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 multiple choice exam based on the provided PDF, with hard difficulty:

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

2. In the context of cloud computing, what does the acronym IaaS stand for?
A. Internet as a Service
B. Information as a Service
C. Infrastructure as a Service
D. Integration as a Service

3. Which of the following is NOT a characteristic of a zero trust network architecture?
A. Microsegmentation
B. Frequent re-authentication
C. Asset-centric security
D. Perimeter-based security

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 accessible by outside visitors
C. To implement network address translation
D. To provide a space for decommissioned hardware

5. In IPv6, what is the primary purpose of the address range fc00:: to fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff?
A. Documentation
B. Internal network use (not routable on the internet)
C. Multicast
D. Link-local addressing

6. Which of the following is NOT a typical responsibility of a Managed Service Provider (MSP)?
A. Network and security monitoring
B. Help desk service management
C. Physical security of the client's premises
D. Patch management services

7. What is the most essential representation of data at Layer 1 of the OSI model?
A. Frame
B. Packet
C. Bit
D. Byte

8. In the context of cloud deployment models, what distinguishes a community cloud?
A. It is always publicly accessible
B. It is developed for a particular community with shared concerns
C. It is a combination of public and private clouds
D. It is hosted exclusively on-premises

9. What is the primary difference between TCP and UDP at the Transport Layer?
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 real-time applications, while UDP is not

10. Which of the following is NOT a benefit of implementing network segmentation?
A. Improved access control
B. Limiting the scope of regulatory compliance
C. Containing security breaches
D. Increased broadcast domain size

11. What is the purpose of the subnet mask in IPv4 addressing?
A. To identify the network portion of an IP address
B. To encrypt the IP address
C. To compress the IP address
D. To translate between public and private IP addresses

12. In the defence in depth strategy, which layer is responsible for controls such as encryption and data leak prevention directly applied to the data itself?
A. Application layer
B. Host layer
C. Data layer
D. Network layer

13. What is the primary security concern with embedded systems and IoT devices?
A. They consume too much bandwidth
B. They often have multiple access routes and need special isolation
C. They are too expensive to replace
D. They cannot be updated or patched

14. Which of the following is NOT a common use case for Network Access Control (NAC) deployment?
A. Medical devices
B. BYOD/mobile devices

C. Datacenter servers
D. Guest users and contractors

15. What does VLAN hopping refer to?
A. A technique to improve VLAN performance
B. The process of changing VLAN configurations
C. An attack allowing traffic interception from other VLANs
D. A method for load balancing between VLANs

16. What is the main difference between an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS)?
A. An IPS is placed in-line with traffic and can block attacks
B. An IDS can only monitor wireless networks
C. An IPS is a host-based system, while an IDS is network-based
D. An IDS provides encryption, while an IPS does not

17. In cloud service models, who is typically responsible for operating system patches in a Platform as a Service (PaaS) deployment?
A. The cloud service customer
B. The cloud service provider
C. A third-party vendor
D. The application developer

18. What is the primary purpose of the Internet Control Message Protocol (ICMP)?
A. To establish encrypted tunnels
B. To determine the health of a network or a specific link
C. To assign IP addresses dynamically
D. To filter malicious traffic

19. Which statement accurately describes microsegmentation?
A. It focuses on creating large, isolated network segments
B. It is a strategy that places firewalls at every connection point
C. It relies solely on physical segmentation of the network
D. It is incompatible with zero trust architectures

20. What is the loopback address in IPv4?
A. 192.168.1.1
B. 255.255.255.255
C. 127.0.0.1
D. 0.0.0.0

21. Which of the following is NOT a private IPv4 address range?
A. 10.0.0.0 to 10.255.255.255
B. 172.16.0.0 to 172.31.255.255
C. 192.168.0.0 to 192.168.255.255
D. 169.254.0.0 to 169.254.255.255

22. What is the primary difference between a hub and a switch?

A. A switch is a Layer 3 device, while a hub is a Layer 1 device
B. A hub uses MAC addresses to forward traffic, while a switch broadcasts to all ports
C. A switch knows the addresses of connected devices and routes traffic accordingly
D. A hub provides more security features than a switch

23. In the context of cloud computing, what does elasticity refer to?
A. The ability to stretch the capabilities of virtual machines
B. The automatic scaling of resources based on demand
C. The flexibility in payment options
D. The use of elastic load balancers

24. What is the main purpose of a Memorandum of Understanding (MOU) in the context of business continuity?
A. To define service level agreements
B. To establish legal ownership of assets
C. To agree on sharing resources in case of an emergency
D. To set pricing for cloud services

25. Which of the following is a true statement about the relationship between the OSI model and the TCP/IP model?
A. They have the same number of layers
B. The TCP/IP model was developed after the OSI model
C. The TCP/IP model is more widely used in practical networks
D. The OSI model is more simplified than the TCP/IP model

26. What is the primary security risk associated with using FTP?
A. It's more vulnerable to DDoS attacks
B. It sends usernames and passwords in plaintext
C. It doesn't support file transfers larger than 2GB
D. It requires open ports on the firewall

27. In the context of network design, what does "defense in depth" refer to?
A. The use of military-grade encryption
B. Implementing security controls at multiple layers
C. The depth of packet inspection
D. The number of firewalls in the network

28. What is the main advantage of software-defined networking (SDN)?
A. Increased network performance
B. Simplified hardware requirements
C. Centralized network provisioning and configuration
D. Enhanced physical security

29. Which of the following is NOT a typical feature of a Next-Generation Firewall (NGFW)?
A. Deep packet inspection
B. Intrusion prevention capabilities
C. Physical segmentation of networks
D. Application awareness and control

30. What is the purpose of the Address Resolution Protocol (ARP)?
A. To map IP addresses to MAC addresses
B. To assign IP addresses dynamically
C. To resolve domain names to IP addresses
D. To encrypt data link layer communications

31. In the context of cloud computing, what does multi-tenancy mean?
A. Multiple cloud providers serving one customer
B. One physical server hosting multiple virtual machines for different customers
C. A customer using services from multiple cloud providers
D. Replication of data across multiple data centers

32. What is the primary function of a load balancer?
A. To distribute network traffic across multiple servers
B. To balance the electrical load in a data center
C. To manage the workload between CPUs in a server
D. To equalize bandwidth usage among users

33. Which of the following is NOT a common method for creating network segmentation?
A. Using VLANs
B. Implementing physical airgaps
C. Configuring Access Control Lists (ACLs)
D. Deploying honeypots

34. What is the main purpose of implementing least privilege in network security?
A. To reduce the cost of user licenses
B. To simplify the network topology
C. To minimize the potential damage from a compromised account
D. To increase network performance

35. In the context of disaster recovery, what does an RPO (Recovery Point Objective) define?
A. The maximum acceptable downtime for a system
B. The maximum acceptable data loss measured in time
C. The order in which systems should be recovered
D. The physical location where backups are stored

36. Which protocol is designed to provide confidentiality, integrity, and authenticity for network communications?
A. HTTPS
B. SMTP
C. IPsec
D. SNMP

37. What is the primary difference between synchronous and asynchronous replication in the context of data backup?
A. Synchronous replication is always faster
B. Asynchronous replication guarantees zero data loss

C. Synchronous replication waits for an acknowledgment before considering the write complete
D. Asynchronous replication requires more bandwidth

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

39. What is the main purpose of implementing network access control (NAC)?
A. To increase network speed
B. To ensure devices connecting to the network comply with security policies
C. To provide remote access to the network
D. To load balance traffic between different network segments

40. In the context of cloud security, what does the shared responsibility model primarily address?
A. The distribution of costs between the provider and the customer
B. The delegation of security responsibilities between the provider and the customer
C. The sharing of infrastructure among multiple customers
D. The distribution of bandwidth among cloud services

41. What is the primary purpose of a Web Application Firewall (WAF)?
A. To accelerate web content delivery
B. To protect web applications from specific application-layer attacks
C. To provide load balancing for web servers
D. To compress web traffic

42. Which of the following is NOT a typical characteristic of an advanced persistent threat (APT)?
A. Targeted attacks
B. Long-term presence in the target environment
C. Short-duration, high-volume data exfiltration
D. Sophisticated evasion techniques

43. What is the main difference between policies and procedures in information security?
A. Policies are technical, while procedures are non-technical
B. Procedures are high-level directives, while policies are detailed steps
C. Policies define what should be done, while procedures define how it should be done
D. Procedures are mandatory, while policies are optional guidelines

44. In the context of encryption, what does "perfect forward secrecy" provide?
A. Unbreakable encryption
B. Protection of past sessions if the long-term secret key is compromised
C. Faster encryption and decryption
D. Compatibility with legacy systems

45. What is the primary purpose of a honeypot in network security?
A. To attract and detect attackers
B. To store backup data
C. To optimize network traffic
D. To provide secure remote access

46. Which of the following best describes the principle of "separation of duties" in information security?
A. Segregating production and development environments
B. Dividing critical tasks among multiple individuals
C. Separating wired and wireless networks
D. Isolating internal and external network traffic

47. What is the main goal of a tabletop exercise in the context of incident response?
A. To physically test the strength of data center tables
B. To evaluate the incident response plan without actual system disruption
C. To benchmark the performance of security tools
D. To train new SOC analysts on security tools

48. In database security, what is the purpose of implementing data masking?
A. To encrypt data at rest
B. To hide sensitive data from unauthorized users while providing a functional alternative
C. To compress data for efficient storage
D. To replicate data across multiple sites

49. What is the primary focus of the NIST Cybersecurity Framework?
A. Compliance with government regulations
B. Implementation of specific security tools
C. Managing cybersecurity risk to critical infrastructure
D. Development of new encryption standards

50. Which of the following is NOT a typical component of a Security Information and Event Management (SIEM) system?
A. Log collection
B. Patch management
C. Correlation and analysis
D. Alerting and reporting

Answer Key: Chapter 4

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