**Name: Dhaval Patel**

**Msc cyber security**

**With the help of DISK MONITORING identify the read and write process having length > 5**

Title :

With the help of **Disk Monitoring** identify the read and write process having length greater than 5.

Objectives :

1. To identify the read and write process having length greater than 5.

Requirements :

Computer system with sufficient processing power, memory, and storage space.

Operating System - Windows OS

Process Explorer - Process Monitor

Procedures/ Experimental Setup :

* Install Disk Monitoring Software:

Download and install the selected disk monitoring tool.

* Configure Monitoring Settings:

Launch the disk monitoring software and configure the monitoring settings to capture disk activity. Specify the target disk or disks for monitoring.

* Start Monitoring:

Initiate the disk monitoring process using the selected tool.

* Analyze Captured Data:

Access the captured data.

* Identify Read and Write Processes:

Analyze the captured data to identify processes with read and write operations. Look for processes with a length greater than 5, indicating significant disk activity.

Results :

During the disk monitoring process, the following results were obtained:

* The disk monitoring tool successfully captured disk activity and identified processes with read and write operations.
* Read and Write Length: The identified processes exhibited read and write lengths greater than 5, indicating significant disk activity.

Result Analysis :

The analysis of the captured disk activity data revealed the following observations:

* Process Identification: By monitoring disk activity, it was possible to identify processes with significant read and write operations. These processes may be responsible for data-intensive tasks, such as file transfers, database operations, or data backups.
* Resource Utilization: Processes with longer read and write lengths may indicate higher resource utilization, potentially impacting system performance or response time. Monitoring such processes can help identify resource-intensive operations and optimize system performance.

Conclusion :

In conclusion, disk monitoring proved to be an effective method for identifying read and write processes with a length greater than 5. The analysis of disk activity data allowed for the identification of processes exhibiting significant disk usage. By monitoring these processes, system administrators or analysts can gain insights into resource-intensive operations and optimize system performance accordingly.

Future Scope :

* Real-time Monitoring: Implementing real-time disk monitoring to capture and analyze disk activity as it happens, providing immediate visibility into processes with significant read and write operations.
* Statistical Analysis: Performing statistical analysis on captured disk activity data to identify trends, patterns, or anomalies in read and write lengths, enabling proactive monitoring and detection of abnormal disk behavior.
* Integration with Performance Monitoring: Integrating disk monitoring with broader system performance monitoring tools to correlate disk activity with system resource utilization, CPU usage, or memory usage for comprehensive system analysis.

References :

* Process Monitor: Official documentation and user guide for Process Monitor tool. Available at: <https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>
* Disk Performance Analysis for Windows: A comprehensive guide on disk performance analysis for Windows systems. Available at: <https://docs.microsoft.com/en-us/windows-server/administration/performance-tuning/role/storage/disk-performance-analysis>