23MCPE672

MANGALORE INSTITUTE OF TECHNOLOGY & ENGINEERING

(A Unit of Rajalaxmi Education Trust®, Mangalore)
Autonomous Institute affiliated to VTU, Belagavi, Approved by AICTE, New Delhi
Accredited by NAAC with A+ Grade & ISO 9001:2015 Certified Institution

Model Question Paper

Fourth Semester MCA Degree Examination

Cyber Intelligence

Time: 3 Hours **Max. Marks: 100**

Note: 1. Answer any FIVE full questions, choosing ONE full question from each module.
2. M: Marks, L: RBT (Revised Bloom's Taxonomy) level, C: Course outcomes.

		Module -1	M	L	C
Q1	a.	An e-commerce startup rapidly expanding its operations is concerned about the increase in cyber threats. As the new cybersecurity analyst, apply the concepts of HUMINT and OSINT to assess external risks to the organization. Develop an intelligence report draft using maneuver warfare mentality to defend key digital assets.	10	L3	CO1
	b.	A government intelligence agency suspects a group is coordinating cyber espionage. Using your knowledge of COMINT and SIGINT, design an interception strategy that respects legal boundaries while maximizing intelligence collection.	10	L3	CO1
		OR			
Q2	a.	A security agency receives a tip about an upcoming cyberattack on government infrastructure. Apply OSINT and HUMINT strategies to gather pre-attack indicators and create a preliminary threat profile.	10	L3	CO1
	b.	Your company's cyber unit is planning operations in a hostile environment. Apply the concepts of **maneuver warfare** and **intelligence-driven operations** to propose a cyber defense strategy that increases adversary uncertainty and preempts likely attack vectors.	10	L3	CO1
		Module- 2			
Q3	a.	Your team is building a threat intelligence platform. Apply the Intelligence Cycle to a suspected insider threat scenario in a data center where log files suggest anomalous access patterns.	10	L3	CO2
	b.	After a critical vulnerability was disclosed, your manager asks you to disseminate an intelligence alert to multiple departments. Apply the intelligence cycle to convert raw vulnerability data into an actionable intelligence.	10	L3	CO2
		OR			
Q4	a.	A large multinational firm suspects one of its employees is leaking information. Make use of Planning, Collection, and Analysis steps of the Intelligence Cycle to detect insider threats.	10	L3	CO2
	b.	You are part of a CERT team responding to an ongoing phishing campaign. Apply the **Dissemination** and **Utilization** stages of the Intelligence Cycle to show how analyzed threat intelligence can be shared and acted upon across multiple departments to prevent further exploitation.	10	L3	CO2
		Module - 3			
Q5	a.	A telecom company is planning to implement a Cyber Intelligence Program. As a consultant, apply your knowledge of Operational Security (OPSEC) and cyber threat management to design the roles, responsibilities, and operational flow for the program.	10	L3	CO3

	b.	A business's sensitive financial data is exposed due to poor operational security practices. Analyze this failure and apply the OPSEC framework to recommend measures preventing such incidents in the future.	10	L3	CO3
OR					
Q6	a.	Your client organization lacks clarity on how to initiate a Cyber Intelligence Program. Use OPSEC and security operations integration to formulate a step-by-step guide to launch the program effectively.	10	L3	CO3
	b.	After an internal audit, it was found that OPSEC controls were inconsistently applied across branches. Build a plan using OPSEC elements to improve compliance and risk mitigation organization-wide.	10	L3	CO3
Module - 4					
Q7	a.	Your team identifies an intrusion attempt targeting your company's R&D division. Use the F3EAD process to formulate a complete response plan for this scenario.	10	L3	CO4
	b.	You are advising a start-up on enhancing its cybersecurity posture through **Active Defense**. Apply the concepts of **entrapment** and **deception technologies** to design an ethical integration plan within their security systems.	10	L3	CO4
OR					
Q8	a.	An attacker has breached your perimeter defenses. Apply the F3EAD and Kill Chain methodologies to identify the attack phase and formulate a containment and remediation strategy.	10	L3	CO4
	b.	Propose a deception-based Active Defense system tailored for a cloud service provider. Identify the ethical and technical safeguards necessary for implementation.	10	L3	CO4
Module - 5					
Q9	a.	During a collaborative investigation, three different companies share threat indicators. As an analyst, design a framework to ensure strategic, tactical, and operational level collaboration between teams.	10	L3	CO5
	b.	A mid-sized IT firm with a low Capability Maturity Model (CMM) score wants to build a threat intelligence program. Apply CMM concepts to guide their roadmap for maturity improvement.	10	L3	CO5
OR					
Q10	a.	A government and private cybersecurity coalition is set to handle a national threat. Apply your knowledge of cyber operations to **utilize** tactical-level and operational-level collaboration for coordinating shared resources, intelligence, and actions to achieve timely threat neutralization. Provide specific examples in your response.	10	L3	CO5
	b.	A threat intel maturity audit reveals a firm is stuck at CMM Level 1. Identify concrete steps and examples that can be applied to advance to Level 3 in terms of policy, tools, and team structuring.	10	L3	CO5

-*****-