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

School of Computer Science and Engineering
&
School of Information Technology and Engineering

Fall Semester 2023-24 UG Seniors (B.Tech 2021 Batch)

Continuous Assessment Test – 1

SLOT: TAA1/TAA2/TCC1/TCC2

Programme Name & Branch: B.Tech & Common to all branches of SCOPE and SITE

Course Name & code: BCSE353E, Information Security Analysis and Audit

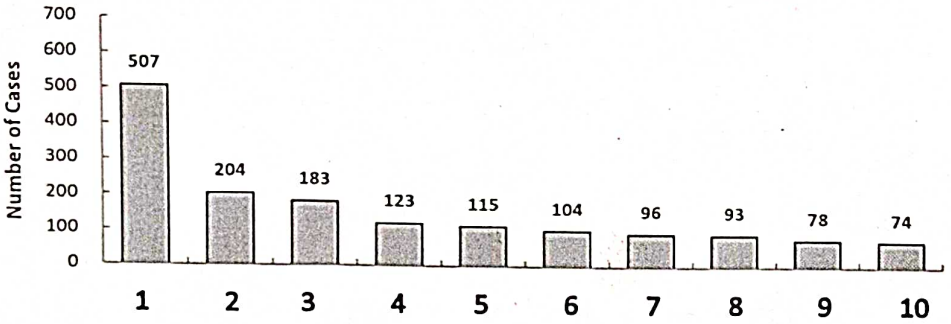
Exam Duration: 90 Min. **Maximum Marks: 50**

General instruction(s):

Answer all the questions

Q.N0	Question	Max. Marks
1.	Cybercriminals have created an email that looks like it originated from PayPal where the body of the email is designed as "Response Required" and states that your account will be suspended if you are not responding to the link, which is embedded in the login word. The attacker will gain useful information and steal the money if the user is tricked successfully. Analyze the scenario and identify the type of attack that fits into this category. Also, explain the other variants of this attack.	10
2.	The company identified a potential for threats coming from outside its network and decided to implement a firewall to protect the important data. The security analyst researched different firewall products and techniques for monitoring traffic to ensure that only authorized traffic was allowed through. Predict the different firewall products and techniques they would have researched and discuss those techniques in detail.	10
3.	a) Compare and contrast, in what way corrective control differs from recovery control with respect to functionality and an application. (5 Marks) b) Compare the various detection methodologies of the Intrusion Detection System. (5 Marks)	10

4.	The following figure shows the number of vulnerabilities reported during the 4th quarter of 2022, in JVN iPedia, where JVN stands for "the Japan Vulnerability Notes." It is a vulnerability information portal site designed to help and ensure Internet security by providing vulnerability information and solutions for software products used in Japan. Analyze the type of vulnerability reported and provide solutions to mitigate this vulnerability.	10



Types of Vulnerabilities Registered in 2022

No	Vulnerability Reported	No	Vulnerability Reported
1	Cross-site scripting	6	Weak passwords
2	Remote code execution	7	Denial-of-service
3	Misconfigured firewalls	8	Elevation of privilege
4	Lack of input validation	9	Unencrypted devices
5	Malicious software	10	Spoofing

5.	Assume you are a company's security analyst. The corporation wants your advice on how to secure the organization's network. Examine the components required to defend the network and explain your choice.	10