Link Control Protocol (LCP)

C.

Challenge Handshake Authentication Protocol (CHAP)

D.

Packet Transfer Protocol (PTP)

Answer

B

Explanation

Link Control Protocol (LCP) is used by the Point-to-Point Protocol (PPP) to determine packet formats. PPP is a data link layer protocol that provides a standard method for transporting network layer packets over point-to-point links, such as serial lines, modems, or dial-up connections. PPP supports various network layer protocols, such as IP, IPX, or AppleTalk, and it can encapsulate them in a common frame format. PPP also provides features such as authentication, compression, error detection, and multilink aggregation. LCP is a subprotocol of PPP that is responsible for establishing, configuring, maintaining, and terminating the point-to-point connection. LCP negotiates and agrees on various options and parameters for the PPP link, such as the maximum transmission unit (MTU), the authentication method, the compression method, the error detection method, and the packet format. LCP uses a series of messages, such as configure-request, configure-ack, configure-nak, configure-reject, terminate-request, terminate-ack, code-reject, protocol-reject, echo-request, echo-reply, and discard-request, to communicate and exchange information between the PPP peers.

The other options are not used by PPP to determine packet formats, but rather for other purposes. Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol that allows the creation of virtual private networks (VPNs) over public networks, such as the Internet. L2TP encapsulates PPP frames in IP datagrams and sends them across the tunnel between two L2TP endpoints. L2TP does not determine the packet format of PPP, but rather uses it as a payload. Challenge Handshake Authentication Protocol (CHAP) is an authentication protocol that is used by PPP to verify the identity of the remote peer before allowing access to the network. CHAP uses a challenge-response mechanism that involves a random number (nonce) and a hash function to prevent replay attacks. CHAP does not determine the packet format of PPP, but rather uses it as a transport. Packet Transfer Protocol (PTP) is not a valid option, as there is no such protocol with this name. There is a Point-to-Point Protocol over Ethernet (PPPoE), which is a protocol that encapsulates PPP frames in Ethernet frames and allows the use of PPP over Ethernet networks. PPPoE does not determine the packet format of PPP, but rather uses it as a payload.

Questions # 45:

Which of the following operates at the Network Layer of the Open System Interconnection (OSI) model?

Options:

A.

Packet filtering

B.

Port services filtering

C.

Content filtering

D.

Application access control



CertsMania

Answer

A

Explanation

Packet filtering operates at the network layer of the Open System Interconnection (OSI) model. The OSI model is a conceptual framework that describes how data is transmitted and processed across different layers of a network. The OSI model consists of seven layers: application, presentation, session, transport, network, data link, and physical. The network layer is the third layer from the bottom of the OSI model, and it is responsible for routing and forwarding data packets between different networks or subnets. The network layer uses logical addresses, such as IP addresses, to identify the source and destination of the data packets, and it uses protocols, such as IP, ICMP, or ARP, to perform the routing and forwarding functions.

Packet filtering is a technique that controls the access to a network or a host by inspecting the incoming and outgoing data packets and applying a set of rules or policies to allow or deny them. Packet filtering can be performed by devices, such as routers, firewalls, or proxies, that operate at the network layer of the OSI model. Packet filtering typically examines the network layer header of the data packets, such as the source and destination IP addresses, the protocol type, or the fragmentation flags, and compares them with the predefined rules or policies. Packet filtering can also examine the transport layer header of the data packets, such as the source and destination port numbers, the TCP flags, or the sequence numbers, and compare them with the rules or policies. Packet filtering can provide a basic level of security and performance for a network or a host, but it also has some limitations, such as the inability to inspect the payload or the content of the data packets, the vulnerability to spoofing or fragmentation attacks, or the complexity and maintenance of the rules or policies.

The other options are not techniques that operate at the network layer of the OSI model, but rather at other layers. Port services filtering is a technique that controls the access to a network or a host by inspecting the transport layer header of the data packets and applying a set of rules or policies to allow or deny them based on the port numbers or the services. Port services filtering operates at the transport layer of the OSI model, which is

the fourth layer from the bottom. Content filtering is a technique that controls the access to a network or a host by inspecting the application layer payload or the content of the data packets and applying a set of rules or policies to allow or deny them based on the keywords, URLs, file types, or other criteria. Content filtering operates at the application layer of the OSI model, which is the seventh and the topmost layer. Application access control is a technique that controls the access to a network or a host by inspecting the application layer identity or the credentials of the users or the processes and applying a set of rules or policies to allow or deny them based on the roles, permissions, or other attributes. Application access control operates at the application layer of the OSI model, which is the seventh and the topmost layer.

Questions # 46:

An input validation and exception handling vulnerability has been discovered on a critical web-based system. Which of the following is MOST suited to quickly implement a control?

Options:

A.

Add a new rule to the application layer firewall

B.

Block access to the service

C.

Install an Intrusion Detection System (IDS)

D.

Patch the application source code

Answer

A

Explanation

Adding a new rule to the application layer firewall is the most suited to quickly implement a control for an input validation and exception handling vulnerability on a critical web-based system. An input validation and exception handling vulnerability is a type of vulnerability that occurs when a web-based system does not properly check, filter, or sanitize the input data that is received from the users or other sources, or does not

properly handle the errors or exceptions that are generated by the system. An input validation and exception handling vulnerability can lead to various attacks, such as:

Injection attacks, such as SQL injection, command injection, or cross-site scripting (XSS), where the attacker inserts malicious code or commands into the input data that are executed by the system or the browser, resulting in data theft, data manipulation, or remote code execution.

Buffer overflow attacks, where the attacker sends more input data than the system can handle, causing the system to overwrite the adjacent memory locations, resulting in data corruption, system crash, or arbitrary code execution.

Denial-of-service (DoS) attacks, where the attacker sends malformed or invalid input data that cause the system to generate excessive errors or exceptions, resulting in system overload, resource exhaustion, or system failure.

An application layer firewall is a device or software that operates at the application layer of the OSI model and inspects the application layer payload or the content of the data packets. An application layer firewall can provide various functions, such as:

Filtering the data packets based on the application layer protocols, such as HTTP, FTP, or SMTP, and the application layer attributes, such as URLs, cookies, or headers.

Blocking or allowing the data packets based on the predefined rules or policies that specify the criteria for the application layer protocols and attributes.

Logging and auditing the data packets for the application layer protocols and attributes.

Modifying or transforming the data packets for the application layer protocols and attributes.

Adding a new rule to the application layer firewall is the most suited to quickly implement a control for an input validation and exception handling vulnerability on a critical web-based system, because it can prevent or reduce the impact of the attacks by filtering or blocking the malicious or invalid input data that exploit the vulnerability. For example, a new rule can be added to the application layer firewall to:

Reject or drop the data packets that contain SQL statements, shell commands, or script tags in the input data, which can prevent or reduce the injection attacks.

Reject or drop the data packets that exceed a certain size or length in the input data, which can prevent or reduce the buffer overflow attacks.

Reject or drop the data packets that contain malformed or invalid syntax or characters in the input data, which can prevent or reduce the DoS attacks.

Adding a new rule to the application layer firewall can be done quickly and easily, without requiring any changes or patches to the web-based system, which can be time-consuming and risky, especially for a critical system. Adding a new rule to the application layer firewall can also be done remotely and centrally, without requiring any physical access or installation on the web-based system, which can be inconvenient and costly, especially for a distributed system.

The other options are not the most suited to quickly implement a control for an input validation and exception handling vulnerability on a critical web-based system, but rather options that have other limitations or drawbacks. Blocking access to the service is not the most suited option, because it can cause disruption and unavailability of the service, which can affect the business operations and customer satisfaction, especially for a critical system. Blocking access to the service can also be a temporary and incomplete solution, as it does not address the root cause of the vulnerability or prevent the attacks from occurring again. Installing an Intrusion Detection System (IDS) is not the most suited option, because IDS only monitors and detects the attacks, and does not prevent or respond to them. IDS can also generate false positives or false negatives, which can affect the accuracy and reliability of the detection. IDS can also be overwhelmed or evaded by the attacks, which can affect the effectiveness and efficiency of the detection. Patching the application source code is not the most suited option, because it can take a long time and require a lot of resources and testing to identify, fix, and deploy the patch, especially for a complex and critical system. Patching the application source code can also introduce new errors or vulnerabilities, which can affect the functionality and security of the system. Patching the application source code can also be difficult or impossible, if the system is proprietary or legacy, which can affect the feasibility and compatibility of the patch.

Questions # 47:

At what level of the Open System Interconnection (OSI) model is data at rest on a Storage Area Network (SAN) located?

Options:

A.

Link layer

B.

Physical layer

C.

Session layer

D.



CertsMania

Application layer

Answer

B

Explanation

Data at rest on a Storage Area Network (SAN) is located at the physical layer of the Open System Interconnection (OSI) model. The OSI model is a conceptual framework that describes how data is transmitted and processed across different layers of a network. The OSI model consists of seven layers: application, presentation, session, transport, network, data link, and physical. The physical layer is the lowest layer of the OSI model, and it is responsible for the transmission and reception of raw bits over a physical medium, such as cables, wires, or optical fibers. The physical layer defines the physical characteristics of the medium, such as voltage, frequency, modulation, connectors, etc. The physical layer also deals with the physical topology of the network, such as bus, ring, star, mesh, etc.

A Storage Area Network (SAN) is a dedicated network that provides access to consolidated and block-level data storage. A SAN consists of storage devices, such as disks, tapes, or arrays, that are connected to servers or clients via a network infrastructure, such as switches, routers, or hubs. A SAN allows multiple servers or clients to share the same storage devices, and it provides high performance, availability, scalability, and security for data storage. Data at rest on a SAN is located at the physical layer of the OSI model, because it is stored as raw bits on the physical medium of the storage devices, and it is accessed by the servers or clients through the physical medium of the network infrastructure.

Questions # 48:

Which of the following is the BEST network defense against unknown types of attacks or stealth attacks in progress?

Options:

A.

Intrusion Prevention Systems (IPS)

B.

Intrusion Detection Systems (IDS)

C.

Stateful firewalls

D.

Network Behavior Analysis (NBA) tools

Answer

D

Explanation



CertsMania

Network Behavior Analysis (NBA) tools are the best network defense against unknown types of attacks or stealth attacks in progress. NBA tools are devices or software that monitor and analyze the network traffic and activities, and detect any anomalies or deviations from the normal or expected behavior. NBA tools use various techniques, such as statistical analysis, machine learning, artificial intelligence, or heuristics, to establish a baseline of the network behavior, and to identify any outliers or indicators of compromise. NBA tools can provide several benefits, such as:

Detecting unknown types of attacks or stealth attacks that are not signature-based or rule-based, and that can evade or bypass other network defenses, such as firewalls, IDS, or IPS.

Detecting advanced persistent threats (APTs) that are low and slow, and that can remain undetected for a long time, by correlating and aggregating the network events and data over time and across different sources.

Detecting insider threats or compromised hosts that are authorized and trusted, but that exhibit malicious or suspicious behavior, by profiling and classifying the network entities and their interactions.

Providing early warning and alerting of the potential or ongoing attacks, and facilitating the investigation and response of the incidents, by providing rich and contextual information about the network behavior and the attack vectors.

The other options are not the best network defense against unknown types of attacks or stealth attacks in progress, but rather network defenses that have other limitations or drawbacks. Intrusion Prevention Systems (IPS) are devices or software that monitor and block the network traffic and activities that match the predefined signatures or rules of known attacks. IPS can provide a proactive and preventive layer of security, but they cannot detect or stop unknown types of attacks or stealth attacks that do not match any signatures or rules, or that can evade or disable the IPS. Intrusion Detection Systems (IDS) are devices or software that monitor and alert the network traffic and activities that match the predefined signatures or rules of known attacks. IDS can provide a reactive and detective layer of security, but they cannot detect or alert unknown types of attacks or stealth attacks that do not match any signatures or rules, or that can evade or disable the IDS. Stateful firewalls are devices or software that filter and control the network traffic and

activities based on the state and context of the network sessions, such as the source and destination IP addresses, port numbers, protocol types, and sequence numbers. Stateful firewalls can provide a granular and dynamic layer of security, but they cannot filter or control unknown types of attacks or stealth attacks that use valid or spoofed network sessions, or that can exploit or bypass the firewall rules.

Questions # 49:

What is the purpose of an Internet Protocol (IP) spoofing attack?

Options:

A.

To send excessive amounts of data to a process, making it unpredictable

B.

To intercept network traffic without authorization

C.

To disguise the destination address from a target's IP filtering devices

D.

To convince a system that it is communicating with a known entity

Answer

D

Explanation

The purpose of an Internet Protocol (IP) spoofing attack is to convince a system that it is communicating with a known entity. IP spoofing is a technique that involves creating and sending IP packets with a forged source IP address, which is usually the IP address of a trusted or authorized host. IP spoofing can be used for various malicious purposes, such as:

Bypassing IP-based access control lists (ACLs) or firewalls that filter traffic based on the source IP address.

Launching denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks by flooding a target system with spoofed packets, or by reflecting or amplifying the

traffic from intermediate systems.

Hijacking or intercepting a TCP session by predicting or guessing the sequence numbers and sending spoofed packets to the legitimate parties.

Gaining unauthorized access to a system or network by impersonating a trusted or authorized host and exploiting its privileges or credentials.

The purpose of IP spoofing is to convince a system that it is communicating with a known entity, because it allows the attacker to evade detection, avoid responsibility, and exploit trust relationships.

The other options are not the main purposes of IP spoofing, but rather the possible consequences or methods of IP spoofing. To send excessive amounts of data to a process, making it unpredictable is a possible consequence of IP spoofing, as it can cause a DoS or DDoS attack. To intercept network traffic without authorization is a possible method of IP spoofing, as it can be used to hijack or intercept a TCP session. To disguise the destination address from a target's IP filtering devices is not a valid option, as IP spoofing involves forging the source address, not the destination address.

Questions # 50:

Which of the following factors contributes to the weakness of Wired Equivalent Privacy (WEP) protocol?

Options:

A.

WEP uses a small range Initialization Vector (IV)

B.

WEP uses Message Digest 5 (MD5)

C.

WEP uses Diffie-Hellman

D.

WEP does not use any Initialization Vector (IV)

Answer

A

Explanation

WEP uses a small range Initialization Vector (IV) is the factor that contributes to the weakness of Wired Equivalent Privacy (WEP) protocol. WEP is a security protocol that provides encryption and authentication for wireless networks, such as Wi-Fi. WEP uses the RC4 stream cipher to encrypt the data packets, and the CRC-32 checksum to verify the data integrity. WEP also uses a shared secret key, which is concatenated with a 24-bit Initialization Vector (IV), to generate the keystream for the RC4 encryption. WEP has several weaknesses and vulnerabilities, such as:

WEP uses a small range Initialization Vector (IV), which results in 16,777,216 (2^{24}) possible values. This might seem large, but it is not enough for a high-volume wireless network, where the same IV can be reused frequently, creating keystream reuse and collisions. An attacker can capture and analyze the encrypted data packets that use the same IV, and recover the keystream and the secret key, using techniques such as the Fluhrer, Mantin, and Shamir (FMS) attack, or the KoreK attack.

WEP uses a weak integrity check, which is the CRC-32 checksum. The CRC-32 checksum is a linear function that can be easily computed and manipulated by anyone who knows the keystream. An attacker can modify the encrypted data packets and the checksum, without being detected, using techniques such as the bit-flipping attack, or the chop-chop attack.

WEP uses a static and shared secret key, which is manually configured and distributed among all the wireless devices that use the same network. The secret key is not changed or refreshed automatically, unless the administrator does it manually. This means that the secret key can be exposed or compromised over time, and that all the wireless devices can be affected by a single key breach. An attacker can also exploit the weak authentication mechanism of WEP, which is based on the secret key, and gain unauthorized access to the network, using techniques such as the authentication spoofing attack, or the shared key authentication attack.

WEP has been deprecated and replaced by more secure protocols, such as Wi-Fi Protected Access (WPA) or Wi-Fi Protected Access II (WPA2), which use stronger encryption and authentication methods, such as the Temporal Key Integrity Protocol (TKIP), the Advanced Encryption Standard (AES), or the Extensible Authentication Protocol (EAP).

The other options are not factors that contribute to the weakness of WEP, but rather factors that are irrelevant or incorrect. WEP does not use Message Digest 5 (MD5), which is a hash function that produces a 128-bit output from a variable-length input. WEP does not use Diffie-Hellman, which is a method for generating a shared secret key between two parties. WEP does use an Initialization Vector (IV), which is a 24-bit value that is concatenated with the secret key.

Questions # 51:

An external attacker has compromised an organization's network security perimeter and installed a sniffer onto an inside computer. Which of the following is the MOST effective layer of security the organization could have implemented to mitigate the attacker's ability to gain further information?

Options:

A.

Implement packet filtering on the network firewalls

B.

Install Host Based Intrusion Detection Systems (HIDS)

C.

Require strong authentication for administrators

D.

Implement logical network segmentation at the switches

Answer

D

Explanation

Implementing logical network segmentation at the switches is the most effective layer of security the organization could have implemented to mitigate the attacker's ability to gain further information. Logical network segmentation is the process of dividing a network into smaller subnetworks or segments based on criteria such as function, location, or security level. Logical network segmentation can be implemented at the switches, which are devices that operate at the data link layer of the OSI model and forward data packets based on the MAC addresses. Logical network segmentation can provide several benefits, such as:

Isolating network traffic and reducing congestion and collisions

Enhancing performance and efficiency of the network

Improving security and confidentiality of the network

Restricting the scope and impact of attacks

Enforcing access control and security policies

Facilitating monitoring and auditing of the network

Logical network segmentation can mitigate the attacker's ability to gain further information by limiting the visibility and access of the sniffer to the segment where it is installed. A sniffer is a tool that captures and analyzes the data packets that are transmitted over a network. A sniffer can be used for legitimate purposes, such as troubleshooting, testing, or monitoring the network, or for malicious purposes, such as eavesdropping, stealing, or modifying the data. A sniffer can only capture the data packets that are within its broadcast domain, which is the set of devices that can communicate with each other without a router. By implementing logical network segmentation at the switches, the organization can create multiple broadcast domains and isolate the sensitive or critical data from the compromised segment. This way, the attacker can only see the data packets that belong to the same segment as the sniffer, and not the data packets that belong to other segments. This can prevent the attacker from gaining further information or accessing other resources on the network.

The other options are not the most effective layers of security the organization could have implemented to mitigate the attacker's ability to gain further information, but rather layers that have other limitations or drawbacks. Implementing packet filtering on the network firewalls is not the most effective layer of security, because packet filtering only examines the network layer header of the data packets, such as the source and destination IP addresses, and does not inspect the payload or the content of the data. Packet filtering can also be bypassed by using techniques such as IP spoofing or fragmentation. Installing Host Based Intrusion Detection Systems (HIDS) is not the most effective layer of security, because HIDS only monitors and detects the activities and events on a single host, and does not prevent or respond to the attacks. HIDS can also be disabled or evaded by the attacker if the host is compromised. Requiring strong authentication for administrators is not the most effective layer of security, because authentication only verifies the identity of the users or processes, and does not protect the data in transit or at rest. Authentication can also be defeated by using techniques such as phishing, keylogging, or credential theft.

Questions # 52:

In a Transmission Control Protocol/Internet Protocol (TCP/IP) stack, which layer is responsible for negotiating and establishing a connection with another node?

Options:

A.

Transport layer

B.

Application layer

C.

Network layer

D.

Session layer



CertsMania

Answer

A

Explanation

The transport layer of the Transmission Control Protocol/Internet Protocol (TCP/IP) stack is responsible for negotiating and establishing a connection with another node. The TCP/IP stack is a simplified version of the OSI model, and it consists of four layers: application, transport, internet, and link. The transport layer is the third layer of the TCP/IP stack, and it is responsible for providing reliable and efficient end-to-end data transfer between two nodes on a network. The transport layer uses protocols, such as Transmission Control Protocol (TCP) or User Datagram Protocol (UDP), to segment, sequence, acknowledge, and reassemble the data packets, and to handle error detection and correction, flow control, and congestion control. The transport layer also provides connection-oriented or connectionless services, depending on the protocol used.

TCP is a connection-oriented protocol, which means that it establishes a logical connection between two nodes before exchanging data, and it maintains the connection until the data transfer is complete. TCP uses a three-way handshake to negotiate and establish a connection with another node. The three-way handshake works as follows:

The client sends a SYN (synchronize) packet to the server, indicating its initial sequence number and requesting a connection.

The server responds with a SYN-ACK (synchronize-acknowledge) packet, indicating its initial sequence number and acknowledging the client's request.

The client responds with an ACK (acknowledge) packet, acknowledging the server's response and completing the connection.

UDP is a connectionless protocol, which means that it does not establish or maintain a connection between two nodes, but rather sends data packets independently and without any guarantee of delivery, order, or integrity. UDP does not use a handshake or any other

mechanism to negotiate and establish a connection with another node, but rather relies on the application layer to handle any connection-related issues.

Questions # 53:

A Business Continuity Plan (BCP) is based on

Options:

- A.
the policy and procedures manual.
- B.
an existing BCP from a similar organization.
- C.
a review of the business processes and procedures.
- D.
a standard checklist of required items and objectives.

Answer

C

Explanation

A Business Continuity Plan (BCP) is based on a review of the business processes and procedures. A BCP is a document that describes the strategies, actions, and resources that an organization will use to ensure the continuity of its critical business functions in the event of a disruption or disaster. A review of the business processes and procedures is a process that analyzes the current state of the organization's operations, such as the inputs, outputs, dependencies, resources, and risks of each business process or procedure. A review of the business processes and procedures helps to identify the critical business functions, the recovery objectives, the recovery strategies, and the recovery roles and responsibilities that form the basis of the BCP. The policy and procedures manual, an existing BCP from a similar organization, and a standard checklist of required items and objectives are not the best sources for basing a BCP, as they may not reflect the specific needs, goals, and context of the organization or its business processes and procedures. References: CISSP All-in-One Exam Guide, Eighth Edition, Chapter 7, Security Operations, page 899. Official (ISC)2 CISSP CBK Reference, Fifth Edition, Chapter 7,

Questions # 54:

Refer to the information below to answer the question.

A large, multinational organization has decided to outsource a portion of their Information Technology (IT) organization to a third-party provider's facility. This provider will be responsible for the design, development, testing, and support of several critical, customer-based applications used by the organization.

The third party needs to have

Options:

A.

processes that are identical to that of the organization doing the outsourcing.

B.

access to the original personnel that were on staff at the organization.

C.

the ability to maintain all of the applications in languages they are familiar with.

D.

access to the skill sets consistent with the programming languages used by the organization.

Answer

D

Explanation

The third party needs to have access to the skill sets consistent with the programming languages used by the organization. The programming languages are the tools or the methods of creating, modifying, testing, and supporting the software applications that perform the functions or the tasks required by the organization. The programming languages can vary in their syntax, semantics, features, or paradigms, and they can require different levels of expertise or experience to use them effectively or efficiently. The third party needs to have access to the skill sets consistent with the programming languages used by the organization, as it can ensure the quality, the compatibility, and the maintainability of the software applications that the third party is responsible for. The

third party does not need to have processes that are identical to that of the organization doing the outsourcing, access to the original personnel that were on staff at the organization, or the ability to maintain all of the applications in languages they are familiar with, as they are related to the methods, the resources, or the preferences of the software development, not the skill sets consistent with the programming languages used by the organization. References: CISSP All-in-One Exam Guide, Eighth Edition, Chapter 8, Software Development Security, page 1000. Official (ISC)2 CISSP CBK Reference, Fifth Edition, Chapter 8, Software Development Security, page 1016.

Questions # 55:

Refer to the information below to answer the question.

Desktop computers in an organization were sanitized for re-use in an equivalent security environment. The data was destroyed in accordance with organizational policy and all marking and other external indications of the sensitivity of the data that was formerly stored on the magnetic drives were removed.

After magnetic drives were degaussed twice according to the product manufacturer's directions, what is the MOST LIKELY security issue with degaussing?

Options:

A.

Commercial products often have serious weaknesses of the magnetic force available in the degausser product.

B.

Degausser products may not be properly maintained and operated.

C.

The inability to turn the drive around in the chamber for the second pass due to human error.

D.

Inadequate record keeping when sanitizing media.

Answer

B

Explanation

The most likely security issue with degaussing is that the degausser products may not be properly maintained and operated. Degaussing is a method of sanitizing magnetic media, such as hard disk drives, by applying a strong magnetic field that erases the data stored on the media. Degaussing can be effective in destroying the data, but it requires that the degausser products are calibrated, tested, and used according to the manufacturer's specifications and instructions. If the degausser products are not properly maintained and operated, they may not generate a sufficient magnetic force to erase the data completely, or they may damage the media or the device. Commercial products often have serious weaknesses of the magnetic force available in the degausser product, the inability to turn the drive around in the chamber for the second pass due to human error, and inadequate record keeping when sanitizing media are not the most likely security issues with degaussing, as they are related to the quality, the technique, or the documentation of the degaussing process, not the maintenance or the operation of the degausser products. References: CISSP All-in-One Exam Guide, Eighth Edition, Chapter 7, Security Operations, page 888. Official (ISC)2 CISSP CBK Reference, Fifth Edition, Chapter 7, Security Operations, page 904.

Questions # 56:

Place the following information classification steps in sequential order.

<u>Steps</u>		<u>Order</u>
Declassify information when appropriate		Step
Apply the appropriate security markings		Step
Conduct periodic classification reviews		Step
Assign a classification level		Step
Document the information assets		Step

Options:

Answer

Answer:

Steps		Order
Declassify information when appropriate	Document the information assets	Step
Apply the appropriate security markings	Assign a classification level	Step
Conduct periodic classification reviews	Apply the appropriate security markings	Step
Assign a classification level	Conduct periodic classification reviews	Step
Document the information assets	Declassify information when appropriate	Step

Explanation

The following information classification steps should be placed in sequential order as follows:

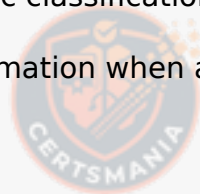
Document the information assets

Assign a classification level

Apply the appropriate security markings

Conduct periodic classification reviews

Declassify information when appropriate



CertsMania

Document the information assets

Assign a classification level

Apply the appropriate security markings

Conduct periodic classification reviews

Declassify information when appropriate

Information classification is a process or a method of categorizing the information assets based on their sensitivity, criticality, or value, and applying the appropriate security controls or measures to protect them. Information classification can help to ensure the confidentiality, the integrity, and the availability of the information assets, and to support the security, the compliance, or the business objectives of the organization. The information classification steps are the activities or the tasks that are involved in the information classification process, and they should be performed in a sequential order, as follows:

Document the information assets: This step involves identifying, inventorying, and describing the information assets that are owned, used, or managed by the organization, such as the data, the documents, the records, or the media. This step can help to determine the scope, the ownership, or the characteristics of the information assets, and to prepare for the next steps of the information classification process.

Assign a classification level: This step involves assigning a classification level or a label to each information asset, based on the sensitivity, the criticality, or the value of the information asset, and the impact or the consequence of the unauthorized or the malicious access, disclosure, modification, or destruction of the information asset. The classification level or the label can indicate the degree or the extent of the security protection or the handling that the information asset requires, such as the confidentiality, the integrity, or the availability. The classification level or the label can vary depending on the organization's policies, standards, or regulations, but some common examples are public, internal, confidential, or secret.

Apply the appropriate security markings: This step involves applying the appropriate security markings or indicators to the information assets, based on the classification level or the label of the information assets. The security markings or indicators can include the visual, the physical, or the electronic symbols, signs, or codes that show the classification level or the label of the information assets, such as the banners, the headers, the footers, the stamps, the stickers, the tags, or the metadata. The

security markings or indicators can help to communicate, inform, or remind the users or the entities of the security protection or the handling that the information assets require, and to prevent or reduce the risk of the unauthorized or the malicious access, disclosure, modification, or destruction of the information assets.

Conduct periodic classification reviews: This step involves conducting periodic classification reviews or assessments of the information assets, to ensure that the classification level or the label and the security markings or indicators of the information assets are accurate, consistent, and up-to-date. The periodic classification reviews or assessments can be triggered by the changes or the events that affect the sensitivity, the criticality, or the value of the information assets, such as the business needs, the legal requirements, the security incidents, or the data lifecycle. The periodic classification reviews or assessments can help to verify, validate, or update the classification level or the label and the security markings or indicators of the information assets, and to maintain or improve the security protection or the handling of the information assets.

Declassify information when appropriate: This step involves declassifying or downgrading the information assets when appropriate, to reduce or remove the security protection or the handling that the information assets require, based on the sensitivity, the criticality, or the value of the information assets, and the impact or the consequence of the unauthorized or the malicious access, disclosure, modification, or destruction of the information assets. The declassification or the downgrade of the information assets can be triggered by the changes or the events that affect the sensitivity, the criticality, or the value of the information assets, such as the expiration, the disposal, the release, or the transfer of the information assets. The declassification or the downgrade of the information assets can help to optimize, balance, or streamline the security protection or the handling of the information assets, and to support the security,

Questions # 57:

Which of the following is the PRIMARY benefit of a formalized information classification program?

Options:

A.

It drives audit processes.

B.

It supports risk assessment.

C.

It reduces asset vulnerabilities.

D.

It minimizes system logging requirements.

Answer

A

Explanation



CertsMania

A formalized information classification program is a set of policies and procedures that define the categories, criteria, and responsibilities for classifying information assets according to their value, sensitivity, and criticality. The primary benefit of such a program is that it supports risk assessment, which is the process of identifying, analyzing, and evaluating the risks to the information assets and the organization. By classifying information assets, the organization can prioritize the protection of the most important and vulnerable assets, determine the appropriate security controls and measures, and allocate the necessary resources and budget. It drives audit processes, it reduces asset vulnerabilities, and it minimizes system logging requirements are all possible benefits of a formalized information classification program, but they are not the primary benefit of doing so. References: CISSP All-in-One Exam Guide, Eighth Edition, Chapter 1, Security and Risk Management, page 39. Official (ISC)2 CISSP CBK Reference, Fifth Edition, Chapter 1, Security and Risk Management, page 52.

Questions # 58:

What is the MOST effective method for gaining unauthorized access to a file protected with a long complex password?

Options:

A.

Brute force attack

B.

Frequency analysis

C.

Social engineering

D.



CertsMania

Dictionary attack

Answer

C

Explanation

The most effective method for gaining unauthorized access to a file protected with a long complex password is social engineering. Social engineering is a type of attack that exploits the human factor or the psychological weaknesses of the target, such as trust, curiosity, greed, or fear, to manipulate them into revealing sensitive information, such as passwords, or performing malicious actions, such as opening malicious attachments or clicking malicious links. Social engineering can bypass the technical security controls, such as encryption or authentication, and can be more efficient and successful than other methods that rely on brute force or guesswork. Brute force attack, frequency analysis, and dictionary attack are not the most effective methods for gaining unauthorized access to a file protected with a long complex password, as they require a lot of time, resources, and computing power, and they can be thwarted by the use of strong passwords, password policies, or password managers. References: CISSP All-in-One Exam Guide, Eighth Edition, Chapter 6, Security Assessment and Testing, page 813. Official (ISC)2 CISSP CBK Reference, Fifth Edition, Chapter 6, Security Assessment and Testing, page 829.

Questions # 59:

Which of the following is the MOST effective practice in managing user accounts when an employee is terminated?

Options:

A.

Implement processes for automated removal of access for terminated employees.

B.

Delete employee network and system IDs upon termination.

C.

Manually remove terminated employee user-access to all systems and applications.

D.

Disable terminated employee network ID to remove all access.

Answer

A

Explanation

The most effective practice in managing user accounts when an employee is terminated is to implement processes for automated removal of access for terminated employees. This practice can ensure that the access rights of the terminated employee are revoked as soon as possible, preventing any unauthorized or malicious use of the account. Automated removal of access can be achieved by using software tools or scripts that can disable or delete the account, remove it from any groups or roles, and revoke any permissions or privileges associated with the account. Automated removal of access can also reduce the human errors or delays that may occur in manual processes, and provide an audit trail of the actions taken. Deleting employee network and system IDs upon termination, manually removing terminated employee user-access to all systems and applications, and disabling terminated employee network ID to remove all access are all possible ways to manage user accounts when an employee is terminated, but they are not as effective as automated removal of access. Deleting employee network and system IDs upon termination may cause problems with data retention, backup, or recovery, and may not remove all traces of the account from the systems. Manually removing terminated employee user-access to all systems and applications may be time-consuming, error-prone, or incomplete, and may depend on the cooperation and coordination of different administrators or departments. Disabling terminated employee network ID to remove all access may not be sufficient, as the account may still exist and be reactivated, or may have access to some resources that are not controlled by the network ID.

Questions # 60:

After following the processes defined within the change management plan, a super user has upgraded a device within an Information system.

What step would be taken to ensure that the upgrade did NOT affect the network security posture?

Options:

- A.
Conduct an Assessment and Authorization (A&A)
- B.

Conduct a security impact analysis

C.

Review the results of the most recent vulnerability scan

D.

Conduct a gap analysis with the baseline configuration

Answer

B

Explanation

A security impact analysis is a process of assessing the potential effects of a change on the security posture of a system. It helps to identify and mitigate any security risks that may arise from the change, such as new vulnerabilities, configuration errors, or compliance issues. A security impact analysis should be conducted after following the change management plan and before implementing the change in the production environment. Conducting an A&A, reviewing the results of a vulnerability scan, or conducting a gap analysis with the baseline configuration are also possible steps to ensure the security of a system, but they are not specific to the change management process. **References:** CISSP All-in-One Exam Guide, Eighth Edition, Chapter 8: Software Development Security, page 961; Official (ISC)2 Guide to the CISSP CBK, Fifth Edition, Chapter 8: Security Operations, page 1013.

Questions # 61:

Which of the following is the MOST challenging issue in apprehending cyber criminals?

Options:

A.

They often use sophisticated method to commit a crime.

B.

It is often hard to collect and maintain integrity of digital evidence.

C.

The crime is often committed from a different jurisdiction.

D.

There is often no physical evidence involved.

Answer

C

Explanation



CertsMania

The most challenging issue in apprehending cyber criminals is that the crime is often committed from a different jurisdiction. This means that the cyber criminals may operate from a different country or region than the victim or the target, and thus may be subject to different laws, regulations, and enforcement agencies. This can create difficulties and delays in identifying, locating, and prosecuting the cyber criminals, as well as in obtaining and preserving the digital evidence. The other issues, such as the sophistication of the methods, the integrity of the evidence, and the lack of physical evidence, are also challenges in apprehending cyber criminals, but they are not as significant as the jurisdiction issue. **References:** CISSP All-in-One Exam Guide, Eighth Edition, Chapter 4: Security Operations, page 475; Official (ISC)2 Guide to the CISSP CBK, Fifth Edition, Chapter 4: Communication and Network Security, page 544.

Questions # 62:

“Stateful” differs from “Static” packet filtering firewalls by being aware of which of the following?

Options:

A.

Difference between a new and an established connection

B.

Originating network location

C.

Difference between a malicious and a benign packet payload

D.

Originating application session

Answer

A

Explanation

Stateful firewalls differ from static packet filtering firewalls by being aware of the difference between a new and an established connection. A stateful firewall is a firewall that keeps track of the state of network connections and transactions, and uses this information to make filtering decisions. A stateful firewall maintains a state table that records the source and destination IP addresses, port numbers, protocols, and sequence numbers of each connection. A stateful firewall can distinguish between a new connection, which requires a three-way handshake to be completed, and an established connection, which has already completed the handshake and is ready to exchange data. A stateful firewall can also detect when a connection is terminated or idle, and remove it from the state table. A stateful firewall can provide more security and efficiency than a static packet filtering firewall, which only examines the header of each packet and compares it to a set of predefined rules. A static packet filtering firewall does not keep track of the state of connections, and cannot differentiate between new and established connections. A static packet filtering firewall may allow or block packets based on the source and destination IP addresses, port numbers, and protocols, but it cannot inspect the payload or the sequence numbers of the packets. A static packet filtering firewall may also be vulnerable to spoofing or flooding attacks, as it cannot verify the authenticity or validity of the packets. The other options are not aspects that stateful firewalls are aware of, but static packet filtering firewalls are not. Both types of firewalls can check the originating network location of the packets, but they cannot check the difference between a malicious and a benign packet payload, or the originating application session of the packets. **References:** Stateless vs Stateful Packet Filtering Firewalls - GeeksforGeeks; Stateful vs Stateless Firewall: Differences and Examples - Fortinet; Stateful Inspection Firewalls Explained - Palo Alto Networks.

Questions # 63:

Which of the following is the BEST metric to obtain when gaining support for an Identify and Access

Management (IAM) solution?

Options:

A.

Application connection successes resulting in data leakage

B.

Administrative costs for restoring systems after connection failure

C.

Employee system timeouts from implementing wrong limits

D.

Help desk costs required to support password reset requests

Answer

D

Explanation

Identify and Access Management (IAM) is the process of managing the identities and access rights of users and devices in an organization. IAM solutions can provide various benefits, such as improving security, compliance, productivity, and user experience. However, implementing an IAM solution may also require significant investment and resources, and therefore, it is important to obtain support from the stakeholders and decision-makers. One of the best metrics to obtain when gaining support for an IAM solution is the help desk costs required to support password reset requests. This metric can demonstrate the following advantages of an IAM solution:

Reducing the workload and expenses of the help desk staff, who often spend a large amount of time and money on handling password reset requests from users who forget or lose their passwords.

Enhancing the security and compliance of the organization, by reducing the risks of unauthorized access, identity theft, phishing, and credential compromise, which can result from weak or shared passwords, or passwords that are not changed frequently or securely.

Improving the productivity and user experience of the users, by enabling them to reset their own passwords quickly and easily, without having to contact the help desk or wait for a response. This can also reduce the downtime and frustration of the users, and increase their satisfaction and loyalty.

To Get Premium Files for CISSP Visit

<https://www.certsmania.com/isc/cissp-practice>

For More Free Questions Visit

<https://www.certsmania.com/isc/pdf/cissp>



CertsMania