

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

<https://www.2passeasy.com/dumps/CISSP/>



NEW QUESTION 1

- (Exam Topic 1)

An important principle of defense in depth is that achieving information security requires a balanced focus on which PRIMARY elements?

- A. Development, testing, and deployment
- B. Prevention, detection, and remediation
- C. People, technology, and operations
- D. Certification, accreditation, and monitoring

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 1)

Intellectual property rights are PRIMARY concerned with which of the following?

- A. Owner's ability to realize financial gain
- B. Owner's ability to maintain copyright
- C. Right of the owner to enjoy their creation
- D. Right of the owner to control delivery method

Answer: D

NEW QUESTION 5

- (Exam Topic 1)

Which of the following types of technologies would be the MOST cost-effective method to provide a reactive control for protecting personnel in public areas?

- A. Install mantraps at the building entrances
- B. Enclose the personnel entry area with polycarbonate plastic
- C. Supply a duress alarm for personnel exposed to the public
- D. Hire a guard to protect the public area

Answer: D

NEW QUESTION 6

- (Exam Topic 2)

Which one of the following affects the classification of data?

- A. Assigned security label
- B. Multilevel Security (MLS) architecture
- C. Minimum query size
- D. Passage of time

Answer: D

NEW QUESTION 7

- (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 8

- (Exam Topic 3)

Which technique can be used to make an encryption scheme more resistant to a known plaintext attack?

- A. Hashing the data before encryption
- B. Hashing the data after encryption
- C. Compressing the data after encryption
- D. Compressing the data before encryption

Answer: A

NEW QUESTION 9

- (Exam Topic 3)

The use of private and public encryption keys is fundamental in the implementation of which of the following?

- A. Diffie-Hellman algorithm
- B. Secure Sockets Layer (SSL)
- C. Advanced Encryption Standard (AES)
- D. Message Digest 5 (MD5)

Answer: A

NEW QUESTION 10

- (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)

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

- A. Add a new rule to the application layer firewall
- B. Block access to the service
- C. Install an Intrusion Detection System (IDS)
- D. Patch the application source code

Answer: A

NEW QUESTION 14

- (Exam Topic 4)

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. Install Host Based Intrusion Detection Systems (HIDS)
- C. Require strong authentication for administrators
- D. Implement logical network segmentation at the switches

Answer: D

NEW QUESTION 16

- (Exam Topic 5)

A manufacturing organization wants to establish a Federated Identity Management (FIM) system with its 20 different supplier companies. Which of the following is the BEST solution for the manufacturing organization?

- A. Trusted third-party certification
- B. Lightweight Directory Access Protocol (LDAP)
- C. Security Assertion Markup language (SAML)
- D. Cross-certification

Answer: C

NEW QUESTION 18

- (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 20

- (Exam Topic 5)

What is the BEST approach for controlling access to highly sensitive information when employees have the same level of security clearance?

- A. Audit logs
- B. Role-Based Access Control (RBAC)
- C. Two-factor authentication
- D. Application of least privilege

Answer: B

NEW QUESTION 24

- (Exam Topic 6)

Which of the following is a PRIMARY benefit of using a formalized security testing report format and structure?

- A. Executive audiences will understand the outcomes of testing and most appropriate next steps for corrective actions to be taken
- B. Technical teams will understand the testing objectives, testing strategies applied, and business risk associated with each vulnerability
- C. Management teams will understand the testing objectives and reputational risk to the organization
- D. Technical and management teams will better understand the testing objectives, results of each test phase, and potential impact levels

Answer: D

NEW QUESTION 27

- (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 30

- (Exam Topic 7)

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

- A. Guaranteed recovery of all business functions
- B. Minimization of the need decision making during a crisis
- C. Insurance against litigation following a disaster
- D. Protection from loss of organization resources

Answer: D

NEW QUESTION 34

- (Exam Topic 7)

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

- A. Warm site
- B. Hot site
- C. Mirror site
- D. Cold site

Answer: A

NEW QUESTION 36

- (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 38

- (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 39

- (Exam Topic 7)

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

- A. Walkthrough
- B. Simulation
- C. Parallel
- D. White box

Answer: B

NEW QUESTION 40

- (Exam Topic 7)

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

- A. Take the computer to a forensic lab
- B. Make a copy of the hard drive
- C. Start documenting
- D. Turn off the computer

Answer: C

NEW QUESTION 41

- (Exam Topic 7)

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

- A. Determine the cause of the incident
- B. Disconnect the system involved from the network
- C. Isolate and contain the system involved
- D. Investigate all symptoms to confirm the incident

Answer: D

NEW QUESTION 45

- (Exam Topic 8)

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

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

Answer: B

NEW QUESTION 48

- (Exam Topic 8)

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

- A. After the system preliminary design has been developed and the data security categorization has been performed
- B. After the vulnerability analysis has been performed and before the system detailed design begins
- C. After the system preliminary design has been developed and before the data security categorization begins
- D. After the business functional analysis and the data security categorization have been performed

Answer: C

NEW QUESTION 50

- (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 55

- (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 60

- (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 61

- (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 66

- (Exam Topic 9)

Logical access control programs are MOST effective when they are

- A. approved by external auditors.
- B. combined with security token technology.
- C. maintained by computer security officers.
- D. made part of the operating system.

Answer: D

NEW QUESTION 69

- (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 74

- (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 76

- (Exam Topic 9)

An organization allows ping traffic into and out of their network. An attacker has installed a program on the network that uses the payload portion of the ping packet to move data into and out of the network. What type of attack has the organization experienced?

- A. Data leakage
- B. Unfiltered channel
- C. Data emanation
- D. Covert channel

Answer: D

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 81

- (Exam Topic 9)

Which layer of the Open Systems Interconnections (OSI) model implementation adds information concerning the logical connection between the sender and receiver?

- A. Physical
- B. Session
- C. Transport
- D. Data-Link

Answer: C

NEW QUESTION 82

- (Exam Topic 9)

The type of authorized interactions a subject can have with an object is

- A. control.
- B. permission.
- C. procedure.
- D. protocol.

Answer: B

NEW QUESTION 85

- (Exam Topic 9)

The Structured Query Language (SQL) implements Discretionary Access Controls (DAC) using

- A. INSERT and DELETE.
- B. GRANT and REVOKE.
- C. PUBLIC and PRIVATE.
- D. ROLLBACK and TERMINATE.

Answer: B

NEW QUESTION 90

- (Exam Topic 9)

Which of the following is considered best practice for preventing e-mail spoofing?

- A. Spam filtering
- B. Cryptographic signature
- C. Uniform Resource Locator (URL) filtering
- D. Reverse Domain Name Service (DNS) lookup

Answer: B

NEW QUESTION 94

- (Exam Topic 9)

Including a Trusted Platform Module (TPM) in the design of a computer system is an example of a technique to what?

- A. Interface with the Public Key Infrastructure (PKI)
- B. Improve the quality of security software
- C. Prevent Denial of Service (DoS) attacks
- D. Establish a secure initial state

Answer: D

NEW QUESTION 96

- (Exam Topic 9)

Multi-threaded applications are more at risk than single-threaded applications to

- A. race conditions.
- B. virus infection.

- C. packet sniffing.
- D. database injection.

Answer: A

NEW QUESTION 97

- (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 98

- (Exam Topic 9)

Which of the following is an authentication protocol in which a new random number is generated uniquely for each login session?

- A. Challenge Handshake Authentication Protocol (CHAP)
- B. Point-to-Point Protocol (PPP)
- C. Extensible Authentication Protocol (EAP)
- D. Password Authentication Protocol (PAP)

Answer: A

NEW QUESTION 101

- (Exam Topic 9)

As one component of a physical security system, an Electronic Access Control (EAC) token is BEST known for its ability to

- A. overcome the problems of key assignments.
- B. monitor the opening of windows and doors.
- C. trigger alarms when intruders are detected.
- D. lock down a facility during an emergency.

Answer: A

NEW QUESTION 103

- (Exam Topic 9)

When building a data center, site location and construction factors that increase the level of vulnerability to physical threats include

- A. hardened building construction with consideration of seismic factors.
- B. adequate distance from and lack of access to adjacent buildings.
- C. curved roads approaching the data center.
- D. proximity to high crime areas of the city.

Answer: D

NEW QUESTION 107

- (Exam Topic 9)

Which of the following does the Encapsulating Security Payload (ESP) provide?

- A. Authorization and integrity
- B. Availability and integrity
- C. Integrity and confidentiality
- D. Authorization and confidentiality

Answer: C

NEW QUESTION 110

- (Exam Topic 9)

Which one of the following is the MOST important in designing a biometric access system if it is essential that no one other than authorized individuals are admitted?

- A. False Acceptance Rate (FAR)
- B. False Rejection Rate (FRR)
- C. Crossover Error Rate (CER)
- D. Rejection Error Rate

Answer: A

NEW QUESTION 111

- (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 113

- (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 115

- (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 116

- (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 121

- (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 123

- (Exam Topic 9)

The use of strong authentication, the encryption of Personally Identifiable Information (PII) on database servers, application security reviews, and the encryption of data transmitted across networks provide

- A. data integrity.
- B. defense in depth.
- C. data availability.
- D. non-repudiation.

Answer: B

NEW QUESTION 128

- (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 129

- (Exam Topic 9)

Which of the following is the MAIN reason that system re-certification and re-accreditation are needed?

- A. To assist data owners in making future sensitivity and criticality determinations
- B. To assure the software development team that all security issues have been addressed
- C. To verify that security protection remains acceptable to the organizational security policy
- D. To help the security team accept or reject new systems for implementation and production

Answer: C

NEW QUESTION 130

- (Exam Topic 9)

The BEST way to check for good security programming practices, as well as auditing for possible backdoors, is to conduct

- A. log auditing.
- B. code reviews.
- C. impact assessments.
- D. static analysis.

Answer: B

NEW QUESTION 132

- (Exam Topic 9)

Which of the following is a security limitation of File Transfer Protocol (FTP)?

- A. Passive FTP is not compatible with web browsers.
- B. Anonymous access is allowed.
- C. FTP uses Transmission Control Protocol (TCP) ports 20 and 21.
- D. Authentication is not encrypted.

Answer: D

NEW QUESTION 134

- (Exam Topic 9)

Which one of the following effectively obscures network addresses from external exposure when implemented on a firewall or router?

- A. Network Address Translation (NAT)
- B. Application Proxy
- C. Routing Information Protocol (RIP) Version 2
- D. Address Masking

Answer: A

NEW QUESTION 136

- (Exam Topic 9)

Which of the following can BEST prevent security flaws occurring in outsourced software development?

- A. Contractual requirements for code quality
- B. Licensing, code ownership and intellectual property rights
- C. Certification of the quality and accuracy of the work done
- D. Delivery dates, change management control and budgetary control

Answer: C

NEW QUESTION 137

- (Exam Topic 9)

The birthday attack is MOST effective against which one of the following cipher technologies?

- A. Chaining block encryption
- B. Asymmetric cryptography
- C. Cryptographic hash
- D. Streaming cryptography

Answer: C

NEW QUESTION 140

- (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 144

- (Exam Topic 9)

Which type of control recognizes that a transaction amount is excessive in accordance with corporate policy?

- A. Detection
- B. Prevention
- C. Investigation
- D. Correction

Answer: A

NEW QUESTION 148

- (Exam Topic 9)

What is an effective practice when returning electronic storage media to third parties for repair?

- A. Ensuring the media is not labeled in any way that indicates the organization's name.
- B. Disassembling the media and removing parts that may contain sensitive data.
- C. Physically breaking parts of the media that may contain sensitive data.
- D. Establishing a contract with the third party regarding the secure handling of the media.

Answer: D

NEW QUESTION 151

- (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 155

- (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 159

- (Exam Topic 9)

Which of the following elements MUST a compliant EU-US Safe Harbor Privacy Policy contain?

- A. An Explanation: of how long the data subject's collected information will be retained for and how it will be eventually disposed.
- B. An Explanation: of who can be contacted at the organization collecting the information if corrections are required by the data subject.
- C. An Explanation: of the regulatory frameworks and compliance standards the information collecting organization adheres to.
- D. An Explanation: of all the technologies employed by the collecting organization in gathering information on the data subject.

Answer: B

NEW QUESTION 162

- (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 166

- (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 168

- (Exam Topic 9)

Which of the following is an appropriate source for test data?

- A. Production data that is secured and maintained only in the production environment.
- B. Test data that has no similarities to production data.
- C. Test data that is mirrored and kept up-to-date with production data.
- D. Production data that has been sanitized before loading into a test environment.

Answer: D

NEW QUESTION 171

- (Exam Topic 9)

Following the completion of a network security assessment, which of the following can BEST be demonstrated?

- A. The effectiveness of controls can be accurately measured
- B. A penetration test of the network will fail
- C. The network is compliant to industry standards
- D. All unpatched vulnerabilities have been identified

Answer: A

NEW QUESTION 174

- (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 178

- (Exam Topic 9)

While impersonating an Information Security Officer (ISO), an attacker obtains information from company employees about their User IDs and passwords. Which method of information gathering has the attacker used?

- A. Trusted path
- B. Malicious logic
- C. Social engineering
- D. Passive misuse

Answer: C

NEW QUESTION 182

- (Exam Topic 9)

Why MUST a Kerberos server be well protected from unauthorized access?

- A. It contains the keys of all clients.
- B. It always operates at root privilege.
- C. It contains all the tickets for services.
- D. It contains the Internet Protocol (IP) address of all network entities.

Answer: A

NEW QUESTION 184

- (Exam Topic 9)

What maintenance activity is responsible for defining, implementing, and testing updates to application systems?

- A. Program change control
- B. Regression testing
- C. Export exception control
- D. User acceptance testing

Answer: A

NEW QUESTION 188

- (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 191

- (Exam Topic 9)

Which of the following actions should be performed when implementing a change to a database schema in a production system?

- A. Test in development, determine dates, notify users, and implement in production
- B. Apply change to production, run in parallel, finalize change in production, and develop a back-out strategy
- C. Perform user acceptance testing in production, have users sign off, and finalize change
- D. Change in development, perform user acceptance testing, develop a back-out strategy, and implement change

Answer: D

NEW QUESTION 194

- (Exam Topic 9)

An Intrusion Detection System (IDS) is generating alarms that a user account has over 100 failed login attempts per minute. A sniffer is placed on the network, and a variety of passwords for that user are noted. Which of the following is MOST likely occurring?

- A. A dictionary attack
- B. A Denial of Service (DoS) attack
- C. A spoofing attack
- D. A backdoor installation

Answer: A

NEW QUESTION 195

- (Exam Topic 9)

What is the MOST important purpose of testing the Disaster Recovery Plan (DRP)?

- A. Evaluating the efficiency of the plan
- B. Identifying the benchmark required for restoration
- C. Validating the effectiveness of the plan
- D. Determining the Recovery Time Objective (RTO)

Answer: C

NEW QUESTION 196

- (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 198

- (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 203

- (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 205

- (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 208

- (Exam Topic 9)

Which of the following wraps the decryption key of a full disk encryption implementation and ties the hard disk drive to a particular device?

- A. Trusted Platform Module (TPM)
- B. Preboot eXecution Environment (PXE)
- C. Key Distribution Center (KDC)
- D. Simple Key-Management for Internet Protocol (SKIP)

Answer: A

NEW QUESTION 213

- (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 214

- (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 217

- (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 221

- (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 224

- (Exam Topic 10)

Which of the following is a process within a Systems Engineering Life Cycle (SELC) stage?

- A. Requirements Analysis
- B. Development and Deployment
- C. Production Operations
- D. Utilization Support

Answer: A

NEW QUESTION 225

- (Exam Topic 10)

Which of the following describes the concept of a Single Sign-On (SSO) system?

- A. Users are authenticated to one system at a time.
- B. Users are identified to multiple systems with several credentials.
- C. Users are authenticated to multiple systems with one login.
- D. Only one user is using the system at a time.

Answer: C

NEW QUESTION 228

- (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 233

- (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 238

- (Exam Topic 10)

Which of the following provides effective management assurance for a Wireless Local Area Network (WLAN)?

- A. Maintaining an inventory of authorized Access Points (AP) and connecting devices
- B. Setting the radio frequency to the minimum range required
- C. Establishing a Virtual Private Network (VPN) tunnel between the WLAN client device and a VPN concentrator
- D. Verifying that all default passwords have been changed

Answer: A

NEW QUESTION 241

- (Exam Topic 10)

According to best practice, which of the following groups is the MOST effective in performing an information security compliance audit?

- A. In-house security administrators
- B. In-house Network Team
- C. Disaster Recovery (DR) Team
- D. External consultants

Answer: D

NEW QUESTION 243

- (Exam Topic 10)

During an investigation of database theft from an organization's web site, it was determined that the Structured Query Language (SQL) injection technique was used despite input validation with client-side scripting. Which of the following provides the GREATEST protection against the same attack occurring again?

- A. Encrypt communications between the servers
- B. Encrypt the web server traffic
- C. Implement server-side filtering
- D. Filter outgoing traffic at the perimeter firewall

Answer: C

NEW QUESTION 246

- (Exam Topic 10)

What physical characteristic does a retinal scan biometric device measure?

- A. The amount of light reflected by the retina
- B. The size, curvature, and shape of the retina
- C. The pattern of blood vessels at the back of the eye
- D. The pattern of light receptors at the back of the eye

Answer: C

NEW QUESTION 247

- (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 252

- (Exam Topic 10)

What does secure authentication with logging provide?

- A. Data integrity
- B. Access accountability
- C. Encryption logging format
- D. Segregation of duties

Answer: B

NEW QUESTION 257

- (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 260

- (Exam Topic 10)

According to best practice, which of the following is required when implementing third party software in a production environment?

- A. Scan the application for vulnerabilities
- B. Contract the vendor for patching
- C. Negotiate end user application training
- D. Escrow a copy of the software

Answer: A

NEW QUESTION 263

- (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. What MUST the plan include in order to reduce client-side exploitation?

- A. Approved web browsers
- B. Network firewall procedures
- C. Proxy configuration
- D. Employee education

Answer: D

NEW QUESTION 266

- (Exam Topic 10)

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

- A. Brute force attack
- B. Frequency analysis
- C. Social engineering
- D. Dictionary attack

Answer: C

NEW QUESTION 267

- (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 272

- (Exam Topic 10)

What is the MOST critical factor to achieve the goals of a security program?

- A. Capabilities of security resources
- B. Executive management support
- C. Effectiveness of security management
- D. Budget approved for security resources

Answer: B

NEW QUESTION 277

- (Exam Topic 10)

What is the BEST first step for determining if the appropriate security controls are in place for protecting data at rest?

- A. Identify regulatory requirements
- B. Conduct a risk assessment
- C. Determine business drivers
- D. Review the security baseline configuration

Answer: B

NEW QUESTION 279

- (Exam Topic 10)

What is a common challenge when implementing Security Assertion Markup Language (SAML) for identity integration between on-premise environment and an external identity provider service?

- A. Some users are not provisioned into the service.
- B. SAML tokens are provided by the on-premise identity provider.
- C. Single users cannot be revoked from the service.
- D. SAML tokens contain user information.

Answer: A

NEW QUESTION 280

- (Exam Topic 10)

Which of the following methods provides the MOST protection for user credentials?

- A. Forms-based authentication
- B. Digest authentication
- C. Basic authentication
- D. Self-registration

Answer: B

NEW QUESTION 283

- (Exam Topic 10)

Which of the following is the BEST solution to provide redundancy for telecommunications links?

- A. Provide multiple links from the same telecommunications vendor.
- B. Ensure that the telecommunications links connect to the network in one location.
- C. Ensure that the telecommunications links connect to the network in multiple locations.
- D. Provide multiple links from multiple telecommunications vendors.

Answer: D

NEW QUESTION 288

- (Exam Topic 10)

Which of the following is a detective access control mechanism?

- A. Log review
- B. Least privilege
- C. Password complexity
- D. Non-disclosure agreement

Answer: A

NEW QUESTION 289

- (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 292

- (Exam Topic 10)

Which of the following is the MOST effective attack against cryptographic hardware modules?

- A. Plaintext
- B. Brute force
- C. Power analysis
- D. Man-in-the-middle (MITM)

Answer: C

NEW QUESTION 296

- (Exam Topic 10)

During the procurement of a new information system, it was determined that some of the security requirements were not addressed in the system specification. Which of the following is the MOST likely reason for this?

- A. The procurement officer lacks technical knowledge.
- B. The security requirements have changed during the procurement process.
- C. There were no security professionals in the vendor's bidding team.
- D. The description of the security requirements was insufficient.

Answer: D

NEW QUESTION 298

- (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 302

- (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 303

- (Exam Topic 10)

When is security personnel involvement in the Systems Development Life Cycle (SDLC) process MOST beneficial?

- A. Testing phase
- B. Development phase
- C. Requirements definition phase
- D. Operations and maintenance phase

Answer: C

NEW QUESTION 304

- (Exam Topic 10)

With data labeling, which of the following MUST be the key decision maker?

- A. Information security
- B. Departmental management

- C. Data custodian
- D. Data owner

Answer: D

NEW QUESTION 306

- (Exam Topic 10)

Which of the following is the MOST crucial for a successful audit plan?

- A. Defining the scope of the audit to be performed
- B. Identifying the security controls to be implemented
- C. Working with the system owner on new controls
- D. Acquiring evidence of systems that are not compliant

Answer: A

NEW QUESTION 308

- (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 309

- (Exam Topic 10)

Which of the following MUST system and database administrators be aware of and apply when configuring systems used for storing personal employee data?

- A. Secondary use of the data by business users
- B. The organization's security policies and standards
- C. The business purpose for which the data is to be used
- D. The overall protection of corporate resources and data

Answer: B

NEW QUESTION 311

- (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.

Given the number of priorities, which of the following will MOST likely influence the selection of top initiatives?

- A. Severity of risk
- B. Complexity of strategy
- C. Frequency of incidents
- D. Ongoing awareness

Answer: A

NEW QUESTION 313

- (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 316

- (Exam Topic 10)

Refer to the information below to answer the question.

A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive e-mail, search the web, and use instant messaging. The organization's Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.

Which of the following methods is the MOST effective way of removing the Peer-to-Peer (P2P) program from the computer?

- A. Run software uninstall
- B. Re-image the computer

- C. Find and remove all installation files
- D. Delete all cookies stored in the web browser cache

Answer: B

NEW QUESTION 317

- (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 319

- (Exam Topic 10)

For a service provider, which of the following MOST effectively addresses confidentiality concerns for customers using cloud computing?

- A. Hash functions
- B. Data segregation
- C. File system permissions
- D. Non-repudiation controls

Answer: B

NEW QUESTION 323

- (Exam Topic 10)

An organization decides to implement a partial Public Key Infrastructure (PKI) with only the servers having digital certificates. What is the security benefit of this implementation?

- A. Clients can authenticate themselves to the servers.
- B. Mutual authentication is available between the clients and servers.
- C. Servers are able to issue digital certificates to the client.
- D. Servers can authenticate themselves to the client.

Answer: D

NEW QUESTION 326

- (Exam Topic 10)

Which of the following secure startup mechanisms are PRIMARILY designed to thwart attacks?

- A. Timing
- B. Cold boot
- C. Side channel
- D. Acoustic cryptanalysis

Answer: B

NEW QUESTION 328

- (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 333

- (Exam Topic 10)

Without proper signal protection, embedded systems may be prone to which type of attack?

- A. Brute force
- B. Tampering
- C. Information disclosure
- D. Denial of Service (DoS)

Answer: C

NEW QUESTION 334

- (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 335

- (Exam Topic 10)

Refer to the information below to answer the question.

A large, multinational organization has decided to outsource a portion of their Information Technology (IT) organization to a third-party provider's facility. This provider will be responsible for the design, development, testing, and support of several critical, customer-based applications used by the organization. What additional considerations are there if the third party is located in a different country?

- A. The organizational structure of the third party and how it may impact timelines within the organization
- B. The ability of the third party to respond to the organization in a timely manner and with accurate information
- C. The effects of transborder data flows and customer expectations regarding the storage or processing of their data
- D. The quantity of data that must be provided to the third party and how it is to be used

Answer: C

NEW QUESTION 338

- (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 341

- (Exam Topic 10)

Which of the following is the BEST countermeasure to brute force login attacks?

- A. Changing all canonical passwords
- B. Decreasing the number of concurrent user sessions
- C. Restricting initial password delivery only in person
- D. Introducing a delay after failed system access attempts

Answer: D

NEW QUESTION 346

- (Exam Topic 10)

Which of the following provides the MOST protection against data theft of sensitive information when a laptop is stolen?

- A. Set up a BIOS and operating system password
- B. Encrypt the virtual drive where confidential files can be stored
- C. Implement a mandatory policy in which sensitive data cannot be stored on laptops, but only on the corporate network
- D. Encrypt the entire disk and delete contents after a set number of failed access attempts

Answer: D

NEW QUESTION 351

- (Exam Topic 10)

What is the MOST important reason to configure unique user IDs?

- A. Supporting accountability
- B. Reducing authentication errors
- C. Preventing password compromise
- D. Supporting Single Sign On (SSO)

Answer: A

NEW QUESTION 355

- (Exam Topic 10)

Refer to the information below to answer the question.

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

Organizational policy requires the deletion of user data from Personal Digital Assistant (PDA) devices before disposal. It may not be possible to delete the user data if the device is malfunctioning. Which destruction method below provides the BEST assurance that the data has been removed?

- A. Knurling
- B. Grinding
- C. Shredding
- D. Degaussing

Answer: C

NEW QUESTION 360

- (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 364

- (Exam Topic 11)

Which of the following prevents improper aggregation of privileges in Role Based Access Control (RBAC)?

- A. Hierarchical inheritance
- B. Dynamic separation of duties
- C. The Clark-Wilson security model
- D. The Bell-LaPadula security model

Answer: B

NEW QUESTION 369

- (Exam Topic 11)

The application of which of the following standards would BEST reduce the potential for data breaches?

- A. ISO 9000
- B. ISO 20121
- C. ISO 26000
- D. ISO 27001

Answer: D

NEW QUESTION 372

- (Exam Topic 11)

A health care provider is considering Internet access for their employees and patients. Which of the following is the organization's MOST secure solution for protection of data?

- A. Public Key Infrastructure (PKI) and digital signatures
- B. Trusted server certificates and passphrases
- C. User ID and password
- D. Asymmetric encryption and User ID

Answer: A

NEW QUESTION 377

- (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 382

- (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 387

- (Exam Topic 11)

Which of the following statements is TRUE regarding state-based analysis as a functional software testing technique?

- A. It is useful for testing communications protocols and graphical user interfaces.
- B. It is characterized by the stateless behavior of a process implemented in a function.
- C. Test inputs are obtained from the derived boundaries of the given functional specifications.
- D. An entire partition can be covered by considering only one representative value from that partition.

Answer: A

NEW QUESTION 390

- (Exam Topic 11)

Order the below steps to create an effective vulnerability management process.

Step		Order
Identify risks		1
Implement patch deployment		2
Implement recurring scanning schedule		3
Identify assets		4
Implement change management		5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step		Order
Identify risks	Identify assets	1
Implement patch deployment	Identify risks	2
Implement recurring scanning schedule	Implement change management	3
Identify assets	Implement patch deployment	4
Implement change management	Implement recurring scanning schedule	5

NEW QUESTION 391

- (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 396

- (Exam Topic 11)

What should happen when an emergency change to a system must be performed?

- A. The change must be given priority at the next meeting of the change control board.
- B. Testing and approvals must be performed quickly.
- C. The change must be performed immediately and then submitted to the change board.
- D. The change is performed and a notation is made in the system log.

Answer: B

NEW QUESTION 399

- (Exam Topic 11)

Which of the following is a reason to use manual patch installation instead of automated patch management?

- A. The cost required to install patches will be reduced.
- B. The time during which systems will remain vulnerable to an exploit will be decreased.
- C. The likelihood of system or application incompatibilities will be decreased.
- D. The ability to cover large geographic areas is increased.

Answer: C

NEW QUESTION 403

- (Exam Topic 11)

Which of the following has the GREATEST impact on an organization's security posture?

- A. International and country-specific compliance requirements
- B. Security violations by employees and contractors
- C. Resource constraints due to increasing costs of supporting security
- D. Audit findings related to employee access and permissions process

Answer: A

NEW QUESTION 406

- (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 410

- (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 412

- (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

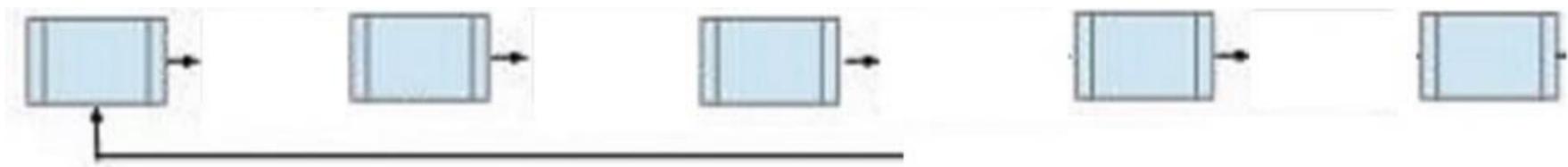
NEW QUESTION 415

- (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.



- Risk Assessment
- Business Impact Analysis
- Mitigation Strategy Development
- BC\DR Plan Development
- Training, Testing & Auditing
- Plan Maintenance

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



- Risk Assessment
- Business Impact Analysis
- Mitigation Strategy Development
- BC\DR Plan Development
- Training, Testing & Auditing
- Plan Maintenance

NEW QUESTION 416

- (Exam Topic 11)

Regarding asset security and appropriate retention, which of the following INITIAL top three areas are important to focus on?

- A. Security control baselines, access controls, employee awareness and training
- B. Human resources, asset management, production management
- C. Supply chain lead time, inventory control, encryption
- D. Polygraphs, crime statistics, forensics

Answer: A

NEW QUESTION 419

- (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 424

- (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 428

- (Exam Topic 11)

Which of the following is the MOST likely cause of a non-malicious data breach when the source of the data breach was an un-marked file cabinet containing sensitive documents?

- A. Ineffective data classification
- B. Lack of data access controls
- C. Ineffective identity management controls
- D. Lack of Data Loss Prevention (DLP) tools

Answer: A

NEW QUESTION 429

- (Exam Topic 11)

Which of the following entities is ultimately accountable for data remanence vulnerabilities with data replicated by a cloud service provider?

- A. Data owner
- B. Data steward
- C. Data custodian
- D. Data processor

Answer: A

NEW QUESTION 433

- (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 434

- (Exam Topic 11)

An organization has hired a security services firm to conduct a penetration test. Which of the following will the organization provide to the tester?

- A. Limits and scope of the testing.
- B. Physical location of server room and wiring closet.
- C. Logical location of filters and concentrators.
- D. Employee directory and organizational chart.

Answer: A

NEW QUESTION 438

- (Exam Topic 11)

When planning a penetration test, the tester will be MOST interested in which information?

- A. Places to install back doors
- B. The main network access points
- C. Job application handouts and tours
- D. Exploits that can attack weaknesses

Answer: B

NEW QUESTION 440

- (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 445

- (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 450

- (Exam Topic 11)

A software security engineer is developing a black box-based test plan that will measure the system's reaction to incorrect or illegal inputs or unexpected operational errors and situations. Match the functional testing techniques on the left with the correct input parameters on the right.

Functional Testing Techniques		Input Parameter Selection
State-Based Analysis		Select one input that does not belong to any of the identified partitions.
Equivalence Class Analysis		Select inputs that are at the external limits of the domain of valid values.
Decision Table Analysis		Select invalid combinations of input values.
Boundary Value Analysis		Select unexpected inputs corresponding to each known condition.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Functional Testing Techniques		Input Parameter Selection
State-Based Analysis	Equivalence Class Analysis	Select one input that does not belong to any of the identified partitions.
Equivalence Class Analysis	Boundary Value Analysis	Select inputs that are at the external limits of the domain of valid values.
Decision Table Analysis	Decision Table Analysis	Select invalid combinations of input values.
Boundary Value Analysis	State-Based Analysis	Select unexpected inputs corresponding to each known condition.

NEW QUESTION 453

- (Exam Topic 11)

Which of the following explains why record destruction requirements are included in a data retention policy?

- A. To comply with legal and business requirements
- B. To save cost for storage and backup
- C. To meet destruction guidelines
- D. To validate data ownership

Answer: A

NEW QUESTION 456

- (Exam Topic 11)

The BEST example of the concept of "something that a user has" when providing an authorized user access to a computing system is

- A. the user's hand geometry.
- B. a credential stored in a token.
- C. a passphrase.
- D. the user's face.

Answer: B

NEW QUESTION 460

- (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 461

- (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 463

- (Exam Topic 11)

A security professional is asked to provide a solution that restricts a bank teller to only perform a savings deposit transaction but allows a supervisor to perform corrections after the transaction. Which of the following is the MOST effective solution?

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

Answer: C

NEW QUESTION 466

- (Exam Topic 11)

For privacy protected data, which of the following roles has the highest authority for establishing dissemination rules for the data?

- A. Information Systems Security Officer
- B. Data Owner
- C. System Security Architect
- D. Security Requirements Analyst

Answer: B

NEW QUESTION 470

- (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 473

- (Exam Topic 11)

The implementation of which features of an identity management system reduces costs and administration overhead while improving audit and accountability?

- A. Two-factor authentication
- B. Single Sign-On (SSO)
- C. User self-service
- D. A metadirectory

Answer: C

NEW QUESTION 477

- (Exam Topic 11)

Application of which of the following Institute of Electrical and Electronics Engineers (IEEE) standards will prevent an unauthorized wireless device from being attached to a network?

- A. IEEE 802.1F
- B. IEEE 802.1H
- C. IEEE 802.1Q
- D. IEEE 802.1X

Answer: D

NEW QUESTION 480

- (Exam Topic 11)

Drag the following Security Engineering terms on the left to the BEST definition on the right.

Security Engineering

Security Risk Treatment

Definition

The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.

Threat Assessment

A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence.

Protection Needs

The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.

Risk

The method used to identify feasible security risk mitigation options and plans.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Security Engineering

Definition

Security Risk Treatment

Protection Needs

The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.

Threat Assessment

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence.

Protection Needs

Threat Assessment

The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.

Risk

Security Risk Treatment

The method used to identify feasible security risk mitigation options and plans.

NEW QUESTION 484

- (Exam Topic 11)

The PRIMARY security concern for handheld devices is the

- A. strength of the encryption algorithm.
- B. spread of malware during synchronization.
- C. ability to bypass the authentication mechanism.
- D. strength of the Personal Identification Number (PIN).

Answer: C

NEW QUESTION 485

- (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 487

- (Exam Topic 11)

Data leakage of sensitive information is MOST often concealed by which of the following?

- A. Secure Sockets Layer (SSL)
- B. Secure Hash Algorithm (SHA)
- C. Wired Equivalent Privacy (WEP)
- D. Secure Post Office Protocol (POP)

Answer: A

NEW QUESTION 488

- (Exam Topic 11)

What does an organization FIRST review to assure compliance with privacy requirements?

- A. Best practices
- B. Business objectives
- C. Legal and regulatory mandates
- D. Employee's compliance to policies and standards

Answer: C

NEW QUESTION 492

- (Exam Topic 11)

An organization has decided to contract with a cloud-based service provider to leverage their identity as a service offering. They will use Open Authentication (OAuth) 2.0 to authenticate external users to the organization's services.

As part of the authentication process, which of the following must the end user provide?

- A. An access token
- B. A username and password
- C. A username
- D. A password

Answer: A

NEW QUESTION 494

- (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 497

- (Exam Topic 11)

Which of the following methods can be used to achieve confidentiality and integrity for data in transit?

- A. Multiprotocol Label Switching (MPLS)
- B. Internet Protocol Security (IPSec)
- C. Federated identity management
- D. Multi-factor authentication

Answer: B

NEW QUESTION 502

- (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 506

- (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 509

- (Exam Topic 11)

A network scan found 50% of the systems with one or more critical vulnerabilities. Which of the following represents the BEST action?

- A. Assess vulnerability risk and program effectiveness.
- B. Assess vulnerability risk and business impact.
- C. Disconnect all systems with critical vulnerabilities.
- D. Disconnect systems with the most number of vulnerabilities.

Answer: B

NEW QUESTION 512

- (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 517

- (Exam Topic 11)

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

- A. After the system preliminary design has been developed and the data security categorization has been performed
- B. After the business functional analysis and the data security categorization have been performed
- C. After the vulnerability analysis has been performed and before the system detailed design begins
- D. After the system preliminary design has been developed and before the data security categorization begins

Answer: B

NEW QUESTION 522

- (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 524

- (Exam Topic 11)

Which of the following BEST describes the purpose of the security functional requirements of Common Criteria?

- A. Level of assurance of the Target of Evaluation (TOE) in intended operational environment
- B. Selection to meet the security objectives stated in test documents
- C. Security behavior expected of a TOE
- D. Definition of the roles and responsibilities

Answer: C

NEW QUESTION 526

- (Exam Topic 11)

A Simple Power Analysis (SPA) attack against a device directly observes which of the following?

- A. Static discharge
- B. Consumption
- C. Generation
- D. Magnetism

Answer: B

NEW QUESTION 528

- (Exam Topic 11)

In the Open System Interconnection (OSI) model, which layer is responsible for the transmission of binary data over a communications network?

- A. Application Layer
- B. Physical Layer
- C. Data-Link Layer
- D. Network Layer

Answer:

B

NEW QUESTION 533

- (Exam Topic 11)

While investigating a malicious event, only six days of audit logs from the last month were available. What policy should be updated to address this problem?

- A. Retention
- B. Reporting
- C. Recovery
- D. Remediation

Answer: A

NEW QUESTION 537

- (Exam Topic 11)

Which of the following is the MOST important output from a mobile application threat modeling exercise according to Open Web Application Security Project (OWASP)?

- A. Application interface entry and endpoints
- B. The likelihood and impact of a vulnerability
- C. Countermeasures and mitigations for vulnerabilities
- D. A data flow diagram for the application and attack surface analysis

Answer: D

NEW QUESTION 540

- (Exam Topic 11)

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

- A. Improper deployment of the Service-Oriented Architecture (SOA)
- B. Absence of a Business Intelligence (BI) solution
- C. Inadequate cost modeling
- D. Insufficient Service Level Agreement (SLA)

Answer: D

NEW QUESTION 541

- (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 544

- (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 549

- (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 551

- (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 555

- (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 558

- (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 559

- (Exam Topic 12)

What is the difference between media marking and media labeling?

- A. Media marking refers to the use of human-readable security attributes, while media labeling refers to the use of security attributes in internal data structures.
- B. Media labeling refers to the use of human-readable security attributes, while media marking refers to the use of security attributes in internal data structures.
- C. Media labeling refers to security attributes required by public policy/law, while media marking refers to security required by internal organizational policy.
- D. Media marking refers to security attributes required by public policy/law, while media labeling refers to security attributes required by internal organizational policy.

Answer: D

NEW QUESTION 561

- (Exam Topic 12)

Match the name of access control model with its associated restriction.

Drag each access control model to its appropriate restriction access on the right.

<u>Access Control Model</u>	<u>Restrictions</u>
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:

- 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 roles permissions to particular duties based on job function
- Rule Based access control – Dynamically assigns roles to subjects based on criteria assigned by a custodian.

NEW QUESTION 562

- (Exam Topic 12)

The restoration priorities of a Disaster Recovery Plan (DRP) are based on which of the following documents?

- A. Service Level Agreement (SLA)
- B. Business Continuity Plan (BCP)
- C. Business Impact Analysis (BIA)
- D. Crisis management plan

Answer: B

NEW QUESTION 565

- (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 570

- (Exam Topic 12)

A company has decided that they need to begin maintaining assets deployed in the enterprise. What approach should be followed to determine and maintain ownership information to bring the company into compliance?

- A. Enterprise asset management framework
- B. Asset baseline using commercial off the shelf software
- C. Asset ownership database using domain login records
- D. A script to report active user logins on assets

Answer: A

NEW QUESTION 571

- (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 572

- (Exam Topic 12)

Which of the following is a strategy of grouping requirements in developing a Security Test and Evaluation (ST&E)?

- A. Tactical, strategic, and financial
- B. Management, operational, and technical
- C. Documentation, observation, and manual
- D. Standards, policies, and procedures

Answer: B

NEW QUESTION 576

- (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 578

- (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 580

- (Exam Topic 12)

Which of the following is MOST important when deploying digital certificates?

- A. Validate compliance with X.509 digital certificate standards
- B. Establish a certificate life cycle management framework
- C. Use a third-party Certificate Authority (CA)
- D. Use no less than 256-bit strength encryption when creating a certificate

Answer: B

NEW QUESTION 582

- (Exam Topic 12)

During which of the following processes is least privilege implemented for a user account?

- A. Provision
- B. Approve
- C. Request
- D. Review

Answer: A

NEW QUESTION 584

- (Exam Topic 12)

Which of the following is a document that identifies each item seized in an investigation, including date and time seized, full name and signature or initials of the person who seized the item, and a detailed description of the item?

- A. Property book
- B. Chain of custody form
- C. Search warrant return
- D. Evidence tag

Answer: D

NEW QUESTION 588

- (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 589

- (Exam Topic 12)

The PRIMARY purpose of accreditation is to:

- A. comply with applicable laws and regulations.
- B. allow senior management to make an informed decision regarding whether to accept the risk of operating the system.
- C. protect an organization's sensitive data.
- D. verify that all security controls have been implemented properly and are operating in the correct manner.

Answer: B

NEW QUESTION 594

- (Exam Topic 12)

Match the access control type to the example of the control type. Drag each access control type net to its corresponding example.

<u>Access Control Type</u>	<u>Example</u>
Administrative	Labeling of sensitive data
Technical	Biometrics for authentication
Logical	Constrained user interface
Physical	Radio Frequency Identification (RFID) badge

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Administrative – labeling of sensitive data
 Technical – Constrained user interface
 Logical – Biometrics for authentication
 Physical – Radio Frequency Identification (RFID) badge

NEW QUESTION 595

- (Exam Topic 12)

Which of the following BEST describes Recovery Time Objective (RTO)?

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

Answer: A

NEW QUESTION 600

- (Exam Topic 12)

A database administrator is asked by a high-ranking member of management to perform specific changes to the accounting system database. The administrator is specifically instructed to not track or evidence the change in a ticket. Which of the following is the BEST course of action?

- A. Ignore the request and do not perform the change.
- B. Perform the change as requested, and rely on the next audit to detect and report the situation.
- C. Perform the change, but create a change ticket regardless to ensure there is complete traceability.
- D. Inform the audit committee or internal audit directly using the corporate whistleblower process.

Answer: D

NEW QUESTION 602

- (Exam Topic 12)

In general, servers that are facing the Internet should be placed in a demilitarized zone (DMZ). What is MAIN purpose of the DMZ?

- A. Reduced risk to internal systems.
- B. Prepare the server for potential attacks.
- C. Mitigate the risk associated with the exposed server.
- D. Bypass the need for a firewall.

Answer: A

NEW QUESTION 603

- (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 605

- (Exam Topic 12)

A company was ranked as high in the following National Institute of Standards and Technology (NIST) functions: Protect, Detect, Respond and Recover. However, a low maturity grade was attributed to the Identify function. In which of the following the controls categories does this company need to improve when analyzing its processes individually?

- A. Asset Management, Business Environment, Governance and Risk Assessment
- B. Access Control, Awareness and Training, Data Security and Maintenance
- C. Anomalies and Events, Security Continuous Monitoring and Detection Processes
- D. Recovery Planning, Improvements and Communications

Answer: A

NEW QUESTION 610

- (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 612

- (Exam Topic 12)

At which layer of the Open Systems Interconnect (OSI) model are the source and destination address for a datagram handled?

- A. Transport Layer
- B. Data-Link Layer
- C. Network Layer
- D. Application Layer

Answer: C

NEW QUESTION 617

- (Exam Topic 12)

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

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

Answer: B

NEW QUESTION 619

- (Exam Topic 12)

Which of the following approaches is the MOST effective way to dispose of data on multiple hard drives?

- A. Delete every file on each drive.
- B. Destroy the partition table for each drive using the command line.
- C. Degauss each drive individually.
- D. Perform multiple passes on each drive using approved formatting methods.

Answer: D

NEW QUESTION 622

- (Exam Topic 12)

What is an advantage of Elliptic Curve Cryptography (ECC)?

- A. Cryptographic approach that does not require a fixed-length key
- B. Military-strength security that does not depend upon secrecy of the algorithm
- C. Opportunity to use shorter keys for the same level of security
- D. Ability to use much longer keys for greater security

Answer: C

NEW QUESTION 625

- (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 629

- (Exam Topic 12)

Which of the following is BEST suited for exchanging authentication and authorization messages in a multi-party decentralized environment?

- A. Lightweight Directory Access Protocol (LDAP)
- B. Security Assertion Markup Language (SAML)
- C. Internet Mail Access Protocol
- D. Transport Layer Security (TLS)

Answer: B

NEW QUESTION 633

- (Exam Topic 12)

In the Software Development Life Cycle (SDLC), maintaining accurate hardware and software inventories is a critical part of

- A. systems integration.
- B. risk management.
- C. quality assurance.
- D. change management.

Answer: D

NEW QUESTION 634

- (Exam Topic 12)

An organization regularly conducts its own penetration tests. Which of the following scenarios MUST be covered for the test to be effective?

- A. Third-party vendor with access to the system
- B. System administrator access compromised
- C. Internal attacker with access to the system
- D. Internal user accidentally accessing data

Answer: C

NEW QUESTION 636

- (Exam Topic 12)

A security architect plans to reference a Mandatory Access Control (MAC) model for implementation. This indicates that which of the following properties are being prioritized?

- A. Confidentiality
- B. Integrity
- C. Availability
- D. Accessibility

Answer: C

NEW QUESTION 641

- (Exam Topic 12)

In order to assure authenticity, which of the following are required?

- A. Confidentiality and authentication
- B. Confidentiality and integrity
- C. Authentication and non-repudiation
- D. Integrity and non-repudiation

Answer: D

NEW QUESTION 643

- (Exam Topic 12)

The goal of a Business Impact Analysis (BIA) is to determine which of the following?

- A. Cost effectiveness of business recovery
- B. Cost effectiveness of installing software security patches
- C. Resource priorities for recovery and Maximum Tolerable Downtime (MTD)
- D. Which security measures should be implemented

Answer: C

NEW QUESTION 645

- (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 648

- (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 650

- (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 653

- (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 654

- (Exam Topic 12)

For network based evidence, which of the following contains traffic details of all network sessions in order to detect anomalies?

- A. Alert data
- B. User data
- C. Content data
- D. Statistical data

Answer: D

NEW QUESTION 658

- (Exam Topic 12)

Reciprocal backup site agreements are considered to be

- A. a better alternative than the use of warm sites.
- B. difficult to test for complex systems.
- C. easy to implement for similar types of organizations.
- D. easy to test and implement for complex systems.

Answer: B

NEW QUESTION 661

- (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 665

- (Exam Topic 12)

When building a data classification scheme, which of the following is the PRIMARY concern?

- A. Purpose
- B. Cost effectiveness
- C. Availability

D. Authenticity

Answer: D

NEW QUESTION 667

- (Exam Topic 12)

Which technology is a prerequisite for populating the cloud-based directory in a federated identity solution?

- A. Notification tool
- B. Message queuing tool
- C. Security token tool
- D. Synchronization tool

Answer: C

NEW QUESTION 668

- (Exam Topic 12)

During the Security Assessment and Authorization process, what is the PRIMARY purpose for conducting a hardware and software inventory?

- A. Calculate the value of assets being accredited.
- B. Create a list to include in the Security Assessment and Authorization package.
- C. Identify obsolete hardware and software.
- D. Define the boundaries of the information system.

Answer: A

NEW QUESTION 669

- (Exam Topic 12)

Which of the following countermeasures is the MOST effective in defending against a social engineering attack?

- A. Mandating security policy acceptance
- B. Changing individual behavior
- C. Evaluating security awareness training
- D. Filtering malicious e-mail content

Answer: C

NEW QUESTION 673

- (Exam Topic 12)

Which of the following is the PRIMARY reason to perform regular vulnerability scanning of an organization network?

- A. Provide vulnerability reports to management.
- B. Validate vulnerability remediation activities.
- C. Prevent attackers from discovering vulnerabilities.
- D. Remediate known vulnerabilities.

Answer: B

NEW QUESTION 678

- (Exam Topic 13)

Which one of the following data integrity models assumes a lattice of integrity levels?

- A. Take-Grant
- B. Biba
- C. Harrison-Ruzzo
- D. Bell-LaPadula

Answer: B

NEW QUESTION 681

- (Exam Topic 13)

Which of the following is the BEST reason for writing an information security policy?

- A. To support information security governance
- B. To reduce the number of audit findings
- C. To deter attackers
- D. To implement effective information security controls

Answer: A

NEW QUESTION 685

- (Exam Topic 13)

Which of the following is the MOST effective method to mitigate Cross-Site Scripting (XSS) attacks?

- A. Use Software as a Service (SaaS)

- B. Whitelist input validation
- C. Require client certificates
- D. Validate data output

Answer: B

NEW QUESTION 690

- (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 691

- (Exam Topic 13)

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

- A. Implement processes for automated removal of access for terminated employees.
- B. Delete employee network and system IDs upon termination.
- C. Manually remove terminated employee user-access to all systems and applications.
- D. Disable terminated employee network ID to remove all access.

Answer: B

NEW QUESTION 692

- (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 697

- (Exam Topic 13)

A control to protect from a Denial-of-Service (DoS) attack has been determined to stop 50% of attacks, and additionally reduces the impact of an attack by 50%. What is the residual risk?

- A. 25%
- B. 50%
- C. 75%
- D. 100%

Answer: A

NEW QUESTION 702

- (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 707

- (Exam Topic 13)

Why is planning in Disaster Recovery (DR) an interactive process?

- A. It details off-site storage plans
- B. It identifies omissions in the plan
- C. It defines the objectives of the plan
- D. It forms part of the awareness process

Answer: B

NEW QUESTION 709

- (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 711

- (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 714

- (Exam Topic 13)

Who is responsible for the protection of information when it is shared with or provided to other organizations?

- A. Systems owner
- B. Authorizing Official (AO)
- C. Information owner
- D. Security officer

Answer: C

Explanation:

Section: Security Operations

NEW QUESTION 718

- (Exam Topic 13)

In an organization where Network Access Control (NAC) has been deployed, a device trying to connect to the network is being placed into an isolated domain. What could be done on this device in order to obtain proper connectivity?

- A. Connect the device to another network jack
- B. Apply remediation's according to security requirements
- C. Apply Operating System (OS) patches
- D. Change the Message Authentication Code (MAC) address of the network interface

Answer: B

NEW QUESTION 719

- (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 723

- (Exam Topic 13)

An international medical organization with headquarters in the United States (US) and branches in France wants to test a drug in both countries. What is the organization allowed to do with the test subject's data?

- A. Aggregate it into one database in the US
- B. Process it in the US, but store the information in France
- C. Share it with a third party
- D. Anonymize it and process it in the US

Answer: C

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 725

- (Exam Topic 13)

Which of the following are important criteria when designing procedures and acceptance criteria for acquired software?

- A. Code quality, security, and origin
- B. Architecture, hardware, and firmware
- C. Data quality, provenance, and scaling
- D. Distributed, agile, and bench testing

Answer: A

NEW QUESTION 730

- (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 734

- (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 736

- (Exam Topic 13)

Drag the following Security Engineering terms on the left to the BEST definition on the right.

Security Engineering Term

Definition

Risk		A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of
Security Risk Treatment		The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Protection Needs Assessment		The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Threat Assessment		The method used to identify feasible security risk mitigation options and plans.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Risk - A measure of the extent to which an entity is threatened by a potential circumstance of event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence.

Protection Needs Assessment - The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should be asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Threat assessment - The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Security Risk Treatment - The method used to identify feasible security risk mitigation options and plans.

NEW QUESTION 737

- (Exam Topic 13)

Unused space in a disk cluster is important in media analysis because it may contain which of the following?

- A. Residual data that has not been overwritten
- B. Hidden viruses and Trojan horses
- C. Information about the File Allocation table (FAT)
- D. Information about patches and upgrades to the system

Answer: A

NEW QUESTION 738

- (Exam Topic 13)

Which of the following could be considered the MOST significant security challenge when adopting DevOps practices compared to a more traditional control framework?

- A. Achieving Service Level Agreements (SLA) on how quickly patches will be released when a security flaw is found.
- B. Maintaining segregation of duties.
- C. Standardized configurations for logging, alerting, and security metrics.
- D. Availability of security teams at the end of design process to perform last-minute manual audits and reviews.

Answer: B

NEW QUESTION 739

- (Exam Topic 13)

A Denial of Service (DoS) attack on a syslog server exploits weakness in which of the following protocols?

- A. Point-to-Point Protocol (PPP) and Internet Control Message Protocol (ICMP)
- B. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)
- C. Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP)
- D. Transport Layer Security (TLS) and Secure Sockets Layer (SSL)

Answer: B

NEW QUESTION 744

- (Exam Topic 13)

Which security modes is MOST commonly used in a commercial environment because it protects the integrity of financial and accounting data?

- A. Biba
- B. Graham-Denning
- C. Clark-Wilson
- D. Beil-LaPadula

Answer: C

NEW QUESTION 745

- (Exam Topic 13)

What is the process of removing sensitive data from a system or storage device with the intent that the data cannot be reconstructed by any known technique?

- A. Purging
- B. Encryption
- C. Destruction
- D. Clearing

Answer: A

NEW QUESTION 749

- (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 754

- (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 756

- (Exam Topic 13)

An organization has outsourced its financial transaction processing to a Cloud Service Provider (CSP) who will provide them with Software as a Service (SaaS). If there was a data breach who is responsible for monetary losses?

- A. The Data Protection Authority (DPA)
- B. The Cloud Service Provider (CSP)
- C. The application developers
- D. The data owner

Answer: B

NEW QUESTION 759

- (Exam Topic 13)

A security practitioner is tasked with securing the organization's Wireless Access Points (WAP). Which of these is the MOST effective way of restricting this environment to authorized users?

- A. Enable Wi-Fi Protected Access 2 (WPA2) encryption on the wireless access point
- B. Disable the broadcast of the Service Set Identifier (SSID) name
- C. Change the name of the Service Set Identifier (SSID) to a random value not associated with the organization
- D. Create Access Control Lists (ACL) based on Media Access Control (MAC) addresses

Answer: D

NEW QUESTION 760

- (Exam Topic 13)

Which of the following methods of suppressing a fire is environmentally friendly and the MOST appropriate for a data center?

- A. Inert gas fire suppression system
- B. Halon gas fire suppression system
- C. Dry-pipe sprinklers
- D. Wet-pipe sprinklers

Answer: C

NEW QUESTION 765

- (Exam Topic 13)

Which of the following is a responsibility of the information owner?

- A. Ensure that users and personnel complete the required security training to access the Information System (IS)
- B. Defining proper access to the Information System (IS), including privileges or access rights
- C. Managing identification, implementation, and assessment of common security controls
- D. Ensuring the Information System (IS) is operated according to agreed upon security requirements

Answer: C

NEW QUESTION 770

- (Exam Topic 13)

Which type of test would an organization perform in order to locate and target exploitable defects?

- A. Penetration
- B. System
- C. Performance
- D. Vulnerability

Answer: A

NEW QUESTION 772

- (Exam Topic 13)

The core component of Role Based Access Control (RBAC) must be constructed of defined data elements. Which elements are required?

- A. Users, permissions, operations, and protected objects
- B. Roles, accounts, permissions, and protected objects
- C. Users, roles, operations, and protected objects
- D. Roles, operations, accounts, and protected objects

Answer: C

NEW QUESTION 774

- (Exam Topic 13)

In a change-controlled environment, which of the following is MOST likely to lead to unauthorized changes to production programs?

- A. Modifying source code without approval
- B. Promoting programs to production without approval
- C. Developers checking out source code without approval
- D. Developers using Rapid Application Development (RAD) methodologies without approval

Answer: B

NEW QUESTION 778

- (Exam Topic 13)

Assessing a third party's risk by counting bugs in the code may not be the best measure of an attack surface within the supply chain. Which of the following is LEAST associated with the attack surface?

- A. Input protocols
- B. Target processes
- C. Error messages
- D. Access rights

Answer: C

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 780

- (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 781

- (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 783

- (Exam Topic 13)

Transport Layer Security (TLS) provides which of the following capabilities for a remote access server?

- A. Transport layer handshake compression
- B. Application layer negotiation
- C. Peer identity authentication
- D. Digital certificate revocation

Answer: C

NEW QUESTION 785

- (Exam Topic 13)

Which of the following entails identification of data and links to business processes, applications, and data stores as well as assignment of ownership responsibilities?

- A. Security governance
- B. Risk management
- C. Security portfolio management
- D. Risk assessment

Answer: B

NEW QUESTION 788

- (Exam Topic 13)

What MUST each information owner do when a system contains data from multiple information owners?

- A. Provide input to the Information System (IS) owner regarding the security requirements of the data
- B. Review the Security Assessment report (SAR) for the Information System (IS) and authorize the IS to operate.
- C. Develop and maintain the System Security Plan (SSP) for the Information System (IS) containing the data
- D. Move the data to an Information System (IS) that does not contain data owned by other information owners

Answer: C

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 792

- (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 794

- (Exam Topic 13)

After following the processes defined within the change management plan, a super user has upgraded a device within an Information system. What step would be taken to ensure that the upgrade did NOT affect the network security posture?

- A. Conduct an Assessment and Authorization (A&A)
- B. Conduct a security impact analysis
- C. Review the results of the most recent vulnerability scan
- D. Conduct a gap analysis with the baseline configuration

Answer: B

Explanation:

Section: Security Assessment and Testing

NEW QUESTION 795

- (Exam Topic 13)

What is the foundation of cryptographic functions?

- A. Encryption
- B. Cipher
- C. Hash
- D. Entropy

Answer: A

NEW QUESTION 798

- (Exam Topic 13)

At a MINIMUM, audits of permissions to individual or group accounts should be scheduled

- A. annually
- B. to correspond with staff promotions
- C. to correspond with terminations
- D. continually

Answer: A

NEW QUESTION 803

- (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 808

- (Exam Topic 13)

What does a Synchronous (SYN) flood attack do?

- A. Forces Transmission Control Protocol /Internet Protocol (TCP/IP) connections into a reset state
- B. Establishes many new Transmission Control Protocol / Internet Protocol (TCP/IP) connections
- C. Empties the queue of pending Transmission Control Protocol /Internet Protocol (TCP/IP) requests
- D. Exceeds the limits for new Transmission Control Protocol /Internet Protocol (TCP/IP) connections

Answer: B

NEW QUESTION 812

- (Exam Topic 13)

Who has the PRIMARY responsibility to ensure that security objectives are aligned with organization goals?

- A. Senior management
- B. Information security department
- C. Audit committee
- D. All users

Answer: C

NEW QUESTION 814

- (Exam Topic 13)

A minimal implementation of endpoint security includes which of the following?

- A. Trusted platforms
- B. Host-based firewalls
- C. Token-based authentication
- D. Wireless Access Points (AP)

Answer: A

NEW QUESTION 816

- (Exam Topic 13)

An organization has discovered that users are visiting unauthorized websites using anonymous proxies. Which of the following is the BEST way to prevent future occurrences?

- A. Remove the anonymity from the proxy
- B. Analyze Internet Protocol (IP) traffic for proxy requests
- C. Disable the proxy server on the firewall
- D. Block the Internet Protocol (IP) address of known anonymous proxies

Answer: C

NEW QUESTION 817

- (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 820

- (Exam Topic 13)

Which of the following alarm systems is recommended to detect intrusions through windows in a high-noise, occupied environment?

- A. Acoustic sensor
- B. Motion sensor
- C. Shock sensor
- D. Photoelectric sensor

Answer: C

NEW QUESTION 824

- (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 828

- (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 833

- (Exam Topic 13)

What is the correct order of steps in an information security assessment?

Place the information security assessment steps on the left next to the numbered boxes on the right in the correct order.

<u>Actions</u>		<u>Steps</u>
Define the perimeter.		Step 1
Identify the vulnerability.		Step 2
Assess the risk.		Step 3
Determine the actions.		Step 4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

Steps

Define the perimeter.
Identify the vulnerability.
Assess the risk.
Determine the actions.

Identify the vulnerability.	Step 1
Define the perimeter.	Step 2
Assess the risk.	Step 3
Determine the actions.	Step 4

NEW QUESTION 837

- (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 842

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CISSP Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CISSP Product From:

<https://www.2passeasy.com/dumps/CISSP/>

Money Back Guarantee

CISSP Practice Exam Features:

- * CISSP Questions and Answers Updated Frequently
- * CISSP Practice Questions Verified by Expert Senior Certified Staff
- * CISSP Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CISSP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year