Dezyne École College

Bachelor of Computer Application (B.C.A.) Second Year-6th Semester

Cyber Security

Part A: Short Answer Questions

(10 Questions × 2 Marks = 20 Marks)
(Answer in about 50 words)

1. Define cyber security.
2. What is the CIA Triad?
3. Mention two types of cyber attackers.
4. What is a vulnerability?
5. Define risk management in cyber security.
6. What is penetration testing?
7. What does EDR stand for?
8. Define mobile security.
9. What is cryptography used for?
10. Mention two security models.
11. What is user behavior analytics (UBA)?
12. Define endpoint detection and response.
13. What is phishing?
14. Mention any two cyber security tools.
15. What is firewall?
16. Define social engineering.
17. What is spoofing?
18. What is a botnet?
19. Mention two physical security controls.
20. What is threat intelligence?

Part B: Descriptive/Long Answer Questions

(Attempt any 5 out of 10 × 10 Marks = 50 Marks)
(Answer in about 400 words)

Unit I – Introduction and Models

21. Explain the CIA Triad and its relevance in cyber security.

22. Discuss the taxonomy of various attacks and the types of attackers.
23. What is cyber security governance? Explain challenges and constraints.
24. Explain different layers of security in cyber systems.
25. Describe cryptography and how it supports data security.

Unit II – Security Technologies and Threat Management

26. Explain Mobile Security and Advanced Data Security with examples.
27. Discuss cloud security and endpoint detection mechanisms.
28. What is penetration testing? Explain methods and importance.
29. Describe vulnerabilities in complex network architectures.
30. Explain firewalls, intrusion detection systems, and anti-malware tools.
31. What are zero-day vulnerabilities? Explain with examples.
32. Discuss any three common cyber-attacks and how to prevent them.

Unit III – Security Policies and Risk Controls

33. Explain operating system security hardening techniques.
34. Discuss security policy creation and role-based access controls.
35. Explain local protection tools and local intrusion detection tools.
36. How does one configure a secure browser and manage software updates?
37. Describe the importance of threat management and backup policies.

Unit IV – Tools and Lifecycle

38. Write a note on any four of the following tools: Nmap, Hydra, John the Ripper, Aircrack-ng, Wireshark.
39. What is the Cyber Kill Chain? Explain the seven stages.
40. Discuss the cyber-attack strategies used by red teams.
41. Explain the process of weaponization, exploitation, and exfiltration.
42. What is threat life cycle management? Describe each stage.
43. Define reconnaissance and how attackers use it in cybercrime.
44. Explain the purpose and use of user behavior analytics (UBA).
45. What is data loss prevention (DLP)? Discuss tools and policies.

Additional Application-Based Questions

46. Compare authentication and authorization with examples.
47. Describe ethical hacking and how it helps in cyber defense.
48. What is digital forensics and its role in cyber security?
49. Discuss the impact of social media on cyber security risks.
50. Explain the concept of security awareness training for employees.
51. Discuss malware types: Trojan horse, worms, ransomware, and adware.
52. Explain the significance of multi-factor authentication.
53. Discuss cybersecurity challenges in cloud computing.
54. Describe recent trends in cyber security threats in India.

55. Explain biometrics in access control systems.
56. Describe network segmentation and its role in limiting breaches.
57. How can organizations defend against DDoS attacks?
58. What are honeypots and how are they used in cyber defense?
59. Explain browser security threats and mitigation techniques.
60. Discuss future trends and emerging technologies in cyber security.