

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: 50024

B.E. / B.Tech. DEGREE END-SEMESTER EXAMINATIONS – NOV. / DEC. 2025

Fifth Semester

Computer Science and Engineering

U23CSV32 – CYBER 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.	State how the principle of “Least Privilege” enhances security in access control models.	2	K2	CO1
2.	Define the role of each component in the AAA framework (Authentication, Authorization, and Accounting) in securing network access.	2	K2	CO1
3.	Define Security Governance and explain its role in cyber security management.	2	K2	CO2
4.	Briefly describe ‘Bell-LaPadula’ and ‘Clark-Wilson’, cyber security models.	2	K2	CO2
5.	What is the purpose of the Certification and Accreditation (C&A) process in cyber security?	2	K2	CO3
6.	What are the primary goals of a <i>cyber security audit</i> and how is the <i>audit frequency</i> determined mathematically in relation to risk level (R)?	2	K2	CO3
7.	How do firewalls, anti-virus software, and cryptographic controls collectively contribute to system hardening?	2	K2	CO4
8.	Differentiate between legitimate and fraudulent encryption methods. Give an example of how fraudulent encryption is used in cyber-attacks.	2	K2	CO4
9.	Differentiate between Black-box, White-box, and Gray-box penetration testing with respect to tester knowledge and testing scope.	2	K2	CO5

10. How can ethical hacking techniques be applied to prevent Identity Theft and Cyber Stalking? 2 K2 CO5

PART – B

(5 x 13 = 65 Marks)

Q.No.	Questions	Marks	KL	CO
11.	a) Describe the key components of cyber security network architecture and their functions. (OR)	13	K2	CO1
	b) Discuss the various types of cyber threats faced by organizations and individuals. Explain how these threats exploit system vulnerabilities to compromise security. Illustrate your answer with examples of common attack methods.	13	K2	CO1
12.	a) Describe the Risk Management Framework (RMF) as defined by NIST. Explain each phase of RMF and how it integrates with the organization's security governance process. (OR)	13	K2	CO2
	b) Define Cyber Security Governance. Discuss the roles, responsibilities and models involved in security management and their importance for regulatory compliance.	13	K2	CO2
13.	a) Explain the significance of cyber security standards and controls in protecting organizational assets. (OR)	13	K3	CO3
	b) Explain methods to ensure alignment between the cyber security policy and actual security practices.	13	K3	CO3
14.	a) Explain the concept of Modern Encryption Methods such as Quantum Cryptography and Homomorphic Encryption. Discuss how they address limitations of classical encryption algorithms. (OR)	13	K2	CO4
	b) Differentiate between Internal and External Security Threats. Explain a stepwise approach to determine an organization's exposure to internal threats and evaluate the risk of external attacks using qualitative and quantitative assessment methods.	13	K3	CO4
15.	a) Discuss the challenges of implementing IDS/IPS in large-scale enterprise networks. Suggest optimization strategies to reduce false positives and improve detection accuracy. (OR)	13	K3	CO5

- | | | | | |
|----|--|----|----|-----|
| b) | Discuss Digital Forensics Tools: EnCase, FTK and Autopsy. Compare their features and applications in real-world cybercrime investigations. | 13 | K3 | CO5 |
|----|--|----|----|-----|

PART – C

(1 x 15 = 15 Marks)

Q.No.	Questions	Marks	KL	CO
16. a)	How can an organization compare its Cyber Security Policy with actual practices? Design a Policy Compliance Matrix to identify and quantify compliance deviations.	15	K3	CO3
(OR)				
b)	As a cyber security auditor, how would you evaluate whether a company's implemented controls truly align with its written policies? Discuss the steps and tools you would use to perform this evaluation effectively.	15	K4	CO4