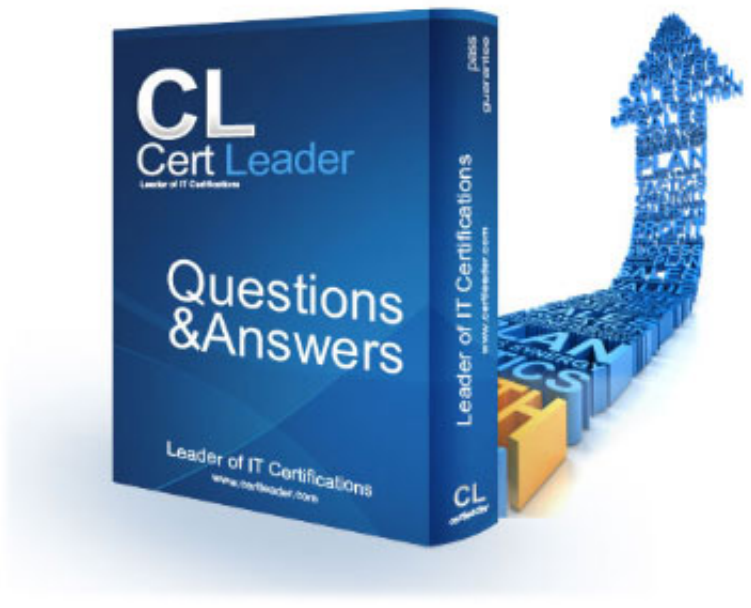
CISSP Dumps

Certified Information Systems Security Professional (CISSP)

https://www.certleader.com/CISSP-dumps.html



NEW QUESTION 1
- (Exam Topic 1)
A company whose Information Technology (IT) services are being delivered from a Tier 4 data center, is preparing a companywide Business Continuity Planning (BCP). Which of the following failures should the IT manager be concerned with?

A. Application
B. Storage
C. Power
D. Network

Answer: C

NEW QUESTION 2
- (Exam Topic 1)
When assessing an organization's security policy according to standards established by the International Organization for Standardization (ISO) 27001 and 27002, when can management responsibilities be defined?

A. Only when assets are clearly defined
B. Only when standards are defined
C. Only when controls are put in place
D. Only procedures are defined

Answer: A

NEW QUESTION 3
- (Exam Topic 1)
All of the following items should be included in a Business Impact Analysis (BIA) questionnaire EXCEPT questions that

A. determine the risk of a business interruption occurring
B. determine the technological dependence of the business processes
C. Identify the operational impacts of a business interruption
D. Identify the financial impacts of a business interruption

Answer: B

NEW QUESTION 4
- (Exam Topic 2)
Which of the following BEST describes the responsibilities of a data owner?

A. Ensuring quality and validation through periodic audits for ongoing data integrity
B. Maintaining fundamental data availability, including data storage and archiving
C. Ensuring accessibility to appropriate users, maintaining appropriate levels of data security
D. Determining the impact the information has on the mission of the organization

Answer: C

NEW QUESTION 5
- (Exam Topic 3)
Which of the following mobile code security models relies only on trust?

A. Code signing
B. Class authentication
C. Sandboxing
D. Type safety

Answer: A

NEW QUESTION 6
- (Exam Topic 3)
Which security service is served by the process of encryption plaintext with the sender's private key and decrypting cipher text with the sender's public key?

A. Confidentiality
B. Integrity
C. Identification
D. Availability

Answer: A

NEW QUESTION 7
- (Exam Topic 3)
Who in the organization is accountable for classification of data information assets?

A. Data owner
B. Data architect
C. Chief Information Security Officer (CISO)

D. Chief Information Officer (CIO)

Answer: A

NEW QUESTION 8
- (Exam Topic 3)
What is the second phase of Public Key Infrastructure (PKI) key/certificate life-cycle management?

A. Implementation Phase
B. Initialization Phase
C. Cancellation Phase
D. Issued Phase

Answer: D

NEW QUESTION 9
- (Exam Topic 4)
Which of the following operates at the Network Layer of the Open System Interconnection (OSI) model?

A. Packet filtering
B. Port services filtering
C. Content filtering
D. Application access control

Answer: A

NEW QUESTION 10
- (Exam Topic 4)
In a Transmission Control Protocol/Internet Protocol (TCP/IP) stack, which layer is responsible for negotiating and establishing a connection with another node?

A. Transport layer
B. Application layer
C. Network layer
D. Session layer

Answer: A

NEW QUESTION 10
- (Exam Topic 5)
Users require access rights that allow them to view the average salary of groups of employees. Which control would prevent the users from obtaining an individual employee's salary?

A. Limit access to predefined queries
B. Segregate the database into a small number of partitions each with a separate security level
C. Implement Role Based Access Control (RBAC)
D. Reduce the number of people who have access to the system for statistical purposes

Answer: C

NEW QUESTION 13
- (Exam Topic 6)
Which of the following could cause a Denial of Service (DoS) against an authentication system?

A. Encryption of audit logs
B. No archiving of audit logs
C. Hashing of audit logs
D. Remote access audit logs

Answer: D

NEW QUESTION 15
- (Exam Topic 6)
A Virtual Machine (VM) environment has five guest Operating Systems (OS) and provides strong isolation. What MUST an administrator review to audit a user's access to data files?

A. Host VM monitor audit logs
B. Guest OS access controls
C. Host VM access controls
D. Guest OS audit logs

Answer: A

NEW QUESTION 16
- (Exam Topic 6)
In which of the following programs is it MOST important to include the collection of security process data?

A. Quarterly access reviews
B. Security continuous monitoring
C. Business continuity testing
D. Annual security training

Answer: A

NEW QUESTION 17
- (Exam Topic 7)
Recovery strategies of a Disaster Recovery planning (DRIP) MUST be aligned with which of the following?

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

NEW QUESTION 18
- (Exam Topic 7)
Which of the following is a PRIMARY advantage of using a third-party identity service?

A. Consolidation of multiple providers
B. Directory synchronization
C. Web based logon
D. Automated account management

Answer: D

NEW QUESTION 23
- (Exam Topic 7)
What is the MOST important step during forensic analysis when trying to learn the purpose of an unknown application?

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

NEW QUESTION 24
- (Exam Topic 7)
With what frequency should monitoring of a control occur when implementing Information Security Continuous Monitoring (ISCM) solutions?

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: B

NEW QUESTION 27
- (Exam Topic 7)
What is the PRIMARY reason for implementing change management?

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

NEW QUESTION 30
- (Exam Topic 8)
Which of the following is the BEST method to prevent malware from being introduced into a production environment?

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

NEW QUESTION 34
- (Exam Topic 8)

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?

A. Least privilege
B. Privilege escalation
C. Defense in depth
D. Privilege bracketing

Answer: A

NEW QUESTION 39
- (Exam Topic 8)
Which of the following is the PRIMARY risk with using open source software in a commercial software construction?

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: D

NEW QUESTION 40
- (Exam Topic 8)
The configuration management and control task of the certification and accreditation process is incorporated in which phase of the System Development Life Cycle (SDLC)?

A. System acquisition and development
B. System operations and maintenance
C. System initiation
D. System implementation

Answer: A

Explanation:
Reference https://online.concordiA.edu/computer-science/system-development-life-cycle-phases/

NEW QUESTION 41
- (Exam Topic 9)
The three PRIMARY requirements for a penetration test are

A. A defined goal, limited time period, and approval of management
B. A general objective, unlimited time, and approval of the network administrator
C. An objective statement, disclosed methodology, and fixed cost
D. A stated objective, liability waiver, and disclosed methodology

Answer: A

NEW QUESTION 46
- (Exam Topic 9)
Internet Protocol (IP) source address spoofing is used to defeat

A. address-based authentication.
B. Address Resolution Protocol (ARP).
C. Reverse Address Resolution Protocol (RARP).
D. Transmission Control Protocol (TCP) hijacking.

Answer: A

NEW QUESTION 51
- (Exam Topic 9)
Which of the following is ensured when hashing files during chain of custody handling?

A. Availability
B. Accountability
C. Integrity
D. Non-repudiation

Answer: C

NEW QUESTION 55
- (Exam Topic 9)
Which of the following MUST be part of a contract to support electronic discovery of data stored in a cloud environment?

A. Integration with organizational directory services for authentication
B. Tokenization of data
C. Accommodation of hybrid deployment models
D. Identification of data location

Answer: D

NEW QUESTION 59
- (Exam Topic 9)
To prevent inadvertent disclosure of restricted information, which of the following would be the LEAST effective process for eliminating data prior to the media being discarded?

A. Multiple-pass overwriting
B. Degaussing
C. High-level formatting
D. Physical destruction

Answer: C

NEW QUESTION 62
- (Exam Topic 9)
A vulnerability test on an Information System (IS) is conducted to

A. exploit security weaknesses in the IS.
B. measure system performance on systems with weak security controls.
C. evaluate the effectiveness of security controls.
D. prepare for Disaster Recovery (DR) planning.

Answer: C

NEW QUESTION 67
- (Exam Topic 9)
The key benefits of a signed and encrypted e-mail include

A. confidentiality, authentication, and authorization.
B. confidentiality, non-repudiation, and authentication.
C. non-repudiation, authorization, and authentication.
D. non-repudiation, confidentiality, and authorization.

Answer: B

NEW QUESTION 70
- (Exam Topic 9)
An internal Service Level Agreement (SLA) covering security is signed by senior managers and is in place. When should compliance to the SLA be reviewed to ensure that a good security posture is being delivered?

A. As part of the SLA renewal process
B. Prior to a planned security audit
C. Immediately after a security breach
D. At regularly scheduled meetings

Answer: D

NEW QUESTION 73
- (Exam Topic 9)
Why is a system's criticality classification important in large organizations?

A. It provides for proper prioritization and scheduling of security and maintenance tasks.
B. It reduces critical system support workload and reduces the time required to apply patches.
C. It allows for clear systems status communications to executive management.
D. It provides for easier determination of ownership, reducing confusion as to the status of the asset.

Answer: A

NEW QUESTION 78
- (Exam Topic 9)
Which one of the following transmission media is MOST effective in preventing data interception?

A. Microwave
B. Twisted-pair
C. Fiber optic
D. Coaxial cable

Answer: C

NEW QUESTION 82
- (Exam Topic 9)
An advantage of link encryption in a communications network is that it

A. makes key management and distribution easier.

B. protects data from start to finish through the entire network.
C. improves the efficiency of the transmission.
D. encrypts all information, including headers and routing information.

Answer: D

NEW QUESTION 83
- (Exam Topic 9)
Which of the following is an attacker MOST likely to target to gain privileged access to a system?

A. Programs that write to system resources
B. Programs that write to user directories
C. Log files containing sensitive information
D. Log files containing system calls

Answer: A

NEW QUESTION 85
- (Exam Topic 9)
Which of the following is the best practice for testing a Business Continuity Plan (BCP)?

A. Test before the IT Audit
B. Test when environment changes
C. Test after installation of security patches
D. Test after implementation of system patches

Answer: B

NEW QUESTION 89
- (Exam Topic 9)
Which of the following is an essential element of a privileged identity lifecycle management?

A. Regularly perform account re-validation and approval
B. Account provisioning based on multi-factor authentication
C. Frequently review performed activities and request justification
D. Account information to be provided by supervisor or line manager

Answer: A

NEW QUESTION 93
- (Exam Topic 9)
A practice that permits the owner of a data object to grant other users access to that object would usually provide

A. Mandatory Access Control (MAC).
B. owner-administered control.
C. owner-dependent access control.
D. Discretionary Access Control (DAC).

Answer: D

NEW QUESTION 98
- (Exam Topic 9)
An organization is selecting a service provider to assist in the consolidation of multiple computing sites including development, implementation and ongoing support of various computer systems. Which of the following MUST be verified by the Information Security Department?

A. The service provider's policies are consistent with ISO/IEC27001 and there is evidence that the service provider is following those policies.
B. The service provider will segregate the data within its systems and ensure that each region's policies are met.
C. The service provider will impose controls and protections that meet or exceed the current systemscontrols and produce audit logs as verification.
D. The service provider's policies can meet the requirements imposed by the new environment even if they differ from the organization's current policies.

Answer: D

NEW QUESTION 101
- (Exam Topic 9)
Which of the following is a security feature of Global Systems for Mobile Communications (GSM)?

A. It uses a Subscriber Identity Module (SIM) for authentication.
B. It uses encrypting techniques for all communications.
C. The radio spectrum is divided with multiple frequency carriers.
D. The signal is difficult to read as it provides end-to-end encryption.

Answer: A

NEW QUESTION 105
- (Exam Topic 9)

Which of the following assessment metrics is BEST used to understand a system's vulnerability to potential exploits?

A. Determining the probability that the system functions safely during any time period
B. Quantifying the system's available services
C. Identifying the number of security flaws within the system
D. Measuring the system's integrity in the presence of failure

Answer: C

NEW QUESTION 106
- (Exam Topic 9)
An auditor carrying out a compliance audit requests passwords that are encrypted in the system to verify that the passwords are compliant with policy. Which of the following is the BEST response to the auditor?

A. Provide the encrypted passwords and analysis tools to the auditor for analysis.
B. Analyze the encrypted passwords for the auditor and show them the results.
C. Demonstrate that non-compliant passwords cannot be created in the system.
D. Demonstrate that non-compliant passwords cannot be encrypted in the system.

Answer: C

NEW QUESTION 109
- (Exam Topic 9)
Which of the following statements is TRUE for point-to-point microwave transmissions?

A. They are not subject to interception due to encryption.
B. Interception only depends on signal strength.
C. They are too highly multiplexed for meaningful interception.
D. They are subject to interception by an antenna within proximity.

Answer: D

NEW QUESTION 111
- (Exam Topic 9)
Which one of the following describes granularity?

A. Maximum number of entries available in an Access Control List (ACL)
B. Fineness to which a trusted system can authenticate users
C. Number of violations divided by the number of total accesses
D. Fineness to which an access control system can be adjusted

Answer: D

NEW QUESTION 115
- (Exam Topic 9)
What would be the PRIMARY concern when designing and coordinating a security assessment for an Automatic Teller Machine (ATM) system?

A. Physical access to the electronic hardware
B. Regularly scheduled maintenance process
C. Availability of the network connection
D. Processing delays

Answer: A

NEW QUESTION 117
- (Exam Topic 9)
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?

A. Implement packet filtering on the network firewalls
B. Require strong authentication for administrators
C. Install Host Based Intrusion Detection Systems (HIDS)
D. Implement logical network segmentation at the switches

Answer: D

NEW QUESTION 120
- (Exam Topic 9)
In Business Continuity Planning (BCP), what is the importance of documenting business processes?

A. Provides senior management with decision-making tools
B. Establishes and adopts ongoing testing and maintenance strategies
C. Defines who will perform which functions during a disaster or emergency
D. Provides an understanding of the organization's interdependencies

Answer: D

NEW QUESTION 124
- (Exam Topic 9)
A security consultant has been asked to research an organization's legal obligations to protect privacy-related information. What kind of reading material is MOST relevant to this project?

A. The organization's current security policies concerning privacy issues
B. Privacy-related regulations enforced by governing bodies applicable to the organization
C. Privacy best practices published by recognized security standards organizations
D. Organizational procedures designed to protect privacy information

Answer: B

NEW QUESTION 126
- (Exam Topic 9)
Which of the following is the FIRST step of a penetration test plan?

A. Analyzing a network diagram of the target network
B. Notifying the company's customers
C. Obtaining the approval of the company's management
D. Scheduling the penetration test during a period of least impact

Answer: C

NEW QUESTION 131
- (Exam Topic 9)
Which one of the following is a fundamental objective in handling an incident?

A. To restore control of the affected systems
B. To confiscate the suspect's computers
C. To prosecute the attacker
D. To perform full backups of the system

Answer: A

NEW QUESTION 135
- (Exam Topic 9)
When transmitting information over public networks, the decision to encrypt it should be based on

A. the estimated monetary value of the information.
B. whether there are transient nodes relaying the transmission.
C. the level of confidentiality of the information.
D. the volume of the information.

Answer: C

NEW QUESTION 136
- (Exam Topic 9)
Alternate encoding such as hexadecimal representations is MOST often observed in which of the following forms of attack?

A. Smurf
B. Rootkit exploit
C. Denial of Service (DoS)
D. Cross site scripting (XSS)

Answer: D

NEW QUESTION 139
- (Exam Topic 9)
Which of the following would be the FIRST step to take when implementing a patch management program?

A. Perform automatic deployment of patches.
B. Monitor for vulnerabilities and threats.
C. Prioritize vulnerability remediation.
D. Create a system inventory.

Answer: D

NEW QUESTION 140
- (Exam Topic 9)
In a basic SYN flood attack, what is the attacker attempting to achieve?

A. Exceed the threshold limit of the connection queue for a given service
B. Set the threshold to zero for a given service
C. Cause the buffer to overflow, allowing root access
D. Flush the register stack, allowing hijacking of the root account

Answer:

A

NEW QUESTION 142
- (Exam Topic 9)
Which of the following is a network intrusion detection technique?

A. Statistical anomaly
B. Perimeter intrusion
C. Port scanning
D. Network spoofing

Answer: A

NEW QUESTION 144
- (Exam Topic 9)
When implementing controls in a heterogeneous end-point network for an organization, it is critical that

A. hosts are able to establish network communications.
B. users can make modifications to their security software configurations.
C. common software security components be implemented across all hosts.
D. firewalls running on each host are fully customizable by the user.

Answer: C

NEW QUESTION 149
- (Exam Topic 9)
When designing a networked Information System (IS) where there will be several different types of individual access, what is the FIRST step that should be taken to ensure all access control requirements are addressed?

A. Create a user profile.
B. Create a user access matrix.
C. Develop an Access Control List (ACL).
D. Develop a Role Based Access Control (RBAC) list.

Answer: B

NEW QUESTION 151
- (Exam Topic 9)
When constructing an Information Protection Policy (IPP), it is important that the stated rules are necessary, adequate, and

A. flexible.
B. confidential.
C. focused.
D. achievable.

Answer: D

NEW QUESTION 155
- (Exam Topic 9)
Which of the following is the BEST mitigation from phishing attacks?

A. Network activity monitoring
B. Security awareness training
C. Corporate policy and procedures
D. Strong file and directory permissions

Answer: B

NEW QUESTION 159
- (Exam Topic 9)
An organization is designing a large enterprise-wide document repository system. They plan to have several different classification level areas with increasing levels of controls. The BEST way to ensure document confidentiality in the repository is to

A. encrypt the contents of the repository and document any exceptions to that requirement.
B. utilize Intrusion Detection System (IDS) set drop connections if too many requests for documents are detected.
C. keep individuals with access to high security areas from saving those documents into lower security areas.
D. require individuals with access to the system to sign Non-Disclosure Agreements (NDA).

Answer: C

NEW QUESTION 161
- (Exam Topic 9)
A system has been scanned for vulnerabilities and has been found to contain a number of communication ports that have been opened without authority. To which of the following might this system have been subjected?

A. Trojan horse

B. Denial of Service (DoS)
C. Spoofing
D. Man-in-the-Middle (MITM)

Answer: A

NEW QUESTION 164
- (Exam Topic 9)
Which of the following does Temporal Key Integrity Protocol (TKIP) support?

A. Multicast and broadcast messages
B. Coordination of IEEE 802.11 protocols
C. Wired Equivalent Privacy (WEP) systems
D. Synchronization of multiple devices

Answer: C

NEW QUESTION 165
- (Exam Topic 9)
Why must all users be positively identified prior to using multi-user computers?

A. To provide access to system privileges
B. To provide access to the operating system
C. To ensure that unauthorized persons cannot access the computers
D. To ensure that management knows what users are currently logged on

Answer: C

NEW QUESTION 166
- (Exam Topic 9)
An engineer in a software company has created a virus creation tool. The tool can generate thousands of polymorphic viruses. The engineer is planning to use the tool in a controlled environment to test the company's next generation virus scanning software. Which would BEST describe the behavior of the engineer and why?

A. The behavior is ethical because the tool will be used to create a better virus scanner.
B. The behavior is ethical because any experienced programmer could create such a tool.
C. The behavior is not ethical because creating any kind of virus is bad.
D. The behavior is not ethical because such a tool could be leaked on the Internet.

Answer: A

NEW QUESTION 171
- (Exam Topic 9)
Which of the following Disaster Recovery (DR) sites is the MOST difficult to test?

A. Hot site
B. Cold site
C. Warm site
D. Mobile site

Answer: B

NEW QUESTION 176
- (Exam Topic 9)
Which of the following statements is TRUE of black box testing?

A. Only the functional specifications are known to the test planner.
B. Only the source code and the design documents are known to the test planner.
C. Only the source code and functional specifications are known to the test planner.
D. Only the design documents and the functional specifications are known to the test planner.

Answer: A

NEW QUESTION 177
- (Exam Topic 9)
Two companies wish to share electronic inventory and purchase orders in a supplier and client relationship. What is the BEST security solution for them?

A. Write a Service Level Agreement (SLA) for the two companies.
B. Set up a Virtual Private Network (VPN) between the two companies.
C. Configure a firewall at the perimeter of each of the two companies.
D. Establish a File Transfer Protocol (FTP) connection between the two companies.

Answer: B

NEW QUESTION 180
- (Exam Topic 9)

Which Hyper Text Markup Language 5 (HTML5) option presents a security challenge for network data leakage prevention and/or monitoring?

A. Cross Origin Resource Sharing (CORS)
B. WebSockets
C. Document Object Model (DOM) trees
D. Web Interface Definition Language (IDL)

Answer: B

NEW QUESTION 182
- (Exam Topic 9)
What should be the INITIAL response to Intrusion Detection System/Intrusion Prevention System (IDS/IPS) alerts?

A. Ensure that the Incident Response Plan is available and current.
B. Determine the traffic's initial source and block the appropriate port.
C. Disable or disconnect suspected target and source systems.
D. Verify the threat and determine the scope of the attack.

Answer: D

NEW QUESTION 186
- (Exam Topic 9)
At a MINIMUM, a formal review of any Disaster Recovery Plan (DRP) should be conducted

A. monthly.
B. quarterly.
C. annually.
D. bi-annually.

Answer: C

NEW QUESTION 189
- (Exam Topic 10)
Which of the following is the BEST reason to review audit logs periodically?

A. Verify they are operating properly
B. Monitor employee productivity
C. Identify anomalies in use patterns
D. Meet compliance regulations

Answer: C

NEW QUESTION 194
- (Exam Topic 10)
Which of the following is an example of two-factor authentication?

A. Retina scan and a palm print
B. Fingerprint and a smart card
C. Magnetic stripe card and an ID badge
D. Password and Completely Automated Public Turing test to tell Computers and Humans Apart(CAPTCHA)

Answer: B

NEW QUESTION 199
- (Exam Topic 10)
When dealing with compliance with the Payment Card Industry-Data Security Standard (PCI-DSS), an organization that shares card holder information with a service provider MUST do which of the following?

A. Perform a service provider PCI-DSS assessment on a yearly basis.
B. Validate the service provider's PCI-DSS compliance status on a regular basis.
C. Validate that the service providers security policies are in alignment with those of the organization.
D. Ensure that the service provider updates and tests its Disaster Recovery Plan (DRP) on a yearly basis.

Answer: B

NEW QUESTION 201
- (Exam Topic 10)
An online retail company has formulated a record retention schedule for customer transactions. Which of the following is a valid reason a customer transaction is kept beyond the retention schedule?

A. Pending legal hold
B. Long term data mining needs
C. Customer makes request to retain
D. Useful for future business initiatives

Answer: A

NEW QUESTION 202
- (Exam Topic 10)
Refer to the information below to answer the question.
A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns.
In addition to web browsers, what PRIMARY areas need to be addressed concerning mobile code used for malicious purposes?

A. Text editors, database, and Internet phone applications
B. Email, presentation, and database applications
C. Image libraries, presentation and spreadsheet applications
D. Email, media players, and instant messaging applications

Answer: D

NEW QUESTION 207
- (Exam Topic 10)
Which item below is a federated identity standard?

A. 802.11i
B. Kerberos
C. Lightweight Directory Access Protocol (LDAP)
D. Security Assertion Markup Language (SAML)

Answer: D

NEW QUESTION 209
- (Exam Topic 10)
Which of the following assures that rules are followed in an identity management architecture?

A. Policy database
B. Digital signature
C. Policy decision point
D. Policy enforcement point

Answer: D

NEW QUESTION 214
- (Exam Topic 10)
Which of the following is the MOST difficult to enforce when using cloud computing?

A. Data access
B. Data backup
C. Data recovery
D. Data disposal

Answer: D

NEW QUESTION 218
- (Exam Topic 10)
Multi-Factor Authentication (MFA) is necessary in many systems given common types of password attacks. Which of the following is a correct list of password attacks?

A. Masquerading, salami, malware, polymorphism
B. Brute force, dictionary, phishing, keylogger
C. Zeus, netbus, rabbit, turtle
D. Token, biometrics, IDS, DLP

Answer: B

NEW QUESTION 219
- (Exam Topic 10)
Which of the following BEST mitigates a replay attack against a system using identity federation and Security Assertion Markup Language (SAML) implementation?

A. Two-factor authentication
B. Digital certificates and hardware tokens
C. Timed sessions and Secure Socket Layer (SSL)
D. Passwords with alpha-numeric and special characters

Answer: C

NEW QUESTION 224
- (Exam Topic 10)
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
What MUST the access control logs contain in addition to the identifier?

A. Time of the access
B. Security classification
C. Denied access attempts
D. Associated clearance

Answer: A

NEW QUESTION 229
- (Exam Topic 10)
A security manager has noticed an inconsistent application of server security controls resulting in vulnerabilities on critical systems. What is the MOST likely cause of this issue?

A. A lack of baseline standards
B. Improper documentation of security guidelines
C. A poorly designed security policy communication program
D. Host-based Intrusion Prevention System (HIPS) policies are ineffective

Answer: A

NEW QUESTION 233
- (Exam Topic 10)
Refer to the information below to answer the question.
During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.
If the intrusion causes the system processes to hang, which of the following has been affected?

A. System integrity
B. System availability
C. System confidentiality
D. System auditability

Answer: B

NEW QUESTION 235
- (Exam Topic 10)
Which of the following is a MAJOR consideration in implementing a Voice over IP (VoIP) network?

A. Use of a unified messaging.
B. Use of separation for the voice network.
C. Use of Network Access Control (NAC) on switches.
D. Use of Request for Comments (RFC) 1918 addressing.

Answer: B

NEW QUESTION 237
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.
Which of the following will indicate where the IT budget is BEST allocated during this time?

A. Policies
B. Frameworks
C. Metrics
D. Guidelines

Answer: C

NEW QUESTION 242
- (Exam Topic 10)
Refer to the information below to answer the question.
A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns.
In the plan, what is the BEST approach to mitigate future internal client-based attacks?

A. Block all client side web exploits at the perimeter.
B. Remove all non-essential client-side web services from the network.
C. Screen for harmful exploits of client-side services before implementation.
D. Harden the client image before deployment.

Answer: D

NEW QUESTION 244
- (Exam Topic 10)
When implementing a secure wireless network, which of the following supports authentication and authorization for individual client endpoints?

A. Temporal Key Integrity Protocol (TKIP)

B. Wi-Fi Protected Access (WPA) Pre-Shared Key (PSK)
C. Wi-Fi Protected Access 2 (WPA2) Enterprise
D. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)

Answer: C

NEW QUESTION 245
- (Exam Topic 10)
Refer to the information below to answer the question.
In a Multilevel Security (MLS) system, the following sensitivity labels are used in increasing levels of sensitivity: restricted, confidential, secret, top secret. Table A lists the clearance levels for four users, while Table B lists the security classes of four different files.

Table A

User	Clearance Level
A	Restricted
B	Confidential
C	Secret
D	Top Secret

Table B

Files	Security Class
1	Restricted
2	Confidential
3	Secret
4	Top Secret

In a Bell-LaPadula system, which user cannot write to File 3?

A. User A
B. User B
C. User C
D. User D

Answer: D

NEW QUESTION 250
- (Exam Topic 10)
Which of the following is a BEST practice when traveling internationally with laptops containing Personally Identifiable Information (PII)?

A. Use a thumb drive to transfer information from a foreign computer.
B. Do not take unnecessary information, including sensitive information.
C. Connect the laptop only to well-known networks like the hotel or public Internet cafes.
D. Request international points of contact help scan the laptop on arrival to ensure it is protected.

Answer: B

NEW QUESTION 255
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
Which of the following is considered the MOST important priority for the information security officer?

A. Formal acceptance of the security strategy
B. Disciplinary actions taken against unethical behavior
C. Development of an awareness program for new employees
D. Audit of all organization system configurations for faults

Answer: A

NEW QUESTION 258
- (Exam Topic 10)
Which of the following BEST describes Recovery Time Objective (RTO)?

A. Time of data validation after disaster
B. Time of data restoration from backup after disaster
C. Time of application resumption after disaster
D. Time of application verification after disaster

Answer: C

NEW QUESTION 262
- (Exam Topic 10)
What is the BEST method to detect the most common improper initialization problems in programming languages?

A. Use and specify a strong character encoding.
B. Use automated static analysis tools that target this type of weakness.
C. Perform input validation on any numeric inputs by assuring that they are within the expected range.
D. Use data flow analysis to minimize the number of false positives.

Answer: B

NEW QUESTION 267
- (Exam Topic 10)
Which of the following problems is not addressed by using OAuth (Open Standard to Authorization) 2.0 to integrate a third-party identity provider for a service?

A. Resource Servers are required to use passwords to authenticate end users.
B. Revocation of access of some users of the third party instead of all the users from the third party.
C. Compromise of the third party means compromise of all the users in the service.
D. Guest users need to authenticate with the third party identity provider.

Answer: C

NEW QUESTION 268
- (Exam Topic 10)
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
Which of the following BEST describes the access control methodology used?

A. Least privilege
B. Lattice Based Access Control (LBAC)
C. Role Based Access Control (RBAC)
D. Lightweight Directory Access Control (LDAP)

Answer: C

NEW QUESTION 272
- (Exam Topic 10)
Host-Based Intrusion Protection (HIPS) systems are often deployed in monitoring or learning mode during their initial implementation. What is the objective of starting in this mode?

A. Automatically create exceptions for specific actions or files
B. Determine which files are unsafe to access and blacklist them
C. Automatically whitelist actions or files known to the system
D. Build a baseline of normal or safe system events for review

Answer: D

NEW QUESTION 275
- (Exam Topic 10)
The use of proximity card to gain access to a building is an example of what type of security control?

A. Legal
B. Logical
C. Physical
D. Procedural

Answer: C

NEW QUESTION 277
- (Exam Topic 10)
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
In addition to authentication at the start of the user session, best practice would require re-authentication

A. periodically during a session.
B. for each business process.
C. at system sign-off.
D. after a period of inactivity.

Answer: D

NEW QUESTION 278
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
The security program can be considered effective when

A. vulnerabilities are proactively identified.
B. audits are regularly performed and reviewed.
C. backups are regularly performed and validated.
D. risk is lowered to an acceptable level.

Answer: D

NEW QUESTION 279
- (Exam Topic 10)
From a security perspective, which of the following is a best practice to configure a Domain Name Service (DNS) system?

A. Configure secondary servers to use the primary server as a zone forwarder.
B. Block all Transmission Control Protocol (TCP) connections.
C. Disable all recursive queries on the name servers.
D. Limit zone transfers to authorized devices.

Answer: D

NEW QUESTION 281
- (Exam Topic 10)
What is the PRIMARY reason for ethics awareness and related policy implementation?

A. It affects the workflow of an organization.
B. It affects the reputation of an organization.
C. It affects the retention rate of employees.
D. It affects the morale of the employees.

Answer: B

NEW QUESTION 282
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.
When determining appropriate resource allocation, which of the following is MOST important to monitor?

A. Number of system compromises
B. Number of audit findings
C. Number of staff reductions
D. Number of additional assets

Answer: B

NEW QUESTION 286
- (Exam Topic 10)
Which of the following is the PRIMARY benefit of a formalized information classification program?

A. It drives audit processes.
B. It supports risk assessment.
C. It reduces asset vulnerabilities.
D. It minimizes system logging requirements.

Answer: B

NEW QUESTION 289
- (Exam Topic 10)
A risk assessment report recommends upgrading all perimeter firewalls to mitigate a particular finding. Which of the following BEST supports this recommendation?

A. The inherent risk is greater than the residual risk.
B. The Annualized Loss Expectancy (ALE) approaches zero.
C. The expected loss from the risk exceeds mitigation costs.
D. The infrastructure budget can easily cover the upgrade costs.

Answer: C

NEW QUESTION 294
- (Exam Topic 10)
A thorough review of an organization's audit logs finds that a disgruntled network administrator has intercepted emails meant for the Chief Executive Officer (CEO) and changed them before forwarding them to their intended recipient. What type of attack has MOST likely occurred?

A. Spoofing
B. Eavesdropping
C. Man-in-the-middle
D. Denial of service

Answer: C

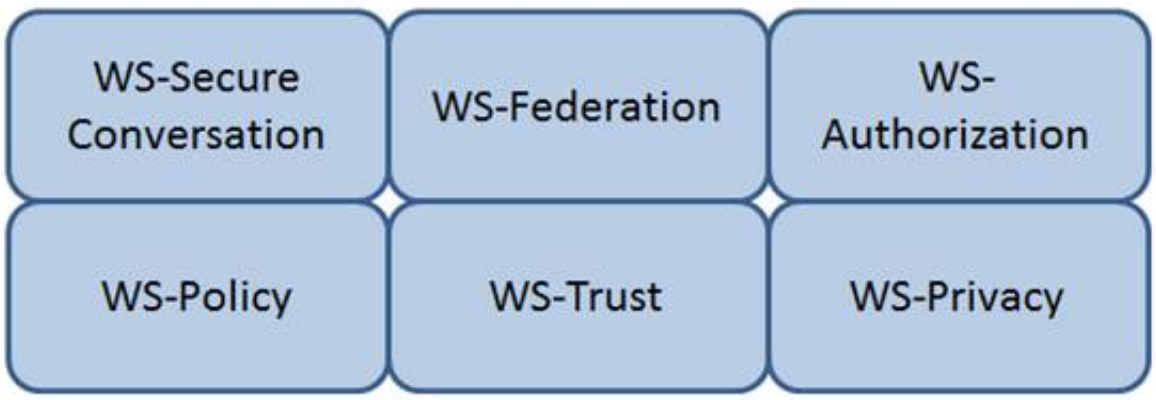
NEW QUESTION 297
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.

The effectiveness of the security program can PRIMARILY be measured through

A. audit findings.
B. risk elimination.
C. audit requirements.
D. customer satisfaction.

Answer: A

NEW QUESTION 299
- (Exam Topic 11)
Which Web Services Security (WS-Security) specification handles the management of security tokens and the underlying policies for granting access? Click on the correct specification in the image below.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
WS-Authorization
Reference: Java Web Services: Up and Running" By Martin Kalin page 228

NEW QUESTION 303
- (Exam Topic 11)
Which of the following BEST describes the purpose of performing security certification?

A. To identify system threats, vulnerabilities, and acceptable level of risk
B. To formalize the confirmation of compliance to security policies and standards
C. To formalize the confirmation of completed risk mitigation and risk analysis
D. To verify that system architecture and interconnections with other systems are effectively implemented

Answer: B

NEW QUESTION 307
- (Exam Topic 11)
Which of the following is generally indicative of a replay attack when dealing with biometric authentication?

A. False Acceptance Rate (FAR) is greater than 1 in 100,000
B. False Rejection Rate (FRR) is greater than 5 in 100
C. Inadequately specified templates
D. Exact match

Answer: D

NEW QUESTION 308
- (Exam Topic 11)
If an identification process using a biometric system detects a 100% match between a presented template and a stored template, what is the interpretation of this result?

A. User error
B. Suspected tampering
C. Accurate identification
D. Unsuccessful identification

Answer: B

NEW QUESTION 310
- (Exam Topic 11)
A security professional has been asked to evaluate the options for the location of a new data center within a multifloor building. Concerns for the data center include emanations and physical access controls.
Which of the following is the BEST location?

A. On the top floor
B. In the basement
C. In the core of the building
D. In an exterior room with windows

Answer: C

NEW QUESTION 314
- (Exam Topic 11)
Which of the following is a function of Security Assertion Markup Language (SAML)?

A. File allocation
B. Redundancy check
C. Extended validation
D. Policy enforcement

Answer: D

NEW QUESTION 319
- (Exam Topic 11)
Which of the following BEST describes a Protection Profile (PP)?

A. A document that expresses an implementation independent set of security requirements for an IT product that meets specific consumer needs.
B. A document that is used to develop an IT security product from its security requirements definition.
C. A document that expresses an implementation dependent set of security requirements which contains only the security functional requirements.
D. A document that represents evaluated products where there is a one-to-one correspondence between a PP and a Security Target (ST).

Answer: A

NEW QUESTION 320
- (Exam Topic 11)
Data remanence refers to which of the following?

A. The remaining photons left in a fiber optic cable after a secure transmission.
B. The retention period required by law or regulation.
C. The magnetic flux created when removing the network connection from a server or personal computer.
D. The residual information left on magnetic storage media after a deletion or erasure.

Answer: D

NEW QUESTION 323
- (Exam Topic 11)
Which of the following is the BEST approach to take in order to effectively incorporate the concepts of business continuity into the organization?

A. Ensure end users are aware of the planning activities
B. Validate all regulatory requirements are known and fully documented
C. Develop training and awareness programs that involve all stakeholders
D. Ensure plans do not violate the organization's cultural objectives and goals

Answer: C

NEW QUESTION 326
- (Exam Topic 11)
If compromised, which of the following would lead to the exploitation of multiple virtual machines?

A. Virtual device drivers
B. Virtual machine monitor
C. Virtual machine instance
D. Virtual machine file system

Answer: B

NEW QUESTION 327
- (Exam Topic 11)
A mobile device application that restricts the storage of user information to just that which is needed to accomplish lawful business goals adheres to what privacy principle?

A. Onward transfer
B. Collection Limitation
C. Collector Accountability
D. Individual Participation

Answer: B

NEW QUESTION 330
- (Exam Topic 11)
How can lessons learned from business continuity training and actual recovery incidents BEST be used?

A. As a means for improvement
B. As alternative options for awareness and training
C. As indicators of a need for policy
D. As business function gap indicators

Answer: A

NEW QUESTION 331
- (Exam Topic 11)
How does an organization verify that an information system's current hardware and software match the standard system configuration?

A. By reviewing the configuration after the system goes into production
B. By running vulnerability scanning tools on all devices in the environment
C. By comparing the actual configuration of the system against the baseline
D. By verifying all the approved security patches are implemented

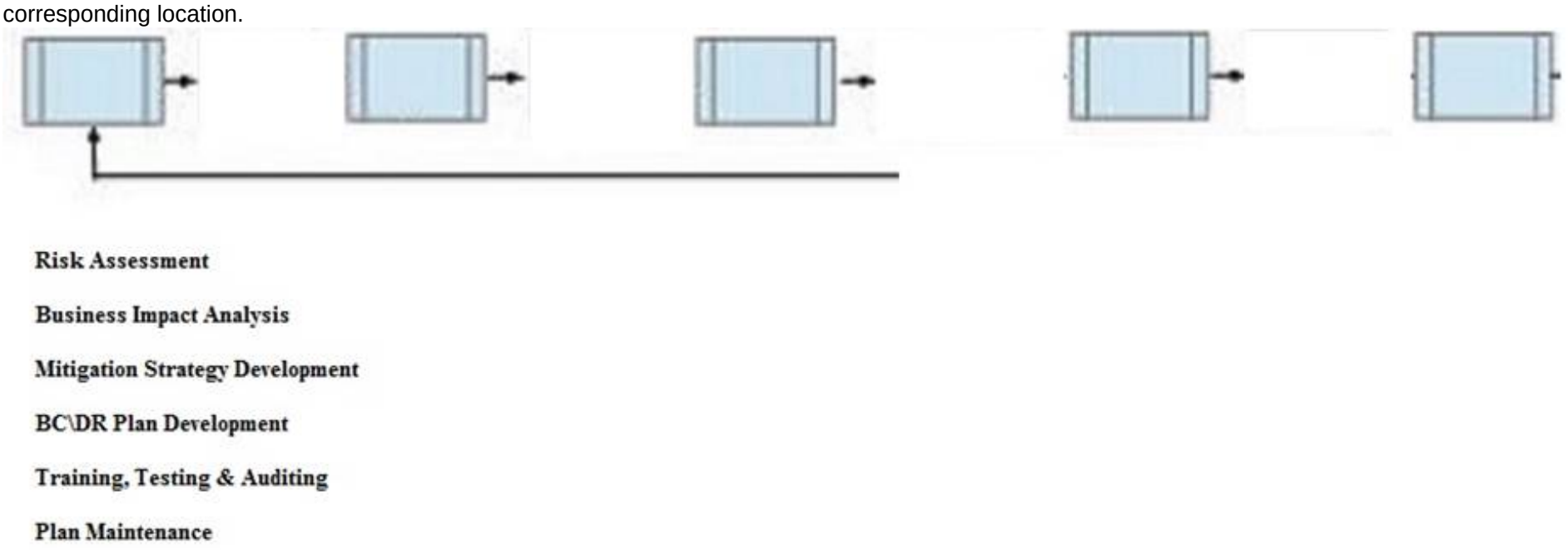
Answer: C

NEW QUESTION 335
- (Exam Topic 11)
Which of the following PRIMARILY contributes to security incidents in web-based applications?

A. Systems administration and operating systems
B. System incompatibility and patch management
C. Third-party applications and change controls
D. Improper stress testing and application interfaces

Answer: C

NEW QUESTION 338
- (Exam Topic 11)
During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.
What is the best approach for the CISO?
Below are the common phases to creating a Business Continuity/Disaster Recovery (BC/DR) plan. Drag the remaining BC\DR phases to the appropriate corresponding location.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 343
- (Exam Topic 11)
Disaster Recovery Plan (DRP) training material should be

A. consistent so that all audiences receive the same training.
B. stored in a fire proof safe to ensure availability when needed.
C. only delivered in paper format.
D. presented in a professional looking manner.

Answer: A

NEW QUESTION 344
- (Exam Topic 11)
Which of the following is most helpful in applying the principle of LEAST privilege?

A. Establishing a sandboxing environment
B. Setting up a Virtual Private Network (VPN) tunnel
C. Monitoring and reviewing privileged sessions
D. Introducing a job rotation program

Answer: A

NEW QUESTION 346
- (Exam Topic 11)
Which of the following analyses is performed to protect information assets?

A. Business impact analysis
B. Feasibility analysis
C. Cost benefit analysis
D. Data analysis

Answer: A

NEW QUESTION 348
- (Exam Topic 11)
Which of the following is the BIGGEST weakness when using native Lightweight Directory Access Protocol (LDAP) for authentication?

A. Authorizations are not included in the server response
B. Unsalted hashes are passed over the network
C. The authentication session can be replayed
D. Passwords are passed in cleartext

Answer: D

NEW QUESTION 349
- (Exam Topic 11)
Which of the following disaster recovery test plans will be MOST effective while providing minimal risk?

A. Read-through
B. Parallel
C. Full interruption
D. Simulation

Answer: B

NEW QUESTION 352

- (Exam Topic 11)
Which of the following standards/guidelines requires an Information Security Management System (ISMS) to be defined?

A. International Organization for Standardization (ISO) 27000 family
B. Information Technology Infrastructure Library (ITIL)
C. Payment Card Industry Data Security Standard (PCIDSS)
D. ISO/IEC 20000

Answer: A

NEW QUESTION 357
- (Exam Topic 11)
What is the PRIMARY difference between security policies and security procedures?

A. Policies are used to enforce violations, and procedures create penalties
B. Policies point to guidelines, and procedures are more contractual in nature
C. Policies are included in awareness training, and procedures give guidance
D. Policies are generic in nature, and procedures contain operational details

Answer: D

NEW QUESTION 359
- (Exam Topic 11)
During a fingerprint verification process, which of the following is used to verify identity and authentication?

A. A pressure value is compared with a stored template
B. Sets of digits are matched with stored values
C. A hash table is matched to a database of stored value
D. A template of minutiae is compared with a stored template

Answer: D

NEW QUESTION 361
- (Exam Topic 11)
Which of the following command line tools can be used in the reconnaisance phase of a network vulnerability assessment?

A. dig
B. ifconfig
C. ipconfig
D. nbtstat

Answer: A

NEW QUESTION 363
- (Exam Topic 11)
Which of the following BEST describes a rogue Access Point (AP)?

A. An AP that is not protected by a firewall
B. An AP not configured to use Wired Equivalent Privacy (WEP) with Triple Data Encryption Algorithm (3DES)
C. An AP connected to the wired infrastructure but not under the management of authorized network administrators
D. An AP infected by any kind of Trojan or Malware

Answer: C

NEW QUESTION 366
- (Exam Topic 11)
Which of the following describes the BEST configuration management practice?

A. After installing a new system, the configuration files are copied to a separate back-up system and hashed to detect tampering.
B. After installing a new system, the configuration files are copied to an air-gapped system and hashed to detect tampering.
C. The firewall rules are backed up to an air-gapped system.
D. A baseline configuration is created and maintained for all relevant systems.

Answer: D

NEW QUESTION 370
- (Exam Topic 11)
After acquiring the latest security updates, what must be done before deploying to production systems?

A. Use tools to detect missing system patches
B. Install the patches on a test system
C. Subscribe to notifications for vulnerabilities
D. Assess the severity of the situation

Answer: B

NEW QUESTION 374
- (Exam Topic 11)
Which of the following is an essential step before performing Structured Query Language (SQL) penetration tests on a production system?

A. Verify countermeasures have been deactivated.
B. Ensure firewall logging has been activated.
C. Validate target systems have been backed up.
D. Confirm warm site is ready to accept connections.

Answer: C

NEW QUESTION 376
- (Exam Topic 11)
What type of encryption is used to protect sensitive data in transit over a network?

A. Payload encryption and transport encryption
B. Authentication Headers (AH)
C. Keyed-Hashing for Message Authentication
D. Point-to-Point Encryption (P2PE)

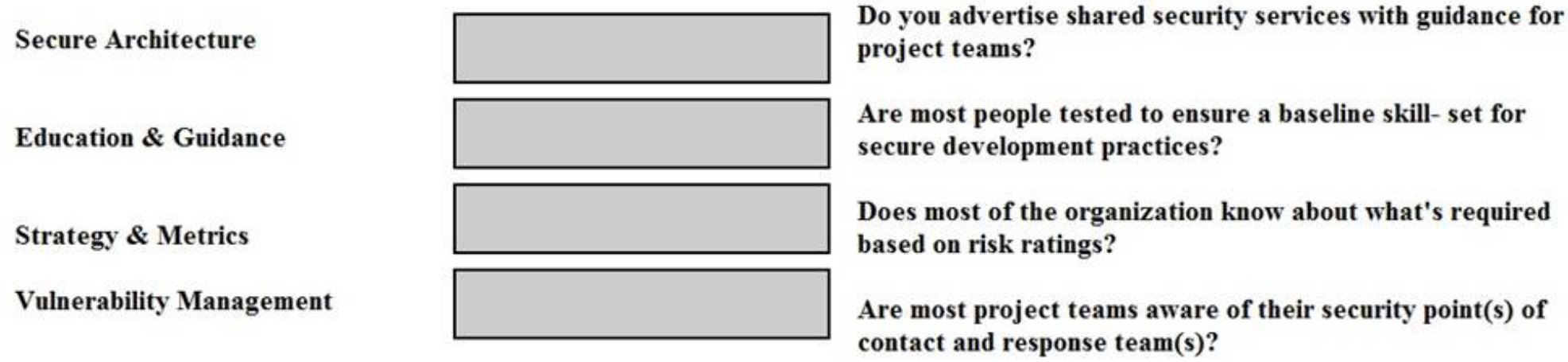
Answer: A

NEW QUESTION 378
- (Exam Topic 11)
An organization has developed a major application that has undergone accreditation testing. After receiving the results of the evaluation, what is the final step before the application can be accredited?

A. Acceptance of risk by the authorizing official
B. Remediation of vulnerabilities
C. Adoption of standardized policies and procedures
D. Approval of the System Security Plan (SSP)

Answer: A

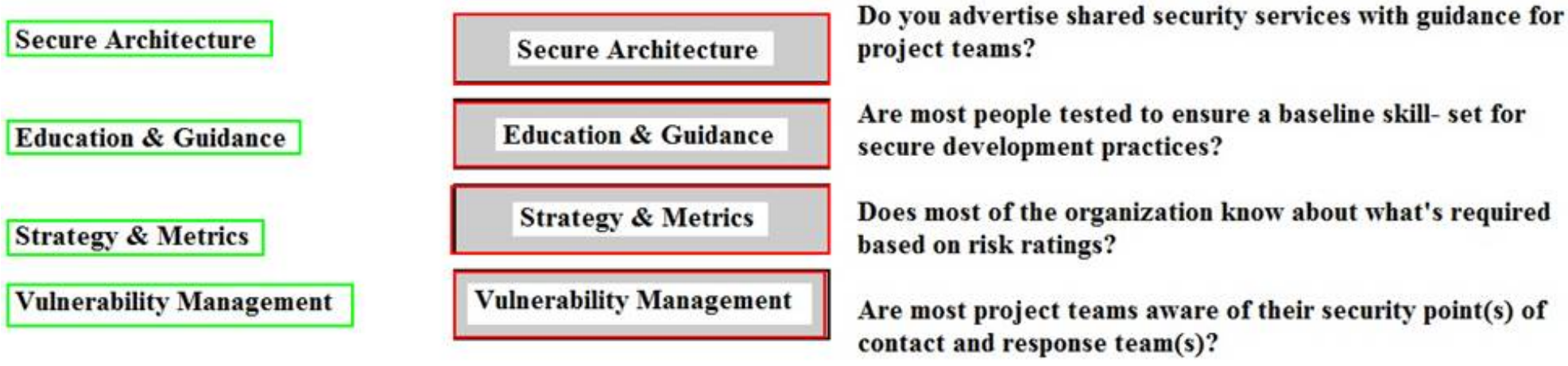
NEW QUESTION 381
- (Exam Topic 11)
Match the objectives to the assessment questions in the governance domain of Software Assurance Maturity Model (SAMM).



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 384
- (Exam Topic 11)
Which methodology is recommended for penetration testing to be effective in the development phase of the life-cycle process?

A. White-box testing
B. Software fuzz testing
C. Black-box testing
D. Visual testing

Answer: A

NEW QUESTION 386
- (Exam Topic 11)
The PRIMARY characteristic of a Distributed Denial of Service (DDoS) attack is that it

A. exploits weak authentication to penetrate networks.
B. can be detected with signature analysis.
C. looks like normal network activity.
D. is commonly confused with viruses or worms.

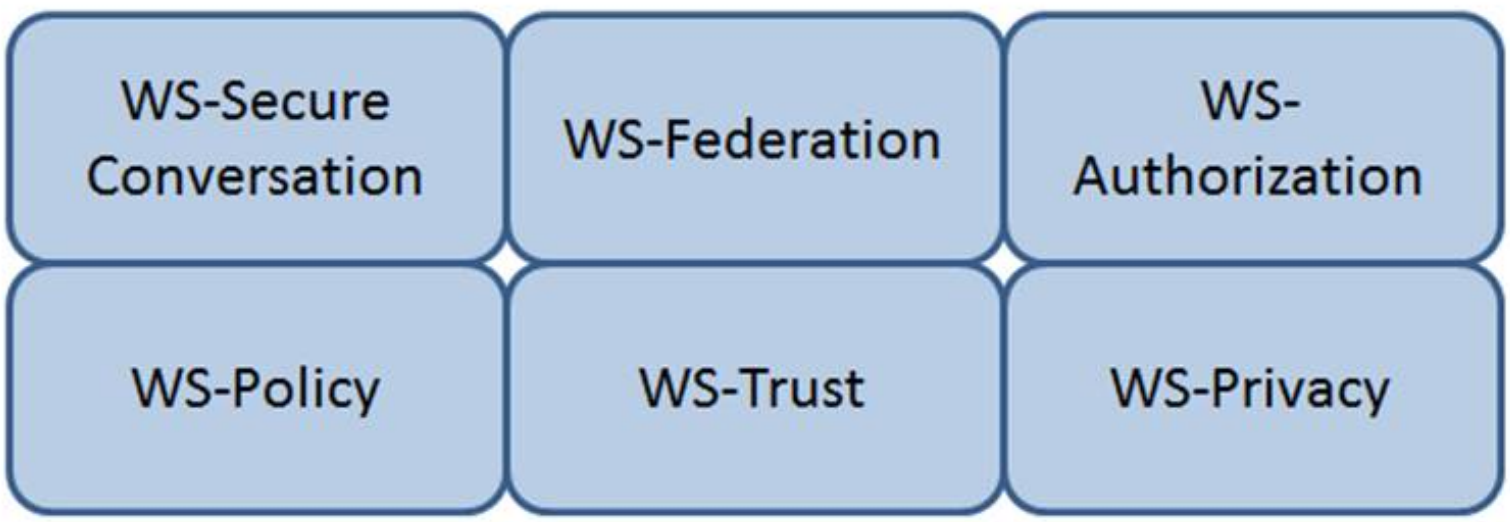
Answer: C

NEW QUESTION 387
- (Exam Topic 11)
Which of the following is an advantage of on-premise Credential Management Systems?

A. Improved credential interoperability
B. Control over system configuration
C. Lower infrastructure capital costs
D. Reduced administrative overhead

Answer: B

NEW QUESTION 388
- (Exam Topic 11)
Which Web Services Security (WS-Security) specification negotiates how security tokens will be issued, renewed and validated? Click on the correct specification in the image below.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
WS-Trust
The protocol used for issuing security tokens is based on WS-Trust. WS-Trust is a Web service specification that builds on WS-Security. It describes a protocol used for issuance, exchange, and validation of security tokens. WS-Trust provides a solution for interoperability by defining a protocol for issuing and exchanging security tokens, based on token format, namespace, or trust boundaries.
Reference: https://msdn.microsoft.com/en-us/library/ff650503.aspx

NEW QUESTION 392

- (Exam Topic 11)
Which of the following controls is the FIRST step in protecting privacy in an information system?

A. Data Redaction
B. Data Minimization
C. Data Encryption
D. Data Storage

Answer: B

NEW QUESTION 396
- (Exam Topic 11)
Software Code signing is used as a method of verifying what security concept?

A. Integrity
B. Confidentiality
C. Availability
D. Access Control

Answer: A

NEW QUESTION 397
- (Exam Topic 11)
Which one of the following is a common risk with network configuration management?

A. Patches on the network are difficult to keep current.
B. It is the responsibility of the systems administrator.
C. User ID and passwords are never set to expire.
D. Network diagrams are not up to date.

Answer: D

NEW QUESTION 398
- (Exam Topic 11)
Which of the following is the MOST effective method of mitigating data theft from an active user workstation?

A. Implement full-disk encryption
B. Enable multifactor authentication
C. Deploy file integrity checkers
D. Disable use of portable devices

Answer: D

NEW QUESTION 402
- (Exam Topic 11)
The PRIMARY outcome of a certification process is that it provides documented

A. system weaknesses for remediation.
B. standards for security assessment, testing, and process evaluation.
C. interconnected systems and their implemented security controls.
D. security analyses needed to make a risk-based decision.

Answer: D

NEW QUESTION 404
- (Exam Topic 11)
What security risk does the role-based access approach mitigate MOST effectively?

A. Excessive access rights to systems and data
B. Segregation of duties conflicts within business applications
C. Lack of system administrator activity monitoring
D. Inappropriate access requests

Answer: A

NEW QUESTION 408
- (Exam Topic 11)
Discretionary Access Control (DAC) is based on which of the following?

A. Information source and destination
B. Identification of subjects and objects
C. Security labels and privileges
D. Standards and guidelines

Answer: B

NEW QUESTION 409
- (Exam Topic 11)
What type of test assesses a Disaster Recovery (DR) plan using realistic disaster scenarios while maintaining minimal impact to business operations?

A. Parallel
B. Walkthrough
C. Simulation
D. Tabletop

Answer: C

NEW QUESTION 414
- (Exam Topic 11)
For an organization considering two-factor authentication for secure network access, which of the following is MOST secure?

A. Challenge response and private key
B. Digital certificates and Single Sign-On (SSO)
C. Tokens and passphrase
D. Smart card and biometrics

Answer: D

NEW QUESTION 418
- (Exam Topic 11)
Which of the following BEST avoids data remanence disclosure for cloud hosted resources?

A. Strong encryption and deletion of the keys after data is deleted.
B. Strong encryption and deletion of the virtual host after data is deleted.
C. Software based encryption with two factor authentication.
D. Hardware based encryption on dedicated physical servers.

Answer: A

NEW QUESTION 422
- (Exam Topic 11)
Who is ultimately responsible to ensure that information assets are categorized and adequate measures are taken to protect them?

A. Data Custodian
B. Executive Management
C. Chief Information Security Officer
D. Data/Information/Business Owners

Answer: B

NEW QUESTION 424
- (Exam Topic 11)
Which of the following is a recommended alternative to an integrated email encryption system?

A. Sign emails containing sensitive data
B. Send sensitive data in separate emails
C. Encrypt sensitive data separately in attachments
D. Store sensitive information to be sent in encrypted drives

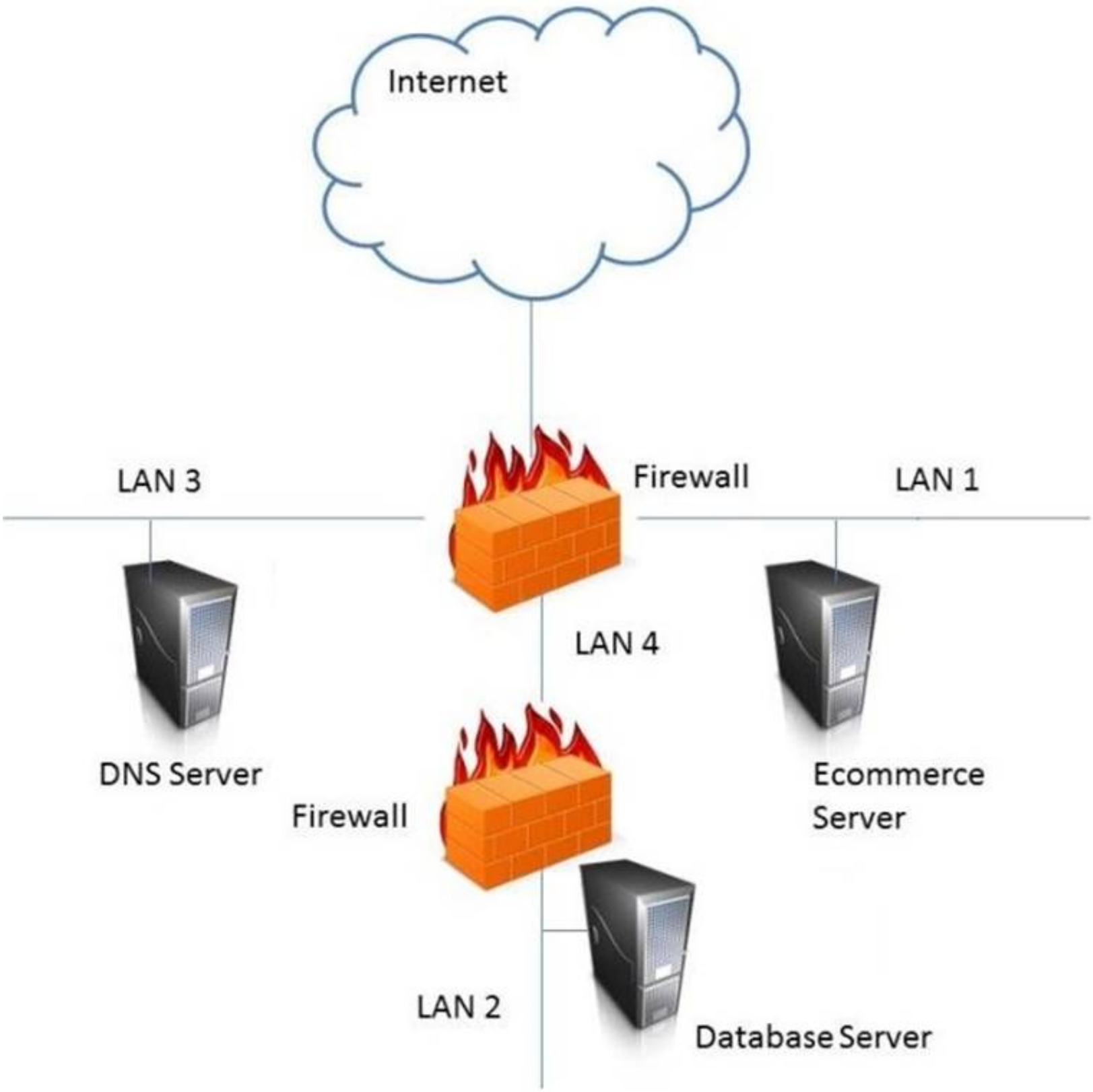
Answer: C

NEW QUESTION 425
- (Exam Topic 11)
While inventorying storage equipment, it is found that there are unlabeled, disconnected, and powered off devices. Which of the following is the correct procedure for handling such equipment?

A. They should be recycled to save energy.
B. They should be recycled according to NIST SP 800-88.
C. They should be inspected and sanitized following the organizational policy.
D. They should be inspected and categorized properly to sell them for reuse.

Answer: C

NEW QUESTION 429
- (Exam Topic 11)
In the network design below, where is the MOST secure Local Area Network (LAN) segment to deploy a Wireless Access Point (WAP) that provides contractors access to the Internet and authorized enterprise services?



A. Mastered
B. Not Mastered

Answer: A

Explanation:
LAN 4

NEW QUESTION 431
- (Exam Topic 11)
Which of the following is the PRIMARY benefit of implementing data-in-use controls?

A. If the data is lost, it must be decrypted to be opened.
B. If the data is lost, it will not be accessible to unauthorized users.
C. When the data is being viewed, it can only be printed by authorized users.
D. When the data is being viewed, it must be accessed using secure protocols.

Answer: C

NEW QUESTION 435
- (Exam Topic 11)
In order for a security policy to be effective within an organization, it MUST include

A. strong statements that clearly define the problem.
B. a list of all standards that apply to the policy.
C. owner information and date of last revision.
D. disciplinary measures for non compliance.

Answer: D

NEW QUESTION 436
- (Exam Topic 11)
The BEST method to mitigate the risk of a dictionary attack on a system is to

A. use a hardware token.
B. use complex passphrases.
C. implement password history.
D. encrypt the access control list (ACL).

Answer: A

NEW QUESTION 438
- (Exam Topic 11)
The MAIN reason an organization conducts a security authorization process is to

A. force the organization to make conscious risk decisions.
B. assure the effectiveness of security controls.
C. assure the correct security organization exists.
D. force the organization to enlist management support.

Answer: A

NEW QUESTION 440
- (Exam Topic 11)
Which of the following could elicit a Denial of Service (DoS) attack against a credential management system?

A. Delayed revocation or destruction of credentials
B. Modification of Certificate Revocation List
C. Unauthorized renewal or re-issuance
D. Token use after decommissioning

Answer: B

NEW QUESTION 443
- (Exam Topic 11)
A global organization wants to implement hardware tokens as part of a multifactor authentication solution for remote access. The PRIMARY advantage of this implementation is

A. the scalability of token enrollment.
B. increased accountability of end users.
C. it protects against unauthorized access.
D. it simplifies user access administration.

Answer: C

NEW QUESTION 444
- (Exam Topic 11)
Which of the following provides the minimum set of privileges required to perform a job function and restricts the user to a domain with the required privileges?

A. Access based on rules
B. Access based on user's role
C. Access determined by the system
D. Access based on data sensitivity

Answer: B

NEW QUESTION 447
- (Exam Topic 12)
As a best practice, the Security Assessment Report (SAR) should include which of the following sections?

A. Data classification policy
B. Software and hardware inventory
C. Remediation recommendations
D. Names of participants

Answer: B

NEW QUESTION 451
- (Exam Topic 12)
An Intrusion Detection System (IDS) has recently been deployed in a Demilitarized Zone (DMZ). The IDS detects a flood of malformed packets. Which of the following BEST describes what has occurred?

A. Denial of Service (DoS) attack
B. Address Resolution Protocol (ARP) spoof
C. Buffer overflow
D. Ping flood attack

Answer: A

NEW QUESTION 454
- (Exam Topic 12)
Network-based logging has which advantage over host-based logging when reviewing malicious activity about a victim machine?

A. Addresses and protocols of network-based logs are analyzed.
B. Host-based system logging has files stored in multiple locations.
C. Properly handled network-based logs may be more reliable and valid.
D. Network-based systems cannot capture users logging into the console.

Answer: A

NEW QUESTION 456
- (Exam Topic 12)
Which Radio Frequency Interference (RFI) phenomenon associated with bundled cable runs can create information leakage?

A. Transference
B. Covert channel
C. Bleeding
D. Cross-talk

Answer: D

NEW QUESTION 460
- (Exam Topic 12)
Which of the following sets of controls should allow an investigation if an attack is not blocked by preventive controls or detected by monitoring?

A. Logging and audit trail controls to enable forensic analysis
B. Security incident response lessons learned procedures
C. Security event alert triage done by analysts using a Security Information and Event Management (SIEM) system
D. Transactional controls focused on fraud prevention

Answer: C

NEW QUESTION 465
- (Exam Topic 12)
Which of the following restricts the ability of an individual to carry out all the steps of a particular process?

A. Job rotation
B. Separation of duties
C. Least privilege
D. Mandatory vacations

Answer: B

NEW QUESTION 468
- (Exam Topic 12)
An application developer is deciding on the amount of idle session time that the application allows before a timeout. The BEST reason for determining the session timeout requirement is

A. organization policy.
B. industry best practices.
C. industry laws and regulations.
D. management feedback.

Answer: A

NEW QUESTION 472
- (Exam Topic 12)
Which type of security testing is being performed when an ethical hacker has no knowledge about the target system but the testing target is notified before the test?

A. Reversal
B. Gray box
C. Blind
D. White box

Answer: B

NEW QUESTION 473
- (Exam Topic 12)
Which of the following is an advantage of on-premise Credential Management Systems?

A. Lower infrastructure capital costs

B. Control over system configuration
C. Reduced administrative overhead
D. Improved credential interoperability

Answer: B

NEW QUESTION 476
- (Exam Topic 12)
Which of the following command line tools can be used in the reconnaissance phase of a network vulnerability assessment?

A. dig
B. ipconfig
C. ifconfig
D. nbstat

Answer: A

NEW QUESTION 480
- (Exam Topic 12)
Although code using a specific program language may not be susceptible to a buffer overflow attack,

A. most calls to plug-in programs are susceptible.
B. most supporting application code is susceptible.
C. the graphical images used by the application could be susceptible.
D. the supporting virtual machine could be susceptible.

Answer: C

NEW QUESTION 485
- (Exam Topic 12)
Which of the following would BEST describe the role directly responsible for data within an organization?

A. Data custodian
B. Information owner
C. Database administrator
D. Quality control

Answer: A

NEW QUESTION 490
- (Exam Topic 12)
What is the BEST way to encrypt web application communications?

A. Secure Hash Algorithm 1 (SHA-1)
B. Secure Sockets Layer (SSL)
C. Cipher Block Chaining Message Authentication Code (CBC-MAC)
D. Transport Layer Security (TLS)

Answer: D

NEW QUESTION 491
- (Exam Topic 12)
How does a Host Based Intrusion Detection System (HIDS) identify a potential attack?

A. Examines log messages or other indications on the system.
B. Monitors alarms sent to the system administrator
C. Matches traffic patterns to virus signature files
D. Examines the Access Control List (ACL)

Answer: C

NEW QUESTION 492
- (Exam Topic 12)
When writing security assessment procedures, what is the MAIN purpose of the test outputs and reports?

A. To force the software to fail and document the process
B. To find areas of compromise in confidentiality and integrity
C. To allow for objective pass or fail decisions
D. To identify malware or hidden code within the test results

Answer: C

NEW QUESTION 496
- (Exam Topic 12)
An employee of a retail company has been granted an extended leave of absence by Human Resources (HR). This information has been formally communicated

to the access provisioning team. Which of the following is the BEST action to take?

A. Revoke access temporarily.
B. Block user access and delete user account after six months.
C. Block access to the offices immediately.
D. Monitor account usage temporarily.

Answer: D

NEW QUESTION 497
- (Exam Topic 12)
Which of the following BEST represents the concept of least privilege?

A. Access to an object is denied unless access is specifically allowed.
B. Access to an object is only available to the owner.
C. Access to an object is allowed unless it is protected by the information security policy.
D. Access to an object is only allowed to authenticated users via an Access Control List (ACL).

Answer: A

NEW QUESTION 500
- (Exam Topic 12)
Which of the following is the PRIMARY reason for employing physical security personnel at entry points in facilities where card access is in operation?

A. To verify that only employees have access to the facility.
B. To identify present hazards requiring remediation.
C. To monitor staff movement throughout the facility.
D. To provide a safe environment for employees.

Answer: D

NEW QUESTION 502
- (Exam Topic 12)
An organization's information security strategic plan MUST be reviewed

A. whenever there are significant changes to a major application.
B. quarterly, when the organization's strategic plan is updated.
C. whenever there are major changes to the business.
D. every three years, when the organization's strategic plan is updated.

Answer: C

NEW QUESTION 505
- (Exam Topic 12)
Which of the following is a weakness of Wired Equivalent Privacy (WEP)?

A. Length of Initialization Vector (IV)
B. Protection against message replay
C. Detection of message tampering
D. Built-in provision to rotate keys

Answer: A

NEW QUESTION 507
- (Exam Topic 12)
An organization publishes and periodically updates its employee policies in a file on their intranet. Which of the following is a PRIMARY security concern?

A. Ownership
B. Confidentiality
C. Availability
D. Integrity

Answer: C

NEW QUESTION 512
- (Exam Topic 12)
Which of the following is a characteristic of the initialization vector when using Data Encryption Standard (DES)?

A. It must be known to both sender and receiver.
B. It can be transmitted in the clear as a random number.
C. It must be retained until the last block is transmitted.
D. It can be used to encrypt and decrypt information.

Answer: B

NEW QUESTION 513

- (Exam Topic 12)
In configuration management, what baseline configuration information MUST be maintained for each computer system?

A. Operating system and version, patch level, applications running, and versions.
B. List of system changes, test reports, and change approvals
C. Last vulnerability assessment report and initial risk assessment report
D. Date of last update, test report, and accreditation certificate

Answer: A

NEW QUESTION 516
- (Exam Topic 12)
Which of the following are effective countermeasures against passive network-layer attacks?

A. Federated security and authenticated access controls
B. Trusted software development and run time integrity controls
C. Encryption and security enabled applications
D. Enclave boundary protection and computing environment defense

Answer: C

NEW QUESTION 517
- (Exam Topic 12)
When evaluating third-party applications, which of the following is the GREATEST responsibility of Information Security?

A. Accept the risk on behalf of the organization.
B. Report findings to the business to determine security gaps.
C. Quantify the risk to the business for product selection.
D. Approve the application that best meets security requirements.

Answer: C

NEW QUESTION 522
- (Exam Topic 12)
A user sends an e-mail request asking for read-only access to files that are not considered sensitive. A Discretionary Access Control (DAC) methodology is in place. Which is the MOST suitable approach that the administrator should take?

A. Administrator should request data owner approval to the user access
B. Administrator should request manager approval for the user access
C. Administrator should directly grant the access to the non-sensitive files
D. Administrator should assess the user access need and either grant or deny the access

Answer: A

NEW QUESTION 524
- (Exam Topic 12)
Backup information that is critical to the organization is identified through a

A. Vulnerability Assessment (VA).
B. Business Continuity Plan (BCP).
C. Business Impact Analysis (BIA).
D. data recovery analysis.

Answer: D

NEW QUESTION 528
- (Exam Topic 12)
What is the MOST important element when considering the effectiveness of a training program for Business Continuity (BC) and Disaster Recovery (DR)?

A. Management support
B. Consideration of organizational need
C. Technology used for delivery
D. Target audience

Answer: B

NEW QUESTION 531
- (Exam Topic 12)
What balance MUST be considered when web application developers determine how informative application error messages should be constructed?

A. Risk versus benefit
B. Availability versus auditability
C. Confidentiality versus integrity
D. Performance versus user satisfaction

Answer: A

NEW QUESTION 533
- (Exam Topic 13)
A security analyst for a large financial institution is reviewing network traffic related to an incident. The analyst determines the traffic is irrelevant to the investigation but in the process of the review, the analyst also finds that an applications data, which included full credit card cardholder data, is transferred in clear text between the server and user's desktop. The analyst knows this violates the Payment Card Industry Data Security Standard (PCI-DSS). Which of the following is the analyst's next step?

A. Send the log file co-workers for peer review
B. Include the full network traffic logs in the incident report
C. Follow organizational processes to alert the proper teams to address the issue.
D. Ignore data as it is outside the scope of the investigation and the analyst's role.

Answer: C

Explanation:
Section: Security Operations

NEW QUESTION 536
- (Exam Topic 13)
Which of the following steps should be performed FIRST when purchasing Commercial Off-The-Shelf (COTS) software?

A. undergo a security assessment as part of authorization process
B. establish a risk management strategy
C. harden the hosting server, and perform hosting and application vulnerability scans
D. establish policies and procedures on system and services acquisition

Answer: D

NEW QUESTION 539
- (Exam Topic 13)
Which of the following is the MOST important security goal when performing application interface testing?

A. Confirm that all platforms are supported and function properly
B. Evaluate whether systems or components pass data and control correctly to one another
C. Verify compatibility of software, hardware, and network connections
D. Examine error conditions related to external interfaces to prevent application details leakage

Answer: B

NEW QUESTION 541
- (Exam Topic 13)
An organization's security policy delegates to the data owner the ability to assign which user roles have access to a particular resource. What type of authorization mechanism is being used?

A. Discretionary Access Control (DAC)
B. Role Based Access Control (RBAC)
C. Media Access Control (MAC)
D. Mandatory Access Control (MAC)

Answer: A

NEW QUESTION 544
- (Exam Topic 13)
Due to system constraints, a group of system administrators must share a high-level access set of credentials. Which of the following would be MOST appropriate to implement?

A. Increased console lockout times for failed logon attempts
B. Reduce the group in size
C. A credential check-out process for a per-use basis
D. Full logging on affected systems

Answer: C

Explanation:
Section: Security Operations

NEW QUESTION 546
- (Exam Topic 13)
Which of the following MUST be in place to recognize a system attack?

A. Stateful firewall
B. Distributed antivirus
C. Log analysis
D. Passive honeypot

Answer: A

NEW QUESTION 551
- (Exam Topic 13)
What protocol is often used between gateway hosts on the Internet?

A. Exterior Gateway Protocol (EGP)
B. Border Gateway Protocol (BGP)
C. Open Shortest Path First (OSPF)
D. Internet Control Message Protocol (ICMP)

Answer: B

NEW QUESTION 553
- (Exam Topic 13)
As part of the security assessment plan, the security professional has been asked to use a negative testing strategy on a new website. Which of the following actions would be performed?

A. Use a web scanner to scan for vulnerabilities within the website.
B. Perform a code review to ensure that the database references are properly addressed.
C. Establish a secure connection to the web server to validate that only the approved ports are open.
D. Enter only numbers in the web form and verify that the website prompts the user to enter a valid input.

Answer: D

NEW QUESTION 558
- (Exam Topic 13)
A company seizes a mobile device suspected of being used in committing fraud. What would be the BEST method used by a forensic examiner to isolate the powered-on device from the network and preserve the evidence?

A. Put the device in airplane mode
B. Suspend the account with the telecommunication provider
C. Remove the SIM card
D. Turn the device off

Answer: A

NEW QUESTION 560
- (Exam Topic 13)
What capability would typically be included in a commercially available software package designed for access control?

A. Password encryption
B. File encryption
C. Source library control
D. File authentication

Answer: A

NEW QUESTION 562
- (Exam Topic 13)
Which of the following is a direct monetary cost of a security incident?

A. Morale
B. Reputation
C. Equipment
D. Information

Answer: C

NEW QUESTION 564
- (Exam Topic 13)
Which security access policy contains fixed security attributes that are used by the system to determine a user’s access to a file or object?

A. Mandatory Access Control (MAC)
B. Access Control List (ACL)
C. Discretionary Access Control (DAC)
D. Authorized user control

Answer: A

NEW QUESTION 569
- (Exam Topic 13)
Even though a particular digital watermark is difficult to detect, which of the following represents a way it might still be inadvertently removed?

A. Truncating parts of the data
B. Applying Access Control Lists (ACL) to the data
C. Appending non-watermarked data to watermarked data
D. Storing the data in a database

Answer: A

NEW QUESTION 571
- (Exam Topic 13)
Which of the following combinations would MOST negatively affect availability?

A. Denial of Service (DoS) attacks and outdated hardware
B. Unauthorized transactions and outdated hardware
C. Fire and accidental changes to data
D. Unauthorized transactions and denial of service attacks

Answer: A

NEW QUESTION 575
- (Exam Topic 13)
Which of the following is the MOST efficient mechanism to account for all staff during a speedy nonemergency evacuation from a large security facility?

A. Large mantrap where groups of individuals leaving are identified using facial recognition technology
B. Radio Frequency Identification (RFID) sensors worn by each employee scanned by sensors at each exitdoor
C. Emergency exits with push bars with coordinates at each exit checking off the individual against a predefined list
D. Card-activated turnstile where individuals are validated upon exit

Answer: B

Explanation:
Section: Security Operations

NEW QUESTION 580
- (Exam Topic 13)
Which of the following is a benefit in implementing an enterprise Identity and Access Management (IAM) solution?

A. Password requirements are simplified.
B. Risk associated with orphan accounts is reduced.
C. Segregation of duties is automatically enforced.
D. Data confidentiality is increased.

Answer: A

NEW QUESTION 584
- (Exam Topic 13)
When determining who can accept the risk associated with a vulnerability, which of the following is MOST important?

A. Countermeasure effectiveness
B. Type of potential loss
C. Incident likelihood
D. Information ownership

Answer: C

NEW QUESTION 588
- (Exam Topic 13)
Which of the following is the BEST reason for the use of security metrics?

A. They ensure that the organization meets its security objectives.
B. They provide an appropriate framework for Information Technology (IT) governance.
C. They speed up the process of quantitative risk assessment.
D. They quantify the effectiveness of security processes.

Answer: B

NEW QUESTION 591
- (Exam Topic 13)
Mandatory Access Controls (MAC) are based on:

A. security classification and security clearance
B. data segmentation and data classification
C. data labels and user access permissions
D. user roles and data encryption

Answer: A

NEW QUESTION 592
- (Exam Topic 13)
Which of the following is a common characteristic of privacy?

A. Provision for maintaining an audit trail of access to the private data
B. Notice to the subject of the existence of a database containing relevant credit card data
C. Process for the subject to inspect and correct personal data on-site
D. Database requirements for integration of privacy data

Answer: A

NEW QUESTION 595
- (Exam Topic 13)
What is the MOST significant benefit of an application upgrade that replaces randomly generated session keys with certificate based encryption for communications with backend servers?

A. Non-repudiation
B. Efficiency
C. Confidentially
D. Privacy

Answer: A

NEW QUESTION 598
- (Exam Topic 13)
Match the name of access control model with its associated restriction.
Drag each access control model to its appropriate restriction access on the right.

Access Control Model		Restrictions
Mandatory Access Control		End user cannot set controls
Discretionary Access Control (DAC)		Subject has total control over objects
Role Based Access Control (RBAC)		Dynamically assigns permissions to particular duties based on job function
Rule based access control		Dynamically assigns roles to subjects based on criteria assigned by a custodian

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Access Control Model		Restrictions
Mandatory Access Control	Mandatory Access Control	End user cannot set controls
Discretionary Access Control (DAC)	Discretionary Access Control (DAC)	Subject has total control over objects
Role Based Access Control (RBAC)	Role Based Access Control (RBAC)	Dynamically assigns permissions to particular duties based on job function
Rule based access control	Rule based access control	Dynamically assigns roles to subjects based on criteria assigned by a custodian

NEW QUESTION 603
- (Exam Topic 13)
Proven application security principles include which of the following?

A. Minimizing attack surface area
B. Hardening the network perimeter
C. Accepting infrastructure security controls
D. Developing independent modules

Answer: A

NEW QUESTION 606
- (Exam Topic 13)
Which of the following is considered a secure coding practice?

A. Use concurrent access for shared variables and resources
B. Use checksums to verify the integrity of libraries
C. Use new code for common tasks
D. Use dynamic execution functions to pass user supplied data

Answer: B

NEW QUESTION 608
- (Exam Topic 13)
Which of the following would an attacker BEST be able to accomplish through the use of Remote Access Tools (RAT)?

A. Reduce the probability of identification
B. Detect further compromise of the target
C. Destabilize the operation of the host
D. Maintain and expand control

Answer: D

NEW QUESTION 611
- (Exam Topic 13)
What is the PRIMARY goal of fault tolerance?

A. Elimination of single point of failure
B. Isolation using a sandbox
C. Single point of repair
D. Containment to prevent propagation

Answer: A

NEW QUESTION 613
- (Exam Topic 13)
An organization recently conducted a review of the security of its network applications. One of the vulnerabilities found was that the session key used in encrypting sensitive information to a third party server
had been hard-coded in the client and server applications. Which of the following would be MOST effective in mitigating this vulnerability?

A. Diffle-Hellman (DH) algorithm
B. Elliptic Curve Cryptography (ECC) algorithm
C. Digital Signature algorithm (DSA)
D. Rivest-Shamir-Adleman (RSA) algorithm

Answer: A

NEW QUESTION 614
- (Exam Topic 13)
Within the company, desktop clients receive Internet Protocol (IP) address over Dynamic Host Configuration Protocol (DHCP).
Which of the following represents a valid measure to help protect the network against unauthorized access?

A. Implement path management
B. Implement port based security through 802.1x
C. Implement DHCP to assign IP address to server systems
D. Implement change management

Answer: B

NEW QUESTION 619
- (Exam Topic 13)
Which of the following is MOST appropriate for protecting confidentially of data stored on a hard drive?

A. Triple Data Encryption Standard (3DES)
B. Advanced Encryption Standard (AES)
C. Message Digest 5 (MD5)
D. Secure Hash Algorithm 2(SHA-2)

Answer: B

NEW QUESTION 622
- (Exam Topic 13)
Which of the following is the MOST challenging issue in apprehending cyber criminals?

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

NEW QUESTION 627
- (Exam Topic 13)
When developing a business case for updating a security program, the security program owner MUST do which of the following?

A. Identify relevant metrics
B. Prepare performance test reports
C. Obtain resources for the security program
D. Interview executive management

Answer: A

NEW QUESTION 632
- (Exam Topic 13)
A vulnerability assessment report has been submitted to a client. The client indicates that one third of the hosts that were in scope are missing from the report.
In which phase of the assessment was this error MOST likely made?

A. Enumeration
B. Reporting
C. Detection
D. Discovery

Answer: A

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 633
- (Exam Topic 13)
Which of the following mandates the amount and complexity of security controls applied to a security risk?

A. Security vulnerabilities
B. Risk tolerance
C. Risk mitigation
D. Security staff

Answer: C

NEW QUESTION 636
- (Exam Topic 13)
Which Identity and Access Management (IAM) process can be used to maintain the principle of least privilege?

A. identity provisioning
B. access recovery
C. multi-factor authentication (MFA)
D. user access review

Answer: A

NEW QUESTION 637
- (Exam Topic 13)
A chemical plan wants to upgrade the Industrial Control System (ICS) to transmit data using Ethernet instead of RS422. The project manager wants to simplify administration and maintenance by utilizing the office network infrastructure and staff to implement this upgrade.
Which of the following is the GREATEST impact on security for the network?

A. The network administrators have no knowledge of ICS
B. The ICS is now accessible from the office network
C. The ICS does not support the office password policy
D. RS422 is more reliable than Ethernet

Answer: B

NEW QUESTION 642
- (Exam Topic 13)
A security professional determines that a number of outsourcing contracts inherited from a previous merger do not adhere to the current security requirements.
Which of the following BEST minimizes the risk of this happening again?

A. Define additional security controls directly after the merger
B. Include a procurement officer in the merger team
C. Verify all contracts before a merger occurs
D. Assign a compliancy officer to review the merger conditions

Answer: D

NEW QUESTION 644
- (Exam Topic 13)
An organization adopts a new firewall hardening standard. How can the security professional verify that the technical staff correct implemented the new standard?

A. Perform a compliance review
B. Perform a penetration test
C. Train the technical staff
D. Survey the technical staff

Answer: B

Explanation:
Section: Security Operations

NEW QUESTION 645
- (Exam Topic 13)
A user has infected a computer with malware by connecting a Universal Serial Bus (USB) storage device. Which of the following is MOST effective to mitigate future infections?

A. Develop a written organizational policy prohibiting unauthorized USB devices
B. Train users on the dangers of transferring data in USB devices
C. Implement centralized technical control of USB port connections
D. Encrypt removable USB devices containing data at rest

Answer: C

NEW QUESTION 649
- (Exam Topic 13)
Extensible Authentication Protocol-Message Digest 5 (EAP-MD5) only provides which of the following?

A. Mutual authentication
B. Server authentication
C. User authentication
D. Streaming ciphertext data

Answer: C

NEW QUESTION 651
- (Exam Topic 13)
Which of the following is the GREATEST benefit of implementing a Role Based Access Control (RBAC) system?

A. Integration using Lightweight Directory Access Protocol (LDAP)
B. Form-based user registration process
C. Integration with the organizations Human Resources (HR) system
D. A considerably simpler provisioning process

Answer: D

NEW QUESTION 654
- (Exam Topic 13)
As part of an application penetration testing process, session hijacking can BEST be achieved by which of the following?

A. Known-plaintext attack
B. Denial of Service (DoS)
C. Cookie manipulation
D. Structured Query Language (SQL) injection

Answer: D

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 657
- (Exam Topic 13)
Which of the following is the MOST important part of an awareness and training plan to prepare employees for emergency situations?

A. Having emergency contacts established for the general employee population to get information
B. Conducting business continuity and disaster recovery training for those who have a direct role in the recovery
C. Designing business continuity and disaster recovery training programs for different audiences
D. Publishing a corporate business continuity and disaster recovery plan on the corporate website

Answer: C

NEW QUESTION 662
- (Exam Topic 13)
A company receives an email threat informing of an Imminent Distributed Denial of Service (DDoS) attack targeting its web application, unless ransom is paid. Which of the following techniques BEST addresses that threat?

A. Deploying load balancers to distribute inbound traffic across multiple data centers
B. Set Up Web Application Firewalls (WAFs) to filter out malicious traffic
C. Implementing reverse web-proxies to validate each new inbound connection
D. Coordinate with and utilize capabilities within Internet Service Provider (ISP)

Answer: D

NEW QUESTION 663
- (Exam Topic 13)
During examination of Internet history records, the following string occurs within a Unique Resource Locator (URL):
http://www.companysite.com/products/products.asp?productid=123
or 1=1
What type of attack does this indicate?

A. Directory traversal
B. Structured Query Language (SQL) injection
C. Cross-Site Scripting (XSS)
D. Shellcode injection

Answer: C

NEW QUESTION 667
- (Exam Topic 13)
A Security Operations Center (SOC) receives an incident response notification on a server with an active intruder who has planted a backdoor. Initial notifications are sent and communications are established. What MUST be considered or evaluated before performing the next step?

A. Notifying law enforcement is crucial before hashing the contents of the server hard drive
B. Identifying who executed the incident is more important than how the incident happened
C. Removing the server from the network may prevent catching the intruder
D. Copying the contents of the hard drive to another storage device may damage the evidence

Answer: C

Explanation:
Section: Security Operations

NEW QUESTION 672
- (Exam Topic 13)
Who would be the BEST person to approve an organizations information security policy?

A. Chief Information Officer (CIO)
B. Chief Information Security Officer (CISO)
C. Chief internal auditor
D. Chief Executive Officer (CEO)

Answer: B

Explanation:
Section: Security Operations

NEW QUESTION 673
- (Exam Topic 13)
Which of the following is the BEST metric to obtain when gaining support for an Identify and Access Management (IAM) solution?

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

NEW QUESTION 677
- (Exam Topic 13)
Which of the following is BEST achieved through the use of eXtensible Access Markup Language (XACML)?

A. Minimize malicious attacks from third parties
B. Manage resource privileges
C. Share digital identities in hybrid cloud
D. Defined a standard protocol

Answer:

D

NEW QUESTION 681

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CISSP Exam with Our Prep Materials Via below:

https://www.certleader.com/CISSP-dumps.html