***Cyber security Lab Exercise 7:***

1. Perform Registry analysis and get boot time logging using process monitor tool

***Aim:***

The aim of the Process Monitor tool, often referred to as ProcMon, is to monitor and display real-time file system, Registry, and process/thread activity on a Windows operating system. Developed by Sys internals (now part of Microsoft), Process Monitor is a powerful utility for system administrators, developers, and IT professionals for diagnosing and troubleshooting system issues.

***Key purposes of Process Monitor include:***

1. Real-Time System Monitoring: Capturing and displaying real-time data on file system changes, Registry changes, and process/thread activity, allowing users to observe what is happening on their system as it occurs.

2. Troubleshooting and Debugging: Helping to diagnose and resolve issues related to system performance, application errors, and other operational problems by providing detailed insights into system activity.

3. Security Analysis: Identifying suspicious or malicious activity by monitoring unexpected changes or unusual patterns in system processes, files, and Registry keys.

4. Compliance and Auditing: Providing a detailed log of system activity that can be used for auditing purposes, ensuring compliance with security policies and regulations.

5. Understanding Application Behavior: Offering developers and IT professionals an in-depth view of how applications interact with the system, which can be useful for optimizing performance, debugging, and development.

6. Detecting Configuration Issues: Highlighting misconfigurations or incorrect system settings by showing the exact changes being made to the system.