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: VII**
Branch: Information Science and Engineering	**Duration: 3 hrs.**
Course Code: 22IS7PEISF	**Max Marks: 100**
Course: Information Security and Forensic	

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)	Identify and describe four fundamental functions of access control systems.	*CO1*		**5**
	b)	Analyze the factors that an organization should consider when selecting the right firewall for their needs.	*CO3*	*PO2*	**8**
	c)	Illustrate Packet Filtering Firewall with neat a diagram.	*CO2*	*PO1*	**7**
		OR			
2	a)	Identify the best practices of Firewall?	*CO1*		**5**
	b)	Illustrate Screened host Firewall with a neat a diagram.	*CO2*	*PO1*	**7**
	c)	Design a strategy for protecting remote connections using a combination of firewalls and VPNs.	*CO3*	*PO2*	**8**
		UNIT - II			
3	a)	When an IDPS detects a possible intrusion, it has a number of response options. Identify the response for configuring an IDPS.	*CO2*	*PO1*	**10**
	b)	Develop a comprehensive plan for the deployment of intrusion detection and prevention systems in an organization.	*CO4*	*PO4*	**10**
		OR			
4	a)	Outline the strengths and limitations of IDPS.	*CO1*		**5**
	b)	Describe three basic criteria upon which effectiveness of biometric technologies are evaluated.	*CO1*		**5**
	c)	A control strategy determines how an organization supervises and maintains the configuration of an IDPS. In this context, outline the a comparison between the three basic control strategies.	*CO2*	*PO1*	**10**

			UNIT - III			
	5	a)	Illustrate the process to enable extended logging for an IIS Web/FTP server and changing the location of log files.	***CO3***	***PO2***	**10**
		b)	Illustrate the different methods through which network intruders can gain unauthorized access to a system. Provide examples for each method and explain how they exploit vulnerabilities in the network.	***CO2***	***PO1***	**10**
			OR			
	6	a)	Develop a comprehensive guide on best practices for analyzing network data in forensic investigations.	***CO4***	***PO4***	**7**
		b)	Provide the legal issues involved in creating and using logs.	***CO1***		**5**
		c)	Illustrate Log file authenticity, IIS centralized binary logging, ODBC logging in maintaining credible IIS Log Files.	***CO2***	***PO1***	**8**
			UNIT - IV			
	7	a)	Describe DNS poisoning and its usage. Provide the steps involved in one DNS poisoning technique.	***CO3***	***PO2***	**10**
		b)	Investigate the main categories of attacks launched against networks. Explain any two attacks in detail.	***CO3***	***PO2***	**10**
			OR			
	8	a)	Evaluate the importance of documenting evidence for legal and forensic purposes in network investigations.	***CO4***	***PO4***	**10**
		b)	Examine the challenges associated with evidence gathering at the Data Link Layer.	***CO4***	***PO4***	**10**
			UNIT - V			
	9	a)	Discuss cookie poisoning attack. Explain in detail how does an attacker modify the contents of a cookie to steal personal information or defraud websites.	***CO3***	***PO2***	**10**
		b)	Analyze the vulnerabilities that make web applications susceptible to Cross-Site Scripting attacks.	***CO3***	***PO2***	**10**
			OR			
	10	a)	Elucidate the risks associated with different types of web attacks.	***CO2***	***PO1***	**10**
		b)	Explicate Dynamic IP and Static IP with proper example.	***CO2***	***PO1***	**10**

******