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: 6023

M.E. / M.Tech. DEGREE END-SEMESTER EXAMINATIONS – JUNE / JULY 2024
Second Semester
Information Technology
P23IT206 – NETWORKS AND SYSTEMS SECURITY
(Regulation 2023)

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.	How can an organization effectively test its network security against various types of attacks, and what are the key steps involved in conducting such tests?	2	K3	CO1
2.	What strategies and technologies can be implemented to guard against network intrusions, and how can these measures be tailored to the specific security needs of an organization?	2	K3	CO1
3.	How does basic Unix security principles, such as protecting user accounts and strengthening authentication mechanisms, contribute to minimizing security vulnerabilities and ensuring secure system access?	2	K2	CO2
4.	What strategies can be employed to mitigate security weaknesses inherent in the Linux operating system, including the concepts of hardening Linux and implementing proactive defense measures, to enhance overall system security?	2	K2	CO2
5.	What are the different stages involved in the Botnet Business Model? also discuss the purpose for each phase.	2	K3	CO3
6.	What is the “Shielding the Wire” concept in network security, including purpose, process and limitation.	2	K2	CO3
7.	What are the different categories or classifications of network threats?	2	K2	CO4

8.	How can organizations effectively implement security protocols to safeguard Wireless Ad Hoc Networks against potential threats and vulnerabilities?	2	K2	CO4
9.	Give the classification of attacks on Wireless Ad Hoc Network?	2	K2	CO5
10.	How does an RFID system utilize symmetric-key cryptography to secure communication between RFID tags and readers, and what are the key steps involved in this process?	2	K2	CO5

PART – B

(5 x 13 = 65 Marks)

Q.No.		Questions	Marks	KL	CO
11.	a)	How would you assess the effectiveness of the "Ten Steps to Building a Secure Organization" in bolstering the security posture of an organization? Discuss the evaluation matrix.	13	K3	CO1
		(OR)			
	b)	How does Vivekanandha College of Engineering for Women decide on modern cryptography techniques to ensure secure communication across diverse departments and classes? Detail the criteria used for selection, alignment with security objectives, adaptability to departmental needs, and strategies for educating faculty and students.	13	K3	CO1
12.	a)	Discuss the significance of superuser privileges compared to normal user access on server management. Highlight the security threats associated with unrestricted superuser privileges and the benefits of limiting them. Provide a use case scenario demonstrating the implementation of a control mechanism to restrict superuser access on a college website server, emphasizing security enhancement while maintaining operational functionality.	13	K3	CO2
		(OR)			
	b)	Examine the security weaknesses of the Linux operating system, categorize the associated threats, and propose solutions. Provide a use case scenario to demonstrate the implementation of security measures and their impact on mitigating threats.	13	K3	CO2
13.	a)	How does the Dolev-Yao Adversary Model aid in evaluating the security of cryptographic protocols and systems? Provide a structured sequence detailing the steps involved in utilizing this model for rigorous security analysis, emphasizing its significance in identifying vulnerabilities and ensuring protocol robustness.	13	K4	CO3

		(OR)			
	b)	How does Network Access Control (NAC) contribute to enhancing network security, and what are the key techniques employed in its implementation? Evaluate the challenges associated with deploying NAC solutions within diverse network environments, considering factors such as scalability, interoperability, and enforcement complexity.	13	K4	CO3
14.	a)	How does an Intrusion Detection System (IDS) operate, and what are its fundamental working principles? Evaluate the classification of IDS types based on detection methods and deployment architectures. Discuss the challenges inherent in effectively deploying and managing IDS solutions, considering factors such as false positives, evasion techniques, and scalability issues.	13	K5	CO4
		(OR)			
	b)	Evaluate the role of key establishment in enhancing security within wireless networks. Discuss its purposes, types, tools, and challenges, including potential attacks targeting these mechanisms.	13	K5	CO4
15.	a)	How does Wired Equivalent Privacy (WEP) encryption and decryption contribute to securing wireless networks, and what is its primary purpose? Evaluate the steps involved in both encryption and decryption processes within the WEP protocol. Assess the strengths and weaknesses of WEP encryption, considering factors such as its effectiveness in protecting data confidentiality and its susceptibility to vulnerabilities.	13	K5	CO5
		(OR)			
	b)	How do Radio Frequency Identification (RFID) systems address challenges in various use cases, and what are the primary efficiency factors influencing their effectiveness? Evaluate potential attacks targeting RFID systems and discuss mitigation strategies. Assess the efficiency of RFID technology across different use cases, considering factors such as reliability, scalability, and cost-effectiveness.	13	K5	CO5

PART – C

(1 x 15 = 15 Marks)

Q.No.		Questions	Marks	KL	CO
16.	a)	Design a comprehensive security solution to address the presented attack scenario, considering the diverse network infrastructure and communication channels within the college network. Outline the security objectives, evaluation criteria, and steps involved in implementing the solution. Describe various techniques and technologies utilized at each stage to mitigate potential security threats effectively.	15	K6	CO4
		(OR)			
	b)	Design a comprehensive security solution tailored for a small software company with multiple departments and datacenter with API communication across the globe. The solution should address diverse network infrastructure and communication channels. Outline security objectives, evaluation criteria, and steps for implementation, emphasizing various techniques and technologies to effectively mitigate potential security threats.	15	K6	CO4