Name:

Enrolment No:

UPES

End Semester Examination, May 2024

Course: IT Security **Semester: II**
Program: MCA **Time : 03 hrs.**
Course Code: CSCS7007P **Max. Marks: 100**

SECTION A

S. No.		Marks	CO
Q 1	Explain with an example how a breach in data security can adversely affect an organization's operations and reputation.	**4**	**CO1**
Q 2	Discuss the concept of phishing as a network-based threat.	**4**	**CO2**
Q 3	What is a relational database and what are its principal ingredients?	**4**	**CO 3**
Q 4	Discuss the importance of vulnerability assessment in maintaining effective physical security.	**4**	**CO 4**
Q 5	Explain the difference between a security audit message and a security alarm.	**4**	**CO5**
	SECTION B		
Q 6	Explore the difference between security and privacy in the context of information management. Provide examples to illustrate these differences and explain why both aspects are essential for ensuring comprehensive data protection.	**10**	**CO1**
Q 7	Examine the security challenges posed by wireless networks, particularly focusing on Rogue Access Points and Denial-of-Service (DoS) attacks.	**10**	**CO2**
Q 8	Describe the various approaches to physical security and evaluate their effectiveness in safeguarding assets and facilities. Compare the advantages and disadvantages of perimeter security, security lighting, and access control systems.	**10**	**CO4**
Q 9	Explain in detail the various aspects of SQL injection attacks, including avenues of SQL injection, and strategies for countermeasures. OR Discuss the essential tools utilized in network security, cryptography, and system security, highlighting their roles in mitigating cyber threats and vulnerabilities.	**10**	**CO3**

SECTION-C			
Q 10	What are the key steps involved in the system security planning process, and how does operating system hardening contribute to enhancing overall system security?	**20**	**CO3**
Q 11	Analyze the challenges associated with log management, notification, reporting, monitoring, and control in the context of IT audits and compliance. OR Differentiate between physical security, network security, operating system security, and application security, explain their distinct roles, principles, and methodologies in safeguarding information assets. Compare and contrast the objectives, challenges, and best practices associated with each domain of security.	**20**	**CO5**