BIRLA INSTITUTE OF TECHNOLOGY, MESRA, RANCHI
(END SEMESTER EXAMINATION)

CLASS:	**MCA**	**SEMESTER : II**
BRANCH:	**MCA**	**SESSION : SP/2023**

SUBJECT: CA433 INTRUSION DETECTION SYSTEM

TIME:	**3 Hours**	**FULL MARKS: 50**

INSTRUCTIONS:
1. The question paper contains 5 questions each of 10 marks and total 50 marks.
2. Attempt all questions.
3. The missing data, if any, may be assumed suitably.
***4*. Before attempting the question paper, be sure that you have got the correct question paper.**
5. Tables/Data hand book/Graph paper etc. to be supplied to the candidates in the examination hall.

			CO	BL
Q.1(a)	Differentiate between Intrusion Detection System and Intrusion Prevention System.	[5]	1	4
Q.1(b)	Discuss the goals of Network Intrusion Detection System. Explain the need of a firewall.	[5]	2	2
Q.2(a)	Explain about the Attacks on the network layer.	[5]	2	2
Q.2(b)	Distinguish between Denial-of-Service Attack and distributed Denial-of-Service Attack.	[5]	3	4
Q.3(a)	Explain metrics for evaluating the effectiveness of an Intrusion Detection System.	[5]	2	2
Q.3(b)	Explain Statistical anomaly detection based Detection technique.	[5]	2	2
Q.4(a)	Explain the purpose of Botnets.What is a web based Botnet?	[5]	3	2
Q.4(b)	What is fast Flux? Differentiate between single flux and double flux.	[5]	3	3
Q.5(a)	Explain the steps followed in a a zero-day attack. What are the attack vectors of a zero-day attack?	[5]	4	2
Q.5(b)	Explain the issues and Impact of insider threats. Explain the method to prevent an insider attack.	[5]	3	2

:::::01/05/2023 E:::::