ISC2

Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

NEW QUESTION 1
- (Exam Topic 15)
Which of the following does the security design process ensure within the System Development Life Cycle (SDLC)?

A. Proper security controls, security goals, and fault mitigation are properly conducted.
B. Proper security controls, security objectives, and security goals are properly initiated.
C. Security goals, proper security controls, and validation are properly initiated.
D. Security objectives, security goals, and system test are properly conducted.

Answer: B

NEW QUESTION 2
- (Exam Topic 15)
Wireless users are reporting intermittent Internet connectivity. Connectivity is restored when the users disconnect and reconnect, utilizing the web authentication process each time.
The network administrator can see the devices connected to the APs at all times. Which of the following steps will MOST likely determine the cause of the issue?

A. Verify the session time-out configuration on the captive portal settings
B. Check for encryption protocol mismatch on the client's wireless settings.
C. Confirm that a valid passphrase is being used during the web authentication.
D. Investigate for a client's disassociation caused by an evil twin AP

Answer: A

NEW QUESTION 3
- (Exam Topic 15)
A database server for a financial application is scheduled for production deployment. Which of the following controls will BEST prevent tampering?

A. Service accounts removal
B. Data validation
C. Logging and monitoring
D. Data sanitization

Answer: B

NEW QUESTION 4
- (Exam Topic 15)
Which of the following actions should be taken by a security professional when a mission critical computer network attack is suspected?

A. Isolate the network, log an independent report, fix the problem, and redeploy the computer.
B. Isolate the network, install patches, and report the occurrence.
C. Prioritize, report, and investigate the occurrence.
D. Turn the rooter off, perform forensic analysis, apply the appropriate fin, and log incidents.

Answer: C

NEW QUESTION 5
- (Exam Topic 15)
Which of the following Disaster recovery (DR) testing processes is LEAST likely to disrupt normal business operations?

A. Parallel
B. Simulation
C. Table-top
D. Cut-over

Answer: C

NEW QUESTION 6
- (Exam Topic 15)
In a multi-tenant cloud environment, what approach will secure logical access to assets?

A. Hybrid cloud
B. Transparency/Auditability of administrative access
C. Controlled configuration management (CM)
D. Virtual private cloud (VPC)

Answer: D

NEW QUESTION 7
- (Exam Topic 15)
Management has decided that a core application will be used on personal cellular phones. As an implementation requirement, regularly scheduled analysis of the security posture needs to be conducted. Management has also directed that continuous monitoring be implemented. Which of the following is required to accomplish management’s directive?

A. Strict integration of application management, configuration management (CM), and phone management

B. Management application installed on user phones that tracks all application events and cellular traffic
C. Enterprise-level security information and event management (SIEM) dashboard that provides full visibility of cellular phone activity
D. Routine reports generated by the user's cellular phone provider that detail security events

Answer: B

NEW QUESTION 8
- (Exam Topic 15)
Which of the following is the PRIMARY goal of logical access controls?

A. Restrict access to an information asset.
B. Ensure integrity of an information asset.
C. Restrict physical access to an information asset.
D. Ensure availability of an information asset.

Answer: C

NEW QUESTION 9
- (Exam Topic 15)
Which of the following vulnerability assessment activities BEST exemplifies the Examine method of assessment?

A. Ensuring that system audit logs capture all relevant data fields required by the security controls baseline
B. Performing Port Scans of selected network hosts to enumerate active services
C. Asking the Information System Security Officer (ISSO) to describe the organization’s patch management processes
D. Logging into a web server using the default administrator account and a default password

Answer: D

NEW QUESTION 10
- (Exam Topic 15)
Which of the following needs to be tested to achieve a Cat 6a certification for a company's data cabling?

A. RJ11
B. LC ports
C. Patch panel
D. F-type connector

Answer: C

NEW QUESTION 11
- (Exam Topic 15)
Which is the PRIMARY mechanism for providing the workforce with the information needed to protect an agency’s vital information resources?

A. Incorporating security awareness and training as part of the overall information security program
B. An information technology (IT) security policy to preserve the confidentiality, integrity, and availability of systems
C. Implementation of access provisioning process for coordinating the creation of user accounts
D. Execution of periodic security and privacy assessments to the organization

Answer: A

NEW QUESTION 12
- (Exam Topic 15)
Of the following, which BEST provides non- repudiation with regards to access to a server room?

A. Fob and Personal Identification Number (PIN)
B. Locked and secured cages
C. Biometric readers
D. Proximity readers

Answer: C

NEW QUESTION 13
- (Exam Topic 15)
Compared to a traditional network, which of the following is a security-related benefit that software-defined networking (SDN) provides?

A. Centralized network provisioning
B. Centralized network administrator control
C. Reduced network latency when scaled
D. Reduced hardware footprint and cost

Answer: B

NEW QUESTION 14
- (Exam Topic 15)
Which of the following techniques evaluates the secure design principles of network OF software architectures?

A. Risk modeling
B. Threat modeling
C. Fuzzing
D. Waterfall method

Answer: B

NEW QUESTION 15
- (Exam Topic 15)
Which part of an operating system (OS) is responsible for providing security interfaces among the hardware, OS, and other parts of the computing system?

A. Time separation
B. Trusted Computing Base (TCB)
C. Reference monitor
D. Security kernel

Answer: D

NEW QUESTION 16
- (Exam Topic 14)
Functional security testing is MOST critical during which phase of the system development life cycle (SDLC)?

A. Operations / Maintenance
B. Implementation
C. Acquisition / Development
D. Initiation

Answer: B

NEW QUESTION 17
- (Exam Topic 14)
Which of the following is a PRIMARY challenge when running a penetration test?

A. Determining the cost
B. Establishing a business case
C. Remediating found vulnerabilities
D. Determining the depth of coverage

Answer: D

NEW QUESTION 18
- (Exam Topic 14)
Which of the following is the MOST significant benefit to implementing a third-party federated identity architecture?

A. Attribute assertions as agencies can request a larger set of attributes to fulfill service delivery
B. Data decrease related to storing personal information
C. Reduction in operational costs to the agency
D. Enable business objectives so departments can focus on mission rather than the business of identitymanagement

Answer: C

NEW QUESTION 19
- (Exam Topic 14)
What is a common mistake in records retention?

A. Having the organization legal department create a retention policy
B. Adopting a retention policy based on applicable organization requirements
C. Having the Human Resource (HR) department create a retention policy
D. Adopting a retention policy with the longest requirement period

Answer: C

NEW QUESTION 20
- (Exam Topic 14)
Which of the following provides the BEST method to verify that security baseline configurations are maintained?

A. Perform regular system security testing.
B. Design security early in the development cycle.
C. Analyze logs to determine user activities.
D. Perform quarterly risk assessments.

Answer: A

NEW QUESTION 21
- (Exam Topic 13)

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

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

Answer: D

NEW QUESTION 22
- (Exam Topic 13)
What can happen when an Intrusion Detection System (IDS) is installed inside a firewall-protected internal network?

A. The IDS can detect failed administrator logon attempts from servers.
B. The IDS can increase the number of packets to analyze.
C. The firewall can increase the number of packets to analyze.
D. The firewall can detect failed administrator login attempts from servers

Answer: A

NEW QUESTION 23
- (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 24
- (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 25
- (Exam Topic 9)
The key benefits of a signed and encrypted e-mail include

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

Answer: B

NEW QUESTION 26
- (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 27
- (Exam Topic 9)
The PRIMARY purpose of a security awareness program is to

A. ensure that everyone understands the organization's policies and procedures.
B. communicate that access to information will be granted on a need-to-know basis.
C. warn all users that access to all systems will be monitored on a daily basis.
D. comply with regulations related to data and information protection.

Answer: A

NEW QUESTION 28
- (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 29
- (Exam Topic 7)
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. Absence of a Business Intelligence (BI) solution
B. Inadequate cost modeling
C. Improper deployment of the Service-Oriented Architecture (SOA)
D. Insufficient Service Level Agreement (SLA)

Answer: D

NEW QUESTION 30
- (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 31
......