Name: **Enrolment No:**	

UPES

End Semester Examination, December 2024

Programme Name: MCA / M. Tech **Semester: 1**
Course Name : Cyber Threat Intelligence **Time : 03 hrs**
Course Code : CSCS7013 **Max. Marks: 100**
Nos. of page(s) : 02

Instructions:

- Attempt all questions.
- Draw diagrams wherever necessary.

SECTION A
(20 marks) 5 Questions.
Attempt all questions.

S. No.		Marks	CO
Q 1.	Mention ten different types of OSINT sources.	**4**	**CO1**
Q 2.	Discuss Wireshark, Network Miner and FakeNet.	**4**	**CO1**
Q 3.	What do you understand by Groups, Software and Campaigns in the Mire ATT&CK Framework?	**4**	**CO2**
Q 4.	Give examples of at least three Cloud-based portals to perform Malware Analysis.	**4**	**CO3**
Q 5.	Define the following with two examples each: a. Asset b. Exploit c. Breach d. Attack e. Hash	**4**	**CO1**

SECTION B
(40 Marks) 4 questions.
Attempt all questions.

Q 6.	a. Discuss about Open-Source Intelligence, the process you would follow, and the common techniques involved. b. What do you understand by OSINT Framework?	**10**	**CO1**
Q 7.	Describe at least two tools each for a. Social-media search. b. People Investigations c. Email Investigations	**10**	**CO1**

	d. Hunting Breached Credentials e. Dark Web Research		
Q 8.	There are various open-source threat intelligence feeds that offer up-to-date data on current cyber threats and vulnerabilities, serving as a crucial asset for cybersecurity experts to keep track of emerging risks and security teams leverage these to gain threat intelligence. Discuss at least five CTI feeds.	**10**	**CO2**
Q 9.	Discuss Malware Analysis, its Objectives, Types and enumerate at least two virtual machines you would use for malware analysis.	**10**	**CO3**
SECTION C **(40 Marks) 2 Questions.** **Attempt all questions.**			
Q 10.	a. Discuss the Cyber Kill Chain and its phases in detail. b. Discuss Diamond Model, its dimensions and elements.	**20**	**CO2**
Q 11.	Explain the Mitre ATT&CK framework and its fourteen tactics and discuss the use of Mitre Navigator. OR Describe the following: a. Clustering & Correlation with examples b. Steps involved during Attribution phase c. How PassiveDNS used in CTI d. Sinkhole process and its benefits.	**20**	**CO3**