9/5/2025(E)

SOMAIYA
VIDYAVIHAR UNIVERSITY

Semester: January 2025 –April 2025		
Maximum Marks: 100	Examination: ESE Examination	Duration: 3 Hrs.
Programme code: 01 Programme: B.Tech Computer Engineering	Class: TY B.Tech	Semester: VI (SVU 2020)
Institute/School/Department: K. J. Somaiya School of Engineering	Name of the department: Computer Engineering	
Course Code: 116U01C602	Name of the Course: Information Security	
Instructions: 1)Draw neat diagrams 2) All questions are compulsory 3) Assume suitable data wherever necessary		

Que. No.	Question	Max. Marks
Q1	Solve any **Four**	**20**
i)	Do error detecting codes play a role in information security? Justify your answer with appropriate example.	5
ii)	Distinguish between link encryption and End-to-End encryption.	5
iii)	How is mandatory access control different from discretionary access control? Support your answer with suitable example.	5
iv)	List the different authentication techniques for web-based applications.	5
v)	Explain what is a Replay Attack with the help of a real-world example.	5
vi)	What do you understand by Intellectual Property Rights?	5

Que. No.	Question	Max. Marks
Q2 A	Solve the following	**10**
i)	What do you understand by input sanitization?	5
ii)	List the various secure coding techniques to prevent programming flaws.	5
	OR	
Q2 A	What are malwares? Explain the different methods of malware detection.	10
Q 2 B	Solve *any* **One**	**10**
i)	Assume that you are writing a program for a banking system where multiple threads can update a user's account balance. Explain how a race condition could lead to incorrect balance calculations with suitable example. Suggest a method to prevent the race condition.	10
ii)	A website takes a filename from a query string like this: https://example.com/view?file=report.txt. An attacker inputs ../../../../etc/passwd and successfully views the system's password file. Explain what went wrong, the type of attack & how to fix it.	10

Que. No.	Question	Max. Marks
Q3	Solve *any* **Two**	20
i)	Define bait in terms of security. Explain the common bait tactics in phishing attacks.	10

ii)	Explain any five attacks on the browsers.	10
iii)	What do you understand by page-in-the-middle attack? List the best practices to stay safe from page-in-the-middle attack.	10

Que. No.	Question	Max. Marks
Q4	Solve *any* **Two**	**20**
i)	Describe the following network-based attacks: (a) IP Spoofing. (b) Packet sniffing. (c) Port scanning.	10
ii)	Discuss how a firewall acts as a shield in protecting the networks. Compare the characteristics of a traditional firewall with a next-generation firewall.	10
iii)	Assume that your company has recently experienced a security incident where attackers gained unauthorized access to internal systems through a compromised employee laptop connected to the office Wi-Fi. The attackers used this access to move laterally within the network and exfiltrate sensitive client data. After investigating, it was discovered that: (a) The laptop was missing endpoint protection. (b) The Wi-Fi was protected with a weak password and no guest network. (c) The internal network had no segmentation. (d) Firewall logs showed unusual traffic, but alerts were not monitored. 1. Identify three major security weaknesses in this scenario. 2. Suggest one mitigation strategy for each weakness. 3. Recommend five general best practices that could improve overall network security for the company.	10

Que. No.	Question	Max. Marks
Q5	Solve *any* **four**	**20**
i)	Public Key Cryptography.	5
ii)	Time-of-Check to Time-of-Use (ToCToU)	5
iii)	OWASP	5
iv)	Demilitarized zones (DMZ).	5
v)	Software Piracy.	5
vi)	Indian IT Act 2000.	5