U.S.N.										

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

Autonomous Institute Affiliated to VTU

May / June 2025 Semester End Main Examinations

Programme: B.E. **Semester: VIII**

Branch: Institutional Elective **Duration: 3 hrs.**

Course Code: 22IS8OEISF **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.

				CO	PO	Marks
			UNIT - I			
1	a)		List and explain the four fundamental functions of access control systems.	CO1		**5**
	b)		List and explain the Firewalls categorized by processing mode and represent the diagram illustrating the where in the OSI model each of the firewall processing modes inspects data.	CO1		**10**
	c)		Explain how Application gateway works.	CO1		**5**
			OR			
2	a)		Your organization is looking to upgrade its firewall solution. Based on this scenario, compare and contrast two different firewall architectures -Screened Host Firewalls and Dual-Homed Host Firewalls recommend the best solution for the organization.	CO1		**10**
	b)		Illustrate the implementation of VPN using transport and tunnel modes with relevant diagram.	CO1		**10**
			UNIT - II			
3	a)		Classify pros and cons of deploying the NIDPS in the four locations with neat diagram.	CO1		**10**
	b)		Illustrate the functionality of IDPS detection methods.	CO1		**10**
			OR			
4	a)		Outline the comparison study of Honeypots and Honeynets.	CO1		**6**
	b)		Infer the strengths and limitations of IDPS with example.	CO1		**6**
	c)		Illustrate Fully Distributed Control Strategy with neat diagram.	CO1		**8**
			UNIT - III			
5	a)		Interpret the importance of audit logs. Access the legal issues involved with creating and using logs.	CO2	PO1	**10**

		b)	An organization is concerned about the security of their IIS logs and wants to ensure that they are maintained in a credible state. What steps should the organization take to ensure that their IIS logs are credible and can be used as evidence in an investigation.	*CO1*	*PO1*	**10**
			OR			
	6	a)	Explain the procedure of End-to-end forensic investigation.	*CO2*	*PO1*	**7**
		b)	How do you examine intrusion and security events? Illustrate with examples.	*CO2*	*PO1*	**7**
		c)	Identify the methods used by network intruders to enter a system.	*CO2*	*PO1*	**6**
			UNIT - IV			
	7	a)	List and explain the steps involved in DNS poisoning technique.	*CO3*	*PO2*	**5**
		b)	Explain the types of DNS poisoning and how the organizations can better protect against DNS poisoning attacks and respond to potential threats.	*CO3*	*PO2*	**10**
		c)	Show the way of gathering evidence at DHCP in detail.	*CO3*	*PO2*	**5**
			OR			
	8	a)	Explain the way of gathering evidence from ARP Table and ways that an investigator can document the ARP table.	*CO3*	*PO2*	**10**
		b)	Outline the difficulty in reconstructing evidence for a network investigation. Review the three types of analysis that an investigator must perform during evidence reconstruction.	*CO3*	*PO2*	**10**
			UNIT - V			
	9	a)	Interpret any 5 web attacks and Indications of a web attack.	*CO4*	*PO2*	**10**
		b)	Show cross-site scripting attack for web applications. How do you detect such type of attack using regular expression?	*CO4*	*PO2*	**10**
			OR			
	10	a)	When does buffer overflow occur? What are the effects of buffer overflow and how it can be detected?	*CO4*	*PO2*	**10**
		b)	The analyst has determined that the website is suffering from Cookie Poisoning. What is the purpose of Cookie Poisoning and how does it work? How can the analyst mitigate this type of attack on the website?	*CO4*	*PO2*	**10**

****