



# MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

(A constituent unit of MAHE, Manipal)

## II SEMESTER M.TECH. (CSIS) END SEMESTER EXAMINATIONS – MAY/JUNE 2023

### SUBJECT: SYSTEM AND NETWORK SECURITY [CSE 5013]

Date of Exam: (29-05-2023)

Time of Exam: 9.30 AM – 12.30 PM

MAX.MARKS: 50

#### INSTRUCTIONS TO CANDIDATES:-

- Answer **ALL** the questions.
- Missing data may be suitable assumed.

- |     |   |    |
|-----|---|----|
| 1A. | Classify different DOS boot record infection techniques.  | 4M |
| 1B. | Explain the infection strategies of Memory-Resident viruses.  | 2M |
| 1C. | Illustrate the Master Boot Record, boot strap loader, Partition table and its entries.  | 4M |
| 2A. | Categorise different Application-Layer attacks. Justify how an attacker may exploit the vulnerabilities, through content attacks with suitable examples.                                      | 4M |
| 2B. | Explain how security controls can be grouped into several threat vector categories.   | 2M |
| 2C. | Write the formal definition of risk. Distinguish quantitative and qualitative approach to risk analysis.  | 4M |
| 3A. | Illustrate the role of traffic normalizer, system service scanner, detection engine and traffic shaper in Network Based Intrusion Prevention Systems (NIPS).                                  | 4M |
| 3B. | Demonstrate Network Based Intrusion detection system (NIDS) with a relevant architectural diagram.  | 4M |
| 3C. | List out the benefits of Host Based Intrusion Prevention Systems and explain the same.  | 2M |
| 4A. | Differentiate between Discretionary and Mandatory Access Control in Operating System Security.  | 4M |
| 4B. | Explain different Firewall services. What are the limitations of firewall in computer networks?   | 2M |
| 4C. | Design a three-pronged firewall and illustrate the purpose of Demilitarized Zone (DMZ) in firewalls. Analyze the advantages and disadvantages of DMZ's in an organization's computer network. | 4M |
| 5A. | Distinguish between Authentication Header (AH) and Encapsulating Security Payload (ESP) protocols of IPsec with relevant diagrams.  | 2M |
| 5B. | Illustrate with a neat diagram, how user Anand after logging in a Kerberos V4 network (i) gets a ticket to Babu (ii) how Anand logs from his workstation into Babu's workstation?             | 4M |
| 5C. | Compare and contrast the two types of Phase-1 IKE exchanges with relevant diagrams.   | 4M |