**CH 12 - Operations Security Answers**

1. Which of the following in not a critical security aspect of Operations Controls?
   1. Controls over hardware
   2. Data media used
   3. Operators using resources
   4. **Environmental controls**
2. Configuration Management is a requirement for the following level(s) of the Orange Book?
   1. B3 and A1
   2. B1, B2 and B3
   3. A1
   4. **B2, B3, and A1**
3. Which of the following is a communication path that is not protected by the system's normal security mechanisms?
   1. A trusted path
   2. A protection domain
   3. **A covert channel**
   4. A maintenance hook
4. What best describes a scenario when an employee has been shaving off pennies from multiple accounts and depositing the funds into his own bank account?
   1. Data fiddling
   2. Data diddling
   3. **Salami techniques**
   4. Trojan horses
5. Which of the following is not an example of an operational control?
   1. backup and recovery
   2. **audit trails**
   3. contingency planning
   4. operations procedures
6. Which of the following should be performed by an operator?
   1. Changing profiles
   2. Approving changes
   3. Adding and removal of users
   4. **Installing system software**
7. What security procedure forces an operator into collusion with an operator of a different category to have access to unauthorized data?
   1. Enforcing regular password changes.
   2. Management monitoring of audit logs.
   3. **Limiting the specific accesses of operations personnel.**
   4. Job rotation of people through different assignments.
8. Which one of the following functions provides the least effective organizational reporting structure for the Information Systems Security function?
   1. IS quality assurance
   2. IS resource management
   3. **IS operations**
   4. Corporate security
9. It is a violation of the "separation of duties" principle when which of the following individuals access the security systems software?
   1. security administrator
   2. security analyst
   3. systems auditor
   4. **systems programmer**
10. Configuration Management controls what?
    1. Auditing of changes to the Trusted Computing Base
    2. Control of changes to the Trusted Computing Base
    3. Changes in the configuration access to the Trusted Computing Base
    4. **Auditing and controlling any changes to the Trusted Computing Base**
11. Which of the following is not a component of an Operations Security "triples"?
    1. Asset
    2. Threat
    3. Vulnerability
    4. **Risk**
12. Which of the following is the most commonly used technique to gather security-related information like passwords?
    1. Network sniffers
    2. Shoulder surfing
    3. **Social engineering**
    4. Dumpster diving
13. Which of the following is used to interrupt opportunity to create collusion to subvert operation for fraudulent purposes?
    1. Separation of duties
    2. **Rotation of duties**
    3. Principle of need-to-know
    4. Principle of least privilege
14. This type of vulnerability enables the intruder to re-route data traffic from a network device to a personal machine. This diversion enables the intruder to capture data traffic to and from the devices for analysis or modification, or to steal the password file from the server and gain access to user accounts:
    1. Network Address Translation
    2. **Network Address Hijacking**
    3. Network Address Supernetting
    4. Network Address Sniffing
15. Which of the following is NOT an element of software control?
    1. **secure software development**
    2. software testing
    3. safe software storage
    4. anti-virus management
16. Which of the following is not concerned with configuration management?
    1. Hardware
    2. Software
    3. Documentation
    4. **They all are concerned with configuration management.**
17. Which of the following functions is less likely to be performed by a typical security administrator?
    1. Setting user clearances and initial passwords
    2. **Adding and removing system users**
    3. Setting or changing file sensitivity labels
    4. Reviewing audit data
18. Which of the following focuses on the basic features and architecture of a system?
    1. **operational assurance**
    2. life cycle assurance
    3. covert channel assurance
    4. level A1
19. Intrusion Detection (ID) and Response is not a:
    1. **preventive control.**
    2. detective control.
    3. monitoring control.
    4. reactive control.
20. According to the Orange Book, which security level is the first to require configuration management?
    1. **B2**
    2. B3
    3. A1
    4. B1
21. Operations Security seeks to primarily protect against which of the following?
    1. object reuse
    2. facility disaster
    3. compromising emanations
    4. **asset threats**
22. The concept of the Trusted Computing Base (from the Orange Book) includes which of the following?
    1. trusted hardware only
    2. trusted software only
    3. **trusted hardware and software**
    4. trusted computer operators and system managers
23. Operation security requires the implementation of physical security to control which of the following?
    1. **unauthorized personnel access**
    2. incoming hardware
    3. contingency conditions
    4. evacuation procedures
24. When backing up an applications system's data, which of the following is a key question to be answered first?
    1. When to make backups
    2. Where to keep backups
    3. **What records to backup**
    4. How to store backups
25. Which of the following logical access exposures involves changing data before, or as it is entered into the computer?
    1. **Data diddling**
    2. Salami techniques
    3. Trojan horses
    4. Viruses
26. Which of the following rules is less likely to support the concept of least privilege?
    1. The number of administrative accounts should be kept to a minimum.
    2. Administrators should use regular accounts when performing routine operations like reading mail.
    3. Permissions on tools that are likely to be used by hackers should be as restrictive as possible.
    4. **Only data to and from critical systems and applications should be allowed through the firewall.**
27. Which of the following are functions that are compatible in a properly segregated environment?
    1. Data entry and job scheduling
    2. Database administration and systems security
    3. **Systems analyst and application programming**
    4. Security administration and systems programming
28. Which trusted facility management concept implies that two operators must review and approve the work of each other?
    1. **Two-man control**
    2. Dual control
    3. Double control
    4. Segregation control
29. When it comes to magnetic media sanitization, what difference can be made between clearing and purging information?
    1. Clearing completely erases the media whereas purging only removes file headers, allowing the recovery of files.
    2. **Clearing renders information unrecoverable by a keyboard attack and purging renders information unrecoverable against laboratory attack.**
    3. They both involve rewriting the media.
    4. Clearing renders information unrecoverable against a laboratory attack and purging renders information unrecoverable to a keyboard attack.
30. Which of the following statements pertaining to ethical hacking is incorrect?
    1. An organization should use ethical hackers who do not sell auditing, consulting, hardware, software, firewall, hosting, and/or networking services.
    2. Testing should be done remotely
    3. Ethical hacking should not involve writing to or modifying the target systems.
    4. **Ethical hackers should never use tools that have the potential of exploiting vulnerabilities in the organization's IT system.**
31. Which of the following is the most reliable, secure means of removing data from magnetic storage media such as a magnetic tape, or a cassette?
    1. **Degaussing**
    2. Parity Bit Manipulation
    3. Certification
    4. Buffer overflow
32. Who is responsible for setting user clearances to computer-based information?
    1. **Security administrators**
    2. Operators
    3. Data owners
    4. Data custodians
33. What should a company do first when disposing of personal computers that once were used to store confidential data?
    1. Overwrite all data on the hard disk with zeroes
    2. Delete all data contained on the hard disk
    3. **Demagnetize the hard disk**
    4. Low level format the hard disk
34. Which of the following files should the security administrator be restricted to READ only access?
    1. Security parameters
    2. User passwords
    3. User profiles
    4. **System log**
35. Which of the following is true related to network sniffing?
    1. **Sniffers allow an attacker to monitor data passing across a network.**
    2. Sniffers alter the source address of a computer to disguise and exploit weak authentication methods.
    3. Sniffers take over network connections.
    4. Sniffers send IP fragments to a system that overlap with each other.
36. Ensuring that printed reports reach proper users and that receipts are signed before releasing sensitive documents are examples of:
    1. Deterrent controls
    2. **Output controls**
    3. Information flow controls
    4. Asset controls
37. The continual effort of making sure that the correct polices, procedures and standards are in place and being followed is described as what?
    1. Due care
    2. Due concern
    3. **Due diligence**
    4. Due practice
38. Notifying the appropriate parties to take action in order to determine the extent of the severity of an incident and to remediate the incident's effects includes:
    1. Intrusion Evaluation (IE) and Response
    2. Intrusion Recognition (IR) and Response
    3. Intrusion Protection (IP) and Response
    4. **Intrusion Detection (ID) and Response**
39. Which of the following questions is less likely to help in assessing identification and authentication controls?
    1. Is a current list maintained and approved of authorized users and their access?
    2. Are passwords changed at least every ninety days or earlier if needed?
    3. Are inactive user identifications disabled after a specified period of time?
    4. **Is there a process for reporting incidents?**
40. Which of the following security controls might force an operator into collusion with personnel assigned organizationally within a different function in order to gain access to unauthorized data?
    1. **Limiting the local access of operations personnel**
    2. Job rotation of operations personnel
    3. Management monitoring of audit logs
    4. Enforcing regular password changes
41. Which of the following ensures that security is not breached when a system crash or other system failure occurs?
    1. **trusted recovery**
    2. hot swappable
    3. redundancy
    4. secure boot
42. This baseline sets certain thresholds for specific errors or mistakes allowed and the amount of these occurrences that can take place before it is considered suspicious?
    1. Checkpoint level
    2. Ceiling level
    3. **Clipping level**
    4. Threshold level
43. If an operating system permits executable objects to be used simultaneously by multiple users without a refresh of the objects, what security problem is most likely to exist?
    1. **disclosure of residual data**
    2. unauthorized obtaining of a privileged execution state
    3. data leakage through covert channels
    4. denial of service through a deadly embrace
44. Overwriting and/or degaussing is used to clear and purge all of the following except which of the following?
    1. random access memory
    2. **read-only memory**
    3. magnetic core memory
    4. magnetic hard disks
45. Which of the following should not be accessible by a computer operator?
    1. Operations documentation
    2. Computer console
    3. **Source code of applications**
    4. Information security guidelines
46. In what way can violation clipping levels assist in violation tracking and analysis?
    1. **Clipping levels set a baseline for normal user errors, and violations exceeding that threshold will be recorded for analysis of why the violations occurred.**
    2. Clipping levels enable a security administrator to customize the audit trail to record only those violations which are deemed to be security relevant.
    3. Clipping levels enable the security administrator to customize the audit trail to record only actions for users with access to usercodes with a privileged status.
    4. Clipping levels enable a security administrator to view all reductions in security levels which have been made to usercodes which have incurred violations.
47. According to the Orange Book, which security level is the first to require trusted recovery?
    1. A1
    2. B2
    3. **B3**
    4. B1
48. What is the most secure way to dispose of information on a CD-ROM?
    1. Sanitizing
    2. Physical damage
    3. Degaussing
    4. **Physical destruction**
49. Which of the following is not a proper component of Media Viability Controls?
    1. Storage
    2. **Writing**
    3. Handling
    4. Marking
50. Which of the following are functions that are compatible in a properly segregated environment?
    1. Application programming and computer operation.
    2. Systems programming and job control analysis.
    3. Access authorization and database administration.
    4. **System development and systems maintenance.**
51. Which of the following is the BEST way to handle obsolete magnetic tapes before disposing of them ?
    1. Overwriting the tapes
    2. Initializing the tape labels
    3. Erasing the tapes
    4. **Degaussing the tapes**
52. Which of the following is not a technique used for monitoring?
    1. Penetration testing
    2. Intrusion detection
    3. Violation processing (using clipping levels)
    4. **Countermeasures testing**
53. Which of the following questions is less likely to help in assessing controls over audit trails?
    1. Does the audit trail provide a trace of user actions?
    2. **Are incidents monitored and tracked until resolved?**
    3. Is access to online logs strictly controlled?
    4. Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail?
54. The high availability of multiple all-inclusive, easy-to-use hacking tools that do not require much technical knowledge has brought a growth in the number of which type of attackers?
    1. Black hats
    2. White hats
    3. **Script kiddies**
    4. Phreakers
55. Which of the following questions is less likely to help in assessing controls over hardware and software maintenance?
    1. Is access to all program libraries restricted and controlled?
    2. **Are integrity verification programs used by applications to look for evidences of data tampering, errors, and omissions?**
    3. Is there version control?
    4. Are system components tested, documented, and approved prior to promotion to production?
56. This type of control is used to ensure that transactions are properly entered into the system once. Elements of this type of control may include counting data and time stamping it with the date it was entered or edited?
    1. Processing Controls
    2. Output Controls
    3. **Input Controls**
    4. Input/Output Controls
57. Which of the following refers to the data left on the media after the media has been erased?
    1. **remanence**
    2. recovery
    3. sticky bits
    4. semi-hidden
58. Which TCSEC (Orange Book) level requires the system to clearly identify functions of security administrator to perform security-related functions?
    1. C2
    2. B1
    3. B2
    4. **B3**
59. What is the most effective means of determining how controls are functioning within an operating system?
    1. Interview with computer operator
    2. **Review of software control features and/or parameters**
    3. Review of operating system manual
    4. Interview with product vendor
60. A periodic review of user account management should not determine:
    1. Conformity with the concept of least privilege.
    2. Whether active accounts are still being used.
    3. **Strength of user-chosen passwords.**
    4. Whether management authorizations are up-to-date.
61. When two operators review and approve the work of each other, this is known as?
    1. Dual Control
    2. **Two-man Control**
    3. Two-fold Control
    4. Twin Control
62. Which of the following is not an Orange Book-defined life cycle assurance requirement?
    1. Security testing
    2. Design specification and testing
    3. Trusted distribution
    4. **System integrity**
63. Which of the following would be best suited to provide information during a review of the controls over the process of defining IT service levels?
    1. Systems programmer
    2. Legal staff
    3. **Business unit manager**
    4. Programmer
64. Which of the following are NOT a countermeasure to traffic analysis?
    1. Padding messages
    2. **Eavesdropping**
    3. Sending noise
    4. Covert channel analysis
65. Which level of "least privilege" enables operators the right to modify data directly in its original location, in addition to data copied from the original location?
    1. **Access Change**
    2. Read/Write
    3. Access Rewrite
    4. Access Modify
66. It is important that the security controls and mechanisms that are in place have a degree of?
    1. Complexity
    2. Non-transparency
    3. **Transparency**
    4. Simplicity
67. Which of the following yellow-book defined types of system recovery happens after a system fails in an uncontrolled manner in response to a TCB or media failure and the system cannot be brought to a consistent state?
    1. Recovery restart
    2. System reboot
    3. Emergency system restart
    4. **System cold start**
68. Which of the following should not be performed by an operator?
    1. Mounting disk or tape
    2. Backup and recovery
    3. **Data entry**
    4. Handling hardware
69. According to the Orange Book, trusted facility management is not required for which of the following security levels?
    1. **B1**
    2. B2
    3. B3
    4. A1
70. Hardware availability reports allow the identification of the following problems except for:
    1. Inadequate training for operators
    2. Excessive operating systems maintenance
    3. **User dissatisfaction**
    4. Inadequate hardware facilities
71. Which of the following Operation Security controls is intended to prevent unauthorized intruders from internally or externally accessing the system, and to lower the amount and impact of unintentional errors that are entering the system?
    1. Detective Controls
    2. **Preventative Controls**
    3. Corrective Controls
    4. Directive Controls
72. Which of the following is not appropriate in addressing object reuse?
    1. Degaussing magnetic tapes when they're no longer needed.
    2. **Deleting files on disk before reusing the space.**
    3. Clearing memory blocks before they are allocated to a program or data.
    4. Clearing buffered pages, documents, or screens from the local memory of a terminal or printer.
73. What is the main issue with media reuse?
    1. Degaussing
    2. **Data remanence**
    3. Media destruction
    4. Purging
74. Physically securing backup tapes from unauthorized access is obviously a security concern and is considered a function of the:
    1. **Operations Security Domain.**
    2. Operations Security Domain Analysis.
    3. Telecommunications and Network Security Domain.
    4. Business Continuity Planning and Disater Recovery Planning.
75. Which of the following is not a valid reason to use external penetration service firms rather than corporate resources?
    1. They are more cost-effective
    2. They offer a lack of corporate bias
    3. **They use highly talented ex-hackers**
    4. They insure a more complete reporting
76. Which of the following are functions that are compatible in a properly segregated environment?
    1. Computer operations and system development.
    2. System development and change management.
    3. **Change/problem and quality assurance.**
    4. Security administration and change management.
77. Which of the following is NOT a media viability control used to protect the viability of data storage media?
    1. **clearing**
    2. marking
    3. handling
    4. storage
78. The primary reason for enabling software audit trails is which of the following?
    1. Improve system efficiency.
    2. Improve response time for users.
    3. **Establish responsibility and accountability.**
    4. Provide useful information to track down processing errors.
79. Which of the following is the lowest TCSEC class wherein the systems must support separate operator and system administrator roles?
    1. **B2**
    2. B1
    3. A1
    4. A2
80. An electrical device (AC or DC) which can generate coercive magnetic force for the purpose of reducing magnetic flux density to zero on storage media or other magnetic media is called:
    1. a magnetic field.
    2. **a degausser.**
    3. magnetic remanence.
    4. magnetic saturation.
81. What setup should an administrator use for regularly testing the strength of user passwords?
    1. A networked workstation so that the live password database can easily be accessed by the cracking program.
    2. A networked workstation so the password database can easily be copied locally and processed by the cracking program.
    3. **A standalone workstation on which the password database is copied and processed by the cracking program.**
    4. A password-cracking program is unethical; therefore it should not be used.
82. The number of violations that will be accepted or forgiven before a violation record is produced is called which of the following?
    1. **clipping level**
    2. acceptance level
    3. forgiveness level
    4. water level
83. What is the main objective of proper separation of duties?
    1. To prevent employees from disclosing sensitive information.
    2. To ensure access controls are in place.
    3. **To ensure that no single individual can compromise a system.**
    4. To ensure that audit trails are not tampered with.
84. Which of the following ensures that a TCB is designed, developed, and maintained with formally controlled standards that enforces protection at each stage in the system's life cycle?
    1. **life cycle assurance**
    2. operational assurance
    3. covert timing assurance
    4. covert storage assurance
85. Which of the following are functions that are compatible in a properly segregated environment?
    1. **Security administration and quality assurance**
    2. Security administration and data entry
    3. Security administration and application programming
    4. Application programming and data entry
86. Which of the following exposures associated with the spooling of sensitive reports for offline printing could be considered the MOST serious?
    1. Sensitive data may be read by operators
    2. Data can be altered without authorization
    3. Output would be lost in case of system failure
    4. **Other unauthorized copies of reports could be printed**
87. Fault tolerance countermeasures are designed to combat threats to which of the following?
    1. an uninterruptible power supply.
    2. backup and retention capability.
    3. **design reliability.**
    4. data integrity.
88. Which of the following is a detective control?
    1. Segregation of duties
    2. Back-up procedures
    3. **Audit trails**
    4. Physical access control
89. Unrestricted access to production programs should be given to which of the following?
    1. maintenance programmers only
    2. system owner, on request
    3. **no one**
    4. auditors
90. Which of the following computer crime is more often associated with insiders?
    1. IP spoofing
    2. Password sniffing
    3. **Data diddling**
    4. Denial of service (DOS)
91. Which of the following is not a preventive operational control?
    1. Protect laptops, personal computers and workstations.
    2. Control software viruses.
    3. Control data media access and disposal.
    4. **Conduct security awareness and technical training.**
92. Which of the following questions is less likely to help in assessing controls over production?
    1. Are there processes for ensuring that only authorized users pick up, receive, or deliver input and output information and media?
    2. Are audit trails used for receipt of sensitive inputs/outputs?
    3. Is media sanitized for reuse?
    4. **Are confidentiality or security agreements required for employees assigned to work with sensitive information?**
93. Which of the following is NOT a technique used to perform a penetration test?
    1. **sending noise**
    2. scanning and probing
    3. war dialing
    4. sniffing
94. According to the Orange Book, which security level is the first to require a system to support separate operator and system administrator roles?
    1. A1
    2. B1
    3. **B2**
    4. B3
95. What is the essential difference between a self-audit and an independent audit?
    1. Tools used
    2. Results
    3. **Objectivity**
    4. Competence
96. Which of the following is not an Orange Book-defined operational assurance requirement?
    1. System architecture
    2. Trusted facility management
    3. **Configuration management**
    4. Covert channel analysis