PRN No.	1032210881

Dr. Vishwanath Karad
MIT WORLD PEACE UNIVERSITY | PUNE
TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

School of Computer science and Engineering

Department of Computer Engineering and Technology

FY BTech (CSF) (Academic Year 2024-25)

Mid Term Exam - Semester ...

Course Name: - Attack Reporting and Documentation **Course Code: -CET4042B**

Maximum Marks: 30 **Time: 1 Hr.** **Date:5-Mar-25**

Instructions: -

1. *Attempt any 3 questions from Q. 1 to Q. 4 AND Attempt any 3 questions from Q. 5 to Q. 8*
2. *Figure to the right indicates full marks.*
3. *Use of cell phone is prohibited in the examination hall.*
4. *Neat diagrams must be drawn wherever necessary.*
5. *Assume suitable data, if necessary and clearly state.*
6. *Use of scientific calculator is allowed*

Attempt any 3 questions from Q. 1 to Q. 4			
Q.1	C2 (Applying)	Explain the concept of cybersecurity threats by defining them, describing their nature and scope, and providing three examples.	[5 Marks]
Q.2	C2 (Applying)	Explain at least two key characteristics of phishing and describe any three types of phishing attacks.	[5 Marks]
Q.3	C2 (Applying)	Define an attack vector and explain its key characteristics. Discuss the significance of entry points in cyberattacks in details	[5 Marks]
Q.4	C2 (Applying)	What actions can a defender take in the first five stages of the Cyber Kill Chain to prevent or mitigate an attack?	[5 Marks]
Attempt any 3 questions from Q. 5 to Q. 8			
Q.5	C1 (Understanding)	The Preparation phase is crucial for ensuring an organization can respond to incidents instantly. List and briefly explain any five critical elements that should be	[5 Marks]

Roll No.

		prepared in advance to improve incident response effectiveness.	
Q.6	C1 (Understanding)	Why is cross-departmental coordination crucial for an Incident Response Team? Discuss the importance of clear communication during an incident.	[5 Marks]
Q.7	C1 (Understanding)	An organization is updating its Disaster Recovery Plan (DRP). Explain the significance of Recovery Time Objective (RTO) and Recovery Point Objective (RPO) in this process. How do these metrics influence the selection of disaster recovery strategies?	[5 Marks]
Q.8	C1 (Understanding)	Explain the role of the Central Bureau of Investigation (CBI) in handling cybercrime in India. Mention its jurisdiction, key responsibilities, and legal authority.	[5 Marks]