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 80-question exam covering the main topics from Chapter 4: Network Security

1. What is the primary goal of a network?
A. To isolate computers
B. To share data, information, or resources
C. To increase electricity consumption
D. To complicate communications

2. Which of the following is NOT a basic type of network mentioned in the document?
A. LAN
B. WAN
C. MAN
D. VLAN

3. What device is used to connect multiple devices in a network and is less likely to be seen in business networks?
A. Switch
B. Router
C. Hub
D. Firewall

4. Which network device knows the addresses of connected devices and routes traffic only to the specific port/device?
A. Hub
B. Switch
C. Router
D. Server

5. What is the primary function of a router in a network?
A. To provide information to other computers
B. To control traffic flow and connect similar networks
C. To filter traffic based on defined rules
D. To be an endpoint for communication

6. What is the main purpose of a firewall?
A. To route traffic efficiently
B. To provide information to other computers
C. To filter traffic based on defined rules

D. To assign IP addresses

7. What is an endpoint in network communication?
A. A router
B. A firewall
C. One end of a communication link, often a client or server
D. A hub

8. What does the MAC address represent?
A. The IP address of the device
B. The physical network interface of the device
C. The software version of the device
D. The geographic location of the device

9. How many bytes (octets) are there in an IPv4 address?
A. 2
B. 4
C. 6
D. 8

10. In the most basic form, how many layers does a network model have?
A. 1
B. 2
C. 4
D. 7

11. Which layer is responsible for formatting data for the physical network connection?
A. Upper layer
B. Lower layer
C. Middle layer
D. Application layer

12. How many layers are there in the OSI model?
A. 3
B. 5
C. 7
D. 9

13. Which OSI layer is responsible for routing and forwarding?
A. Network layer
B. Transport layer
C. Session layer
D. Physical layer

14. At which OSI layer does a hub operate?
A. Physical layer
B. Data link layer
C. Network layer

D. Transport layer

15. Which of the following is NOT a protocol used at the TCP/IP Application Layer?
A. Telnet
B. FTP
C. ICMP
D. SMTP

16. What is the difference between TCP and UDP?
A. TCP is connection-oriented, UDP is connectionless
B. TCP is used for emails, UDP for web browsing
C. TCP is faster than UDP
D. UDP provides guaranteed delivery, TCP doesn't

17. What is the main purpose of ICMP?
A. To establish connections
B. To transfer files
C. To determine the health of a network or link
D. To encrypt data

18. What is the total number of IP addresses available in IPv4?
A. 2^16
B. 2^32
C. 2^64
D. 2^128

19. Which of the following is a valid private IP address range?
A. 11.0.0.0 to 11.255.255.255
B. 172.16.0.0 to 172.31.255.255
C. 192.168.0.0 to 192.168.0.255
D. 224.0.0.0 to 239.255.255.255

20. What is the loopback address in IPv4?
A. 255.255.255.255
B. 127.0.0.1
C. 0.0.0.0
D. 1.1.1.1

21. How many bits are used for addressing in IPv6?
A. 32 bits
B. 64 bits
C. 128 bits
D. 256 bits

22. Which of the following is a major security improvement in IPv6 over IPv4?
A. Larger address space
B. Improved quality of service
C. Mandatory IPsec implementation

D. Simplified header format

23. What type of attack involves purposely sending a network packet larger than expected?
A. Fragment attack
B. Man-in-the-middle attack
C. Oversized packet attack
D. Spoofing attack

24. Which of the following is a characteristic of cloud computing according to NIST?
A. Limited scalability
B. On-demand self-service
C. Restricted network access
D. Low measurability

25. In which cloud service model does the provider offer access to software applications?
A. IaaS
B. PaaS
C. SaaS
D. NaaS

26. Which cloud service model provides an environment for customers to build and operate their own software?
A. IaaS
B. PaaS
C. SaaS
D. DaaS

27. In an IaaS model, what is the consumer typically responsible for maintaining?
A. Physical servers
B. Virtualization layer
C. Operating systems and applications
D. Networking infrastructure

28. Which cloud deployment model is created by combining two other deployment models?
A. Public cloud
B. Private cloud
C. Hybrid cloud
D. Community cloud

29. What is a key driver for hybrid cloud deployments?
A. Giving up control of all IT processes
B. Reducing reuse of previous investments
C. Retaining control of critical tasks while leveraging public cloud for non-mission-critical workloads
D. Increasing dependency on a single vendor

30. What type of company manages information technology assets for another company?
A. CSP

B. MSP
C. ISP
D. ASP

31. What does an SLA stand for?
A. System Level Architecture
B. Service Level Agreement
C. Software Licensing Application
D. Secure Link Arrangement

32. Which of the following should be specified in a cloud computing SLA?
A. Customer's internal policies
B. Service availability
C. Provider's profit margins
D. Customer's organizational chart

33. What is the objective of network segmentation?
A. To increase network traffic
B. To allow unrestricted communication between all devices
C. To control traffic among networked devices
D. To eliminate the need for firewalls

34. What is a DMZ in network security?
A. A network area designed to be accessed by outside visitors but isolated from the private network
B. A type of malware
C. A secure network for top-secret data
D. A wireless network protocol

35. What does a VPN provide?
A. A public network accessible to anyone
B. A communication tunnel for point-to-point transmission
C. A local area network within an office
D. A broadband internet connection

36. What is defense in depth?
A. A single, strong firewall
B. A focused protection on one critical asset
C. Using multiple types of access controls in layers
D. Relying solely on encryption for security

37. Which statement best describes zero trust networks?
A. They implicitly trust all internal traffic
B. They use fewer firewalls than traditional networks
C. They are often microsegmented networks with firewalls at many connecting points
D. They focus only on perimeter security

38. What is a key concept of zero trust security model?

A. Trust but verify
B. Never trust, always verify
C. Trust all, verify some
D. Trust internal, verify external

39. What is the primary purpose of Network Access Control (NAC)?
A. To optimize network speed
B. To ensure all devices connecting to a network comply with security policies
C. To block all external devices
D. To allow unrestricted access to the network

40. Which of the following is a critical asset that NAC protects?
A. The organization's profit margins
B. The organization's network
C. The organization's office furniture
D. The organization's fleet vehicles

41. What technology is often used to create software-based LAN segments?
A. NAC
B. VLAN
C. WAN
D. DMZ

42. In the context of VLANs, what does the term "VLAN hopping" refer to?
A. A method for improving VLAN performance
B. An attack allowing a malicious user to see traffic from other VLANs
C. A technique for load balancing between VLANs
D. A way to automatically assign devices to VLANs

43. Which of the following best describes a VPN?
A. It is always an encrypted tunnel
B. It is a point-to-point connection between two hosts that allows them to communicate
C. It is a type of firewall
D. It is a physical network infrastructure

44. What is a potential security risk of using protocols that transmit information in clear text?
A. Increased network speed
B. Improved compatibility
C. Vulnerability to network sniffing
D. Enhanced user authentication

45. Which protocol is a secure alternative to Telnet?
A. SSH
B. HTTP
C. FTP
D. SMTP

46. What is the secure alternative port for SMTP?

A. Port 25
B. Port 443
C. Port 587
D. Port 80

47. Which protocol can be used instead of unencrypted DNS on port 53?
A. DNSSEC
B. DNS over TLS (DoT)
C. HTTPS
D. SFTP

48. What does HTTPS use to protect data in transit between the server and the browser?
A. Symmetric encryption
B. Hashing
C. SSL/TLS
D. Plaintext encoding

49. Why is SSL no longer considered secure?
A. It's too slow
B. It has been compromised
C. It uses too much bandwidth
D. It's not compatible with modern browsers

50. Which version of TLS is recommended for web servers and clients?
A. TLS 1.0
B. TLS 1.1
C. TLS 1.2
D. TLS 1.3 or higher

51. What is a managed service provider (MSP)?
A. A company that only provides internet access
B. A company that manages IT assets for another company
C. A cloud service provider
D. A hardware manufacturer

52. Which of the following is an example of a managed security service?
A. Selling security hardware
B. Publishing security whitepapers
C. Managed detection and response (MDR)
D. Manufacturing security cameras

53. In the OSI model, what is encapsulated data at the Data Link layer called?
A. Segment
B. Packet
C. Frame
D. Bit

54. Which of the following is considered the most essential representation of data at Layer 1 of the OSI model?
A. Byte
B. Frame
C. Packet
D. Bit

55. What is the process of converting a message from plaintext to ciphertext called?
A. Encoding
B. Hashing
C. Encryption
D. Compression

56. What type of attack involves faking the sending address of a transmission?
A. Spoofing attack
B. Phishing attack
C. Sniffing attack
D. Overflow attack

57. Which of the following best describes the Internet of Things (IoT)?
A. A collection of websites
B. A group of interconnected servers
C. Devices that can communicate over the internet to affect and monitor the real world
D. A new internet protocol

58. Why do embedded systems and IoT devices need special attention in terms of security?
A. They are always secure by default
B. They have no impact on the physical world
C. A security breach could cause harm to people and property
D. They cannot be accessed remotely

59. What is microsegmentation in network security?
A. A technique to increase the size of network segments
B. A part of zero-trust strategy that breaks LANs into very small zones using firewalls
C. A method to combine multiple networks into one
D. A way to reduce the number of connected devices

60. What is a defining characteristic of a hybrid cloud?
A. It only uses public cloud resources
B. It combines public and private cloud resources
C. It is exclusively used by one organization
D. It does not connect to the internet

61. In cloud computing, what does PaaS stand for?
A. Protocol as a Service
B. Platform as a Service
C. Process as a Service
D. Peripheral as a Service

62. Which of the following is a responsibility of the cloud service customer in a SaaS model?
A. Application maintenance
B. Operating system updates
C. User-specific application configuration
D. Server hardware upgrades

63. What is the 127.0.0.1 IPv4 address commonly used for?
A. Default router address
B. Loopback testing
C. Public website hosting
D. Dynamic IP assignment

64. Which protocol is used for secure file transfers as an alternative to FTP?
A. SMTP
B. HTTP
C. Telnet
D. SFTP

65. What is the primary function of SMTP?
A. Browsing websites
B. Transferring files
C. Sending emails
D. Remote server administration

66. Which layer of the TCP/IP model is responsible for reliable data delivery?
A. Application Layer
B. Transport Layer
C. Internet Layer
D. Link Layer

67. What is the main difference between TCP and UDP in terms of data delivery?
A. TCP is connectionless, UDP is connection-oriented
B. TCP provides reliable delivery, UDP does not guarantee delivery
C. TCP is only used for email, UDP for web browsing
D. TCP is slower than UDP in all cases

68. What type of cloud deployment model is used when organizations in the same industry share cloud resources?
A. Public cloud
B. Private cloud
C. Hybrid cloud
D. Community cloud

69. Which of the following is a benefit of cloud computing?
A. Increased physical control of servers
B. Reduced need for internet connectivity
C. Pay-per-use metered service

D. Decreased scalability

70. What is the purpose of the subnet mask in an IP network?
A. To identify the network portion of an IP address
B. To encrypt network traffic
C. To assign IP addresses dynamically
D. To block malicious websites

71. In the context of network security, what does "defense in depth" refer to?
A. Implementing a single, very strong security control
B. Using multiple layers of security controls
C. Focusing only on perimeter defense
D. Relying solely on firewalls for protection

72. What is the primary purpose of a DMZ (Demilitarized Zone) in network architecture?
A. To host internal, private services
B. To eliminate the need for firewalls
C. To host public-facing services while protecting the internal network
D. To increase network speed

73. Which of the following is true about Network Access Control (NAC)?
A. It is only concerned with external threats
B. It enforces security policy compliance for devices before granting network access
C. It is a type of firewall
D. It is used exclusively for wireless networks

74. What is the main goal of network segmentation?
A. To increase network complexity
B. To improve network performance only
C. To control and limit traffic between different parts of the network
D. To allow all devices to communicate freely

75. What does BYOD stand for in the context of network security?
A. Build Your Own Database
B. Bring Your Own Device
C. Buy Your Own Domain
D. Back Your Own Data

76. Which of the following is a security concern specifically related to BYOD?
A. Devices are too old
B. Devices are too expensive
C. Personal devices may lack enterprise security controls
D. Personal devices are always less powerful than corporate devices

77. What is a characteristic of IaaS (Infrastructure as a Service) in cloud computing?
A. The provider manages the operating systems
B. The customer has control over the underlying cloud infrastructure
C. It provides ready-to-use software applications

D. The customer can deploy and run arbitrary software, including operating systems

78. In the OSI model, which layer is responsible for establishing, managing, and terminating sessions?
A. Transport Layer
B. Network Layer
C. Session Layer
D. Presentation Layer

79. What is the primary function of the Presentation Layer in the OSI model?
A. Routing and switching
B. Data formatting and encryption
C. Physical transmission of data
D. Reliable data transfer

80. Which of the following is NOT a typical responsibility of the Application Layer in the OSI model?
A. Identifying communication partners
B. Synchronizing communication
C. Determining resource availability
D. Packet sequencing and retransmission