ISC² Certified in Cybersecurity

MCQ ISC2 CC Chapter 4:Network Security

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

Network Security

Here is a 50-question exam covering the main topics from Chapter 4: Network Security

1. What is the primary goal of an Intrusion Detection System (IDS)?
A. To prevent unauthorized access
B. To provide a means for timely and accurate response to intrusions
C. To encrypt all network traffic
D. To segment the network

2. Which of the following is NOT a characteristic of cloud computing?
A. On-demand self-service
B. Broad network access
C. Resource pooling
D. Physical server ownership

3. What does VLAN stand for?
A. Virtual Local Area Network
B. Very Large Area Network
C. Virtual Link Access Node
D. Verified Local Area Network

4. What is the purpose of a Demilitarized Zone (DMZ) in network design?
A. To isolate the internal network from the internet
B. To host public-facing servers
C. To create a buffer zone between two firewalls
D. All of the above

5. Which of the following is an example of a Layer 2 attack?
A. MAC flooding
B. Ping of death
C. SQL injection
D. DNS cache poisoning

6. What is the main difference between TCP and UDP?
A. TCP is connection-oriented, while UDP is connectionless
B. TCP is faster than UDP
C. UDP provides guaranteed delivery, while TCP does not
D. TCP is used for streaming, while UDP is used for file transfer

7. In the OSI model, which layer is responsible for routing?
A. Data Link Layer
B. Network Layer
C. Transport Layer
D. Session Layer

8. What is the primary function of a firewall?
A. Intrusion detection
B. Traffic filtering
C. Data encryption
D. Load balancing

9. Which of the following is NOT a cloud service model?
A. Infrastructure as a Service (IaaS)
B. Platform as a Service (PaaS)
C. Software as a Service (SaaS)
D. Security as a Service (SECaaS)

10. What is the purpose of NAC (Network Access Control)?
A. To control access to network resources based on device and user authentication
B. To manage network bandwidth
C. To encrypt network traffic
D. To monitor network performance

11. What is a characteristic of a zero trust network model?
A. It relies heavily on perimeter security
B. It assumes all network traffic is potentially malicious
C. It grants access based on user roles only
D. It eliminates the need for firewalls

12. Which protocol is used for secure remote administration of network devices?
A. Telnet
B. HTTP
C. FTP
D. SSH

13. What is the primary goal of network segmentation?
A. To increase network speed
B. To reduce the attack surface
C. To simplify network management
D. To enable wireless access

14. What does APT stand for in the context of cybersecurity?
A. Advanced Persistent Threat
B. Application Protocol Tunnel
C. Automated Penetration Testing
D. Active Protection Technology

15. Which of the following is NOT a typical responsibility of a Managed Service Provider (MSP)?
A. Network monitoring
B. Patch management
C. Physical security of client premises
D. Help desk support

16. What is the purpose of a honeynet?
A. To attract and detect potential attackers
B. To optimize network performance
C. To provide secure remote access
D. To facilitate peer-to-peer file sharing

17. Which of the following is a characteristic of malware?
A. It always requires user interaction to activate
B. It is always detectable by antivirus software
C. It can self-replicate and spread to other systems
D. It only affects Windows operating systems

18. What is the main purpose of implementing least privilege in access control?
A. To simplify user management
B. To reduce the potential impact of a security breach
C. To increase system performance
D. To enable single sign-on

19. Which of the following is an example of a passive security attack?
A. Port scanning
B. Eavesdropping
C. SQL injection
D. Denial of Service (DoS)

20. What is the primary function of a SIEM (Security Information and Event Management) system?
A. To block malicious traffic
B. To collect and analyze security event data from various sources
C. To encrypt sensitive data
D. To manage user accounts

21. What does the term "defense in depth" refer to?
A. Using multiple layers of security controls
B. Focusing all security efforts on the network perimeter
C. Implementing the strongest possible firewall
D. Training users in hand-to-hand combat

22. Which of the following is NOT a common element in a Service Level Agreement (SLA)?
A. Response time for incidents
B. System availability percentage
C. Employee salaries
D. Data backup frequency

23. What is the purpose of data loss prevention (DLP) systems?
A. To prevent hardware failures
B. To detect and prevent unauthorized transmission of sensitive data
C. To compress data for efficient storage
D. To accelerate data transfer rates

24. What is a botnet primarily used for?
A. Improving network performance
B. Conducting distributed denial-of-service (DDoS) attacks
C. Automatic software patching
D. Legal peer-to-peer file sharing

25. Which of the following best describes the concept of non-repudiation?
A. Ensuring data confidentiality
B. Preventing unauthorized access
C. Guaranteeing system availability
D. Proving the origin or delivery of data

26. What is the main goal of a penetration test?
A. To identify and exploit vulnerabilities in a controlled manner
B. To train new security personnel
C. To develop new exploits
D. To test the performance of network devices

27. What does BYOD stand for?
A. Bring Your Own Device
B. Build Your Own Database
C. Back Your Own Data
D. Buy Your Office Desktop

28. Which of the following is a characteristic of cloud computing?
A. Limited scalability
B. High upfront costs
C. On-demand self-service
D. Decreased flexibility

29. What is the primary purpose of implementing role-based access control (RBAC)?
A. To simplify the management of user permissions
B. To eliminate the need for user authentication
C. To increase system performance
D. To enable single sign-on

30. What is the main difference between a vulnerability assessment and a penetration test?
A. Vulnerability assessments are automated, while penetration tests are manual
B. Vulnerability assessments identify weaknesses, while penetration tests attempt to exploit them

C. Penetration tests are always conducted internally, while vulnerability assessments are external
D. Vulnerability assessments focus on networks, while penetration tests focus on applications

31. Which of the following is NOT a typical function of a Security Operations Center (SOC)?
A. Continuous monitoring of security events
B. Incident response coordination
C. Physical security management
D. Threat intelligence analysis

32. What is the purpose of a web application firewall (WAF)?
A. To filter network traffic based on IP addresses
B. To protect web applications from specific attacks like SQL injection and cross-site scripting
C. To accelerate the delivery of web content
D. To manage user authentication for websites

33. What does the acronym MITM stand for in the context of network attacks?
A. Manager in the Monitor
B. Man in the Middle
C. Malware in the Machine
D. Message in Transit Manipulation

34. Which of the following is a characteristic of ransomware?
A. It always targets only one specific file type
B. It encrypts user data and demands payment for the decryption key
C. It is easily removed by standard antivirus software
D. It only affects Linux-based systems

35. What is the main purpose of network address translation (NAT)?
A. To conserve public IP addresses
B. To increase network speed
C. To encrypt network traffic
D. To simplify routing tables

36. What is the primary goal of an incident response plan?
A. To prevent all security incidents
B. To minimize the impact of security incidents and recover quickly
C. To identify all possible vulnerabilities in a system
D. To train new security personnel

37. Which of the following is NOT a common feature of next-generation firewalls (NGFWs)?
A. Deep packet inspection
B. Intrusion prevention capabilities
C. Physical access control
D. Application awareness and control

38. What is the purpose of containerization in cloud computing?
A. To physically separate servers in different locations

B. To logically isolate applications and their dependencies
C. To encrypt all data stored in the cloud
D. To limit the bandwidth usage of cloud services

39. What does the principle of least privilege dictate?
A. All users should have equal access rights
B. Users should be granted only the minimum permissions necessary to perform their tasks
C. Administrators should have unlimited access to all systems
D. Guest accounts should have no access restrictions

40. Which of the following is an example of detective control?
A. Firewall
B. Intrusion Detection System (IDS)
C. Encryption
D. Access card

41. What is the main purpose of a disaster recovery plan?
A. To prevent disasters from occurring
B. To outline the steps for restoring IT operations after a disruptive event
C. To provide guidelines for daily system maintenance
D. To define the organization's security policies

42. What does DevSecOps aim to achieve?
A. Separate development, security, and operations teams
B. Integrate security practices within the DevOps process
C. Outsource all security functions to third-party providers
D. Focus solely on the development of security tools

43. What is the purpose of security information and event management (SIEM) systems?
A. To block all incoming network traffic
B. To collect, analyze, and correlate security event data from various sources
C. To automatically patch all systems in the network
D. To manage user passwords

44. Which of the following is NOT a common type of access control?
A. Discretionary Access Control (DAC)
B. Mandatory Access Control (MAC)
C. Role-Based Access Control (RBAC)
D. Time-Based Access Control (TBAC)

45. What is the primary goal of security awareness training?
A. To train employees to become cybersecurity experts
B. To educate users about security risks and best practices
C. To reduce the IT department's workload
D. To comply with government regulations only

46. What is the purpose of data classification?
A. To organize data alphabetically

B. To determine appropriate security controls based on data sensitivity
C. To increase storage efficiency
D. To improve data retrieval speed

47. Which of the following is a characteristic of phishing attacks?
A. They always involve malware
B. They typically impersonate legitimate entities to steal information
C. They only target high-level executives
D. They are easily identified by email filters

48. What is the main function of a security policy?
A. To list all known vulnerabilities in the organization
B. To provide guidelines for securing the organization's assets and data
C. To replace the need for security awareness training
D. To detail the organization's marketing strategy

49. What does the concept of "separation of duties" aim to prevent?
A. Collaboration between departments
B. Cross-training of employees
C. Fraud and errors by dividing tasks among multiple individuals
D. The need for management oversight

50. What is the primary purpose of log management in cybersecurity?
A. To consume disk space
B. To generate additional network traffic
C. To provide an audit trail and support forensic analysis
D. To slow down system performance

Answer Key: Chapter 4

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