A-0857

Total Pages : 4 **Roll No. -------------**

MIT (CS)-102/CEGCS-02

Cyber Security Techniques

(MCA/MSCCS/CEGCS)

3rd/ 1st Semester Examination 2024(Dec.)

Time: 2:00 hrs Max. Marks: 70

Note : This paper is of Seventy (70) marks divided into Two (02) Section A and B. Attempt the questions contained in these sections according to the detailed instructions given therein. Candidates should limit their answers to the questions on the given answer sheet. No additional (B) answer sheet will be issued.

P.T.O.

Section-A (Long-Answer-Type Questions)

Note : Section 'A' contains Five (05) long-answer-type questions of Nineteen (19) marks each. Learners are required to answer any Two (02) questions only.

[2x19=38]

Q.1. What are security policies and why are they important for ensuring the protection of organizational data and information systems? Discuss the components of a typical information security policy and the role of leadership in policy development and enforcement.

Q.2. Explain the different types of cyber attacks focusing on malware-based attacks like viruses, worms, ransomware and Trojans. Discuss how each type of attack works, the damage it can cause, and the best practices for mitigating such threats.

Q.3. What is the role of authentication and authorization mechanisms in securing e-commerce platforms? Discuss the different methods of authentication (e.g., multi-factor authentication, single sign-on) and how these mechanisms can be used to protect user accounts and prevent unauthorized access.

Q.4. What is Cyber security risk management, and why is it essential for organizations to integrate it into their overall security strategy? Discuss the core components of risk management, including risk identification, risk assessment, risk mitigation, and risk monitoring, and how they contribute to protecting organizational assets.

Q.5. What is computer forensics, and how does it differ from traditional forensic methods? Discuss the role of computer forensics in the investigation of cybercrimes, and explain the importance of ensuring the integrity of digital evidence during the forensic process.

Section-B (Short-Answer-Type Questions)

Note : Section 'B' contains Eight (08) short-answer-type questions of Eight (08) marks each. Learners are required to answer any Four (04) questions only.

[4x8=32]

Q.1. What is Pretty Good Privacy (PGP) and how does it provide security for email communications and file storage?

P.T.O.

Q.2. Explain the different types of phishing attack, including spear phishing, vishing and smishing.

Q.3. Explain the differences between hardware and software firewalls and discuss their respective advantages and limitations in network security.

Q.4. What is the Cyber security Capability Maturity Model (C2M2) and how does it help organizations assess and improve their cyber security posture?

Q.5. What is the Hypertext Transfer Protocol (HTTP) and how does it function in client-server communication?

Q.6. What is social engineering by email and how does it differ from traditional forms of social engineering?

Q.7. What are the key government initiatives in India aimed at improving the nation's cyber security posture?

Q.8. Write short notes on:

a. Denial of Service attack

b. Wireless Security

c. Trojan horse

d. URL

****