U.S.N.										

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

Autonomous Institute Affiliated to VTU

January / February 2025 Semester End Main Examinations

Programme: B.E. **Semester: V**

Branch: CSE (IoT & Cybersecurity including Blockchain) **Duration: 3 hrs.**

Course Code: 23IC5PCCSY **Max Marks: 100**

Course: 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)	(i) “Hacking is a science”, Justify the statement and provide what hacking is. (ii) Mr. Ankit Fadia is a self-proclaimed first Indian hacker. He is good at extracting existing code and reusing it for hacking. Which category of hacker does Mr. Fadia belong to? (iii) Distinguish between Data diddling, Espionage, Sabotage and Email Spoofing.	CO2	PO3	**10**
	b)	Compare and contrast cyber warfare, cybercrime, cyber terrorism, and cyber espionage.	CO2	PO3	**05**
	c)	What role does regular vulnerability assessment play in implementing a cybersecurity policy?	CO2	PO1	**05**
		OR			
2	a)	“In late 2014, Sony Pictures Entertainment experienced a significant security breach. By manipulating the input fields of the web application, they could add their commands to the existing queries run by the application.” (i) What kind of attack was the above scenario? Discuss the vulnerabilities that have led to this attack. (ii) Analyze how can this be prevented?	CO2	PO1	**10**
	b)	Outline the key components of a comprehensive cybersecurity policy for an organization.	CO2	PO3	**05**
	c)	Define IP Spoofing? Illustrate with a neat sketch the working of IP Spoofing	CO2	PO3	**05**
		UNIT – II			
3	a)	Investigate the underlying mechanisms of push, pull, and crash attacks in the context of an organization that extensively relies on mobile devices for its daily operations.	CO3	PO3	**10**

		b)	List and explain the popular types of attacks against 3G mobile networks.	*CO1*	*PO1*	**10**
			OR			
	4	a)	(i) Illustrate with a neat diagram the working of RAS security for mobile phones (ii) What are the four common attacks which can take place using Bluetooth. (iii) What are the measures to be taken for security of mobile Devices.	*CO1*	*PO3*	**10**
		b)	Explain the types of credit card fraud. Also explain the techniques involved in credit card fraud.	*CO1*	*PO1*	**10**
			UNIT – III			
	5	a)	A student, Priya, received an email claiming to be from her university's IT department. The email informed her of a system update and asked her to confirm her login credentials to ensure uninterrupted access to university services. The email contained a link to a webpage resembling the university's login portal. Priya entered her credentials, and within hours, her university account was compromised. The attacker accessed sensitive information, including her student ID, course details, and saved payment information. What are the key indicators that the email Priya received was a phishing attempt and What immediate actions should Priya take after realizing her account was compromised. How could the university have prevented this phishing attack?	*CO2*	*PO3*	**10**
		b)	A corporate employee discovers a hardware keylogger attached to their workstation. Analyze the potential impact of the device and recommend steps to secure the system.	*CO1*	*PO3*	**10**
			OR			
	6	a)	An e-commerce company, ShopEase, has an online platform for users to register, log in, and make purchases. A security analyst discovers unusual behavior in the database, where sensitive customer data, such as email addresses and hashed passwords, is being accessed by unauthorized queries. The investigation reveals that the platform is vulnerable to SQL Injection due to improper sanitization of user inputs in the login form. Illustrate how the SQL query in the case study became vulnerable. List and explain the potential impacts of the SQL Injection attack on ShopEase. If the attacker exploits the vulnerability to download the entire database, what legal and ethical consequences might ShopEase face? How should the company respond post-attack to regain customer trust?	*CO2*	*PO3*	**10**

		b)	What is identity theft? Explain with its types with examples. How can information be classified?	*CO2*	*PO3*	**10**
			UNIT – IV			
	7	a)	List various Computer Forensics services available, explain any two of them.	*CO2*	*PO3*	**06**
		b)	With neat diagram explain process model for understanding a seizure and handling of forensics evidence legal framework.	*CO2*	*PO3*	**08**
		c)	Discuss the following phases of Forensics life cycle. (i) Storing and Transporting (ii) Examination/Investigation	*CO2*	*PO3*	**06**
			OR			
	8	a)	Explain the potential issues that can arise if an email message exceeds the character limit specified in RFC 2822.	*CO2*	*PO3*	**08**
		b)	Discuss the precautions to be taken when collecting electronic evidence.	*CO3*	*PO3*	**06**
		c)	How does adherence to RFC 2822 standards benefit email clients and servers in ensuring message compatibility?	*CO3*	*PO3*	**06**
			UNIT – V			
	9	a)	Illustrate the psychology, mindset, and skill sets of hackers and cybercriminals. Based on your findings, formulate a comprehensive framework for predicting and mitigating cybercriminal behavior. Your framework should address factors such as motivation, and technical proficiencies while proposing strategies for organizations to counteract these threats effectively.	*CO3*	*PO3*	**10**
		b)	TechCore Solutions, a mid-sized organization, is encountering significant challenges related to employees' web usage and online activities, leading to potential security vulnerabilities. Develop a detailed web threat management strategy for the organization, focusing on common issues such as unsafe browsing habits, unauthorized access, malware infections, and data leakage. Propose effective measures to enhance web security and ensure compliance with organizational policies.	*CO3*	*PO3*	**10**
			OR			
	10	a)	Compare and contrast the various types of intellectual property in cyberspace. Examine how these types of intellectual property are vulnerable to misuse or infringement in the digital environment.	*CO2*	*PO2*	**10**
		b)	Analyze the relationship between Incident Response, Incident Handling, and Incident Management as interconnected processes. Discuss the interdependencies between their key components.	*CO1*	*PO3*	**10**

****