BIRLA INSTITUTE OF TECHNOLOGY, MESRA, RANCHI

END SEMESTER EXAMINATION

CLASS: MCA **SEMESTER :II**

BRANCH: MCA **SESSION :SP/22**

SUBJECT: CA433 Intrusion Detection System

TIME: 2:00hrs **FULL MARKS: 50**

INSTRUCTIONS:

1. The question paper contains 5theory questions, with options, each of 10 marks and total of 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.**

Q.1	Explain Intrusion Prevention System and Intrusion Detection system. Which are three main types of intrusion detection system?	[10]
or	What is a firewall? How does a VPN work? Which VPN protocols are there?	
Q.2	What do you understand by denial of service? What are the categories of denials of service?	[10]
or	Explain about the attacks on network layers. What do you mean by code injection? Give suitable example.	
Q.3	Explain Statistical anomaly based intrusion detection system. What is Snort?	[10]
or	What do you understand by Anomaly Based Intrusion detection system? Explain snort rules.	
Q.4	How does obfuscation work? How the success of obfuscation methods can be measured?	[10]
or	What are attack tree? Explain the components of a polymorphic malware.	
Q.5	Explain threat issues .How insider threat issues can be detected?	[10]
or	Write notes on Email security issues and IM security issues.	

/* 6th May 2022*/

06/05/2022