CISSP CBK Review Final Exam

1. A risk is the likelihood of a threat source taking advantage of a vulnerability to an information system. Risks left over after implementing safeguards is known as:

   A. Leftover risks.

   B. Residual risks.

   C. Remaining risks.

   D. Exposures.

2. Copyright provides what form of protection:

   A. Protects an author's right to distribute his/her works.

   B. Protects information that provides a competitive advantage.

   C. Protects the right of an author to prevent unauthorized use of his/her works.

   D. Protects the right of an author to prevent viewing of his/her works.

3. As an information systems security professional, what is the highest amount would you recommend to a corporation to invest annually on a countermeasure for protecting their assets valued at $1 million from a potential threat that has an annualized rate of occurrence (ARO) of once every five years and an exposure factor (EF) of 10% :

   A. $100,000.

   B. $20,000.

   C. $200,000.

   D. $40,000.

4. Which of the following describes the first step in establishing an encrypted session using a Data Encryption Standard (DES) key?

   A. Key clustering

   B. Key compression

   C. Key signing

   D. Key exchange

5. In a typical information security program, what is the primary responsibility of information (data) owner?

   A. Ensure the validity and accuracy of data.

   B. Determine the information sensitivity or classification level.

C. Monitor and audit system users.

D. Ensure availability of data.

6. Which of the following is not a component of "chain of evidence":

A. Location evidence obtained.

B. Time evidence obtained.

C. Who discovered the evidence.

D. Identification of person who left the evidence.

7. When an employee transfers within an organization …

A. The employee must undergo a new security review.

B. The old system IDs must be disabled.

C. All access permission should be reviewed.

D. The employee must turn in all access devices.

8. A system security engineer is evaluation methods to store user passwords in an information system, so what may be the best method to store user passwords and meeting the confidentiality security objective?

A. Password-protected file

B. File restricted to one individual

C. One-way encrypted file

D. Two-way encrypted file

9. What is the inverse of confidentiality, integrity, and availability (C.I.A.) triad in risk management?

A. misuse, exposure, destruction

B. authorization, non-repudiation, integrity

C. disclosure, alteration, destruction

D. confidentiality, integrity, availability

10. A CISSP may face with an ethical conflict between their company's policies and the $(ISC)^2$ Code of Ethics. According to the $(ISC)^2$ Code of Ethics, in which order of priority should ethical conflicts be resolved?

A. Duty to principals, profession, public safety, and individuals.

B. Duty to public safety, principals, individuals, and profession.

C. Duty to profession, public safety, individuals, and principals.

D. Duty to public safety, profession, individuals, and principals.

11. Company X is planning to implement rule based access control mechanism for controlling access to its information assets, what type of access control is this usually related to?

A. Discretionary Access Control

B. Task-initiated Access Control

C. Subject-dependent Access Control

D. Token-oriented Access Control

12. In the Common Criteria Evaluation and Validation Scheme (CCEVS), requirements for future products are defined by:

A. Protection Profile.

B. Target of Evaluation.

C. Evaluation Assurance Level 3.

D. Evaluation Assurance Level 7.

13. As an information systems security manager (ISSM), how would you explain the purpose for a system security policy?

A. A definition of the particular settings that have been determined to provide optimum security

B. A brief, high-level statement defining what is and is not permitted during the operation of the system

C. A definition of those items that must be excluded on the system

D. A listing of tools and applications that will be used to protect the system

14. Configuration management provides assurance that changes…?

A. to application software cannot bypass system security features.

B. do not adversely affect implementation of the security policy.

C. to the operating system are always subjected to independent validation and verification.

D. in technical documentation maintain an accurate description of the Trusted Computer Base.

15. Under what circumstance might a certification authority (CA) revoke a certificate?

    A. The certificate owner has not utilized the certificate for an extended period.

    B. The certificate owner public key has been compromised.

    C. The certificate owner' private key has been compromised.

    D. The certificate owner has upgraded his/her web browser.

16. Which of the following entity is ultimately responsible for information security within an organization?

    A. IT Security Officer

    B. Project Managers

    C. Department Directors

    D. Senior Management

17. What type of cryptanalytic attack where an adversary has the least amount of information to work with?

    A. Known-plaintext

    B. Ciphertext-only

    C. Plaintext-only

    D. Chosen-ciphertext

18. In business continuity planning, which of the following is an advantage of a "hot site" over a "cold site"

    A. Air Conditioning

    B. Cost

    C. Short period to become operational

    D. A & C

19. Which of the following is the most effective method for reducing security risks associated with building entrances?

    A. Minimize the number of entrances

    B. Use solid metal doors and frames

    C. Brightly illuminate the entrances

    D. Install tamperproof hinges and glass

20. All of the following methods ensure the stored data are unreadable except…?

    A. writing random data over the old file.
    B. physical alteration of media.
    C. degaussing the disk or tape.
    D. removing the volume header information.

21. Prior to installation of an intrusion prevention system (IPS), a network engineer would place a packet sniffer on the network, what is the purpose for using a packet sniffer?

    A. It tracks network connections.
    B. It monitors network traffic.
    C. It scans network segments for cabling faults.
    D. It detects illegal packets on the network.

22. What determines the assignment of data classifications in a mandatory access control (MAC) philosophy?

    A. The analysis of the users in conjunction with the audit department
    B. The assessment by the information security department
    C. The user's evaluation of a particular information element
    D. The organization's published security policy for data classification

23. A type cryptographic attack where it is based on the probability of two different messages using the same hash function to produce the same message digest is?

    A. Birthday attack
    B. Statistic attack
    C. Differential cryptanalysis attack
    D. Known ciphertext attack

24. An access control system that grants users only those rights necessary for them to perform their work is operating on which security principle?

    A. Discretionary Access
    B. Least Privilege
    C. Mandatory Access

D. Separation of Duties

25. Which of the following is the primary goal of a security awareness program?

A. It provides a vehicle for communicating security procedures.

B. It provides a clear understanding of potential risk and exposure.

C. It provides a forum for disclosing exposure and risk analysis.

D. It provides a forum to communicate user responsibilities.

26. Which of the following evidence collection method is most likely accepted in a court case?

A. Provide a full system backup inventory.

B. Create a file-level archive of all files.

C. Provide a mirror image of the hard drive.

D. Copy all files accessed at the time of the incident.

27. Which of the following characteristics is not of a good stream cipher?

A. Long periods of no repeating patterns.

B. Statistically predictable.

C. Keystream is not linearly related to the key.

D. Statistically unbiased keystream.

28. When a security administrator wants to conduct regular test on the strength of user passwords, what may be the best setup for this test?

A. A networked laptop with Rainbow table that have direct access to the live password database.

B. A standalone workstation with Rainbow table and a copied password database.

C. A networked workstation with Rainbow table and a copied password database.

D. This is not possible, because the password database is encrypted.

29. When engaging an external contractor for a software development project, source code escrow can be used to protect against…?

A. system data loss.

B. vendor bankruptcy.

C. copyright violation.

D. legal liability.

30. Which answer lists the proper steps required to develop a disaster recovery and business continuity plan (DRP/BCP)?

A. Project initiation, business impact analysis, strategy development, plan development, testing, maintenance.

B. Strategy development, project initiation, business impact analysis, plan development, testing, maintenance.

C. Business impact analysis, project initiation, strategy development, plan development, testing, maintenance.

D. Project initiation, plan development, business impact analysis, strategy development, testing, maintenance.

31. Which of the followings is an example of simple substitution algorithm?

A. Rivest, Shamir, Adleman (RSA)

B. Data Encryption Standard (DES)

C. Caesar cipher

D. Blowfish

32. An information security program should include the following elements:

A. Disaster recovery and business continuity planning, and definition of access control requirements and human resources policies.

B. Business impact, threat and vulnerability analysis, delivery of an information security awareness program, and physical security of key installations.

C. Security policy implementation, assignment of roles and responsibilities, and information asset classification.

D. Senior management organizational structure, message distribution standards, and procedures for the operation of security management systems.

33. Which of the following refers to a series of characters used to verify a user's identity?

A. Token serial number

B. User ID

C. Password

D. Security ticket

34. Which e-mail standard relies on "Web of Trust"?

A. Pretty Good Privacy (PGP)

B. Privacy Enhanced Mail (PEM)

C. MIME Object Security Services (MOSS)

D. Secure Multipurpose Internet Mail Extensions (S/MIME)

35. Security of an automated information system is most effective and economical if the system is…?

A. optimized prior to addition of security.

B. customized to meet the specific security threat.

C. subjected to intense security testing.

D. designed originally to meet the information protection needs.

36. Act of obtaining information of a higher level of sensitivity by combining information from lower level of sensitivity is called?

A. Aggregation

B. Data mining

C. Inference

D. Polyinstantiation

37. Which of the following virus types changes its characteristics as it spreads?

A. Boot sector

B. Parasitic

C. Stealth

D. Polymorphic

38. It is important that information about an ongoing computer crime investigation be…?

A. destroyed as soon after trial as possible.

B. reviewed by upper management before being released.

C. replicated to a backup system to ensure availability.

D. limited to as few people as possible.

39. Which answer is not true for Diffie-Hellman algorithm?

A. Security stems from the difficulty of calculating the product of two large prime numbers.

B. It was the first public key exchange algorithm.

C. It is vulnerable to man-in-the-middle attacks.

D. It is used for distribution of a shared key, not for message encryption and decryption.

40. After signing out a laptop computer from the company loaner pool, you discovered there is a memorandum stored in the loaner laptop written to a competitor containing sensitive information about a new product your company is about to release. Based on the $(ISC)^2$ Code of Ethics, what is the first action you should take?

A. Delete the memorandum from the laptop to ensure no one else will see it.

B. Contact the author of the memorandum to let him/her know the memorandum was on the laptop.

C. Immediately inform your company's management of your findings and its potential ramifications.

D. Inform the security awareness trainers that data disclosure prevention in a mobile computing environment needs to be added to their classes.

41. Job rotation…?

A. makes it more difficult to detect fraudulent activities.

B. is the same as separation of duties.

C. requires that more than one person fulfill the tasks of one position within the company, thereby providing both backup and redundancy.

D. does not make it harder for an employee to commit fraudulent activities without other fining out, especially since it aids in obscuring who did what.

42. Which of the following is the least important information to record when logging a security violation?

A. User's name

B. User id.

C. Type of violation

D. Date and time of the violation

43. Which of the following mechanism is used to achieve non-repudiation of a message delivery?

    A. Sender encrypts the message with the recipients public key and signs it with their own private key.

    B. Sender computes a digest of the message and sends it to a Trusted Third Party (TTP) who signs it and stores it for later reference.

    C. Sender sends the message to a TTP who signs it together with a time stamp and sends it on to the recipient.

    D. Sender gets a digitally signed acknowledgment from the recipient containing a copy or digest of the message.

44. What is the trusted registry that guarantees the authenticity of client and server public keys?

    A. Public key notary.

    B. Certification authority.

    C. Key distribution center.

    D. Key revocation certificate.

45. The concept that all accesses must be mediated, protected from unauthorized modification, and verifiable as correct is implemented through what?

    A. A security model.

    B. A reference monitor.

    C. A security kernel.

    D. A trusted computing base.

46. For what reason would a network administrator leverages promiscuous mode on a network interface?

    A. To screen out all network errors that affect network statistical information.

    B. To monitor the network to gain a complete statistical picture of activity.

    C. To monitor only unauthorized activity and use.

    D. To capture only unauthorized internal/external use.

47. Which has the flag used for a TCP 3-way handshake?

    A. Syn ->: Syn-Fin <-: Ack ->

    B. Ack ->: Syn-Ack <-: Syn ->

C. Syn ->: Syn-Ack <-: Ack ->

D. Syn ->: Ack <-: Ack ->

48. During a disaster or emergency, how does a closed-circuit television (CCTV) help management and security to minimize loss?

A. It helps the management to direct resources to the hardest hit area.

B. It records instances of looting and other criminal activities.

C. It documents shortcomings of plans and procedures.

D. It captures the exposure of assets to physical risk.

49. The goal of cryptanalysis is to…?

A. forge coded signals that will be accepted as authentic.

B. ensure that the key has no repeating segments.

C. reduce the system overhead for cryptographic functions.

D. determine the number of encryption permutations required.

50. Which one of the followings cannot be identified by a business impact analysis (BIA)?

A. Analyzing the threats associated with each functional area.

B. Determining risks associated with threats.

C. Identifying major functional areas of information.

D. Determining team members associated with disaster planning.

51. The three primary methods for authenticating users to a system or network are…?

A. passwords, tokens, and biometrics.

B. authorization, identification, and tokens.

C. passwords, encryption, and identification.

D. identification, encryption, and authorization.

52. Pretty Good Privacy (PGP) provides…?

A. confidentiality, integrity, and authenticity.

B. integrity, availability, and authentication.

C. availability, authentication, and non-repudiation.

D. authorization, non-repudiation, and confidentiality.

53. Which of the following can be identified when exceptions occur using operations security detective controls?

A. Unauthorized people seeing printed confidential reports.

B. Unauthorized people destroying confidential reports.

C. Authorized operations people performing unauthorized functions.

D. Authorized operations people not responding to important console messages.

54. When downloading software from Internet, why do vendors publish MD5 hash values when they provide software to customers?

A. Recipients can verify the software's integrity after downloading.

B. Recipients can confirm the authenticity of the site from which they are downloading the patch.

C. Recipients can request future updates to the software by using the assigned hash value.

D. Recipients need the hash value to successfully activate the new software.

55. From a legal perspective, which rule must be addressed when investigating a computer crime?

A. Search and seizure

B. Data protection

C. Engagement

D. Evidence

56. Before powering off a computer system, a computer crime investigator should record contents of the monitor and…?

A. save the contents of the spooler queue.

B. dump the memory contents to a disk.

C. backup the hard drive.

D. collect the owner's boot up disks.

57. Which of the following transaction processing properties ensures once a transaction completes successfully (commits), the updates survive even if there is a system failure?

A. Atomicity.

B. Consistency.

C. Isolation.

D. Durability.

58. Which of the following is not a symmetric key algorithm?

A. RC4.

B. Blowfish.

C. DES.

D. RSA.

59. A security planning process must defines: how security will be managed, who will be responsible, and…?

A. what practices are reasonable and prudent for the enterprise.

B. who will work in the security department.

C. what impact security will have on the intrinsic value of data.

D. how security measures will be tested for effectiveness.

60. A security policy provides a way to…?

A. establish a cost model for security activities.

B. allow management to define system recovery requirements.

C. identify and clarify security goals and objectives.

D. enable management to define system access rules.

61. Which of the following feature does a digital signature provide?

A. It provides the ability to encrypt an individual's confidential data.

B. It ensures an individual's privacy.

C. It identifies the source and verifies the integrity of data.

D. It provides a framework for law and procedures.

62. Computer security is generally considered to be the responsibility of…?

A. everyone in the organization.

B. corporate management.

C. the corporate security staff.

D. everyone with computer access.

63. The practice of embedding a message in a document, image, video or sound recording so that its very existence is hidden is called?

A. Anonymity.

B. Steganography.

C. Shielding.

D. Data diddling.

64. What characteristic of Digital Encryption Standard (DES) used in Electronic Code Book (ECB) mode makes it unsuitable for long messages?

A. Block fragmentation causes message cipher instability.

B. Weak keys will produce symmetrical message holes.

C. Each message block produces a single cipher text block.

D. Repeated message blocks produce repeated cipher text blocks.

65. Separation of duties should be…?

A. enforced in all organizational areas.

B. cost justified for the potential for loss.

C. enforced in the program testing phase of application development.

D. determined by the availability of trained staff.

66. What is the advantage of Rivest, Shamir, Adelman (RSA) public key system over the Digital Signature Algorithm (DSA)?

A. It uses the secure hash algorithm to condense a message before signing.

B. It can be used for encryption.

C. It cannot be compromised through substitution.

D. It uses the function of escrowed encryption.

67. In IPsec, what is the standard format that helps to establish and manage the security association (SA) between two internetworking entities?

A. Internet Security Association and Key Management Protocol (ISAKMP)

B. Internet Key Exchange (IKE)

C. Diffie-Hellman Key Exchange

D. Authentication Header (AH)

68. When securing Internet connections which of the following should be used to protect internal routing and labeling schemes?

A. Virtual Private Networks (VPN)

B. Layer 2 Tunneling Protocol (L2TP)

C. Domain Name Systems (DNS)

D. Network Address Translation (NAT)

69. Which of the following describes the step prior to an encrypted session using Data Encryption Standard (DES)?

A. Key clustering

B. Key compression

C. Key signing

D. Key exchange

70. What is a set of step-by-step instructions used to satisfy control requirements called?

A. Policy

B. Standard

C. Guideline

D. Procedure

71. The accounting branch of a large organization requires an application to process expense vouchers. Each voucher must be input by one of many accounting clerks, verified by the clerk's applicable supervisor, then reconciled by an auditor before the reimbursement check is produced. Which access control technique should be built into the application to best serve these requirements?

A. Mandatory Access Control (MAC)

B. Password Security

C. Role-based Access Control (RBAC)

D. Terminal Access Controller Access System (TACACS)

72. What principle recommends division of responsibilities so that one person cannot commit an undetected fraud?

A. Separation of duties

B. Mutual exclusion

C. Need to know

D. Least privilege

73. In what situation would TEMPEST risks and technologies be of most interest?

A. Where high availability is vital

B. Where the consequences of disclosure are very high

C. Where countermeasures are easy to implement

D. Where data base integrity is crucial

74. Which of the following is true about information that is designated with the highest level of confidentiality in a private sector organization?

A. It is limited to named individuals and creates an audit trail.

B. It is restricted to those in the department of origin for the information.

C. It is available to anyone in the organization whose work relates to the subject and requires authorization for each access.

D. It is classified only by the information security officer and restricted to those who have made formal requests for access.

75. When verifying key control objectives of a system design, the security specialist should ensure that the…?

A. final system design has security administrator approval.

B. auditing procedures have been defined.

C. vulnerability assessment has been completed.

D. impact assessment has been approved.

76. What type of controls is not utilized to achieve management directives to protect company assets?

A. Administrative controls

B. Technical controls

C. Physical controls

D. Financial controls

77. All of the followings are hashing algorithms except…?

A. SHA

B. IDEA

C. HAVAL

D. MD2

78. Security management practice focuses on the continual protection of:

A. Company assets

B. Classified information

C. Security-related hardware and software

D. Company data

79. The likelihood of a threat source taking advantage of a vulnerability is called?

A. Vulnerability

B. Threat

C. Risk

D. Exposure

80. An instance of being exposed to losses is called?

A. Vulnerably

B. Threat

C. Risk

D. Exposure

81. Reference monitor requires which of the following conditions?

A. Policy, mechanism and assurance

B. Isolation, layering and abstraction

C. Isolation, completeness and verifiability

D. Confidentiality, availability and integrity

82. A person in possession of a sample of ciphertext and corresponding plaintext is capable of what type of attack?

A. Known-plaintext

B. Ciphertext only

C. Chosen-plaintext

D. Plaintext

83. Methods of handling risk include all of the followings except:

A. Transferring risk

B. Reducing risk

C. Accepting risk

D. Selling risk

84. Which of the following is not true regarding security policy?

A. It is a general statement

B. It is promulgated by senior IT security staff

C. It describes the role of security in the organization

D. It is broad

85. Which of the following describes the activities that assure protection mechanisms are maintained and operational?

A. Due care

B. Due diligence

C. Due care but not due diligence

D. Due care and due diligence

86. When there is a “separation of duties”, parts of tasks are assigned to different people so that:

A. Collusion is required to perform an unauthorized act.

B. Better planning is required to break into systems.

C. Defense-in-depth is achieved by creating multiple layers an attacker must circumvent.

D. The weakest link, people, are not easily flipped.

87. Which of the following is not a generally accepted benefit of security awareness, training and education?

A. A security awareness program can help operators understand the value of the information.

B. A security education program can help system administrators recognize unauthorized intrusion attempts.

C. A security awareness and training program will help prevent natural disasters from occurring.

D. A security awareness and training program can help an organization reduce the number and severity of errors and omissions.

88. Which statement below is an incorrect description of a security control?

A. Detective controls discover attacks and trigger preventive or corrective controls

B. Corrective controls reduce the likelihood of a deliberate attack

C. Corrective controls reduce the affect of a an attack

D. Controls are the countermeasures for vulnerabilities

89. Physical security is accomplished through proper facility construction, fire and water protection, anti-theft mechanisms, intrusion detection systems, and security procedures that are adhered to and enforced. Which of the following is not a component that achieves this type of security?

A. Technical control mechanisms

B. Administrative control mechanisms

C. Physical control mechanisms

D. Integrity control mechanisms

90. In a typical information security program, who would be responsible for providing reports to the corporate executives and senior management on the effectiveness of the instituted program controls?

A. Auditors

B. Information systems security manager (ISSM)

C. Information systems security officer (ISSO)

D. Information systems security professionals

91. What is the difference between quantitative and qualitative risk analysis?

A. Qualitative analysis uses mathematical formulas and while quantitative analysis does not.

B. Purely qualitative analysis is not possible, while purely quantitative is possible.

C. Quantitative analysis provides formal cost/benefit information while qualitative analysis does not.

D. There is no difference between qualitative and quantitative analysis.

92. If risk is defined as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets" the risk has all of the following elements except?

A. An impact of assets based on threats and vulnerabilities.

B. Controls addressing the threats.

C. Threats to and vulnerabilities of processes and/or assets.

D. Probabilities of the threats.

93. Which statement below most accurately reflects the goal of risk mitigation?

A. Defining the acceptable level of risk the organization can tolerate, then reduce risk to that level.

B. Analyzing and removing all vulnerabilities and threats to security within the organization.

C. Defining the acceptable level of risk the organization can tolerate, and assigning any costs associated with loss or disruption to a third party such as an insurance carrier.

D. Analyzing the effects of a business disruption and preparing the company's response.

94. Risk analysis allows you to do all of the following except:

A. Quantify the impact of potential risks

B. Create an economic balance between the impact of a risk and the cost of a countermeasure

C. Provides a cost/benefit comparison

D. Prevent risk

95. Which of the following is not true with respect to qualitative risk analysis?

A. It uses scenarios.

B. It is based on judgment, intuition and experience.

C. May include the Delphi technique.

D. Results in concrete probability percentages.

96. Which choice below is an accurate statement about standards?

A. Standards are the high-level statements made by senior management in support of information systems security.

B. Standards are the first element created in an effective security policy program.

C. Standards are used to describe how policies will be implemented within an organization.

D. Standards are senior management's directives to create a computer security program.

97. A memory address location specified in a program instruction that contains the address of final memory location is known as:

A. Implied addressing.

B. Indexed addressing.

C. Indirect addressing.

D. Register addressing.

98. Which one of the following hardware devices can be re-programmed?

1 Read Only Memory (ROM).

2 Programmable Read Only Memory (PROM).

3 Erasable Programmable Read Only Memory (EPROM).

4 Electrically Erasable Programmable Read Only Memory (EEPROM).

A. 1 and 3.

B. 3 and 4.

C. 1 and 4.

D. 2 and 3.

99. A processing methodology that executes two or more tasks on a single processor is known as:

A. Scalar.

B. Multiprocessing.

C. Multitasking.

D. Multiprogramming.

100. Which of the following is a high-level language?

A. BASIC.

B. Machine.

C. Assembly.

D. BIOS.

101. Which of the followings are security concerns with distributed systems?

A. Downloaded data from the Internet via the web or through e-mail may infect other computers.

B. Desktop systems may not be properly secured.

C. Unauthorized access to a secured network could be made through remote control or terminal server programs running on a desktop.

D. A, B, and C.

102. Trusted Computing Base (TCB) is comprised of what combination of system components?

1 Hardware.

2 Firmware.

3 Software.

A. 1 and 3.

B. 2 and 3.

C. 1 and 2.

D. All of the above.

103. Reference monitor _____.

A. controls access to subjects.

B. controls access to objects.

C. controls objects access by subjects.

D. controls objects access to subjects.

104. Which security mode best defines where users have both the required clearance and the need-to-know for all data on a system?

A. Dedicated.

B. Limited access.

C. Controlled.

D. Compartmented.

105. Otherwise known as a “trap door”, this vulnerability is often built into a system.

A. Covert channel.

B. Maintenance hook.

C. TOC/TOU.

D. No parameter checking.

106. What criteria went into the Common Criteria standard?

A. TCSEC.

B. ITSEC.

C. Canadian Trusted Computer Evaluation Criteria.

D. All of the above.

107. Which of the following is the European evaluation criteria standard?

A. TCSEC.

B. ITSEC.

C. IPSec.

D. CTCEC.

108. In the following top-down Common Criteria evaluation process, what is the missing component:

Protection Profile → Target of Evaluation → <???> → Security Functionality/Assurance Requirements → Evaluation → Evaluation Assurance Level

A. Certification Domain.

B. Integrity Assessment.

C. Security Domain.

D. Security Target.

109. A cipher that scrambles letters into different positions is referred to as what?

A. Substitution

B. Stream

C. Running key

D. Transposition

110. The HAVAL algorithms perform what function?

A. Hashing

B. Key distribution

C. Digital signature

D. Encryption

111. Which security model focuses on confidentiality only?

A. Bell-LaPadula.

B. Biba.

C. Clark-Wilson.

D. Biba and Clark-Wilson.

112. Which of the following includes the definition of procedures for emergency response?

A. Operations Planning

B. Disaster Recovery Planning

C. Business Continuity Planning

D. Backup Planning

113. Which of the following team should be part of the disaster recovery procedures?

A. Test Team

B. Management Team

C. Salvage Team

D. IT Team

114. A characteristic of security model that enforces information flow in only one direction is:

A. Access triple.

B. Lattice.

C. Star property.

D. Chinese wall.

115. The business continuity planning (BCP) project management and initiation phase does not involve?

A. Establishing members of the BCP team.

B. Determining the need for automated data collection tools.

C. Performing a business impact analysis (BIA).

D. Preparing and presenting status reports.

116. In what way does the RSA algorithm differs from the Data Encryption Standard (DES)?

A. It cannot produce a digital signature.

B. It eliminates the need for a key-distribution center.

C. It is based on a symmetric algorithm.

D. It uses a public key for encryption.

117. Information flow models:

A. Allow for dynamically changing access controls.

B. Ensure one domain does not affect another domain.

C. Ensure that data moves in a way that does not violate security policy.

D. Ensure the system is secure through all state transitions.

118. Which type of network is more likely to include Frame Relay, Switched Multi-megabit Data Services (SMDS), and X.25?

A. Local area network (LAN)

B. Wide area network (WAN)

C. Intranet

D. Internet

119. Which device can Forward, Filter, and Flood?

A. Switch

B. Router

C. Hub

D. Repeater

120. Which of the following is not a good description of Pretty Good Privacy (PGP)?

A. It uses a web of trust between the participants

B. It uses a hierarchical trust model

C. It was created by Phil Zimmerman

D. It uses passphrases

121. Match the correct network connection speed to the correct standard.

Standard	Speed
802.11	?
802.11b	?
802.11g	?

1. 1 & 2 Mbps
2. 4 & 8 Mbps
3. 11 Mbps
4. 54 Mbps

A. 1-3-4

B. 4-3-1

C. 1-3-3

D. 1-4-4

122. Which is not a type of service available with ATM?

A. MBR (Minimum Bit Rate)

B. CBR (Constant Bit Rate)

C. UBR (Unspecified Bit Rate)

D. ABR (Available Bit Rate)

123. MAC (Media Access Control) and LLC (Logical Link Control) have been designated to which layer by the IEEE?

A. Physical Layer

B. Data-Link Layer

C. Network Layer

D. Transport Layer

124. ____ is when a layer 3 packet is modified to fit into a layer 2 network with different characteristics.

A. Segmentation

B. Fragmentation

C. Reassembly

D. Packetization

125. What is the role of asymmetric key cryptography in public key infrastructure (PKI) applications?

A. It is used for key management.

B. It is used for key storage.

C. It is used for key generation.

D. It is used for key recovery.

126. Which routing protocol is used to allow hosts to participate in multicasting?

A. OSPF (Open Shortest Path First)

B. IGMP (Internet Group Management Protocol)

C. RIP (Routing Information Protocol)

D. BGP (Border Gateway Protocol)

127. ARP and RARP are used to map which?

A. MAC addresses to DNS hostnames

B. MAC address to IP address

C. IP addresses to DNS hostnames

D. DNS hostname to NetBIOs

128. Use the unique response from a given system to identify the operating system running on a host is also known as _____.

A. Casing

B. OS fingerprinting

C. Phreaking

D. Phishing

129. Which is the best defense against network sniffing?

A. Use of switches (over hubs)

B. Use of wired networks (not wireless)

C. Use of gateway

D. Encryption

130. A Smurf attack takes advantage of which of the following?

A. ICMP messages to a network's broadcast address.

B. SYN buffers on a host.

C. Overlapping IP fragments.

D. Oversized ICMP packets.

131. Which is not true about fair cryptosystems?

A. It splits the private key into different parts.

B. It gives law enforcement access when legally authorized.

C. It escrows the separate key parts with separate escrow agencies.

D. It uses a tamper proof chip.

132. A system where a user authenticates, is disconnected, and the receiving system connects back to a number in a pre-defined database is also known as which?

A. Callback

B. Call forward

C. Remote Access

D. Port knocking

133. What does Advanced Encryption Standard (AES) do?

A. It creates a message digest for integrity

B. It performs symmetric key distribution

C. It performs bulk data encryption

D. It performs key recovery

134. A Sockets (SOCKS) gateways can be classified as which type of firewall?

A. Stateless filtering

B. Stateful filtering

C. Circuit-level

D. Application-level

135. RFC 1918 extended IPv4 with the introduction of non-routable addresses in support of which technology below?

A. IPSec

B. NAT

C. DMZ

D. DCE

136. In configuration management, a configuration item is?

A. The version of the operating system, which is operating on the work station, that provides information security services.

B. A component whose state is to be recorded and against which changes are to be progressed.

C. The network architecture used by the organization.

D. A series of files that contain sensitive information.

137. In software development life cycle, the Waterfall Model assumes that…?

A. Iteration will be required among the steps in the process.

B. Each step can be completed and finalized without any effect from the later stages that may require rework.

C. Each phase is identical to a completed milestone.

D. Software development requires reworking and repeating some of the phases.

138. What does the Spiral SDLC Model depicts?

A. A spiral that incorporates various phases of software development

B. A spiral that models the behavior of biological neurons

C. The operation of expert systems

D. Information security checklists.

139. What can best be described as an abstract machine which it must mediate all access of subjects to objects?

A. The reference monitor

B. A security domain

C. The security kernel

D. The security perimeter

140. Which provides a physical connection between the network cabling and the computer's internal bus?

A. Switches

B. Hubs

C. Routers

D. Network interface cards (NICs)

141. What is defined as the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept?

A. Protection rings

B. A security kernel

C. A protection domain

D. The reference monitor

142. Critical areas should be lighted:

A. Ten feet high and six feet out.

B. Ten feet high and four feet out.

C. Eight feet high and four feet out.

D. Eight feet high and two feet out.

143. The percentage of loss a realized threat could have on a certain asset is known as the:

A. Single loss expectancy (SLE)

B. Annualized rate of occurrence (ARO)

C. Exposure factor (EF)

D. Asses value (AV)

144. Why does buffer overflow happen?

A. Because they are an easy weakness to exploit

B. Because buffers can only hold so much data

C. Because input data is not checked for appropriate length at time of input

D. Because of insufficient system memory

145. Referential integrity requires that for any foreign key attribute, the referenced relation must have a tuple with the same value for which of the following?

A. candidate key

B. foreign key

C. secondary key

D. primary key

146. What type of malware is self-contained and it does not need to be part of another computer program to propagate?

A. Computer virus

B. Trojan house

C. Computer worm

D. Polymorphic virus

147. Which of the following represents a prolonged high voltage?

A. A power surge

B. A power fault

C. A power sag

D. A power spike

148. What type of malware that is capable of infect a file with an encrypted copy of itself, then modify itself when decoded to make almost impossible to detect by signature-based virus scanner?

A. Computer virus

B. Trojan house

C. Computer worm

D. Polymorphic virus

149. A timely review of system access records would be an example of which basic security function?

A. Avoidance

B. Deterrence

C. Prevention

D. Detection

150. Which of the following is a reasonable response from the intrusion detection system when it detects Internet Protocol (IP) packets where the IP source address is the same as the IP destination address?

A. Allow the packet to be processed by the network and record the event

B. Record selected information about the item and delete the packet

C. Resolve the destination address and process the packet

D. Translate the source address arid resend the packet

151. A major disadvantage of single sign-on (SSO) is:

A. Consistent time-out enforcement across platforms.

B. A compromised password exposes all authorized resources.

C. Use of multiple passwords to remember.

D. Password change control.

152. Which of the following can be identified when exceptions occur using operations security detective controls?

A. Unauthorized people seeing printed confidential reports.

B. Unauthorized people destroying confidential reports.

C. Authorized operations people performing unauthorized functions.

D. Authorized operations people not responding to important console messages.

153. An access system that grants users only those rights necessary for them to perform their work is operating on follows which security principle?

A. Discretionary Access

B. Least Privilege

C. Mandatory Access

D. Separation of Duties

154. Three principal schemes that provide a framework for managing access control are

A. Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role Based Access Control (RBAC).

B. Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Layer Based Access Protocol (LBAP).

C. Mandatory Access Control (MAC), Layer Based Access Protocol (LBAP), and Target Based Access Protocol (TBAP).

D. Role Based Access Control (RBAC), Layer Based Access Protocol (LBAP), and Target Based Access Protocol (TBAP).

155. When a communication link is subject to monitoring, what is the advantage for using an end-to-end encryption solution over link encryption solution?

A. Cleartext is only available to the sending and receiving entities.

B. Routing information is included in the message transmission protocol.

C. Routing information is encrypted by the originator.

D. Each message has a unique encryption key.

156. To which form of access control is a rule based control mechanism usually related?

A. Discretionary Access Control

B. Task-initiated Access Control

C. Subject-dependent Access Control

D. Token-oriented Access Control

157. Which of the following does a digital signature provide?

A. It provides the ability to encrypt an individual's confidential data.

B. It ensures an individual's privacy.

C. It identifies the source and verifies the integrity of data.

D. It provides a framework for law and procedures.

158. What role does biometrics have in logical access control?

A. Certification

B. Authorization

C. Authentication

D. Confirmation

159. When establishing a violation tracking and analysis process, which one of the following parameters is used to keep the quantity of data to manageable levels?

A. Quantity baseline

B. Maximum log size

C. Circular logging

D. Clipping levels

160. The accounting branch of a large organization requires an application to process expense vouchers. Each voucher must be input by one of many accounting clerks, verified by the clerk's applicable supervisor, then reconciled by an auditor before the reimbursement check is produced. What access control technique should be built into the application to meet the information protection needs?

A. Mandatory Access Control (MAC)

B. Password Security

C. Role-based Access Control (RBAC)

D. Terminal Access Controller Access System (TACACS)

161. What best describes two-factor authentication?

A. Something you know

B. Something you have

C. Something you are

D. A combination of two listed above

162. A timely review of system access records would be an example of which basic security function?

A. Avoidance

B. Deterrence

C. Prevention

D. Detection

163. Which protocol makes use of an electronic wallet on a customer's PC and sends encrypted credit card information to merchant's Web server, which digitally signs it and sends it on to its processing bank?

A. SSH

B. SSL

C. S/MIME

D. SET

164. Risk management helps you do all of the followings except:

A. Identify risks

B. Assess risks

C. Reduce risk to an *acceptable level*

D. Completely avoid risk

165. Which of the following identifies the encryption algorithm selected by NIST for the new Advanced Encryption Standard (AES)?

A. RC6

B. Serpent

C. Rijndael

D. Twofish

166. What is the role of internet key exchange (IKE) within the IPsec protocol?

A. Enforcing quality of service.

B. Data signature.

C. Data encryption.

D. Peer authentication and key exchange.

167. Which type of attack is based on the probability of two different messages using the same hash function producing a common message digest?

A. Statistical attack

B. Differential cryptanalysis

C. Differential linear cryptanalysis

D. Birthday attack

168. Which of the following encryption methods is considered unbreakable?

A. DES codebooks

B. One-time pads

C. Elliptic-curve cryptography

D. Symmetric ciphers

169. The Clipper Chip utilizes which concept in public key cryptography?

A. Key Escrow

B. Substitution

C. An undefined algorithm

D. Super strong encryption

170. Public Key algorithms are:

A. Two times faster than secret key algorithms

B. Two times slower than secret key algorithms

C. 1,000 to 10,000 times slower than secret key algorithms

D. 1,000 to 10,000 times faster than secret key algorithms

171. Cryptography does not concern itself with:

A. Availability

B. Authenticity

C. Integrity

D. Confidentiality

172. Which of the following protects Kerberos against replay attacks?

A. Passwords

B. Cryptography

C. Time stamps

D. Tokens

173. Which network topology offers the highest reliability and availability?

A. Bus

B. Star

C. Ring

D. Mesh

174. A public key algorithm that does both encryption and digital signature is which of the following?

A. RSA

B. DES

C. IDEA

D. DSS

175. Which of the following is the correct calculation?

A. Asset value (%) x exposure factor (%) = single loss expectancy (%)

B. Asset value ($) x exposure factor (%) = single loss expectancy ($)

C. Asset value (%) x exposure factor ($) = single loss expectancy ($)

D. Asset value ($) x exposure factor ($) = single loss expectancy ($)

176. Copies of the original discs and other media are considered as what type of evidence?

A. Primary evidence

B. Reliable evidence

C. Hearsay evidence

D. Conclusive evidence.

177. Which of the following statement is most accurate of digital signature?

A. It allows the recipient of data to prove the source and integrity of data.

B. It can be used as a signature system and a cryptosystem.

C. It is a method used to encrypt confidential data.

D. It is the art of transferring handwritten signature to electronic media.

178. The Diffie-Hellman algorithm is primarily used to provide which of the following?

A. Key exchange

B. Integrity

C. Non-repudiation

D. Confidentiality

179. Of the following, which is most true?

A. RSA gets its strength from the complexity of using discrete logarithms in a finite field

B. El Gamal gets its strength from the complexity of using discrete logarithms in a finite field

C. ECC gets its strength from the complexity of factoring the product of two large prime numbers

D. Diffie-Hellman gets its strength from the complexity of factoring the product of two large prime numbers

180. Which security model addresses integrity?

1. Bell-LaPadula.
2. Clark-Wilson.
3. Biba.
4. Chinese Wall.

A. 1 Only.

B. 1 and 2.

C. 2 and 3.

D. 3 and 4.

181. Of the followings, which is the best description of a digital signature?

A. The sender encrypts a message digest with his/her public key

B. The sender encrypts a message digest with his/her private key

C. The recipient encrypts a message digest with his/her public key

D. The recipient encrypts a message digest with his/her private key

182. What encryption operation is used when AES uses S-boxes during the process of encryption?

A. Substitution

B. Key generation

C. Key exchange

D. Chaining

183. Which item is the responsibility of key management?

A. Key generation and destruction

B. Access controls and encryption

C. Key length and algorithm propriety

D. Access control, user authentication and authorization

184. How many bits make up the effective Data Encryption Standard (DES) key?

A. 56

B. 64

C. 32

D. 16

185. The estimated frequency a threat will occur within a year is known as the:

A. Single loss expectancy (SLE)

B. Annualized rate of occurrence (ARO)

C. Exposure factor (EF)

D. Asses value (AV)

186. What is the Clipper Chip key size?

A. 80 bit

B. 64 bit

C. 128 bit

D. 160 bit

187. When an organization is determining which data is sensitive, it must consider all of the following except:

A. Expectations of customers

B. Legislation or regulations

C. Quantity of data

D. Age of the data

188. Data Encryption Standard (DES) uses which algorithm?

A. RSA

B. IDEA

C. Lucifer

D. RC5

189. To speed up RAID disk access, an organization can:

A. Use larger hard drives.

B. Stripe the data across several drives.

C. Mirror critical drives.

D. Disallow ad hoc queries.

190. Which choice below most accurately describes the organization's responsibilities during an unfriendly termination?

A. System access should be removed as quickly as possible after termination.

B. The employee should be given time to remove whatever files he needs from the network.

C. Cryptographic keys can remain the employee's property.

D. Physical removal from the offices would never be necessary.

191. The concept of least privilege…?

A. assures that employees take mandatory vacations.

B. guarantees that only security personnel can view and change audit logs.

C. helps security personnel catch repetitive mistakes.

D. assures that individuals only have the permissions and rights necessary for them to do their job.

192. Which is most likely to help a company detect fraudulent activity:

A. Mandatory vacations

B. Instituting least privilege

C. Logging

D. Mistakes

193. Clipping level is all of the followings except:

A. Certain dates that require trimming down a devices audit logs.

B. Thresholds for certain types of errors or mistakes.

C. Baselines for violation activities.

D. Recorded for further review once they have been exceeded.

194. Proper change control management involves:

A. Having an undisciplined change control process.

B. Having a well-structured change management process.

C. The immediate implementation of all requested changes so as to assure ultimate customer satisfaction.

D. Assuring that all of the CSO‘s request are immediately implemented.

195. All of the followings are acceptable for sanitizing data except:

A. Deleting it.

B. Overwriting it.

C. Degaussing it.

D. Physically destroying it.

196. Trusted recovery may be defined as:

A. Procedures that restore a system and its data in a trusted manner after the system was disrupted or a system failure occurred.

B. Securely restoring a system after a hard drive failure.

C. Finding missing equipment and verifying that security policies were not violated.

D. An operating system regaining a secure state after a brief lapse into an insecure state.

197. Which of the following is incorrect with respect to a system cold start:

A. Occurs when an unexpected trusted computer base (TCB) or medial failure happens.

B. Occurs when recovery procedure cannot recover the system to a more consistent state.

C. The system, TCB, and user objects may remain in an inconsistent state while the system attempts to recover itself.

D. Systems administrator intervention is typically not necessary to restore the system.

198. Which of the following statements is incorrect:

A. Faxing must be incorporated into security policies.

B. Fax machines are more secure than fax servers.

C. Faxes can be logged and audited.

D. Faxes can be encrypted.

199. ____ tunnels NetBEUI and IPX protocols.

A. PPTP

B. IPsec

C. SSL

D. VPN

200. Which of the following statements regarding session hijacking is incorrect:

A. The ability to spoof IP addresses makes it possible.

B. Involves an attacker inserting him/herself in between two conversing devices.

C. Allows the attacker to pretend he/she is one of the actual endpoints.

D. Cannot be safeguarded against, not even through mutual authentication using protocols such as IPsec.

201. Separation of duty can be defeated by:

A. Mutual exclusivity

B. Collusion

C. Dual control

D. Accreditation

202. Recovery controls attempt to:

A. Establish countermeasures to prevent further incidents

B. Return to normal operations

C. Compensate for vulnerabilities in other systems

D. Ensure that audit logs are reviewed regularly

203. Which of the following questions is less likely to help in assessing physical and environmental protection?

A. Is physical access to data transmission lines controlled?

B. Are entry codes changed periodically?

C. Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?

D. Are appropriate fire suppression and prevention devices installed and working?

204. Security guards are appropriate whenever the function required by the security program involves which of the following?

A. The use of discriminating judgment.

B. The need to detect unauthorized access.

C. The use of physical force.

D. The operation of access control devices.

205. _____ communications rely on clocking systems at the sending and receiving ends to sync, rather than stop and start bits.

A. Asynchronous

B. Analog

C. Synchronous

D. Digital

206. Which of the following is a “Class A” fire?

A. Halon

B. Electrical

C. Liquid

D. Common combustibles

207. This IPsec mode encapsulates the entire IP packet between IPsec nodes.

A. Transport

B. PPP

C. Tunnel

D. GRE

208. A momentary power outage is a:

A. Surge

B. Fault

C. Blackout

D. Spike

209. Which security measure would be the best deterrent to the theft of corporate information from a laptop which was left in a hotel room?

A. Install a cable lock on the laptop when it is unattended.

B. Encrypt the data on the hard drive.

C. Store all data on disks and lock them in an in-room safe.

D. Remove the batteries and power supply from the laptop and store them separately from the computer.

210. Which of the following is not EPA-approved replacements for Halon?

A. Water

B. NAF-S-III

C. Argon

D. Bromine

211. Which of the following statements pertaining to fire suppression systems is true?

A. Soda acid is an effective fire suppression method for class C (electrical) fires.

B. CO2 systems are effective because they suppress the oxygen supply required to sustain the fire.

C. Gas masks provide an effective protection against use of CO2 systems.

D. Halon is commonly used because it is highly effective in the fact that it interferes with the chemical combustion of the elements within a fire.

212. Which of the following suppresses combustion through a chemical reaction that kills the fire?

A. Water

B. soda acid

C. Halon

D. CO2

213. Which of the following is a “Class C” fire?

A. common combustibles

B. electrical

C. liquid

D. soda acid

214. When handling electronic evidence, what is the implementation principle for chain of custody that documents the evidence life cycle?

A. Must be signed by the judge.

B. Must be signed by the originator.

C. Ensures that the evidence will be admissible.

D. Must account for everyone who had access to the evidence.

215. Which of the following is a proximity identification device that does not require action by the user and works by responding with an access code to signals transmitted by a reader?

A. A smart card

B. A transponder

C. A passive system sensing device

D. A card swipe

216. A momentary high voltage is a:

A. Surge

B. Fault

C. Blackout

D. spike

217. A device that supplies power when the commercial utility power system fails is called?

A. power divider

B. power conditioner

C. power filter

D. uninterruptible power supply (UPS)

218. The ideal operating humidity range is defined as 40 percent to 60 percent. Low humidity (less than 40 percent) can produce what type of problem on computer parts?

A. Electro-plating

B. Energy-plating

C. Element-plating

D. Static electricity

219. While referring to physical security, what does positive pressurization means?

A. A series of measures that increase pressure on employees in order to make them more productive.

B. The air goes out of a room when a door is opened and outside air does not go into the room.

C. Causes the sprinkler system to go off.

D. The pressure inside your sprinkler system is greater than zero.

220. Which of the following question is less likely to help in assessing physical access controls?

A. Are visitors to sensitive areas signed in and escorted?

B. Does management regularly review the list of persons with physical access to sensitive facilities?

C. Is the operating system configured to prevent circumvention of the security software and application controls?

D. Are keys or other access devices needed to enter the computer room and media library?

221. The National Institute of Standards and Technology (NIST) standard pertaining to perimeter protection states that critical areas should be illuminated up to?

A. Nine feet high and three feet out.

B. Eight feet high and three feet out.

C. Eight feet high and two feet out.

D. Nine feet high and two feet out.

222. Which of the following is true about a "dry pipe" sprinkler system?

A. It minimizes chances of accidental discharge of water.

B. It uses less water than "wet pipe" systems.

C. It is a substitute for carbon dioxide systems.

D. It maximizes chances of accidental discharge of water.

223. The followings are fire detector types except:

A. Smoke activated

B. Heat activated

C. Flame actuated

D. Acoustical-seismic detection system

224. Which of the following asymmetric encryption algorithm is based on the difficulty of factoring large numbers?

A. International Data Encryption Algorithm (IDEA)

B. RSA

C. Elliptic Curve Cryptosystems (ECCs)

D. El Gamal

225. Under what conditions would the use of a Class C fire suppression system be preferable to the use of a Class A fire suppression system?

A. When the fire is in its incipient stage.

B. When the fire involves electrical equipment.

C. When the fire is caused by flammable products.

D. When the fire is located in an enclosed area.

226. Which of the following recovery issue must be considered in disaster recovery planning (DRP)?

A. Continuance of Salaries

B. Expense disbursement

C. Public Relations

D. A & B

227. A business continuity plan (BCP) should have a structure that includes:

A. A detailed section on incident and risk assessment covering all the organization's key business activities.

B. A detailed section on incident and risk assessment covering all the organization's business activities.

C. A brief section on incident and risk assessment covering all the organization's key business activities.

D. A brief section on incident and risk assessment covering all the organization's business activities.

228. What should take place in order to restore a server, its files and data after a major system failure?

A. Restore from storage media backup

B. Perform a parallel test

C. Implement recovery procedures

D. Perform a check list test

229. It is recommended that your disaster recovery plan (DRP) and business continuity plan (BCP) be tested at a minimum of what intervals?

A. Six months

B. When the systems and environment change

C. Two years

D. One year

230. In addition to preventing loss of life and further injury, what other reason is there to immediately initiate an emergency plan after a disaster?

A. Secure the area to prevent any looting, fraud or vandalism.

B. Reduce likelihood of further damage

C. Protect the site for forensic evidence

D. Investigate the extent of the damages

231. When shopping for an off-site backup facility that will ultimately be used to store all your backup media, what is the most important factor to consider?

A. The backup facility should be within 15 minutes of the original facility.

B. The facility should contain an adequate number of PCs and servers and have raised flooring.

C. The facility should have at least one armed guard.

D. The facility should protect against unauthorized access and entry.

232. What is the primary reason for using one-way hashing algorithms on user passwords?

A. It provides the compression necessary to conserve hard disk space on the host system

B. It eliminates the excessive processing required of symmetric encryption.

C. It prevents people from seeing the passwords in clear text

D. It provides a simplified platform for password for most password cracking utilities

233. What is the most critical factor in the development of a disaster recovery plan (DRP)?

A. Business impact analysis (BIA)

B. Annual testing

C. Participation from every department

D. Management support

234. What is the best description of a structured walk through test?

A. It is a test to ensure that the critical systems will run at the alternate site.

B. All departments receive a copy of the disaster recovery plan and walk through it.

C. Representatives from each department come together and go through the test collectively.

D. Operations are shifted to the emergency site and senior management reviews the plan on a line item by line item basis.

235. Which of the following backup facility is most expensive?

A. Cold

B. Hot

C. Warm

D. Mobile

236. A business impact analysis would not likely include which of the following tasks?

A. Calculating risk

B. Identifying threats

C. Selecting team members

D. Identifying critical functions of the company

237. What is the effective length of a secret key in the Data Encryption Standard (DES) algorithm?

A. 56-bit

B. 64-bit

C. 32-bit

D. 16-bit

238. If a site needed sporadic access to another network, which would be the best choice?

A. SVC (secondary virtual circuit)

B. SVC (switched virtual circuit)

C. TVC (temporary virtual circuit)

D. PVC (permanent virtual circuit)

239. Resuming critical business functions includes:

A. Determining the extent of damage

B. Declaring a disaster

C. Establishing the command center

D. Contacting recovery team members

240. The admissibility rule requires that evidence must be excluded if:

A. It is not pertinent.

B. It is not legally obtained.

C. It is not sufficient.

D. It is not relevant.

241. Chain of custody is primarily used to:

A. Protect evidence in a secure storage location.

B. Fix responsibility for protecting evidence.

C. Protect and account for evidence.

D. Ensure that the evidence is returned to the victim in good condition.

242. A unique packaging method or symbol is a:

A. Trade secret.

B. Patent.

C. Trademark.

D. Copyright.

243. Why is computer crime difficult to investigate:

A. Privacy laws protect people from being investigated.

B. Computer crime investigations require special techniques and tools.

C. Criminals can spoof their address.

D. The police have no jurisdiction over the Internet.

244. Privacy laws generally include which of the following provisions:

A. Individuals have the right to remove data that they do not wish disclosed.

B. Government agencies must ensure that their data is accurate.

C. Government agencies must provide access to all other government agencies.

D. Government agencies may not use data for a purpose other than that for which it was initially collected.

245. What is the minimum and customary practice of responsible protection of assets that affects a community or societal norm?

A. Due diligence

B. Risk mitigation

C. Asset protection

D. Due care

246. What is the best description of a stream cipher?

A. The message is divided into blocks and mathematical functions are performed on each block.

B. The sender must encrypt the message with his/her private key so the receiver can decrypt it with her/his public key.

C. The cipher uses a key to create a keystream and XOR's the result with the message.

D. The cipher executes 16 rounds of computation on each bit?

247. Evidence may be not detected through:

A. Out of band communications

B. Accidental discovery

C. Audit trail review

D. Real-time intrusion monitoring.

248. Which of the following is not a valid X.509 V.3 certificate field?

A. Subject's public key information

B. Subject's X.500 name

C. Issuer's unique identifier

D. Subject's digital signature

249. Which network protocol uses a "connected" session?

A. Transmission Control Protocol (TCP)

B. Internet Control Message Protocol (ICMP)

C. Used Defined Protocol (UDP)

D. Layer 2 Transmission Protocol (L2TP)

250. What are the objectives of emergency actions taken at the beginning stage of a disaster? Preventing injuries, loss of life, and …

A. determining damage.

B. protecting evidence.

C. relocating operations.

D. mitigating damage.