ISC^2 Certified in Cybersecurity

MCQ ISC2 CC Chapter 5:Security Operations

Based on documentation by WAN MUHAMMAD AZIM BIN WAN MOHD HAZAN AMRI

7/11/2022

Disclaimer

I used Claude.ai to make this MCQ practice exam by referencing Wan Azim's documentation of ISC2 CC. Claude.ai is used to extract information and create questions alongside their answers.

Huge thanks to Wan Azim for documenting the ISC2 Certified in Cybersecurity course!
For more write-ups or documentation check out my repo at:
https://github.com/MikhailAmzar/reports

Security Operations

Here is a 50-question exam covering the main topics from Chapter 5: Security Operations

1. What is the primary focus of data classification?
A. Maintaining data availability
B. Maintaining data confidentiality based on sensitivity
C. Ensuring data integrity
D. Improving data usability

2. Which of the following is NOT a typical stage in the data security life cycle?
A. Create
B. Store
C. Compress
D. Archive

3. What does the term "data remanence" refer to?
A. Data that is actively being used
B. Data that might be left on media after deletion
C. Data that is stored in the cloud
D. Data that is transmitted over a network

4. Which of the following is a characteristic of symmetric encryption?
A. It uses different keys for encryption and decryption
B. It is faster than asymmetric encryption
C. It does not require key distribution
D. It scales well with a large number of users

5. In asymmetric encryption, which key is used to encrypt data?
A. Private key
B. Public key
C. Shared key
D. Master key

6. What is the purpose of a hash function in cryptography?
A. To encrypt data
B. To generate a fixed-size output from input data
C. To distribute keys securely
D. To decrypt data

7. Which of the following is NOT a common data state addressed by data security?
A. Data at rest
B. Data in use
C. Data in motion
D. Data in transition

8. What is the primary goal of configuration management?
A. To increase system performance
B. To ensure only authorized changes are made
C. To reduce operational costs
D. To automate all system processes

9. What does BYOD stand for in IT security policies?
A. Build Your Own Database
B. Bring Your Own Device
C. Backup Your Online Data
D. Buy Your Own Domain

10. Which of the following is a key component of an Acceptable Use Policy (AUP)?
A. Detailed network diagrams
B. Employee salary information
C. Appropriate use of the organization's assets
D. Customer database schemas

11. What is the main purpose of security awareness training?
A. To teach employees how to code securely
B. To ensure everyone knows what is expected of them
C. To replace the need for security controls
D. To reduce the IT security budget

12. Which of the following is an example of social engineering?
A. Configuring a firewall
B. Updating antivirus software
C. Pretexting
D. Encrypting an email

13. What is the primary difference between education and training in the context of security awareness?
A. Education is more formal than training
B. Training focuses on building specific skills, while education improves overall understanding
C. Education is only for managers, while training is for all employees
D. Training is theoretical, while education is practical

14. What is a whaling attack?
A. A phishing attack targeting high-profile individuals
B. A denial-of-service attack on large organizations
C. An attack on maritime communication systems
D. A brute-force attack on encryption keys

15. Which of the following is a best practice for password protection?
A. Using the same password for multiple systems
B. Sharing passwords with co-workers
C. Writing down passwords and keeping them in a secure location
D. Using different passwords for different systems

16. What is the purpose of data retention policies?
A. To keep all data indefinitely
B. To delete all data immediately after use
C. To define how long different types of data should be kept
D. To encrypt all stored data

17. What is the first step in the change management process?
A. Implementing the change
B. Testing the change
C. Request for change (RFC)
D. Rolling back the change

18. Which of the following is a method for securely disposing of data on magnetic media?
A. Degaussing
B. Defragmentation
C. Compression
D. Formatting

19. What does "ingress monitoring" refer to?
A. Monitoring outgoing network traffic
B. Monitoring incoming network traffic
C. Monitoring internal network traffic
D. Monitoring encrypted traffic

20. What is the primary goal of data loss prevention (DLP) systems?
A. To encrypt all data
B. To detect and prevent unauthorized data transmission
C. To compress data for efficient storage
D. To accelerate data processing

21. Which of the following is NOT typically considered a data state in security?
A. Data at rest
B. Data in use
C. Data in storage
D. Data in motion

22. What is a digital signature primarily used for?
A. Encrypting emails
B. Compressing large files
C. Providing authentication, integrity, and non-repudiation
D. Generating random passwords

23. What is the main advantage of asymmetric encryption over symmetric encryption?
A. It is faster
B. It requires fewer computational resources
C. It solves the problem of key distribution
D. It uses smaller key sizes

24. Which of the following is a characteristic of a good logging system?
A. It only logs successful events
B. It provides information about user IDs, dates, and system activities
C. It automatically deletes logs after 24 hours
D. It is accessible to all users

25. What is the purpose of clearing a device in the context of data destruction?
A. To physically destroy the device
B. To remove all data by overwriting storage media
C. To change the device's ownership
D. To upgrade the device's operating system

26. Which of the following is NOT a typical classification level for data sensitivity?
A. Highly restricted
B. Moderately restricted
C. Semi-restricted
D. Low sensitivity

27. What is the main purpose of labeling in data classification?
A. To make documents look professional
B. To assign clear ownership of documents
C. To implement controls to protect classified information
D. To track the number of documents created

28. What does the term "request for change (RFC)" refer to in change management?
A. A document detailing why a change should not be made
B. The initial stage where a change in procedure or product is sought
C. The final approval for a change
D. A request to undo a previous change

29. Which of the following is a common mistake in records retention?
A. Keeping records for too short a time
B. Applying the longest retention period to all types of information
C. Having different retention periods for different types of data
D. Regularly reviewing retained records

30. What is the primary purpose of log reviews?
A. To improve system performance
B. To identify security incidents and policy violations
C. To generate reports for management
D. To allocate storage resources

31. Which of the following is an example of egress monitoring?
A. Monitoring email content leaving the organization
B. Monitoring login attempts to the corporate network
C. Monitoring CPU usage on servers
D. Monitoring the temperature in the data center

32. What is the main limitation of symmetric encryption when it comes to key management?
A. Keys are too short
B. Keys are too easily guessed
C. Distributing keys securely is challenging
D. Generating keys is computationally intensive

33. Which of the following is NOT a typical component of configuration management?
A. Identification
B. Baseline
C. Randomization
D. Verification and audit

34. What is the primary goal of system hardening?
A. To make the system physically stronger
B. To reduce the attack surface by applying secure configurations
C. To increase system performance
D. To make the system more user-friendly

35. Which type of attack involves an attacker following an authorized person into a restricted area?
A. Phishing
B. Vishing
C. Tailgating
D. Whaling

36. What is the purpose of security baselines?
A. To set the minimum level of security for systems
B. To eliminate the need for security updates
C. To replace security policies
D. To automate all security processes

37. Which of the following is a true statement about plaintext?
A. It is always human-readable
B. It refers to the unencrypted form of data
C. It is more secure than ciphertext
D. It is the output of an encryption algorithm

38. What is the main disadvantage of using password managers?
A. They generate weak passwords
B. They are illegal in most countries
C. They can be compromised, potentially exposing all stored passwords

D. They require monthly subscriptions

39. Which of the following is NOT a typical activity in the data security life cycle?
A. Create
B. Negotiate
C. Share
D. Destroy

40. What is the primary purpose of data classification?
A. To increase data storage efficiency
B. To recognize organizational impacts if the data is compromised
C. To improve data retrieval speed
D. To assign ownership of data

41. In the context of cryptography, what does CIA stand for?
A. Central Intelligence Agency
B. Confidentiality, Integrity, Availability
C. Cryptography, Infrastructure, Architecture
D. Ciphertext, Initialization vector, Algorithm

42. Which of the following is a characteristic of asymmetric encryption?
A. It uses the same key for encryption and decryption
B. It is generally faster than symmetric encryption
C. It uses two different keys (public and private)
D. It is unsuitable for key exchange

43. What is vishing?
A. A type of social engineering attack using voice communication
B. A method for secure voice encryption
C. A tool for voice recognition
D. A protocol for VoIP communication

44. Which stage of the data security life cycle involves temporarily storing data when it's not actively needed?
A. Create
B. Use
C. Archive
D. Destroy

45. What is the primary goal of an information security education program?
A. To improve employees' understanding of security concepts
B. To replace the need for security policies
C. To reduce the organization's security budget
D. To automate security processes

46. Which of the following is NOT typically monitored by a Data Loss Prevention (DLP) solution?
A. Email content
B. File transfers

C. Employee work hours
D. Web postings

47. What is the main purpose of purging a device in the data destruction process?
A. To overwrite data with zeros
B. To remove residual magnetic effects that could allow data recovery
C. To format the storage media
D. To change the device's ownership

48. Which of the following is a true statement about ciphertext?
A. It is always shorter than the original plaintext
B. It is the encrypted form of a message
C. It can be easily understood without decryption
D. It is resistant to all forms of cryptanalysis

49. What is pretexting in the context of social engineering?
A. Writing a preface for a book
B. Impersonating an authority figure to gain access to information
C. Preparing a speech before delivery
D. Designing the layout of a website

50. Which of the following is NOT a typical role of cryptography in information security?
A. Providing confidentiality
B. Ensuring integrity
C. Enforcing availability
D. Supporting non-repudiation

Answer Key: Chapter 5

1. B
2. C
3. B
4. B
5. B
6. B
7. D
8. B
9. B
10. C
11. B
12. C
13. B
14. A
15. D
16. C
17. C
18. A
19. B
20. B
21. C
22. C
23. C
24. B
25. B
26. C
27. C
28. B
29. B
30. B
31. A
32. C
33. C
34. B
35. C
36. A
37. B
38. C
39. B
40. B
41. B
42. C
43. A
44. C
45. A
46. C
47. B
48. B
49. B
50. C