VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of the UGC Act, 1956)

Reg. No. : [redacted]

Final Assessment Test(FAT) - Nov/Dec 2024

Programme	**B.Tech.**	Semester	**Fall Semester 2024-25**
Course Code	**BCSE410L**	Faculty Name	**Prof. Padmanaban R**
Course Title	**Cyber Security**	Slot	**E1+TE1**
		Class Nbr	**CH2024250101792**
Time	**3 hours**	Max. Marks	**100**

General Instructions

- Write only Register Number in the Question Paper where space is provided (right-side at the top) & do not write any other details.

Course Outcomes

Course Outcomes

1. Understand the emerging cybersecurity attacks and their adversarial risk
2. Identify the emerging vulnerabilities and attacks, and countermeasures in cyber-physical systems.
3. Comprehend the need for ethical hacking to minimize the security risk
4. Know the emerging security solutions using automated tools and techniques

Section - I

Answer all Questions (10 × 10 Marks)

*M - Marks

Q.No	Question	*M	CO	BL
01.	A tech company using Windows, Linux, and MacOS devices faced recent security breaches: ransomware on Windows systems, a rootkit attack on a Linux server, and unauthorized remote access tools on MacOS devices. The IT team is now concerned about the security of each OS and the potential risks to business operations and data integrity. A) Tabulate the common vulnerabilities specific to each OS (Windows, Linux, and MacOS) that could have led to these attacks (5 Marks) B) Develop and draw the incident response plan as a flowchart for each of these OS-based attacks to assess the extent of the compromise, contain the damage, and restore systems safely. (5 Marks)	10	1	3

OS \ Vulnerability	Vulnerability1	Vulnerability2	Vulnerability3
Windows OS			
Linux OS			
MacOS			

02	A major e-commerce platform launched a new payment system to handle high transaction volumes and multiple payment methods. It has become a target for cyber attackers aiming to compromise payment data and disrupt services related access control. The security team is tasked with performing an attack tree analysis to identify potential attack vectors and the path taken by attackers to breach the system. A) Identify the root and target node of the attack tree for the payment system, and find the primary goals that the attackers might have when compromising the payment processing system (5 Marks) B) Draw the attack tree and assess the risk levels posed by various threat actors who/which are lying between the root node and target node. (5 Marks)	10	3	6
03,	An employee at a mid-sized financial firm receives an urgent, seemingly legitimate email from the IT department urging them to click a link and verify their credentials to avoid account suspension. The email, part of a phishing campaign by a skilled attacker, mimics company branding and familiar contacts. Soon, other employees report similar emails, raising concerns about a potential breach. A) List the types of access or data could the attacker potentially gain if an employee falls for the phishing email and provides their access credentials (2 Marks) B) Outline an incident response plan that includes detection, containment, eradication, and recovery from the phishing attack. (8 Marks)	10	2	3
04,	A security audit at a tech company revealed weak, reused, and insecurely stored employee passwords. Shortly after, an attempted breach using password-cracking tools heightened concerns about password security. Although partially prevented, the incident prompted a review and the implementation of stronger countermeasures. A) Summarize any five policies to be implemented to strengthen password security and protect the systems against future password-cracking attempts (5 Marks) B) Demonstrate the use of enforcing strong password policies, implementing password managers, and rolling out Multi Factor Authentication methods. (5 Marks)	10	3	1
05	A medium-sized retail business recently launched free in-store Wi-Fi to improve customer convenience. However, the IT team has observed unusual network traffic patterns on the Wi-Fi, particularly during peak hours, raising suspicions of potential security breaches and unauthorized access attempts on the Wi-Fi. A) Develop an algorithm to identify any three types of ongoing attacks on the Wi-Fi (5 Marks) B) Add the attack detection strategies to be followed by the IT team for each type of ongoing attack in the same algorithm. (5 Marks)	10	4	1
06	In a small town, a local bakery named "Sweet Delights" launched an online ordering system. However, the bakery owner noticed that some customers could access orders and personal information of other customers/employees with superior roles. Alex was invited to investigate and report. He found that the system did not properly validate user input such as USER IDs in forms when querying the database for values. Infer the following observations from the report of Alex. A) Identify the vulnerability which manipulates the user inputs to enter into the bakery's database and access restricted information. (5 Marks) B) Suggest any three methods to prevent this improper access. (5 Marks)	10	4	3

07.	#include <stdio.h>
	int main()
	{
	  printf("The value of the Unsigned Int is ");
	  unsigned int size = 4294967295; // Max value for 32-bit unsigned int
	  size += 5;
	  printf(" %u\n", size);
	  printf("The value of the Short Int is ");
	  short int size1 = 32767; // Max value for short int
	  size1 += 5;
	  printf("%hd\n", size1);
	  return 0;
	}
	
	A) Determine the output of the above program and identify the vulnerability. (5 Marks)
	B) Suggest the ways to address the vulnerability along with a new program with any one of your suggestions and the correct output (5 Marks)
		10	3	4

08.	Write some firewall policies / rules for the following attack prevention strategies A) Allow all the incoming or outgoing traffic through some 4 IPs only (2 Marks) B) Allow the incoming or outgoing traffic through a single subnet only (2 Marks) C) Allow only the Telnet traffic only through a specific port (2 Marks) D) Allow only the TLS protocol (2 Marks) E) Deny all the incoming and outgoing traffic through non - standard ports. (2 Marks)	10	2	6
09.	Draw an individual block diagram for each of the following advanced security solutions and describe the features available in these solutions to detect the DDoS attack • Anti Virus Engine (AV) (5 Marks) • Unified Threat Management Systems (UTM) (5 Marks)	10	1	1
10.	A retail company with an extensive e-commerce platform is seeking your advice on selecting security testing tools to ensure their platform is resilient to cyber-attacks. A) Draw a tree diagram to categorize the security testing tools and provide any two distinct features of the tools to enhance the security of e-commerce platform (5 Marks) B) Recommend tools that would be suitable for assessing their platform's security to have low, medium and high security levels. (5 Marks)	10	2	3

BL-Bloom's Taxonomy Levels - (1.Remembering, 2.Understanding, 3.Applying, 4.Analysing, 5.Evaluating, 6.Creating)

⇔⇔⇔