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

CLASS: MCA **SEMESTER :II**
BRANCH: MCA **SESSION : SP/2025**

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)	What are key differences between Intrusion Prevention System and Intrusion Detection system? Explain the working of Host based and Network based Intrusion detection system.	[5]	1	2
Q.1(b)	Why is a Firewall important? Explain the functions and types of firewall.	[5]	2	2
Q.2(a)	Explain Application Layer attack with suitable example.	[5]	2	2
Q.2(b)	Explain and differentiate between Denial of services attack and man in the middle attack.	[5]	2	2
Q.3(a)	Illustrate the Evaluation framework of IDS. Explain Correction detection rate and false alarm rate.	[5]	2	2
Q.3(b)	What is vulnerability? Explain the taxonomy of Anomaly based detection technique.	[5]	2	2
Q.4(a)	What are attack trees? Explain an attack tree with a suitable example.	[5]	4	2
Q.4(b)	Compare the techniques of Obfuscation and deobfuscation. Explain these techniques using suitable examples.	[5]	4	4
Q.5(a)	What are viruses? Explain virus code infection by a suitable example. Explain about the information revealed through static analysis of viruses.	[5]	3	2
Q.5(b)	What the different types of insider threats? Explain decoy and deception.	[5]	3	2

::::::02/05/2025::::::E