



**Continuous Assessment Test- II (CAT-2) – October 2022**

Programme	: B.Tech	Semester	: FS 2022-23
Course Title	: Information security Analysis and Audit	Code	: CSE3501
		Slot	: F2
Faculty	: Dr. S. Nachiyappan Dr. Anusha K, Dr. Rukmani, Dr. Prasad M	Class Nbr	: CH2022231000299, CH2022231000298, CH2022231000660, CH2022231000235
Time	: 90 Minutes	Max. Marks	: 50

Q.No.	Sub. Sec.	Question Description	Marks
1		Consider you are a security administrator in Level 3. Discuss the methods you can use to govern the level 2 and 1 security analyst in an organization when there is a live threat scenario.	10
2		Perform the RCA of the broken access control that has happened in the data center using the fish bone method.	10
3		Analyze the risks by using the color-coding method for the recent FTP attack that has happened in the organization. Suggest a suitable mechanism to reduce risk and increase the profit.	10
4		A Security Analyst encounters the following OWASP classified vulnerabilities in his analysis for an industry. Suggest any two prevention mechanisms for each of the vulnerabilities listed below <ul style="list-style-type: none"><li>• Windows XP is used in some places where the support is stopped long back</li><li>• Metasploit is used to get the username and password to the webserver by automated brute force or dictionary checks</li><li>• Allowing 3<sup>rd</sup> party to purposefully upload his host monitoring code along with regular and automated software updates</li><li>• Not following Secure Software Development Life Cycle (SSDLC)</li><li>• A Cron automated script which was scheduled to raise alarms using automated log analysis for the privilege escalation attack did not raise alarms for a long period.</li></ul>	10
5		A wholesaler conducts a risk analysis on the usage of credits by the current customers. The firm decides to stop extending 90-day advance credits to several customers whose previous transactions are classified as high risk since they have records of data breach through their regular bank accounts. Such customers are asked to pay upfront for new orders.  Implement the risk assessment steps using a neat flow chart for the data breach by the users of the bank accounts to the wholesaler.	10