Post-Class Quiz: Operations Security Domain

1. As an information security officer, how would you explain the difference between due care and due diligence?
   A. Due care is the continuous effort taken to ensure compliance to security policy; and due diligence is the effort performed to maintain the security posture of an enterprise.
   B. Due care is the effort performed to mitigate risks; and due diligence is the continuous effort performed to assess the potential risks.
   C. Due care is the continuous effort performed to assess the potential risks; due diligence is the effort performed to mitigate risks.
   D. Due care is another word for due diligence.

2. A security engineer working with project stakeholders in defining user roles and responsibilities as a part of requirements elicitation process is considered as a _____ activity?
   A. Due care
   B. Due diligence
   C. Legal
   D. Separation of duties

3. According to the "prudent person rule", performing security operations in accordance to the specified standard operating procedure (SOP) is considered as what type of activity?
   A. Due care
   B. Due diligence
   C. Legal
   D. Separation of duties

4. To protect project source code from unauthorized access, the project configuration manager implements access control policy to prevent software developers from modifying the software baseline in configuration management database (CMDB) is an example of?
   A. Need to know
   B. Least privilege
   C. Separation of duties
   D. Meeting the confidentiality

5. 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

6. Change management must include all of the following except:
   A. Be reviewed by security
   B. Be a formal process
   C. Be ready to handle unexpected events
   D. Be subject to acceptance

7. When contracting a vendor for software or hardware provisioning, care must be taken to:
   A. Ensure all changes are kept up-to-date.
   B. Ensure all changes go through a change management process.
   C. Ensure that in-house technical staff learn the system.
   D. Ensure that all activity on the system is monitored.

8. 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.

9. Operations security involves:
   A. Encrypting all data so that it is not so easily eavesdropped on.
   B. Assuring the confidentiality, integrity and authentication of all corporate data.
   C. The continuous maintenance involved in retaining acceptable security levels.
   D. Performing annual vulnerability assessments to assure that vulnerabilities are found and minimized.

10. 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.

11. Emergency fixes to a system must:
    A. Be implemented as rapidly as possible
    B. Be scrutinized subsequently to ensure they were performed correctly
    C. Be performed only by following normal change control procedures
    D. Be made permanent within 72 hours

12. In separation of duties:
    A. High-risk activities are broken up into different parts and distributed to different individuals
    B. Individuals can avoid the need for collusion to commit a fraud
    C. Staff can decrease the likelihood of getting caught when committing fraud by enlisting others for help
    D. Operating system processes are further divided into threads

13. 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

14. 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

15. Which is most likely to help a company detect fraudulent activity:
    A. Mandatory vacations
    B. Instituting least privilege
    C. Logging
    D. Mistakes

16. Every user's attempts and activities while using a resource or information, should be properly:
    A. Monitored, audited, and logged
    B. Monitored, audited, logged, and reported
    C. Monitored, audited, logged, and saved
    D. Monitored, audited, logged, and archived

17. By tracking user access to resources, the security professional can do all of the following except:
    A. Determine if users have excess privileges
    B. Determine if there has been unauthorized access
    C. Determine if repetitive mistakes are being made
    D. Determine if the security budget is being properly administered

18. Clipping levels are all of the following 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

19. The security concept of transparency requires all of the following except:
    A. That controls and mechanisms be hidden
    B. That users perform tasks and duties without having to go through extra steps because of the presence of the security control
    C. That security mechanisms not let users know too much about themselves
    D. That security controls seamlessly operate with all other control mechanisms

20. 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

21. When it comes to change control documentation:
    A. It should be done on a regular basis
    B. It should always be available for future use
    C. It should include items such as patches/updates installed, configuration changes, and the addition of new devices to the network
    D. It should be strictly controlled by the Chief Security Officer in addition to the Change Control Officer (CCO)

22. All of the following are acceptable for sanitizing data except:
    A. Deleting it
    B. Overwriting it
    C. Degaussing it
    D. Physically destroying it

23. 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

24. Which of the following is incorrect with respect to a system reboot:
    A. Occurs after shutting the system down in a controlled manner in response to a TCB failure
    B. Is a response to a trusted computer base (TCB) failure

C. Releases resources and returns the system to a more stable and safe state

D. Can also occur in an uncontrolled manner

25. Which of the following is incorrect with respect to an emergency system restart:

A. It takes place after a system failure happens in an uncontrolled manner

B. Can be the result of either a trusted computer base (TCB) or media failure

C. Does not necessarily involve a reboot

D. The system goes into a maintenance mode and recovers from the actions taken

26. 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

27. 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

28. Which of the following statements regarding port scanning is incorrect:

A. Helps identify the services running on a system

B. Is used for networking mapping

C. Requires the use of different port scanners for different operating systems

D. May be detected with an intrusion detection system (IDS)

29. Which of the following statements regarding network sniffers is incorrect:

A. Are also known as network analyzers or protocol analyzers

B. Are just as effective on switched networks as they are on hubbed networks

C. Can be defended against through encryption

D. May be used to capture data sent in the clear

30. 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

31. Which of the following statements regarding password cracking is incorrect:

A. The larger and more complex the password, the longer it takes to crack

B. Typically, 6 character passwords are adequate as long as they include special characters

C. A dictionary attack feeds a large list of words into a hacking tool

D. A brute forced attack tries many different password variations until it finds the correct password

32. Which of the following statements regarding backdoors is incorrect:

A. Can be detected by access control mechanisms

B. They are programs that allow an attacker to come back into a device at a later date

C. They allow entry without login credentials

D. Can be detected by third-party software applications such as AV and IDS

33. Which of the following statements regarding penetration testing is incorrect:

A. Is a set of procedures

B. It tests and possibly bypasses security controls

C. It‘s goal is to measure an organization‘s resistance to an attack and to uncover any weaknesses

D. Is the same as vulnerability scanning

34. Critical data is not:

A. Subject to classification by regulatory bodies or legislation.

B. Data of high integrity

C. Always protected at the highest levels

D. Instrumental for business operations–it must be available for the organization to stay in business

35. The best technique for preventing and detecting abuse by a user with privileged access is:

A. Good policy

B. Review by management

C. Strong authentication

D. Audit logs that are reviewed quarterly

36. Separation of duty controls can be defeated by:

A. Mutual exclusivity

B. Collusion

C. Dual control

D. Accreditation

37. The Common Criteria defines the term "fail secure" as:

A. A system that is tolerant of component failure

B. The ability of a system to fail in an orderly manner

C. A system failure does not affect normal business operations

D. The preservation of a secure state in the event of a failure

38. 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

39. If a report contains no data should it be printed anyway?

A. No, save paper and be environmentally conscious

B. No, there is no need to print an empty report

C. Yes, so that the owner knows that the report is empty and not just lost

D. Yes, to preserve the regular job flow and prevent errors

40. 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