SSCP Certification Real Exam questions - Satender Kumar

---

1. Which of the following is NOT a component of the CIA Triad in information security?

- A) Confidentiality
- B) Integrity
- C) Accountability
- D) Availability

2. A company has implemented Multi-factor Authentication (MFA) for its users. Which of the following is the most secure combination?

- A) Username and password
- B) Username and pin
- C) Username and biometric authentication
- D) Username and email verification

3. Which of the following protocols is most commonly used for encrypting data in transit for web applications?

- A) HTTP
- B) HTTPS
- C) FTP
- D) SMTP

4. What is the primary purpose of the Zero Trust Architecture (ZTA)?

- A) To ensure internal network security by limiting access to unauthorized users
- B) To allow full access to all internal resources once connected to the network
- C) To monitor data on end-user devices
- D) To rely on perimeter defenses for protecting network data

5. Which of the following is a strategy for minimizing exposure to risk when an organization cannot implement a preferred risk mitigation measure?

- A) Accept
- B) Transfer
- C) Mitigate
- D) Compensate

6. What type of encryption is used in symmetric encryption systems?

- A) Public key
- B) Private key
- C) Shared key
- D) Digital signature

7. What is the primary difference between Role-Based Access Control (RBAC) and Discretionary Access Control (DAC)?

- A) RBAC allows the resource owner to define access permissions, while DAC uses roles to assign permissions.
- B) RBAC defines access based on user roles, whereas DAC allows users to manage their own access.
- C) RBAC and DAC are the same access control models.
- D) RBAC is a more flexible access control model compared to DAC.

8. What is the primary function of a firewall in network security?

- A) To detect network intrusions
- B) To encrypt all network traffic
- C) To control traffic between network zones
- D) To monitor employee activity on the internet

9. Which of the following defines the maximum allowable downtime for a business function after a disaster has occurred?

- A) RTO (Recovery Time Objective)
- B) RPO (Recovery Point Objective)
- C) MTD (Maximum Tolerable Downtime)
- D) BCP (Business Continuity Plan)

10. In cryptography, which of the following methods is used to ensure the integrity of data during transmission?

- A) Symmetric key encryption
- B) Public key encryption
- C) Digital signatures
- D) Hashing

11. What is the key advantage of using two-factor authentication (2FA)?

- A) It ensures secure password management.
- B) It allows access from multiple devices.
- C) It requires a user to provide two different forms of verification to access a system.
- D) It requires only a password for login.

12. Which framework is used for risk management that helps organizations identify, assess, and manage security risks?

- A) NIST RMF (Risk Management Framework)
- B) ISO 27001
- C) PCI DSS
- D) NIST 800-53

13. What does a risk register help with in an organization's risk management process?

- A) Documenting and tracking identified risks
- B) Encrypting sensitive data
- C) Managing employee access to systems
- D) Monitoring security threats

14. Which of the following is an example of a detective control in a security system?

- A) Encryption
- B) Firewalls
- C) Intrusion Detection Systems (IDS)
- D) Access Control Lists (ACLs)

15. Which of the following standards provides guidelines for handling sensitive customer data in the payment card industry?

- A) ISO 27001
- B) PCI DSS
- C) NIST 800-53
- D) HIPAA

16. A company is implementing a cloud-based disaster recovery (DR) solution. Which type of cloud service model is being used if they use cloud storage for backing up critical systems?

- A) IaaS (Infrastructure as a Service)
- B) PaaS (Platform as a Service)
- C) SaaS (Software as a Service)
- D) DRaaS (Disaster Recovery as a Service)

17. Which of the following is NOT a common method for securely transmitting sensitive data over the internet?

- A) HTTPS
- B) SSH
- C) FTP
- D) VPN

18. What is the purpose of a SIEM (Security Information and Event Management) system in a network security environment?

- A) To monitor and manage encryption keys
- B) To perform system audits
- C) To collect and analyze log data in real-time
- D) To install firewalls and intrusion prevention systems

19. Which of the following is a common tool used to perform penetration testing on a system?

- A) Nessus
- B) Wireshark
- C) Metasploit
- D) Snort

20. When an organization's password policy requires passwords to be a minimum of 12 characters, what security principle is being enforced?

- A) Least privilege
- B) Integrity
- C) Complexity

- D) Non-repudiation

21. Which of the following security mechanisms is most commonly used to prevent unauthorized access to data during transmission over a public network?

- A) SSL/TLS
- B) IPsec
- C) HTTPS
- D) SSH

22. What is the purpose of a security patch in system management?

- A) To update the system with new features
- B) To fix vulnerabilities and improve security
- C) To upgrade the operating system
- D) To install software updates

23. Which of the following is the best method to secure data on a laptop in the event of theft?

- A) Use strong password protection for user accounts
- B) Implement full disk encryption
- C) Install anti-virus software
- D) Backup data regularly to the cloud

24. Which cryptographic algorithm is most commonly used in securing web traffic?

- A) AES
- B) RSA
- C) Triple DES
- D) SHA-256

25. Which type of attack is characterized by an attacker intercepting and altering communications between two parties without either party knowing?

- A) Phishing
- B) Man-in-the-middle (MITM) attack
- C) Denial of Service (DoS)
- D) SQL injection

26. What is the primary purpose of user access reviews?

- A) To ensure users have the appropriate level of access for their role
- B) To check the software versions in use across the network
- C) To ensure password policies are being followed
- D) To perform vulnerability assessments on user accounts

27. What does ISO 27001 focus on in an organization?

- A) Network architecture design
- B) Information security management system (ISMS)
- C) Incident response procedures
- D) Encryption standards and policies

28. A company is performing a penetration test. Which of the following best describes the purpose of this test?

- A) To monitor system logs for suspicious activity
- B) To identify vulnerabilities before attackers can exploit them
- C) To back up critical systems
- D) To train staff in recognizing phishing attempts

29. Which of the following is a preventive control for physical security?

- A) Fire alarms
- B) Security guard patrols
- C) CCTV surveillance cameras
- D) Access control systems (e.g., keycards)

30. Which of the following is the most common cause of data breaches in organizations?

- A) Lack of employee training
- B) Poor access controls
- C) Insecure software updates
- D) Insider threats

31. When performing risk assessments, which factor is considered when calculating the Risk Impact?

- A) Cost of recovery after a breach
- B) The likelihood of an attack
- C) The potential consequences of an attack
- D) The speed at which vulnerabilities can be patched

32. Which of the following is an essential element of Data Loss Prevention (DLP) systems?

- A) Regular vulnerability scanning
- B) Monitoring data for unauthorized access or leakage
- C) Encrypting data in transit
- D) Enforcing multi-factor authentication

33. Which of the following types of access control models is based on the idea of a user having access to resources based on their role in the organization?

- A) Mandatory Access Control (MAC)
- B) Discretionary Access Control (DAC)
- C) Role-Based Access Control (RBAC)
- D) Attribute-Based Access Control (ABAC)

34. What is the primary purpose of log management in information security?

- A) To back up critical data
- B) To monitor and track system activities for compliance and security
- C) To monitor employee internet usage
- D) To encrypt sensitive data during transmission

35. Which of the following encryption methods uses a public key for encryption and a private key for decryption?

- A) Symmetric key encryption
- B) RSA encryption
- C) AES encryption
- D) Blowfish encryption

36. A user receives an email that appears to be from their bank asking them to verify their account information. Which type of attack is this an example of?

- A) Spoofing
- B) Phishing
- C) Spear phishing
- D) Man-in-the-middle attack

37. In a cloud-based infrastructure, which of the following would typically be NOT the responsibility of the cloud service provider?

- A) Maintaining the physical hardware
- B) Securing the operating system
- C) Installing and maintaining applications
- D) Ensuring customer data privacy

38. Which of the following is the primary benefit of using containerization in application deployment?

- A) Greater scalability of application resources
- B) Enhanced security by isolating applications in separate containers
- C) Reduction in the need for hardware resources
- D) Simplified software patching and maintenance

39. When performing an incident response investigation, what is the first step after identifying a potential security incident?

- A) Eradication of the threat
- B) Containment of the incident
- C) Incident recovery and system restoration
- D) Identification and analysis of the root cause

40. Which of the following protocols is used for secure remote login to a network device or server?

- A) HTTP
- B) FTP
- C) SSH
- D) Telnet

41. Which of the following is the best way to ensure that data remains intact during a backup process?

- A) Encrypt data before backup
- B) Store backup copies in multiple locations

- C) Use compression techniques during the backup process
- D) Perform regular integrity checks on backup files

42. Which of the following is considered a proactive security control?

- A) Intrusion detection system (IDS)
- B) Firewalls
- C) Antivirus software
- D) Security audits

43. What is the primary function of access control lists (ACLs) in network security?

- A) They define which users and systems can access network resources and what actions they can perform.
- B) They monitor the health of a network.
- C) They detect and report attacks.
- D) They encrypt data in transit.

44. A user is accessing a web application that requires a one-time password sent to their mobile phone. What type of authentication is this?

- A) Two-factor authentication (2FA)
- B) Single sign-on (SSO)
- C) Multi-factor authentication (MFA)
- D) Password-based authentication

45. What is role-based access control (RBAC) primarily used for?

- A) To prevent unauthorized software installation
- B) To restrict access to network resources based on the user's role within the organization
- C) To monitor network activity for suspicious behavior
- D) To configure encryption for sensitive data

46. Which of the following is an example of a physical security control?

- A) Encryption
- B) User authentication
- C) Biometric scanners
- D) Intrusion detection systems (IDS)

47. Which cloud deployment model involves a single organization using a cloud infrastructure hosted either internally or by a third party?

- A) Public cloud
- B) Private cloud
- C) Hybrid cloud
- D) Community cloud

48. What is the term for encryption that secures data at rest, ensuring it is unreadable if the storage media is accessed by unauthorized parties?

- A) Data masking

- B) Data in motion encryption
- C) Full disk encryption (FDE)
- D) File-level encryption

49. Which of the following describes the concept of least privilege?

- A) Users should have access to all resources to avoid unnecessary restrictions.
- B) Users should have only the minimum permissions required to perform their job functions.
- C) Users should be allowed administrative access to resources.
- D) Users should be allowed to access resources based on their role.

50. Which of the following best describes data masking?

- A) Replacing sensitive information with fictitious data that retains its usefulness for analysis.
- B) Encrypting data to prevent unauthorized access.
- C) Deleting sensitive data to protect privacy.
- D) Using password-protected files to store sensitive data.

51. When implementing an information security program, what is the first step in the risk management process?

- A) Risk assessment
- B) Risk treatment
- C) Risk identification
- D) Risk monitoring

52. Which of the following is an essential best practice for configuring firewall rules?

- A) Allow all inbound traffic and restrict outbound traffic
- B) Block all inbound traffic and allow all outbound traffic
- C) Implement least privilege by restricting access to only necessary resources
- D) Allow unrestricted inbound and outbound traffic

53. Which of the following is NOT a feature of public key infrastructure (PKI)?

- A) Digital certificates for user identification
- B) Public and private key pairs for encryption and decryption
- C) Secure transmission of data via IPsec
- D) A certificate authority (CA) for managing and issuing certificates

54. What does security incident response typically start with?

- A) Eradicating the threat
- B) Identifying and analyzing the incident
- C) Restoring the affected systems
- D) Reporting the incident to stakeholders

55. What is the primary advantage of using VPNs (Virtual Private Networks) for remote access?

- A) They allow for faster internet speeds
- B) They provide encrypted communication channels to secure data transmission over the internet

- C) They provide access to public cloud services
- D) They simplify firewall configuration

56. Which of the following best describes a zero-day exploit?

- A) An attack that is launched after a vulnerability has been patched
- B) An attack that exploits a vulnerability that is publicly known but not yet patched
- C) An attack that is easily prevented by applying patches
- D) An attack that occurs on the first day of an employee's access to a system

57. Which of the following is an example of a social engineering attack?

- A) SQL injection
- B) Denial of Service (DoS) attack
- C) Phishing
- D) Brute force attack

58. Which of the following encryption protocols is commonly used to secure email communications?

- A) AES
- B) SSL/TLS
- C) PGP
- D) SHA-256

59. A company wants to ensure that its cloud service provider is committed to protecting its data. Which of the following should the company review?

- A) The service provider's annual budget
- B) The provider's disaster recovery plan
- C) The service provider's incident response procedures
- D) The provider's service-level agreements (SLAs) and data privacy policies

60. When performing a vulnerability assessment, which of the following is the most appropriate first step?

- A) Implementing fixes and patching systems
- B) Conducting a risk assessment to identify potential impacts
- C) Scanning systems for known vulnerabilities
- D) Encrypting sensitive data in the system

61. Which of the following is an example of a preventive control in security?

- A) Intrusion detection system (IDS)
- B) Firewalls
- C) Security audits
- D) Encryption

62. A company wants to ensure that it can recover its critical data in case of a disaster. Which of the following is the most appropriate solution?

- A) Backup and disaster recovery (DR) plan

- B) Anti-malware software
- C) Intrusion prevention system (IPS)
- D) Security patch management

63. Which of the following is NOT a part of the shared responsibility model for cloud security?

- A) Securing the physical infrastructure
- B) Managing operating systems and applications
- C) Protecting data and encryption keys
- D) Performing network traffic monitoring

64. Which of the following tools is commonly used to monitor network traffic for security events?

- A) SNMP (Simple Network Management Protocol)
- B) SIEM (Security Information and Event Management)
- C) WAF (Web Application Firewall)
- D) IDS (Intrusion Detection System)

65. What is the purpose of data tokenization?

- A) To convert sensitive data into non-sensitive data
- B) To encrypt data to ensure confidentiality
- C) To create an audit trail of data access
- D) To compress large files for efficient storage

66. What is a denial-of-service (DoS) attack designed to achieve?

- A) To steal sensitive data from a system
- B) To encrypt files for ransom
- C) To overwhelm and disrupt the availability of a system or network
- D) To gain unauthorized access to a system

67. Which of the following types of attacks exploits a vulnerability before it becomes publicly known?

- A) Zero-day attack
- B) DDoS attack
- C) Phishing
- D) Brute-force attack

---

68. Which of the following is the primary function of a firewall?

- A) To detect unauthorized access attempts
- B) To restrict network traffic based on security rules
- C) To log suspicious user activity
- D) To encrypt data in transit

69. Which of the following types of access control models assigns users access rights based on their roles within an organization?

- A) Role-Based Access Control (RBAC)
- B) Mandatory Access Control (MAC)
- C) Discretionary Access Control (DAC)
- D) Attribute-Based Access Control (ABAC)

70. What type of cryptographic algorithm is used in digital signatures to provide non-repudiation?

- A) Symmetric key encryption
- B) Asymmetric key encryption
- C) Hashing algorithm
- D) Message authentication code (MAC)

71. Which of the following would be considered an example of data in transit?

- A) Encrypted email being sent over the network
- B) Data stored on an encrypted hard drive
- C) A backup file on an internal server
- D) A data archive stored on tape backup

72. What is social engineering?

- A) Using technical tools to manipulate network traffic
- B) An attack where attackers exploit human behavior to gain unauthorized access
- C) Cracking passwords by using a dictionary attack
- D) Implementing encryption on data at rest

73. Which of the following is used to authenticate a user's identity during multi-factor authentication (MFA)?

- A) User’s password
- B) Physical security token
- C) Biometric data (e.g., fingerprint)
- D) All of the above

74. Which of the following is NOT a characteristic of host-based intrusion detection systems (HIDS)?

- A) It monitors events and activities on a single host
- B) It analyzes traffic between networked devices
- C) It looks for unusual behavior and potential security breaches
- D) It alerts administrators to possible security issues

75. What is the main goal of an incident response plan?

- A) To prevent unauthorized access to data
- B) To ensure compliance with data privacy laws
- C) To handle and mitigate the impact of security incidents
- D) To back up critical data in real-time

76. Which of the following is the most secure method for storing sensitive data in a database?

- A) Storing data in plain text with access controls

- B) Using encryption for data at rest
- C) Regularly backing up the database
- D) Restricting access to database servers

77. When performing an internal audit of a company's security measures, which of the following would be an important task?

- A) Patching all outdated software
- B) Evaluating the effectiveness of security policies
- C) Reviewing the company's business continuity plan
- D) Increasing firewall rules

78. Which of the following methods is used to verify the integrity of a file or message?

- A) Symmetric key encryption
- B) Hashing
- C) Digital signature
- D) Public key encryption

79. Which of the following is the best practice to secure an organization's wireless network?

- A) Disable all remote access points
- B) Use **WPA3** encryption
- C) Use **WEP** encryption
- D) Allow open access for faster connection speeds

80. Which of the following is NOT an important element of an effective disaster recovery plan (DRP)?

- A) Documented recovery procedures for critical systems
- B) Regular testing and drills
- C) A plan for restoring non-critical systems first
- D) A comprehensive business continuity plan (BCP)

81. Which of the following is an example of an end-to-end encryption method?

- A) Secure File Transfer Protocol (SFTP)
- B) File Integrity Monitoring (FIM)
- C) Public Key Infrastructure (PKI)
- D) Secure Hypertext Transfer Protocol (HTTPS)

82. What is the primary goal of implementing network segmentation in an enterprise environment?

- A) To ensure all network traffic is encrypted
- B) To control and restrict access to sensitive data and applications
- C) To increase network bandwidth
- D) To simplify firewall rules

83. Which of the following protocols is commonly used for securing wireless communication?

- A) WEP

- B) WPA2
- C) SSL
- D) IPsec

84. Which of the following would be NOT part of the risk assessment process?

- A) Identifying vulnerabilities in a system
- B) Calculating potential financial losses due to an attack
- C) Implementing a data backup strategy
- D) Determining the likelihood of a security breach

85. What is the purpose of implementing Single Sign-On (SSO)?

- A) To allow users to authenticate once and access multiple applications without re-authenticating
- B) To enable users to sign in with biometric authentication
- C) To secure sensitive data through encryption
- D) To monitor user behavior for suspicious activities

86. What does confidentiality refer to in information security?

- A) Ensuring the system is available to authorized users at all times
- B) Ensuring that information is only accessible to those with appropriate authorization
- C) Ensuring that data is not altered during transmission
- D) Ensuring users are not denied access to necessary resources

87. What is the first step in an effective disaster recovery plan (DRP)?

- A) Documenting recovery procedures for critical systems
- B) Ensuring data is encrypted before transmission
- C) Installing and configuring backup servers
- D) Conducting a business impact analysis (BIA)

88. Which of the following is an example of an administrative control in information security?

- A) Encryption of sensitive data
- B) Regular security awareness training
- C) Use of access control lists (ACLs)
- D) Firewalls protecting internal networks

89. Which of the following is NOT a benefit of using Cloud Access Security Broker (CASB)?

- A) Providing visibility and control over user traffic to cloud applications
- B) Enforcing security policies across multiple cloud services
- C) Encrypting data in transit between cloud providers and on-premise systems
- D) Managing hardware resources for cloud applications

90. When using role-based access control (RBAC), who defines the permissions for users?

- A) The user
- B) The network administrator
- C) The application owner

- D) The system administrator

91. Which of the following methods is used to ensure data is protected during file transfer across an insecure network?

- A) Public key encryption
- B) Hashing algorithms
- C) File integrity monitoring
- D) File compression

92. What does IPsec provide for Virtual Private Networks (VPNs)?

- A) Data encryption and integrity
- B) Public key distribution
- C) Packet filtering based on IP addresses
- D) Network load balancing

93. Which of the following best describes the role of Security Information and Event Management (SIEM) systems?

- A) To store logs from all network devices and systems
- B) To monitor network traffic and provide security alerts in real time
- C) To encrypt sensitive data across multiple systems
- D) To manage access control lists for all network devices

94. What is the purpose of a hash function in cryptography?

- A) To encrypt data before transmission
- B) To verify the integrity of data without revealing the original data
- C) To establish a secure channel for communications
- D) To generate random keys for encryption algorithms

95. What is a key element of an effective incident response plan?

- A) Keeping all systems fully patched and up-to-date
- B) Having predefined roles and responsibilities for the incident response team
- C) Monitoring for security events continuously
- D) Encrypting all communications during an incident

96. Which of the following is used to authenticate and secure communications between a web browser and server?

- A) RSA public key encryption
- B) SSL/TLS certificates
- C) AES symmetric encryption
- D) SHA-256 hash function

97. Which of the following best describes a zero-day vulnerability?

- A) A vulnerability that is publicly known and already patched
- B) A vulnerability that is patched within 24 hours of discovery
- C) A vulnerability that is exploited before a patch is available

- D) A vulnerability that affects only one type of software

98. What is the primary purpose of implementing a network intrusion detection system (NIDS)?

- A) To block malicious network traffic
- B) To monitor network traffic for signs of attacks
- C) To encrypt all incoming and outgoing traffic
- D) To authenticate users on the network

99. What is data obfuscation used for in a database environment?

- A) To create backups of sensitive data
- B) To make data unreadable or indistinguishable to unauthorized users
- C) To encrypt data during storage
- D) To monitor and log data access for compliance

100. Which of the following best describes threat intelligence?

- A) Information gathered from external sources to identify potential threats to an organization
- B) Alerts generated by firewalls and intrusion detection systems
- C) The process of identifying vulnerabilities in a system
- D) Real-time analysis of network traffic for malicious patterns

101. What is the most effective method to protect sensitive data from being exposed in case of an accidental data leak?

- A) Encrypting data at rest
- B) Storing data in a secure cloud environment
- C) Using complex passwords for all accounts
- D) Implementing access controls for all systems

102. Which of the following methods is used to verify the integrity of a file?

- A) Digital signature
- B) Symmetric encryption
- C) Multi-factor authentication
- D) VPN encryption

103. Which of the following should be part of a data retention policy?

- A) Guidelines for how long sensitive data should be stored
- B) Instructions for encrypting all company data
- C) Procedures for managing employee logins
- D) Rules for regular password changes

104. Which of the following would be an example of compensating control?

- A) Using firewalls to restrict unauthorized access
- B) Implementing encryption to protect sensitive data
- C) Using a more advanced access control method after an original control fails
- D) Applying patches and updates to mitigate vulnerabilities

105. What is the main purpose of data classification in information security?

- A) To determine which data should be encrypted
- B) To define appropriate access controls based on the sensitivity of the data
- C) To provide an audit trail of all access attempts
- D) To monitor system performance based on data volume

106. What is the role of a Public Key Infrastructure (PKI) system in securing communications?

- A) Encrypts communication between the sender and recipient
- B) Provides a mechanism for managing and distributing encryption keys
- C) Ensures data integrity using hash functions
- D) Authenticates users based on biometrics

107. What does data masking primarily protect against?

- A) Unauthorized access to data during storage
- B) Data theft during system transfer
- C) Leaking sensitive information to unauthorized users
- D) Exposure of data in public reports

108. What is the primary advantage of using a multi-factor authentication (MFA) system?

- A) It improves user experience by reducing password fatigue
- B) It adds layers of security to ensure that only authorized users can access sensitive data
- C) It provides an audit trail of access attempts
- D) It enables automatic password generation for users

109. When should an organization perform a vulnerability assessment?

- A) Only when a system is first deployed
- B) On an annual basis to meet regulatory requirements
- C) Continuously, as part of an ongoing security strategy
- D) Only after an attack has been detected

110. Which of the following is a primary advantage of using cloud services for business continuity?

- A) Physical security of the cloud provider’s data center
- B) The provider’s ability to scale infrastructure on demand
- C) The ability to avoid regulatory compliance requirements
- D) Full control over all hardware resources used in the cloud

111. What is the most secure method to ensure that only authorized users access sensitive data in an organization?

- A) Implementing firewalls
- B) Using **role-based access control (RBAC)**
- C) Encrypting all stored data
- D) Regularly rotating passwords

112. Which of the following is a detective control in information security?

- A) Firewalls
- B) Encryption
- C) Intrusion detection systems (IDS)
- D) Access controls

113. What does the term Zero Trust Architecture (ZTA) mean?

- A) Trusting all internal traffic once it passes through the perimeter
- B) Restricting access to data and applications to authenticated and authorized users only, even inside the network
- C) Allowing access to resources based on user credentials alone
- D) Trusting external users based on IP address location

114. Which of the following best describes a penetration test?

- A) Scanning systems to identify potential vulnerabilities without exploiting them
- B) Simulating a real-world attack to identify and exploit vulnerabilities
- C) Running automated scripts to test system performance
- D) Evaluating the organization's compliance with security regulations

115. What type of attack is commonly associated with spoofing?

- A) Phishing
- B) Man-in-the-middle attack
- C) Denial of Service (DoS)
- D) SQL injection

116. What is the most effective way to protect data during transmission?

- A) Using firewalls to block unauthorized access
- B) Implementing end-to-end encryption
- C) Storing data in a secure cloud environment
- D) Using secure passwords for all accounts

117. Which of the following is the primary focus of a disaster recovery plan (DRP)?

- A) Preventing future attacks
- B) Ensuring business operations continue during and after a disaster
- C) Training employees on security awareness
- D) Detecting security breaches in real-time

118. When securing a network, which of the following should be done first to reduce risk?

- A) Implement firewalls and intrusion detection systems
- B) Conduct a risk assessment to identify the most critical threats
- C) Create a comprehensive security awareness program
- D) Encrypt all network communications

119. Which of the following best describes the principle of least privilege?

- A) Users should only have access to the minimum resources necessary to perform their job
- B) Users should be given broad access to all systems to perform their role

- C) All users should have equal access to resources based on their department
- D) Users should be able to access resources when needed, regardless of their job function

120. What is the best practice for securing a database that contains sensitive information?

- A) Use strong access controls and encryption to protect the data
- B) Allow unrestricted access to the database for authorized users
- C) Use weak encryption to ensure fast data access
- D) Store sensitive data in plain text for easy retrieval

121. What is the primary function of a Network Access Control (NAC) system?

- A) To control which users can access specific applications
- B) To monitor and control network traffic for security breaches
- C) To enforce security policies on devices attempting to connect to a network
- D) To encrypt all data before transmission over the network

122. Which of the following encryption standards is most commonly used to protect data during transmission?

- A) AES
- B) RSA
- C) TLS/SSL
- D) DES

123. Which of the following is a characteristic of a privileged access management (PAM) solution?

- A) It assigns permissions based on user roles.
- B) It tracks and audits actions taken by users with elevated privileges.
- C) It stores encryption keys securely.
- D) It encrypts all data in motion.

124. What is the purpose of data redundancy in information security?

- A) To minimize network traffic
- B) To ensure data availability in the event of a system failure
- C) To prevent unauthorized access to data
- D) To optimize storage space

125. Which of the following technologies can be used to monitor network traffic for suspicious activities?

- A) Network Intrusion Detection System (NIDS)
- B) Digital Signature Algorithm (DSA)
- C) Data Loss Prevention (DLP)
- D) Virtual Private Network (VPN)

126. What is a rootkit designed to do?

- A) Encrypt data in transit
- B) Allow unauthorized access to a system without detection
- C) Perform regular security audits

- D) Monitor network traffic for malware

127. When an organization uses public cloud services, which of the following is most likely NOT the provider's responsibility under the shared responsibility model?

- A) Patching the operating system
- B) Ensuring physical security of data centers
- C) Managing network security controls
- D) Encrypting data before it is stored in the cloud

128. What is the primary goal of firewall segmentation?

- A) To prevent unauthorized access to internal networks
- B) To block all inbound traffic from the internet
- C) To separate sensitive data from non-sensitive data within the same network
- D) To ensure that users can access resources from any device

129. What is the most common method to detect whether data has been altered in transit?

- A) Using hash functions
- B) Encrypting data with RSA
- C) Implementing digital signatures
- D) Using a key exchange protocol

130. Which of the following is NOT a method of securing physical access to critical systems?

- A) Biometric authentication
- B) Firewalls
- C) Locked server cabinets
- D) Security guards

131. Which of the following is a key characteristic of blockchain technology?

- A) It uses a centralized server to validate transactions
- B) It provides anonymity to users by hiding their identities
- C) It maintains a decentralized and immutable ledger of transactions
- D) It encrypts data at rest using symmetric encryption

132. What is the primary function of an Intrusion Prevention System (IPS)?

- A) To detect unauthorized access attempts
- B) To block potential threats in real-time
- C) To monitor network traffic for signs of attacks
- D) To encrypt data during transmission

133. What does data tokenization do?

- A) Encrypted sensitive data before storing it
- B) Replaces sensitive data with non-sensitive placeholders
- C) Manages keys used for encrypting data
- D) Backups data at regular intervals

134. Which of the following cloud models allows for a combination of both private and public clouds?

- A) Public cloud
- B) Private cloud
- C) Hybrid cloud
- D) Community cloud

135. Which of the following is a feature of Endpoint Detection and Response (EDR) systems?

- A) They use artificial intelligence to automatically respond to security incidents
- B) They monitor and respond to suspicious activity on endpoints
- C) They require no configuration after installation
- D) They manage user access to network resources

136. What does the term data integrity refer to?

- A) The process of ensuring data is only accessible by authorized users
- B) The process of preventing unauthorized data from entering the system
- C) The process of ensuring data remains accurate and unaltered during storage and transmission
- D) The encryption of data to protect its confidentiality

137. Which of the following is a common type of social engineering attack?

- A) Phishing
- B) SQL injection
- C) Brute-force attack
- D) Denial-of-Service (DoS)

138. Which security control can be used to protect data on mobile devices?

- A) Mobile Device Management (MDM)
- B) Web Application Firewall (WAF)
- C) Intrusion Detection System (IDS)
- D) Security Information and Event Management (SIEM)

139. What is the purpose of Zero Trust Architecture (ZTA)?

- A) To verify user identity only once per session
- B) To establish access based on the trustworthiness of the device
- C) To never trust any entity, whether inside or outside the network, without verifying it first
- D) To create a secure perimeter to defend against outside attacks

140. Which of the following is a characteristic of a privileged user account?

- A) The account has minimal access to system resources
- B) The account can perform administrative actions on systems
- C) The account is used solely for user authentication
- D) The account is automatically disabled after 30 days of inactivity

141. What type of attack involves overwhelming a target with a large volume of traffic in order to prevent legitimate access?

- A) Man-in-the-middle (MITM)
- B) Distributed Denial of Service (DDoS)
- C) SQL injection
- D) Phishing

142. What is a common method to secure mobile devices from unauthorized access?

- A) Disabling GPS functionality
- B) Implementing full disk encryption
- C) Allowing open access to installed apps
- D) Disabling Wi-Fi capabilities

143. Which authentication method is commonly used for secure communications over the internet?

- A) Username and password
- B) Digital certificates
- C) Biometrics
- D) PIN codes

144. Which of the following security risks is addressed by Multi-Factor Authentication (MFA)?

- A) Network congestion
- B) Unauthorized access from a compromised password
- C) Data leakage from unencrypted files
- D) Overuse of administrative privileges

145. Which type of malicious software is designed to perform actions on a target system without being detected?

- A) Rootkits
- B) Ransomware
- C) Trojans
- D) Worms

146. In the context of data privacy regulations, which of the following would require an organization to maintain the confidentiality of personal data?

- A) PCI DSS
- B) GDPR
- C) HIPAA
- D) All of the above

147. Which of the following is the most secure method for authenticating remote users accessing internal resources?

- A) Username and password authentication
- B) Using Multi-Factor Authentication (MFA)
- C) Using Single Sign-On (SSO)

- D) Encrypting the user's network connection

148. Which of the following controls is best suited for detecting malicious activity on a system?

- A) Intrusion Detection System (IDS)
- B) Encryption
- C) Access Control List (ACL)
- D) Security patches

149. What does compliance auditing primarily focus on?

- A) Ensuring that the organization meets security policies and regulatory requirements
- B) Implementing security measures to mitigate threats
- C) Analyzing network traffic for anomalies
- D) Encrypting sensitive data to ensure confidentiality

150. What is a critical part of a comprehensive security strategy for mobile devices in a corporate environment?

- A) Enabling biometric authentication for all employees
- B) Ensuring that devices are equipped with firewalls
- C) Implementing Mobile Device Management (MDM) policies
- D) Allowing employees to install any apps on their devices