Reg. No. : | | | | | | | | | | | | |

Question Paper Code : 80848

B.E./B.Tech. DEGREE EXAMINATIONS, APRIL/MAY 2024.

Sixth/Seventh/Eighth Semester

Information Technology

IT 8073 — INFORMATION SECURITY

(Common to Computer Science and Engineering/Computer and Communication Engineering/Computer Science and Business Systems)

(Regulations 2017)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Define Security. What are the multiple layers of Security?

2. Why is a methodology crucial to putting information security into practice?

3. Show with the help of points the four important functions for an organization based on the information security.

4. Express the logic behind using a license agreement window and the use of online registration process to combat piracy.

5. Give the meaning of dumpster diving' with respect to information security.

6. What is the asset Valuation? List any two components of asset valuation.

7. Write the drawbacks of ISO 17799/BS 7799.

8. Examine using the diagram for spheres of security.

9. Differentiate signature-based IDPS and behavior-based IDPS (Intrusion Detection and Prevention System).

10. Compare Cryptography and Steganography.

PART B — (5 × 13 = 65 marks)

11. (a) Describe the components of System Development Life Cycle with neat sketch.

Or

(b) Give a succinct explanation of the security of each component of an information security system.

12. (a) Illustrate the methods does a social engineering hacker use to gain information about a users login id and password? How would this method differ if it were targeted towards an administrators assistant versus a data-entry clerk?

Or

(b) (i) Explain the confidentiality policies. (6)

(ii) Discuss in detail about the types of security policies. (7)

13. (a) Design and develop Risk Assessment using sample TVA (Threat Vulnerability Asset) spreadsheet.

Or

(b) (i) Explain in detail Cost Benefit Analysis and Exposure Factor. (8)

(ii) Analyze which is more important to the systems components classification scheme. (5)

14. (a) Design Security Architecture and explain the goals used for achieving it.

Or

(b) Describe contingency planning? How is it different from routine management planning? What are the components of contingency planning?

15. (a) Describe the various types of Intrusion Detection System (IDS), including the benefits and drawbacks of each.

Or

(b) (i) Evaluate Honeypots, Honeynets and Padded cells. (7)

(ii) Assess the dictionary attack, Timing attacks and Defending against attacks. (6)

PART C — (1 × 15 = 15 marks)

16. (a) How has the perception of the hacker changed over recent years? Compose the profile of a hacker today.

Or

(b) Explain how do screened host architectures for firewalls differ from screened subnet firewall architectures? Which of these offers more security for the information assets that remain on the entrusted network?

———————