Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

ME - SEMESTER– 3 (NEW) • EXAMINATION – WINTER - 2023

Subject Code:4735902 Date: 02 Dec 2023

Subject Name:Incident Response and e-Discovery

Time:10:30 AM TO 01:00 PM Total Marks: 70

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

Q.1	**(a)**	What is incident response? Why should you care about incident response?	**07**
Q.1	**(b)**	Explain the incident response life cycle process in detail with relevant example and figure.	**07**
Q.2	**(a)**	List the groups within an organization that may be involved in an incident response. Explain why it is important to communicate with those groups before an incident occurs.	**07**
Q.2	**(b)**	Your organization receives a call from a federal law enforcement agency, informing you that they have information indicating a data breach occurred involving your environment. The agency provides a number of specific details, including the date and time when sensitive data was transferred out of your network, the IP address of the destination, and the nature of the content. Does this information match the characteristics of a good lead? Explain why or why not. What else might you ask for? How can you turn this information into an actionable lead?	**07**
		OR	
Q.2	**(b)**	Suppose DDoS attack is happened in your company then which are the collecting initial facts that you would like to collect as an investigator? Summarize the checklists of incident summary with justification.	**07**
Q.3	**(a)**	When to perform a live response? Utilize the best practices for the collection and apply the three categories to collect live data on Microsoft Windows Systems.	**07**
	(b)	What is a DNS blackhole? When would you use one? Write a BIND zone file that will accept all queries for a malicious domain and answer with an RFC1918 address.	**07**
		OR	
Q.3	**(a)**	How OSS-Fuzz tool is useful for uncovering the programming errors? Explain its working with suitable diagram.	**07**
Q.3	**(b)**	How do you know when to stop fuzzing? Demonstrate it with performance testing example.	**07**

Q.4	**(a)**	In customer data loss scenario, you work in the IT security department for a large online retailer. Your company has been receiving increased complaints from customers regarding e-mail spam. The customers indicate that shortly after becoming a new customer, they begin to receive a large amount of e-mail spam. This scenario is initially a bit less "concrete" than others are, because there is no real alert data or other indication of a security issue. Nevertheless, concern is mounting, and IT security has been asked to investigate then an investigator how will you investigate this scenario?	**07**
Q.4	**(b)**	During an investigation, a database administrator discovers that hundreds of MySQL queries with a long execution time were run from a single workstation. The database did not record the specific query—just the date, time, source, and query execution time. You are tasked to determine what queries were executed. How would you proceed?	**07**

OR

Q.4	**(a)**	When architecting a new network monitoring system, what types of questions should be asked of the IT or network staff? How can you help ensure complete visibility into traffic egressing your networks?	**07**
Q.4	**(b)**	What system information can you gather from a static image?	**07**
Q.5	**(a)**	How would you quickly identify whether a large .pcap file with thousands of sessions contained TCP activity? How would you extract the transferred files?	**07**
Q.5	**(b)**	i) List and explain at least seven Unix-based tools and commands which are useful for data collection. ii) In what situations would collecting an image of memory be most useful to the investigation?	**07**

OR

Q.5	**(a)**	With reference to Q. 4(a), In the customer data loss scenario, a number of steps were taken to verify the customers' complaints. List at least two other useful steps you could have taken to help verify the customers' complaints or isolate the source of the data loss.	**07**
Q.5	**(b)**	Pick a recent data breach and create a containment plan based on the known information. What actions would you implement as part of the eradication effort that you would not implement as part of the containment plan. Explain your choices.	**07**

****