U.S.N.										

B.M.S. College of Engineering, Bengaluru-560019

Autonomous Institute Affiliated to VTU

June 2025 Semester End Main Examinations

Programme: B.E. **Semester: VII**

Branch: Artificial Intelligence and Machine Learning **Duration: 3 hrs.**

Course Code: 24AM7PEACY **Max Marks: 100**

Course: AI for Cyber Security

Instructions: 1. Answer any FIVE full questions, choosing one full question from each unit.
2. Missing data, if any, may be suitably assumed.

Important Note: Completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages. Revealing of identification, appeal to evaluator will be treated as malpractice.

		UNIT - I	*CO*	*PO*	Marks
1	a)	AI can be effectively leveraged to enhance cybersecurity practices. Justify the statement.	*CO1*	*PO2*	**06**
	b)	Analyse the evolution of AI in order to fully evaluate the potential benefits of applying it in the field of cybersecurity.	*CO1*	*PO2*	**08**
	c)	Describe the challenges of AI in Cybersecurity.	*CO1*	*PO1*	**06**
		OR			
2	a)	Attackers can use AI to evade detection by generating data that can fool AI-based systems. Justify the statement with an example.	*CO1*	*PO2*	**08**
	b)	Identify the limitations of expert based systems in identifying threats.	*CO1*	*PO2*	**06**
	c)	Write a note on the following with suitable examples: i) Malware ii) Phishing	*CO1*	*PO1*	**06**
		UNIT - II			
3	a)	Identify the pros and cons of using Logistic Regression in phishing attack detection.	*CO1*	*PO1*	**06**
	b)	Consider a social media platform where users frequently post images, some of which are spam—such as images with promotional content or phishing attempts. Traditional text-based spam detection fails here because spammers are embedding their messages as text within images to evade detection. Provide an AI technique that can be used to detect spam in the given scenario and elaborate the process.	*CO2*	*PO2*	**08**
	c)	Consider the subject line for the emails: **Email 1:** "Win a million dollars now! Click here to claim your prize." **Email 2:** "Meeting at 3 PM. Don't forget to bring the documents." Classify the above emails as spam or non-spam using perceptron.	*CO2*	*PO2*	**06**

			OR			
	4	a)	Identify the pros and cons of using Perceptron for spam filtering.	*CO1*	*PO1*	**06**
		b)	A financial institution is concerned about phishing websites imitating its online banking portal. Cybercriminals often create fake websites to trick users into entering sensitive information, like usernames, passwords and credit card numbers. Apply decision tree model to detect phishing for the given scenario.	*CO2*	*PO2*	**08**
		c)	A company runs an email service and notices a surge in **spam messages** disguised within images. Instead of text-based emails, spammers are embedding promotional text and malicious links into images. These image-based spam messages bypass conventional text filters and affect user experience. Provide a solution to this problem using suitable machine learning model.	*CO2*	*PO2*	**06**
			UNIT - III			
	5	a)	A suspicious email with an attachment has been reported by several employees in a corporate company. The email contains a document that, when opened, triggers unexpected network activity, and the affected systems begin exhibiting abnormal behavior. The company suspects that the attachment contains malware, but it's unclear what type of malware it is. i) Use dynamic malware analysis method to identify malware operation pattern. ii) Describe its potential impact on the organization and the process to mitigate the threat.	*CO2*	*PO2*	**08**
		b)	Compare between static and dynamic malware analysis.	*CO2*	*PO2*	**06**
		c)	Write a note on the following using examples with respect to malware analysis: i) Disassemblers ii) System monitors	*CO3*	*PO1*	**06**
			OR			
	6	a)	Elucidate the tools and techniques used in dynamic malware analysis with suitable examples.	*CO2*	*PO2*	**08**
		b)	Identify the drawbacks of static malware analysis.	*CO2*	*PO2*	**06**
		c)	Describe the anti-analysis tricks that can be employed by the malware attacker to prevent malware analysis.	*CO3*	*PO1*	**06**
			UNIT - IV			
	7	a)	A financial organization recently started noticing a spike in failed login attempts across its internal systems, specifically during non-working hours. After further investigation, it appears that automated bots or attackers may be trying to use fake login credentials in an attempt to gain unauthorized access to sensitive systems. The company uses a multi-factor authentication system, but the login attempts are still causing concern due to the large number of invalid login attempts, which may be an early sign of a brute-force or credential stuffing attack. The attackers appear to	*CO3*	*PO2*	**08**

			be employing tactics like attempting common passwords across multiple accounts or phishing to generate fake logins. Analyze the scenario and provide a solution to carry out fake login management.			
		b)	Are passwords obsolete? Justify the answer.	*CO3*	*PO2*	**06**
		c)	Describe anomalies related to the management of user accounts.	*CO3*	*PO1*	**06**
			OR			
	8	a)	A security analyst for a financial institution uses a Host-Based Intrusion Detection System (HIDS) to monitor critical servers. During routine analysis, the HIDS generates the following alerts: Unauthorized File Access, Privilege Escalation Attempt, Unusual System Changes, Configuration File Modification. i) Provide the steps to investigate these alerts further. ii) Determine if these events represent an active intrusion. Identify the actions that can be implemented to mitigate the risks and secure the affected host.	*CO3*	*PO2*	**08**
		b)	Identify the drawbacks of reactive strategy in fake login management.	*CO3*	*PO2*	**06**
		c)	Distinguish between host-based Intrusion Detection System and Network based Intrusion Detection System.	*CO3*	*PO1*	**06**
			UNIT - V			
	9	a)	Design a Fraud Detection and Prevention System for an e-commerce platform that combines rule-based and data-driven approaches, ensuring scalability, low false positives, and adaptability to emerging fraud tactics.	*CO3*	*PO3*	**08**
		b)	Elucidate how Machine Learning can be used in the field of fraud detection.	*CO3*	*PO1*	**06**
		c)	Identify the advantages and disadvantages of rule based predictive model for fraud detection.	*CO2*	*PO2*	**06**
			OR			
	10	a)	Design an expert-driven predictive model for credit card fraud detection using sample scoring and blocking rules.	*CO3*	*PO3*	**08**
		b)	A customer reports unauthorized transactions on their credit card. Upon investigation, it is discovered that the card details were compromised due to a phishing attack. The attacker used the stolen information to make multiple online purchases from various merchants. The bank's fraud detection system initially flagged the transactions as suspicious due to the sudden change in purchasing patterns, including large amounts spent on electronics and international purchases, which were inconsistent with the cardholder's typical behavior. However, because the cardholder did not immediately report the phishing attempt, some transactions were processed before the card was blocked. Analyze the scenario to identify the problem in the given scenario and provide a solution.	*CO3*	*PO1*	**06**
		c)	Identify the possible credit card fraud scenarios where credit card information can be compromised.	*CO2*	*PO2*	**06**

****