B. TECH. (MINOR) CBCS-2023

B. TECH. (MINOR) Semester-I (Sem-III Level) Cyber Security : WINTER: 2025

SUBJECT: INFORMATION SECURITY

Day : Tuesday | Time : 10:00 AM-01:00 PM

Date : 23/12/2025 | W-29441-2025 | Max. Marks : 60

NB :
1. Assume suitable data, if necessary.
2. Draw neat labelled diagrams WHEREVER necessary.
3. Figures to the right indicate FULL marks for the question.
4. All Questions carry EQUAL marks.
5. All questions are COMPULSORY.

Q. 1	Illustrate the stages of the security life cycle and discuss their role in ensuring ongoing information security management.	(10)
	OR	
Q. 1	Assess the security of a cryptosystem based on different encryption schemes and recommends strategies to mitigate known cryptographic vulnerabilities.	(10)
Q. 2	Distinguish between intruders, hackers, and insiders in the context of security threats and assess their relative impact on information security.	(10)
	OR	
Q. 2	Identify sources of vulnerability in information security, analyze their potential impact, and compare different tools used for vulnerability assessment.	(10)
Q. 3	Differentiate between Discretionary access control, Mandatory access control, Role-based access control models in terms of flexibility, scalability, strengths, weaknesses and security.	(10)
	OR	
Q. 3	Summarize the different types of authentication techniques and explain how multi-factor authentication enhances security.	(10)
Q. 4	Evaluate the role of security auditing and monitoring in detecting policy violations and continuous improvement in security measures.	(10)
	OR	
Q. 4	Discuss the importance of Security Requirements Specifications and their impact on developing effective information security strategies.	(10)
Q. 5	Define the fundamental principles of network security and explain the role of firewalls, VPNs, and intrusion detection systems in protecting network infrastructure.	(10)
	OR	
Q. 5	Analyze the significance of enterprise security in protecting assets, and evaluate the key components of an enterprise security framework.	(10)
Q. 6	Design a case study inspired by the 9/11 incident to demonstrate the integration of continuity planning, disaster recovery, and security audits.	(10)
	OR	
Q. 6	Explain the primary functions of NESSUS and NMAP, and analyze their role in improving information security assessments (auditing).	(10)

* * * * * *