Reg.No.:												

VIVEKANANDHA COLLEGE OF ENGINEERING FOR WOMEN
[AUTONOMOUS INSTITUTION AFFILIATED TO ANNA UNIVERSITY, CHENNAI]
Elayampalayam – 637 205, Tiruchengode, Namakkal Dt., Tamil Nadu.

Question Paper Code: 60019

B.E. / B.Tech. DEGREE END-SEMESTER EXAMINATIONS – NOV. / DEC. 2024
Fifth Semester
Information Technology
U19ITV21- INFORMATION SECURITY
(Regulation 2019)

Time: Three Hours | Maximum: 100 Marks

Answer ALL the questions

Knowledge Levels (KL)	K1 – Remembering	K3 – Applying	K5 - Evaluating
	K2 – Understanding	K4 – Analyzing	K6 - Creating

PART – A

(10 x 2 = 20 Marks)

Q.No.	Questions	Marks	KL	CO
1.	Name the multiple layers of security that a successful organization should have in its place to protect its operations.	2	K1	CO1
2.	Define Risk Identification.	2	K2	CO1
3.	Which protocol is commonly used to securely manage network devices remotely?	2	K1	CO2
4.	Give the names of firewalls categorized by processing mode.	2	K2	CO2
5.	What is the significance of file ownership and permissions in Unix security?	2	K1	CO3
6.	"Although Virtualization is widely Accepted today, it does have its limits". Comment on the statement.	2	K2	CO3
7.	How can encryption help to protect data on mobile devices?	2	K2	CO4
8.	Illustrate the recommended practice for controlling application behavior in response to security threats.	2	K2	CO4
9.	Why encryption is considered a crucial component of data security?	2	K1	CO5
10.	Define the term "Disaster Recovery Plan (DRP)" and its importance.	2	K1	CO5

PART – B

(5 x 13 = 65 Marks)

Q.No.		Questions	Marks	KL	CO
11.	a)	Show the various components of Information Security that a successful organization must have and list the various components of an information system and tell about them.	13	K1	CO1
		(OR)			
	b)	Discuss briefly about security policies, standards procedure and guidelines with example.	13	K1	CO1
12.	a)	Discuss the role of firewalls and intrusion detection/prevention systems (IDS/IPS) in securing a network. Compare their functions and discuss how they complement each other.	13	K1	CO2
		(OR)			
	b)	Illustrate the architecture of a typical VoIP system and describe the roles of its components. How does QoS impact VoIP performance and what strategies can be used to implement QoS in a network?	13	K1	CO2
13.	a)	Demonstrate in detail about Operating System Security Models with neat illustration and discuss its working model in windows and Linux operating system.	13	K2	CO3
		(OR)			
	b)	List the key points and identify the distinctions in different approaches of virtualization levels. Discuss their relative advantages, shortcomings and limitations. Also identify example systems implemented at each level.	13	K2	CO3
14.	a)	Outline the key components of a Security Operations Center (SOC) and discuss their roles in managing an organization's security posture.	13	K2	CO4
		(OR)			
	b)	Describe the Disaster Recovery Planning (DRP) process and discuss the key elements that should be included in a disaster recovery plan.	13	K2	CO4
15.	a)	Explain the concepts of database reliability and integrity and discuss how these concepts are ensured and maintained in a database system. Evaluate the impact of database security breaches on an organization. Provide examples of potential breaches and discuss the strategies an organization can implement to mitigate these risks.	13	K1	CO5
		(OR)			

	b)	Infer the concept of inference in the context of multilevel security systems. How can inference attacks compromise the security of such systems? Propose strategies to mitigate these risks.	13	K1	CO5

PART – C

(1 x 15 = 15 Marks)

Q.No.		Questions	Marks	KL	CO
16.	a)	TechCorp, a mid-sized technology company, experienced a ransomware attack that encrypted critical files across its network. The attack was discovered when employees started receiving ransom notes demanding payment in cryptocurrency. The company's IT team immediately took steps to contain the situation, but the attacker had already encrypted several key databases and disrupted operations. The company's incident response team was activated, and a forensic investigation was initiated. Questions: 1. Outline the steps that TechCorp's incident response team should take to handle the ransomware attack effectively. Discuss how each step contributes to resolving the incident and minimizing damage. 2. Describe the forensic analysis process TechCorp should follow to investigate the ransomware attack. Explain how the forensic investigation will help TechCorp understand the attack, recover from it, and strengthen its security posture. 3. Evaluate the potential challenges TechCorp may face during the incident response and forensic investigation. Provide recommendations to address these challenges and improve future incident response efforts.	15	K4	CO5
		(OR)			
	b)	**Case Study: A Government Agency's IDPS Deployment** A government agency has deployed an Intrusion Detection and Prevention System (IDPS) as part of its cybersecurity strategy. However, the system has been criticized for high operational costs and limited effectiveness in detecting advanced persistent threats (APTs). i) Evaluate the reasons for these issues and propose a strategic plan to optimize the IDPS deployment, including recommendations for cost management, advanced threat detection, and overall security enhancement.	15	K4	CO4