Fundamentals of Information Security [FIS]

Question Bank

Unit-1 and Unit-2

1. Difference between data and information.
2. Difference between Cybersecurity and Information Security.
3. What is the Need of Cybersecurity?
4. What do you mean by CIA Triad?
5. Explain Authentication and non-repudiation.
6. What do you mean by hackers and explain the types of hacking.
7. List and explain types of Hackers.
8. Discuss Phases of Ethical Hacking.
9. List and explain the Phases of Ethical Hacking.
10. List the information you get from Reconnaissance phase of hacking.
11. List and explain Scanning Types.
12. Explain Security Architecture.
13. What do you mean by Security Governance?
14. What is Security Auditing?
15. Explain the Regulations & Frameworks used for security auditing.
16. What is Ethical Hacking?
17. What is Penetration Testing?
18. Explain the types of Penetration Testing
19. Discuss the Ethics as it Relates to Cybersecurity.
20. Differentiate between ethics and laws.
21. Distinguish among types of ethical concerns.
22. Define cyberbullying.
23. Identify actions that constitute cyberbullying.
24. Identify possible warning signs of someone being cyberbullied.
25. Identify laws applicable to cybersecurity.
26. Explain CIA and how it a crucial component in securing the information systems.
27. Describe the warning signs of someone being cyberbullied. What should be the responsibilities of individual and organization?
28. Explain significance of Security Auditing in the context of cybersecurity. (7 Marks)
29. What is Cyber Bullying?Provide preventions. (7 Marks)

Unit-3

30. Differentiate between a cyber threat and a vulnerability. (5 Marks)
31. Describe types of cyber threats. (5 Marks)
32. Analyze types of Malwares. (5 Marks)
33. Describe the concept of malware and the techniques to guard against it. (5 Marks)
34. Identify the perpetrators of different types of malicious hacking. (5 Marks)
35. Discuss the characteristics of vulnerabilities in-depth. (8 Marks)
36. Evaluate the prevention strategies against cyber threats. (8 Marks)
37. Elaborate on the techniques and tools used for protection against cyber threats. (8 Marks)

Unit-4

38. Explain the concepts of authentication and authorization in the context of IdAM. (5 Marks)

39. Describe the principles that govern authentication and authorization in IdAM systems. (5 Marks)
40. Discuss the regulation of access and its importance in IdAM. (5 Marks)
41. Explore the responsibilities and processes involved in access administration within an IdAM framework. (5 Marks)
42. Explain the types of access control.
43. Define IdAM and its role in securing digital identities. (5 Marks)
44. Elaborate on the various methods used for password protection in IdAM systems. (8 Marks)
45. Discuss the risks and preventive measures related to identity theft in the context of IdAM. (8 Marks)
46. Evaluate the impact of access mismanagement on organizational security and propose solutions. (8 Marks)

Unit-5

47. Explain the significance of cyber security in the context of E-Commerce and digital payments.
48. Describe the security considerations for social media platforms in the digital landscape.
49. Analyze the cyber security challenges associated with digital devices in E-Commerce transactions.
50. Discuss the role of various tools and technologies in ensuring cyber security for E-Commerce.
51. Outline the key components of a cyber security plan and crisis management for E-Commerce businesses.
52. Conduct a risk-based assessment of potential threats to E-Commerce platforms and propose mitigation strategies.
53. Explain the importance of audit and compliance in ensuring the security of digital payment systems.
54. Elaborate on cyber security best practices, outlining key do's and don'ts for E-Commerce organizations.
55. Define Social media security and What are the Benefits of social media security for individuals.?