Register No : _____

THE KAVERY ENGINEERING COLLEGE

(An Autonomous Institution)

UG/PG DEGREE END SEMESTER THEORY EXAMINATIONS, APRIL-MAY 2026

Second Semester

Master of Computer Applications

PMCT2425 -CYBER SECURITY

Regulations - 2024

Duration: 3 Hrs. ***Maximum: 100 Marks***

PART – A (ANSWER ALL QUESTIONS) (Marks 10*2=20)

Q.No	Questions	BLT	CO	Marks
1.	What is the definition of cyber security policy?	L1	1	2
2.	Define threat identification?	L1	1	2
3.	Why does mobile need security?	L2	2	2
4.	How to identify office equipment?	L2	2	2
5.	List any two authentication mechanisms commonly used to secure system access	L2	3	2
6.	Define firewall in networking.	L1	3	2
7.	How is cryptography used in email security?	L1	4	2
8.	Compare intrusion detection and vulnerability management	L4	4	2
9.	How can security performance be measured?	L4	5	2
10.	Define security audit?	L1	5	2

PART – B (ANSWER ALL QUESTIONS) (Marks 5*16 = 80)

Q.No			Questions	BLT	CO	Marks
11.	a	i	Discuss about types of security models in cyber security?	L1	1	10
		ii	What are the 5 best methods used for cyber security?	L1	1	6
			Or			
	b	i	Recall the primary function of a cyber security management process?	L1	1	8
		ii	What are the various risk assessment approaches used in cyber security	L1	1	8
12.	a	i	Explain the importance of Human Resource Security in cyber security	L2	2	8
		ii	Outline the process of information classification and the secure handling of classified data within an organization	L2	2	8
			Or			
	b	i	Explain how security can be effectively incorporated into each phase of	L2	2	10

			the Software Development Life Cycle (SDLC).			
		ii	Discuss the significance of disaster management and incident response planning in ensuring business continuity during cyber threats.	L2	2	6
13.	a	i	Describe the role of Business Application Management in maintaining a secure cyber environment.	L3	3	10
		ii	Evaluate the significance of corporate business application security and the methods used to safeguard them from cyber threats.	L3	3	6
			Or			
	b	i	Summarize the core concepts of network management and how tools like firewalls and IP Security contribute to securing network infrastructure.	L3	3	10
		ii	Identify the effectiveness of the OWASP ZAP tool in detecting and reporting web application vulnerabilities.	L3	3	6
14.	a	i	Discuss the impact of cyber security threats on Supply Chain Management and the measures organizations can implement to mitigate associated risks.	L2	4	10
		ii	Explain the importance of Security Architecture in cyber security and how it contributes to building a secure IT infrastructure.	L2	4	6
			Or			
	b	i	Discuss various cryptographic techniques and their roles in cyber systems.	L2	4	8
		ii	Explain the process of conducting forensic investigations in cyber security and the importance of preserving digital evidence.	L2	4	8
15.	a	i	Examine the importance of Security Monitoring and the continuous improvement process in enhancing an organization's cyber security posture.	L4	5	10
		ii	Explain the role of Information Security Compliance Monitoring in ensuring that security policies and legal requirements are effectively met.	L4	5	6
			Or			
	b	i	Inspect how Security Monitoring helps in identifying threats, managing incidents, and maintaining overall network integrity.	L4	5	10
		ii	Explain the purpose of Information Risk Reporting and its impact on organizational decision-making and risk management strategies.	L4	5	6

******