Short Questions

1. What is the primary goal of database security?
2. Define Access Matrix Model.
3. What are the key components of the Take-Grant Model?
4. Explain Acten Model.
5. What does PN Model stand for?
6. Describe Hartson and Hsiao's Model.
7. Explain Fernandez's Model.
8. What is the significance of Bussolati and Martella's Model for Distributed Databases?
9. Outline the principles of Bell and LaPadula's Model.
10. What does Biba's Model focus on?
11. Define Dion's Model.
12. Explain Sea View Model.
13. What are the key features of Jajodia and Sandhu's Model?
14. Describe the Lattice Model for Flow Control.
15. What is User Identification in security mechanisms?
16. Explain Authentication in the context of security mechanisms.
17. How does Memory Protection enhance security?
18. Define Resource Protection.
19. What are Control Flow Mechanisms in security?
20. How does Isolation contribute to security?
21. Name some Operating Systems with strong security functionalities.
22. What is the purpose of Trusted Computer System Evaluation Criteria?
23. Define vulnerability in the context of database security.
24. What is the role of encryption in database security?
25. Explain the concept of access control lists (ACLs).

26. What is role-based access control (RBAC)?
27. Define database auditing.
28. What are the common types of database attacks?
29. Explain SQL injection.
30. What is privilege escalation?
31. Define data masking.
32. How does data encryption differ from data hashing?
33. What is role separation in security?
34. Explain the principle of least privilege.
35. What is a security policy?
36. Define biometric authentication.
37. What is a firewall?
38. Explain the concept of multi-factor authentication.
39. What is a VPN (Virtual Private Network)?
40. Define social engineering in the context of security.
41. What is a honeypot?
42. Explain the difference between penetration testing and vulnerability scanning.
43. What is the role of intrusion detection systems (IDS) in security?
44. Define endpoint security.
45. What is data loss prevention (DLP)?
46. Explain the concept of zero trust security.
47. What is the importance of regular security updates?
48. Define a security breach.
49. What are the key features of a secure password?
50. Explain the principle of encryption at rest.
51. Define network segmentation.
52. What is the difference between symmetric and asymmetric encryption?

53. Explain the concept of a security token.
54. What is a brute force attack?
55. Define session hijacking.
56. What is a man-in-the-middle attack?
57. Explain the term "phishing."
58. What is a denial-of-service (DoS) attack?
59. Define intrusion prevention systems (IPS).
60. Explain the concept of sandboxing.
61. What is malware?
62. Define a security patch.
63. What is the purpose of access control?
64. Explain the concept of security architecture.
65. Define the principle of defense-in-depth.
66. What is a security perimeter?
67. Explain the concept of a security baseline.
68. Define network access control (NAC).
69. What is a security certificate?
70. Explain the concept of security by obscurity.
71. Define incident response.
72. What is a security incident?
73. Explain the concept of a security risk assessment.
74. Define threat modeling.
75. What is the purpose of a security awareness program?
76. Explain the concept of data classification.
77. Define secure coding practices.
78. What is the role of security policies and procedures?
79. Explain the principle of separation of duties.
80. Define intrusion detection.

81. What is a security token service (STS)?
82. Explain the concept of a security audit.
83. Define session management.
84. What is the purpose of a security log?
85. Explain the concept of a security perimeter.
86. Define data exfiltration.
87. What is a security control?
88. Explain the concept of security governance.
89. Define threat intelligence.
90. What is a risk assessment matrix?
91. Explain the concept of an incident response plan.
92. Define data retention policies.
93. What is the purpose of a security incident response team (SIRT)?
94. Explain the concept of a security vulnerability assessment.
95. Define the principle of secure by default.
96. What is a security certificate authority (CA)?
97. Explain the concept of security tokenization.
98. Define the principle of security through obscurity.
99. What is a security policy framework?
100. Explain the concept of a security perimeter.
101. Define the principle of secure coding.
102. What is a security posture?
103. Explain the concept of a security breach notification.
104. Define the principle of continuous monitoring.
105. What is a security risk assessment?
106. Explain the concept of a security control framework.
107. Define the principle of principle of least privilege.
108. What is a security baseline?

109. Explain the concept of a security incident response plan.

110. Define the principle of defense in depth.

111. What is a security architecture framework?

112. Explain the concept of a security audit.

113. Define the principle of separation of duties.

114. What is a security token service (STS)?

115. Explain the concept of a security governance model.

116. Define the principle of threat intelligence.

117. What is a risk assessment matrix?

118. Explain the concept of an incident response plan.

119. Define data retention policies.

120. What is the purpose of a security incident response team (SIRT)?

121. Explain the concept of a security vulnerability assessment.

122. Define the principle of secure by default.

123. What is a security certificate authority (CA)?

124. Explain the concept of security tokenization.

125. Define the principle of security through obscurity.