Number: Cybersecurity Audit Certificate
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: Cybersecurity Audit Certificate

Exam Name: Cybersecurity Audit Certificate

Exam A

QUESTION 1
Cyber threat intelligence aims to research and analyze trends and technical developments in which of the following areas?

A. Industry-specific security regulator
B. Cybercrime, hacktism. and espionage
C. Cybersecurity risk scenarios
D. Cybersecurity operations management

Correct Answer: B
Section:
Explanation:
Cyber threat intelligence aims to research and analyze trends and technical developments in the areas ofcybercrime, hacktivism, and espionage. These are the main sources of malicious cyber activities that pose risks to organizations and individuals. Cyber threat intelligence helps to understand the motivations, capabilities, tactics, techniques, and procedures of various threat actors and groups.

QUESTION 2
Which of the following is an objective of public key infrastructure (PKI)?

A. Creating the private-public key pair for secure communications
B. Independently authenticating the validity of the sender's public key
C. Securely distributing secret keys to the communicating parties
D. Approving the algorithm to be used during data transmission

Correct Answer: B
Section:
Explanation:
An objective of public key infrastructure (PKI) is to independently authenticate the validity of the sender's public key. PKI is a system that uses cryptographic keys to secure communications and transactions. PKI involves a trusted third party called a certificate authority (CA) that issues digital certificates that link a public key with an identity. The recipient can use the CA's public key to verify the sender's certificate and public key.

QUESTION 3
Which of the following is a more efficient form of public key cryptography as it demands less computational power and offers more security per bit?

A. Diffie-Hellman Key Agreement
B. Digital Signature Standard
C. Secret Key Cryptography
D. Elliptic Curve Cryptography

Correct Answer: D
Section:
Explanation:
Elliptic curve cryptography (ECC)is a more efficient form of public key cryptography as it demands less computational power and offers more security per bit. ECC is based on the mathematical properties of elliptic

curves, which are curves that have a special shape that makes them suitable for cryptography. ECC can achieve the same level of security as other public key algorithms with much smaller key sizes, which reduces storage and bandwidth requirements.

QUESTION 4
Which type of tools look for anomalies in user behavior?

A. Rootkit detection tools
B. Trend/variance-detection tools
C. Audit reduction tools
D. Attack-signature-detection tools

Correct Answer: B
Section:
Explanation:
Trend/variance-detection toolsare tools that look for anomalies in user behavior. These tools use statistical methods to establish a baseline of normal user activity and then compare it with current or historical data to identify deviations or outliers. These tools can help to detect unauthorized access, fraud, insider threats, or other malicious activities.

QUESTION 5
The second line of defense in cybersecurity includes:

A. conducting organization-wide control self-assessments.
B. risk management monitoring, and measurement of controls.
C. separate reporting to the audit committee within the organization.
D. performing attack and breach penetration testing.

Correct Answer: B
Section:
Explanation:
The second line of defense in cybersecurity includes risk management monitoring, and measurement of controls. This is because the second line of defense is responsible for ensuring that the first line of defense (the operational managers and staff who own and manage risks) is effectively designed and operating as intended. The second line of defense also provides guidance, oversight, and challenge to the first line of defense. The other options are not part of the second line of defense, but rather belong to the first line of defense (A), the third line of defense C, or an external service provider (D).

QUESTION 6
Within the NIST core cybersecurity framework, which function is associated with using organizational understanding to minimize risk to systems, assets, and data?

A. Detect
B. Identify
C. Recover
D. Respond

Correct Answer: B
Section:
Explanation:
Within the NIST core cybersecurity framework, the identify function is associated with using organizational understanding to minimize risk to systems, assets, and data. This is because the identify function helps organizations to develop an organizational understanding of their cybersecurity risk management posture, as well as the threats, vulnerabilities, and impacts that could affect their business objectives. The other functions are not directly related to using organizational understanding, but rather focus on detecting (A), recovering C, or responding (D) to cybersecurity events.

QUESTION 7
The 'recover' function of the NISI cybersecurity framework is concerned with:

A. planning for resilience and timely repair of compromised capacities and service.
B. identifying critical data to be recovered m case of a security incident.
C. taking appropriate action to contain and eradicate a security incident.
D. allocating costs incurred as part of the implementation of cybersecurity measures.

Correct Answer: A
Section:
Explanation:
The ''recover'' function of the NIST cybersecurity framework is concerned with planning for resilience and timely repair of compromised capacities and service. This is because the recover function helps organizations to restore normal operations as quickly as possible after a cybersecurity incident, while also learning from the incident and improving their security posture. The other options are not part of the recover function, but rather belong to the identify (B), respond C, or protect (D) functions.

QUESTION 8
Availability can be protected through the use of:

A. user awareness training and related end-user training.
B. access controls. We permissions, and encryption.
C. logging, digital signatures, and write protection.
D. redundancy, backups, and business continuity management

Correct Answer: D
Section:
Explanation:
Availability can be protected through the use of redundancy, backups, and business continuity management. This is because these measures help to ensure that systems, data, and services are accessible and functional at all times, even in the event of a disruption or disaster. The other options are not directly related to protecting availability, but rather focus on enhancing confidentiality (A), integrity C, or awareness (D).

QUESTION 9
Which of the following would provide the BEST basis for allocating proportional protection activities when comprehensive classification is not feasible?

A. Single classification level allocation
B. Business process re-engineering
C. Business dependency assessment
D. Comprehensive cyber insurance procurement

Correct Answer: C
Section:
Explanation:
The BEST basis for allocating proportional protection activities when comprehensive classification is not feasible is a business dependency assessment. This is because a business dependency assessment helps to identify the criticality and sensitivity of business processes and their supporting assets, based on their contribution to the organization's objectives and value proposition. This allows for prioritizing protection activities according to the level of risk and impact. The other options are not as effective as a business dependency assessment, because they either use a single classification level allocation (A), which does not account for different levels of risk and impact; require a significant amount of time and resources to perform a business process re-engineering (B); or rely on external parties to cover potential losses without reducing the likelihood or impact of incidents (D).

QUESTION 10
A healthcare organization recently acquired another firm that outsources its patient information processing to a third-party Software as a Service (SaaS) provider. From a regulatory perspective, which of the following is MOST important for the healthcare organization to determine?

A. Cybersecurity risk assessment methodology
B. Encryption algorithms used to encrypt the data
C. Incident escalation procedures
D. Physical location of the data

Correct Answer: C
Section:
Explanation:
From a regulatory perspective, the MOST important thing for the healthcare organization to determine when outsourcing its patient information processing to a third-party Software as a Service (SaaS) provider is the incident escalation procedures. This is because incident escalation procedures define how security incidents involving patient information are reported, communicated, escalated, and resolved between the healthcare organization and the SaaS provider. This is essential for complying with regulatory requirements such as HIPAA, which mandate timely notification and response to breaches of protected health information. The other options are not as important as incident escalation procedures from a regulatory perspective, because they either relate to technical aspects that may not affect compliance (A, B), or operational aspects that may not affect patient information security (D).

QUESTION 11
Which of the following is MOST critical to guiding and managing security activities throughout an organization to ensure objectives are met?

A. Allocating a significant amount of budget to security investments
B. Adopting industry security standards and frameworks
C. Establishing metrics to measure and monitor security performance
D. Conducting annual security awareness training for all employees

Correct Answer: C
Section:
Explanation:
The MOST critical thing to guiding and managing security activities throughout an organization to ensure objectives are met is establishing metrics to measure and monitor security performance. This is because metrics provide quantifiable and objective data that can be used to evaluate the effectiveness and efficiency of security activities, as well as identify gaps and areas for improvement. Metrics also enable communication and reporting of security performance to stakeholders, such as senior management, board members, auditors, regulators, customers, etc. The other options are not as critical as establishing metrics, because they either involve spending money without knowing the return on investment (A), adopting standards without customizing them to fit the organization's context and needs (B), or conducting training without assessing its impact on behavior change (D).

QUESTION 12
Which of the following is the BEST method of maintaining the confidentiality of digital information?

A. Use of access controls, file permissions, and encryption
B. Use of backups and business continuity planning
C. Use of logging digital signatures, and write protection
D. Use of the awareness tracing programs and related end-user testing

Correct Answer: A
Section:
Explanation:

The BEST method of maintaining the confidentiality of digital information is using access controls, file permissions, and encryption. This is because these techniques help to prevent unauthorized access, disclosure, or modification of digital information, by restricting who can access the information, what they can do with it, and how they can access it. The other options are not as effective as using access controls, file permissions, and encryption, because they either relate to protecting availability (B), integrity C, or awareness (D).

QUESTION 13
Which of the following presents the GREATEST challenge to information risk management when outsourcing IT function to a third party?

A. It is difficult to know the applicable regulatory requirements when data is located on another country.
B. Providers may be reluctant to share technical delays on the extent of their information protection mechanisms.
C. Providers may be restricted from providing detailed ^formation on their employees.
D. It is difficult to determine vendor financial viability to assess their potential inability to meet contract requirements.

Correct Answer: B
Section:
Explanation:
The GREATEST challenge to information risk management when outsourcing IT function to a third party is that providers may be reluctant to share technical details on the extent of their information protection mechanisms. This is because providers may consider their information protection mechanisms as proprietary or confidential, or may not want to reveal their weaknesses or vulnerabilities. This makes it difficult for the outsourcing organization to assess the level of security and compliance of the provider, and to monitor and audit their performance. The other options are not as challenging as providers being reluctant to share technical details, because they either involve legal or contractual aspects that can be clarified or negotiated before outsourcing (A, D), or human resource aspects that can be verified or validated by the provider C.

QUESTION 14
The GREATEST advantage of using a common vulnerability scoring system is that it helps with:

A. risk aggregation.
B. risk prioritization.
C. risk elimination.
D. risk quantification

Correct Answer: B
Section:
Explanation:
The GREATEST advantage of using a common vulnerability scoring system is that it helps with risk prioritization. This is because a common vulnerability scoring system provides a standardized and consistent way of measuring and comparing the severity of vulnerabilities, based on their impact and exploitability. This allows organizations to prioritize the remediation of the most critical vulnerabilities and allocate resources accordingly. The other options are not as advantageous as using a common vulnerability scoring system, because they either involve aggregating (A), eliminating C, or quantifying (D) risk, which are not directly related to the scoring system.

QUESTION 15
Which of the following is a client-server program that opens a secure, encrypted command-line shell session from the Internet for remote logon?

A. VPN
B. IPsec
C. SSH
D. SFTP

Correct Answer: C

Section:
Explanation:
The correct answer is C. SSH.
SSH stands for Secure Shell, a client-server program that opens a secure, encrypted command-line shell session from the Internet for remote logon. SSH allows users to remotely access and execute commands on a server without exposing their credentials or data to eavesdropping, tampering or replay attacks. SSH also supports secure file transfer protocols such as SFTP and SCP1.
VPN stands for Virtual Private Network, a technology that creates a secure, encrypted tunnel between two or more devices over a public network such as the Internet. VPN allows users to access resources on a remote network as if they were physically connected to it, while protecting their privacy and identity2.
IPsec stands for Internet Protocol Security, a set of protocols that provides security at the network layer of the Internet. IPsec supports two modes: transport mode and tunnel mode. Transport mode encrypts only the payload of each packet, while tunnel mode encrypts the entire packet, including the header. IPsec can be used to secure VPN connections, as well as other applications that require data confidentiality, integrity and authentication3.
SFTP stands for Secure File Transfer Protocol, a protocol that uses SSH to securely transfer files between a client and a server over a network. SFTP provides encryption, authentication and compression features to ensure the security and reliability of file transfers.
1: SSH (Secure Shell) 2: What is a VPN? How It Works, Types of VPN | Kaspersky 3: IPsec - Wikipedia : [SFTP - Wikipedia]

QUESTION 16
What is the FIRST phase of the ISACA framework for auditors reviewing cryptographic environments?

A. Evaluation of implementation details
B. Hands-on testing
C. Risk-based shakeout
D. Inventory and discovery

Correct Answer: D
Section:
Explanation:
The FIRST phase of the ISACA framework for auditors reviewing cryptographic environments is inventory and discovery. This is because the inventory and discovery phase helps auditors to identify and document the scope, objectives, and approach of the audit, as well as the cryptographic assets, systems, processes, and stakeholders involved in the cryptographic environment. The inventory and discovery phase also helps auditors to assess the maturity and effectiveness of the cryptographic governance and management within the organization. The other phases are not the first phase of the ISACA framework for auditors reviewing cryptographic environments, but rather follow after the inventory and discovery phase, such as evaluation of implementation details (A), hands-on testing (B), or risk-based shakeout C.

QUESTION 17
Which of the following is the BEST indication of mature third-party vendor risk management for an organization?

A. The third party's security program Mows the organization s security program.
B. The organization maintains vendor security assessment checklists.
C. The third party maintains annual assessments of control effectiveness.
D. The organization's security program follows the thud party's security program.

Correct Answer: B
Section:
Explanation:
The BEST indication of mature third-party vendor risk management for an organization is that the organization maintains vendor security assessment checklists. This is because vendor security assessment checklists help the organization to evaluate and monitor the security posture and performance of their third-party vendors, based on predefined criteria and standards. Vendor security assessment checklists also help the organization to identify and mitigate any gaps or issues in the vendor's security controls or processes. The other options are not as indicative of mature third-party vendor risk management for an organization, because they either involve following or mimicking the security program of either party without considering their own needs or risks (A, D), or relying on the vendor's self-assessment without independent verification or validation C.

QUESTION 18
What is the FIRST phase of the ISACA framework for auditors reviewing cryptographic environments?

A. Evaluation of implementation details
B. Hands-on testing
C. Risk-based shakeout
D. Inventory and discovery

Correct Answer: D
Section:
Explanation:
The FIRST phase of the ISACA framework for auditors reviewing cryptographic environments is inventory and discovery. This is because the inventory and discovery phase helps auditors to identify and document the scope, objectives, and approach of the audit, as well as the cryptographic assets, systems, processes, and stakeholders involved in the cryptographic environment. The inventory and discovery phase also helps auditors to assess the maturity and effectiveness of the cryptographic governance and management within the organization. The other phases are not the first phase of the ISACA framework for auditors reviewing cryptographic environments, but rather follow after the inventory and discovery phase, such as evaluation of implementation details (A), hands-on testing (B), or risk-based shakeout C.

QUESTION 19
Which of the following describes specific, mandatory controls or rules to support and comply with a policy?

A. Frameworks
B. Guidelines
C. Basedine
D. Standards

Correct Answer: D
Section:
Explanation:
Specific, mandatory controls or rules to support and comply with a policy are known as standards. This is because standards define the minimum level of performance or behavior that is expected from an organization or its employees in order to achieve a policy objective or requirement. Standards also provide clear and measurable criteria for auditing and monitoring compliance with policies. The other options are not specific, mandatory controls or rules to support and comply with a policy, but rather different types of documents or tools that provide guidance or recommendations for implementing policies or controls, such as frameworks (A), guidelines (B), or baselines C.

QUESTION 20
Which of the following is the MOST important step to determine the risks posed to an organization by social media?

A. Review costs related to the organization's social media outages.
B. Review cybersecurity insurance requirements for the organization s social media.
C. Review the disaster recovery strategy for the organization's social media.
D. Review access control processes for the organization's social media accounts.

Correct Answer: D
Section:
Explanation:
The MOST important step to determine the risks posed to an organization by social media is to review access control processes for the organization's social media accounts. This is because access control processes help to ensure that only authorized users can access, modify, or share the organization's social media accounts and content, and prevent unauthorized or malicious access or disclosure of sensitive or confidential information. Access control processes also help to protect the organization's reputation and brand image from being compromised or damaged by unauthorized or inappropriate social media posts. The other

options are not as important as reviewing access control processes for the organization's social media accounts, because they either relate to costs (A), insurance (B), or recovery C aspects that are not directly related to the risks posed by social media.

QUESTION 21
The protection of information from unauthorized access or disclosure is known as:

A. access control.
B. cryptograph
C. media protect on.
D. confidentiality.

Correct Answer: D
Section:
Explanation:
The protection of information from unauthorized access or disclosure is known as confidentiality. This is because confidentiality is one of the three main objectives of information security, along with integrity and availability. Confidentiality ensures that information is accessible and readable only by those who are authorized and intended to do so, and prevents unauthorized or accidental exposure of information to unauthorized parties. The other options are not the protection of information from unauthorized access or disclosure, but rather different concepts or techniques that are related to information security, such as access control (A), cryptography (B), or media protection C.

QUESTION 22
Security awareness training is MOST effective against which type of threat?

A. Command injection
B. Denial of service
C. Social engineering
D. Social injection

Correct Answer: C
Section:
Explanation:
Security awareness training is MOST effective against social engineering threats. This is because social engineering is a type of attack that exploits human psychology and behavior to manipulate or trick users into revealing sensitive or confidential information, or performing actions that compromise security. Security awareness training helps to educate users about the common types and techniques of social engineering attacks, such as phishing, vishing, baiting, etc., and how to recognize and avoid them. Security awareness training also helps to foster a culture of security within the organization and empower users to report any suspicious or malicious activities. The other options are not types of threats that security awareness training is most effective against, but rather types of attacks that exploit technical vulnerabilities or flaws in systems or applications, such as command injection (A), denial of service (B), or SQL injection (D).

QUESTION 23
A cloud service provider is used to perform analytics on an organization's sensitive dat
a. A data leakage incident occurs in the service providers network from a regulatory perspective, who is responsible for the data breach?

A. The service provider
B. Dependent upon the nature of breath
C. Dependent upon specific regulatory requirements
D. The organization

Correct Answer: D

Section:
Explanation:
A cloud service provider is used to perform analytics on an organization's sensitive data. A data leakage incident occurs in the service provider's network. From a regulatory perspective, the organization is responsible for the data breach. This is because the organization is the data owner and has the ultimate accountability and liability for the security and privacy of its data, regardless of where it is stored or processed. The organization cannot transfer or delegate its responsibility to the service provider, even if there is a contractual agreement or service level agreement that specifies the security obligations of the service provider. The other options are not correct, because they either imply that the service provider is responsible (A), or that the responsibility depends on the nature of breach (B) or specific regulatory requirements C, which are not relevant factors.

QUESTION 24
One way to control the integrity of digital assets is through the use of:

A. policies.
B. frameworks.
C. caching
D. hashing.

Correct Answer: D
Section:
Explanation:
One way to control the integrity of digital assets is through the use of hashing. This is because hashing is a technique that applies a mathematical function to a digital asset, such as a file or a message, and produces a unique and fixed-length value, known as a hash or a digest. Hashing helps to verify the integrity of digital assets, by comparing the hash values before and after transmission or storage, and detecting any changes or modifications to the original asset. The other options are not ways to control the integrity of digital assets, but rather different concepts or techniques that are related to information security, such as policies (A), frameworks (B), or caching C.

QUESTION 25
Which of the following contains the essential elements of effective processes and describes an improvement path considering quality and effectiveness?

A. Capability maturity model integration
B. Balanced scorecard
C. 60 270042009
D. COBIT 5

Correct Answer: A
Section:
Explanation:
The document that contains the essential elements of effective processes and describes an improvement path considering quality and effectiveness is Capability Maturity Model Integration (CMMI). This is because CMMI is a framework that defines five levels of process maturity, from initial to optimized, and provides best practices and guidelines for improving the quality and effectiveness of processes across different domains, such as software development, service delivery, or cybersecurity. The other options are not documents that contain the essential elements of effective processes and describe an improvement path considering quality and effectiveness, but rather different types of documents or tools that provide guidance or recommendations for implementing policies or controls, such as Balanced Scorecard (B), ISO 27004:2009 C, or COBIT 5 (D).

QUESTION 26
Which of the following provides the GREATEST assurance that data can be recovered and restored in a timely manner in the event of data loss?

A. Backups of information are regularly tested.
B. Data backups are available onsite for recovery.

C. The recovery plan is executed during or after an event
D. full data backup is performed daily.

Correct Answer: A
Section:
Explanation:
The feature that provides the GREATEST assurance that data can be recovered and restored in a timely manner in the event of data loss is that backups of information are regularly tested. This is because testing backups helps to ensure that they are valid, complete, and usable, and that they can be restored within the expected time frame and without errors or corruption. Testing backups also helps to identify and resolve any issues or problems with the backup process, media, or software. The other options are not features that provide the greatest assurance that data can be recovered and restored in a timely manner in the event of data loss, but rather different aspects or factors that affect the backup process, such as availability (B), execution C, or frequency (D) of backups.

QUESTION 27
What is the FIRST phase of the ISACA framework for auditors reviewing cryptographic environments?

A. Evaluation of implementation details
B. Hands-on testing
C. Hand-based shakeout
D. Inventory and discovery

Correct Answer: D
Section:
Explanation:
The FIRST phase of the ISACA framework for auditors reviewing cryptographic environments is inventory and discovery. This is because the inventory and discovery phase helps auditors to identify and document the scope, objectives, and approach of the audit, as well as the cryptographic assets, systems, processes, and stakeholders involved in the cryptographic environment. The inventory and discovery phase also helps auditors to assess the maturity and effectiveness of the cryptographic governance and management within the organization. The other phases are not the first phase of the ISACA framework for auditors reviewing cryptographic environments, but rather follow after the inventory and discovery phase, such as evaluation of implementation details (A), hands-on testing (B), or risk-based shakeout C.

QUESTION 28
Which of the following is the BEST indication that an organization's vulnerability management process is operating effectively?

A. Remediation efforts are communicated to management
B. The vulnerability program is formally approved
C. The vulnerability program is reviewed annually.
D. Remediation efforts are prioritized.

Correct Answer: D
Section:
Explanation:
The BEST indication that an organization's vulnerability management process is operating effectively is that remediation efforts are prioritized. This is because prioritizing remediation efforts helps to ensure that the most critical and urgent vulnerabilities are addressed first, based on their severity, impact, and exploitability. Prioritizing remediation efforts also helps to optimize the use of resources and time for mitigating vulnerabilities and reducing risks. The other options are not as indicative of an effective vulnerability management process, because they either involve communicating (A), approving (B), or reviewing C aspects that are not directly related to remediating vulnerabilities.

QUESTION 29
Which of the following backup procedure would only copy files that have changed since the last backup was made?

A. Incremental backup
B. Daily backup
C. Differential backup
D. Full backup

Correct Answer: A
Section:
Explanation:
The backup procedure that would only copy files that have changed since the last backup was made is an incremental backup. This is because an incremental backup is a type of backup that only copies the files that have been created or modified since the previous backup, whether it was a full or an incremental backup. An incremental backup helps to reduce the backup time and storage space, as well as the recovery time, as only the changed files need to be restored. The other options are not backup procedures that would only copy files that have changed since the last backup was made, but rather different types of backup procedures that copy files based on different criteria, such as daily backup (B), differential backup C, or full backup (D).

QUESTION 30
An information security procedure indicates a requirement to sandbox emails. What does this requirement mean?

A. Ensure the emails are encrypted and provide nonrepudiation.
B. Provide a backup of emails in the event of a disaster
C. isolate the emails and test for malicious content
D. Guarantee rapid email delivery through firewalls.

Correct Answer: C
Section:
Explanation:
An information security procedure that indicates a requirement to sandbox emails means that the emails need to be isolated and tested for malicious content. This is because sandboxing is a technique that creates a virtual or isolated environment, where suspicious or untrusted emails can be executed or analyzed without affecting the rest of the system or network. Sandboxing helps to detect and prevent malware, phishing, or spam attacks that may be embedded in emails, and protect the users and the organization from potential harm. The other options are not what sandboxing emails means, but rather different concepts or techniques that are related to information security, such as encryption and nonrepudiation (A), backup and recovery (B), or firewall and delivery (D).

QUESTION 31
Which of the following features of continuous auditing provides the BEST level of assurance over traditional sampling?

A. Reports can be generated more frequently for management.
B. Automated tools provide more reliability than an auditors personal judgment
C. Voluminous dale can be analyzed at a high speed to show relevant patterns.
D. Continuous auditing tools are less complex for auditors to manage.

Correct Answer: C
Section:
Explanation:
The feature of continuous auditing that provides the BEST level of assurance over traditional sampling is that voluminous data can be analyzed at a high speed to show relevant patterns. This is because continuous auditing is a technique that uses automated tools and processes to perform audit activities on a continuous or near-real-time basis, and to analyze large amounts of data from various sources and systems. Continuous auditing helps to provide a higher level of assurance than traditional sampling, by covering the entire population of transactions or events, rather than a subset or sample, and by identifying trends, anomalies, or exceptions that may indicate risks or issues. The other options are not features of continuous auditing that provide the best level of assurance over traditional sampling, but rather different aspects or benefits of continuous auditing, such as reporting frequency (A), reliability (B), or complexity (D).

QUESTION 32
Which process converts extracted information to a format understood by investigators?

A. Reporting
B. Ingestion
C. imaging
D. Filtering

Correct Answer: A
Section:
Explanation:
The process that converts extracted information to a format understood by investigators is reporting. This is because reporting is a technique that involves presenting and communicating the results and findings of an investigation in a clear, concise, and accurate manner, using appropriate formats, such as tables, charts, graphs, etc. Reporting helps to convey the meaning and significance of the extracted information to the investigators, as well as other stakeholders, such as management, auditors, regulators, etc. The other options are not processes that convert extracted information to a format understood by investigators, but rather different techniques that are related to information extraction or analysis, such as ingestion (B), imaging C, or filtering (D).

QUESTION 33
Which of the following is MOST important to verify when reviewing the effectiveness of an organization's identity management program?

A. Processes are approved by the process owner.
B. Processes are aligned with industry best practices.
C. Processes are centralized and standardized.
D. Processes are updated and documented annually.

Correct Answer: B
Section:
Explanation:
The MOST important thing to verify when reviewing the effectiveness of an organization's identity management program is whether the processes are aligned with industry best practices. Identity management is the process of managing the identities and access rights of users across an organization's systems and resources. Industry best practices provide guidelines and standards for how to implement identity management in a secure, efficient, and compliant manner.

QUESTION 34
he MOST significant limitation of vulnerability scanning is the fact that modern scanners only detect:

A. common vulnerabilities.
B. unknown vulnerabilities.
C. known vulnerabilities.
D. zero-day vulnerabilities.

Correct Answer: C
Section:
Explanation:
The MOST significant limitation of vulnerability scanning is the fact that modern scanners only detect known vulnerabilities. This is because vulnerability scanners rely on databases or repositories of known vulnerabilities, such as CVE (Common Vulnerabilities and Exposures), to compare and identify the weaknesses or flaws in systems or applications. Vulnerability scanners cannot detect unknown vulnerabilities, such as zero-day vulnerabilities, that have not been reported or disclosed yet, and may be exploited by attackers before they are patched or fixed. The other options are not the most significant limitation of vulnerability scanning, because they either involve detecting common (A), unknown (B), or zero-day (D) vulnerabilities, which are not the capabilities or limitations of modern scanners.

QUESTION 35
Which of the following is a passive activity that could be used by an attacker during reconnaissance to gather information about an organization?

A. Using open source discovery
B. Scanning the network perimeter
C. Social engineering
D. Crafting counterfeit websites

Correct Answer: A
Section:
Explanation:
A passive activity that could be used by an attacker during reconnaissance to gather information about an organization is using open source discovery. This is because open source discovery is a technique that involves collecting and analyzing publicly available information about an organization, such as its website, social media, press releases, annual reports, etc. Open source discovery does not require any direct interaction or communication with the target organization or its systems or network, and therefore does not generate any traffic or alerts that could be detected by the organization's security controls. The other options are not passive activities that could be used by an attacker during reconnaissance to gather information about an organization, but rather active activities that involve direct or indirect interaction or communication with the target organization or its systems or network, such as scanning the network perimeter (B), social engineering C, or crafting counterfeit websites (D).

QUESTION 36
Which of the following is the GREATEST advantage of using a virtual private network (VPN) over dedicated circuits and dial-in servers?

A. It is more secure
B. It is more reliable
C. It is higher speed.
D. It is more cost effective.

Correct Answer: D
Section:
Explanation:
The GREATEST advantage of using a virtual private network (VPN) over dedicated circuits and dial-in servers is that it is more cost effective. This is because a VPN is a technology that creates a secure and encrypted connection between a client and a server over an existing public network, such as the Internet. A VPN reduces the cost of establishing and maintaining a secure communication channel, as it does not require any additional hardware, software, or infrastructure, unlike dedicated circuits and dial-in servers, which require dedicated lines, modems, routers, switches, etc. The other options are not the greatest advantage of using a VPN over dedicated circuits and dial-in servers, because they either involve security (A), reliability (B), or speed C aspects that may not be significantly different or better than dedicated circuits and dial-in servers.

QUESTION 37
Using digital evidence to provide validation that an attack has actually occurred is an example of;

A. computer forensic
B. extraction.
C. identification.
D. data acquisition.

Correct Answer: A
Section:
Explanation:
Using digital evidence to provide validation that an attack has actually occurred is an example of computer forensics. This is because computer forensics is a discipline that involves the identification, preservation,

analysis, and presentation of digital evidence from various sources, such as computers, networks, mobile devices, etc., to support investigations of cyber incidents or crimes. Computer forensics helps to provide validation that an attack has actually occurred, by examining the digital traces or artifacts left by the attackers on the compromised systems or devices, and by reconstructing the sequence and timeline of events that led to the attack. The other options are not examples of using digital evidence to provide validation that an attack has actually occurred, but rather different techniques or processes that are related to computer forensics, such as extraction (B), identification C, or data acquisition (D).

QUESTION 38
What is the FIRST activity associated with a successful cyber attack?

A. Exploitation
B. Reconnaissance
C. Maintaining a presence
D. Creating attack tools

Correct Answer: B
Section:
Explanation:
The FIRST activity associated with a successful cyber attack is reconnaissance. This is because reconnaissance is a phase of the cyber attack lifecycle that involves gathering information about the target organization or system, such as its network topology, IP addresses, open ports, services, vulnerabilities, etc. Reconnaissance helps to identify potential entry points and weaknesses that can be exploited by the attackers in later phases of the attack. The other options are not the first activity associated with a successful cyber attack, but rather follow after reconnaissance in the cyber attack lifecycle, such as exploitation (A), maintaining a presence C, or creating attack tools (D).

QUESTION 39
Which of the following BEST facilitates the development of metrics for repotting to senior management on vulnerability management efforts?

A. Reviewing business impact analysis (BIA) results
B. Regularly benchmarking the number of new vulnerabilities identified with industry peers
C. Tracking vulnerabilities and the remediation efforts to mitigate them
D. Monitoring the frequency of vulnerability assessments using automated scans

Correct Answer: C
Section:
Explanation:
The BEST feature that facilitates the development of metrics for reporting to senior management on vulnerability management efforts is tracking vulnerabilities and the remediation efforts to mitigate them. This is because tracking vulnerabilities and remediation efforts helps to measure and monitor the performance and effectiveness of vulnerability management efforts, by providing quantifiable and objective data on the number, severity, impact, status, and resolution time of vulnerabilities. Tracking vulnerabilities and remediation efforts also helps to identify and communicate any gaps or issues in vulnerability management efforts to senior management and other stakeholders. The other options are not features that facilitate the development of metrics for reporting to senior management on vulnerability management efforts, but rather different aspects or factors that affect vulnerability management efforts, such as reviewing business impact analysis (BIA) results (A), benchmarking with industry peers (B), or monitoring the frequency of vulnerability assessments (D).