**Today Assignment – Date: August 6,2025**

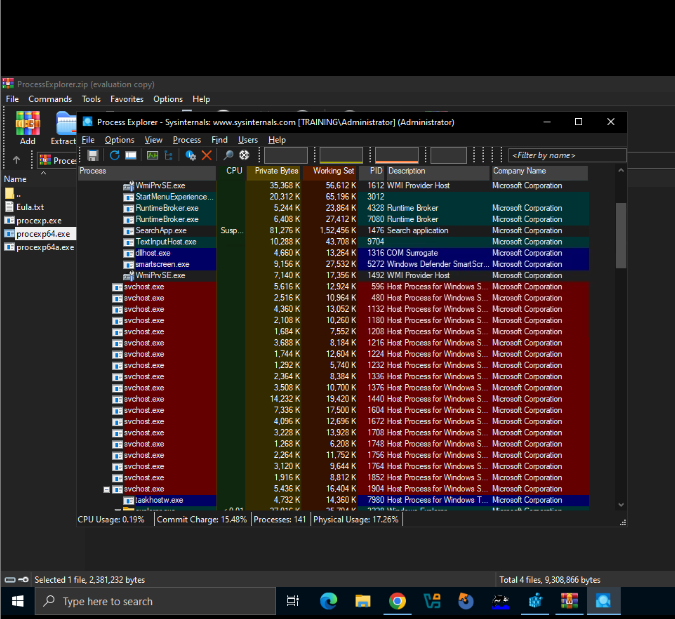
**Name: 34733-Prasang Kumar Singh**

**Gmail:** [**thakurprasang23@gmail.com**](mailto:thakurprasang23@gmail.com)

**Today Topic:-  
Windows tools for debugging ,steps to create for Microsoft Inture portal**

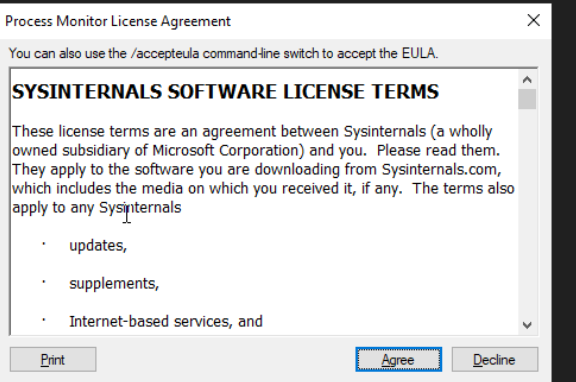
**1. Process Explorer:**

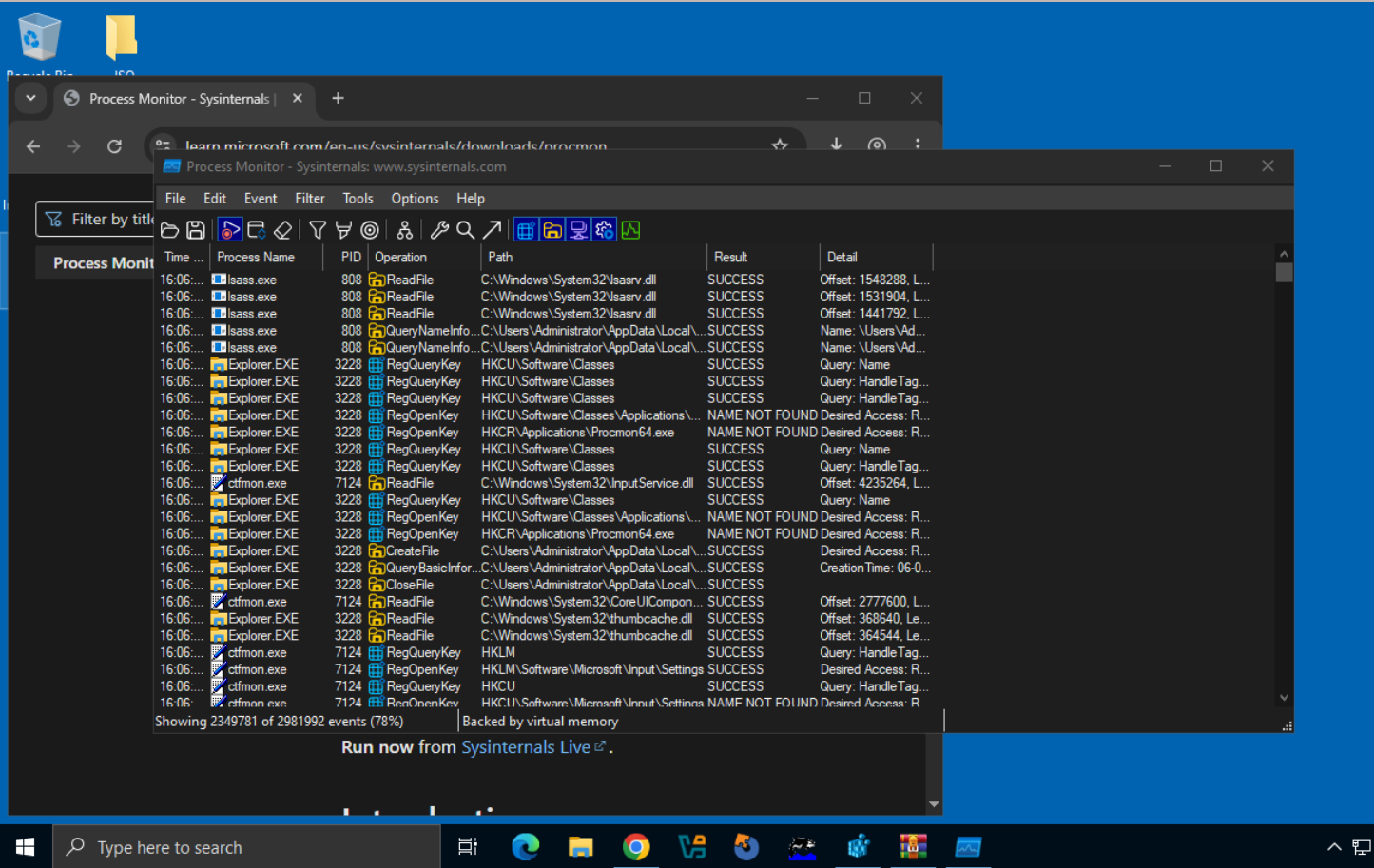
It is a powerful tool used to view and manage all currently running processes on a system. It gives detailed insights such as memory usage, open handles, and files associated with each process. This tool plays a vital role in identifying resource bottlenecks, troubleshooting issues related to specific processes, and detecting any suspicious or potentially malicious activity running in the background.



**2.Process Monitor**

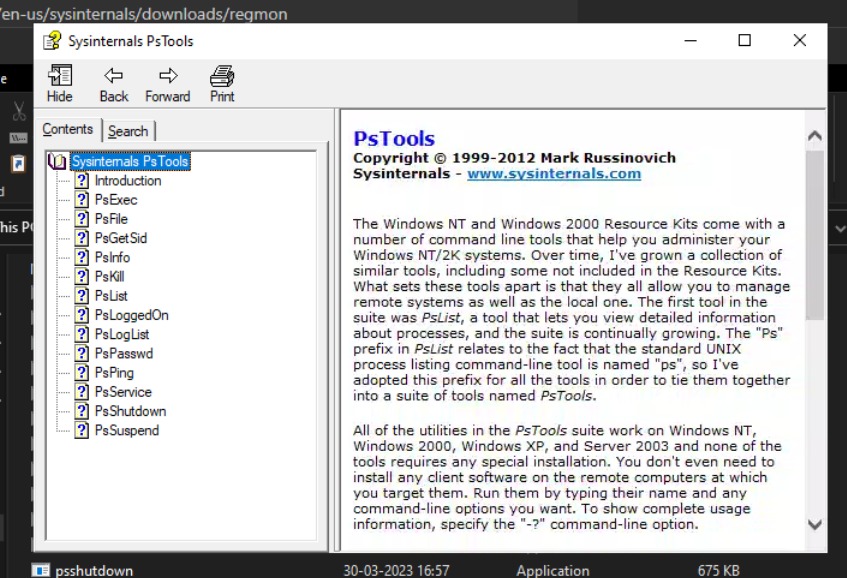
Process Monitor is a powerful system monitoring tool used to track and analyze real-time activities of the file system, registry, and processes in Windows. It provides detailed information about running processes, including memory usage, thread activity, open files, registry access, and more. This tool is especially helpful for troubleshooting system and application errors, diagnosing performance issues, monitoring software installations, and detecting suspicious or unauthorized process behaviour, making it an essential utility for IT professionals and system administrators.



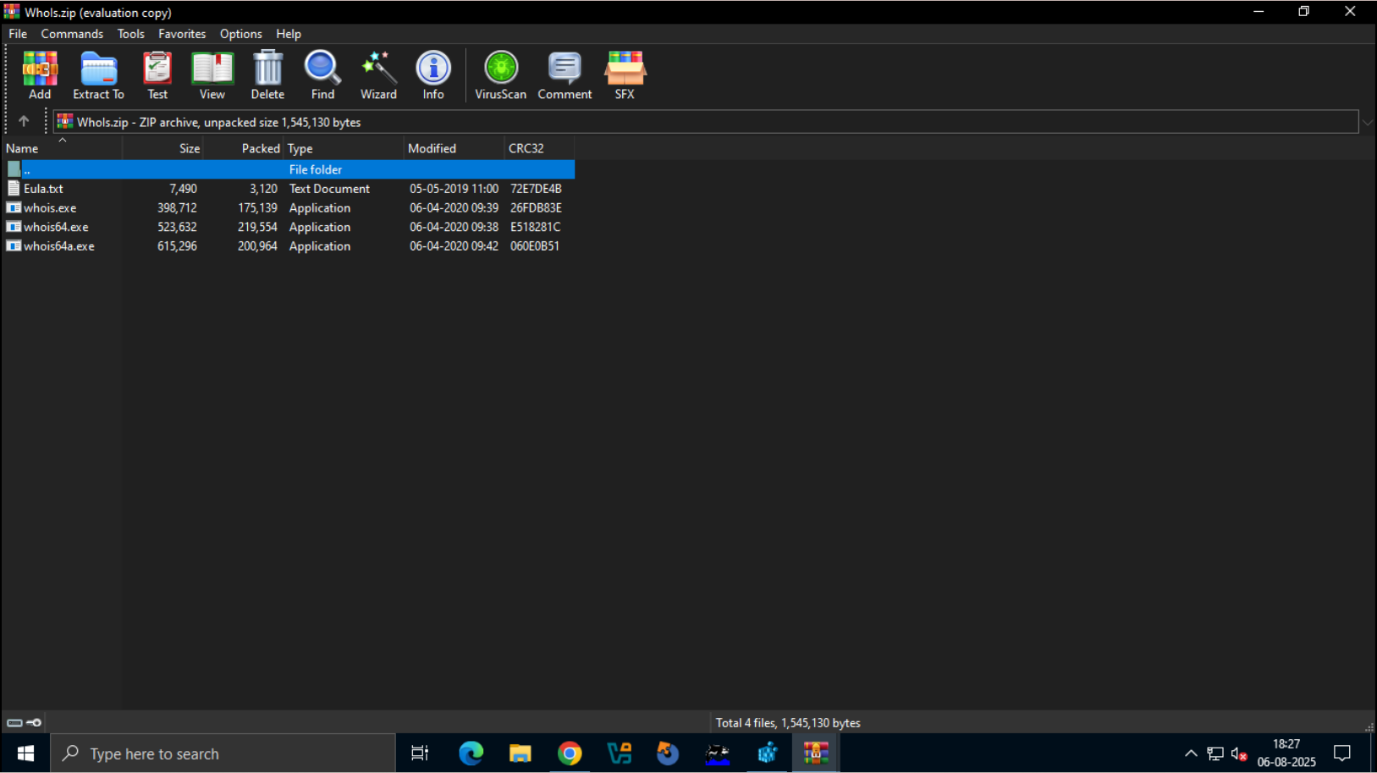


**3.PS tools**

PsTools (Process Status Tools) is a suite of command-line utilities developed by Sysinternals for system administration and troubleshooting tasks in Windows environments. It includes various tools such as PsExec, PsLoggedOn, PsKill, PsFile, PsList, and others, each designed for specific administrative functions. These tools allow administrators to perform tasks like viewing who is logged on, listing running processes, managing files, and even executing commands on remote systems without requiring remote desktop access. PsTools is widely used for both local and remote administration, making it a valuable toolkit for IT professionals.

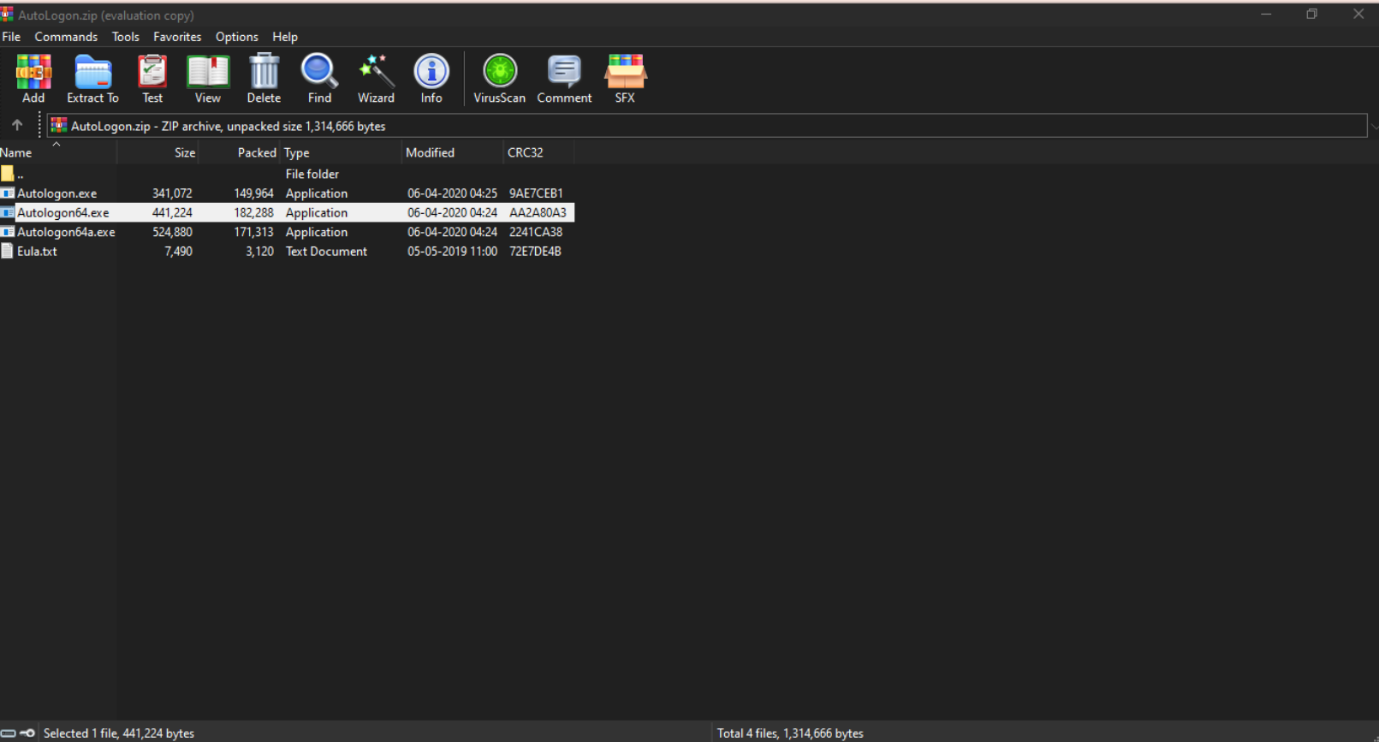


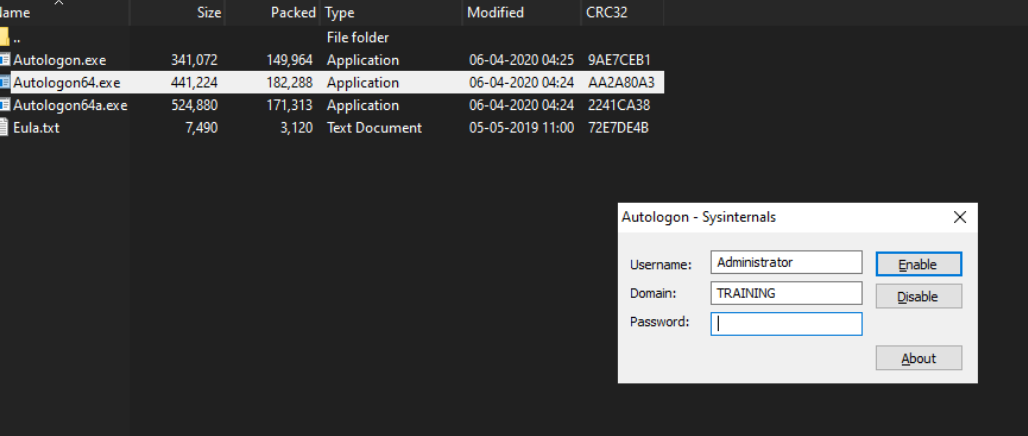
**4.Whois**

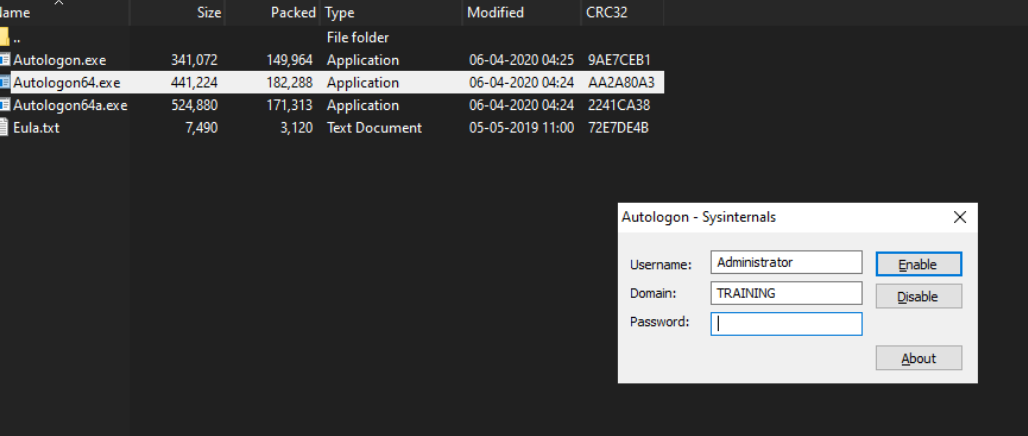
****Whois is a command-line utility commonly used to gather detailed information about domain names and IP addresses. Although not originally a Sysinternals tool, it is often included in administrative toolkits. It works by querying Whois databases to retrieve domain registration details such as the owner’s name, contact information, registration date, and expiration date. This tool is especially useful for network troubleshooting, identifying domain ownership, tracking malicious activity, and checking domain name availability.

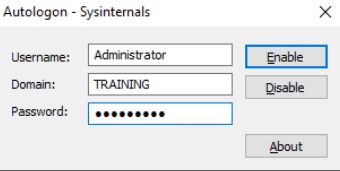
**5.Autologon**

It is a graphical utility designed to automate the login process on a Windows system by securely storing user credentials in the registry. Once configured, it allows a specific user account to log in automatically without requiring manual input of the username and password each time the system boots. This tool is especially useful in scenarios like headless systems, kiosks, or automated testing environments where manual login is impractical or unnecessary.



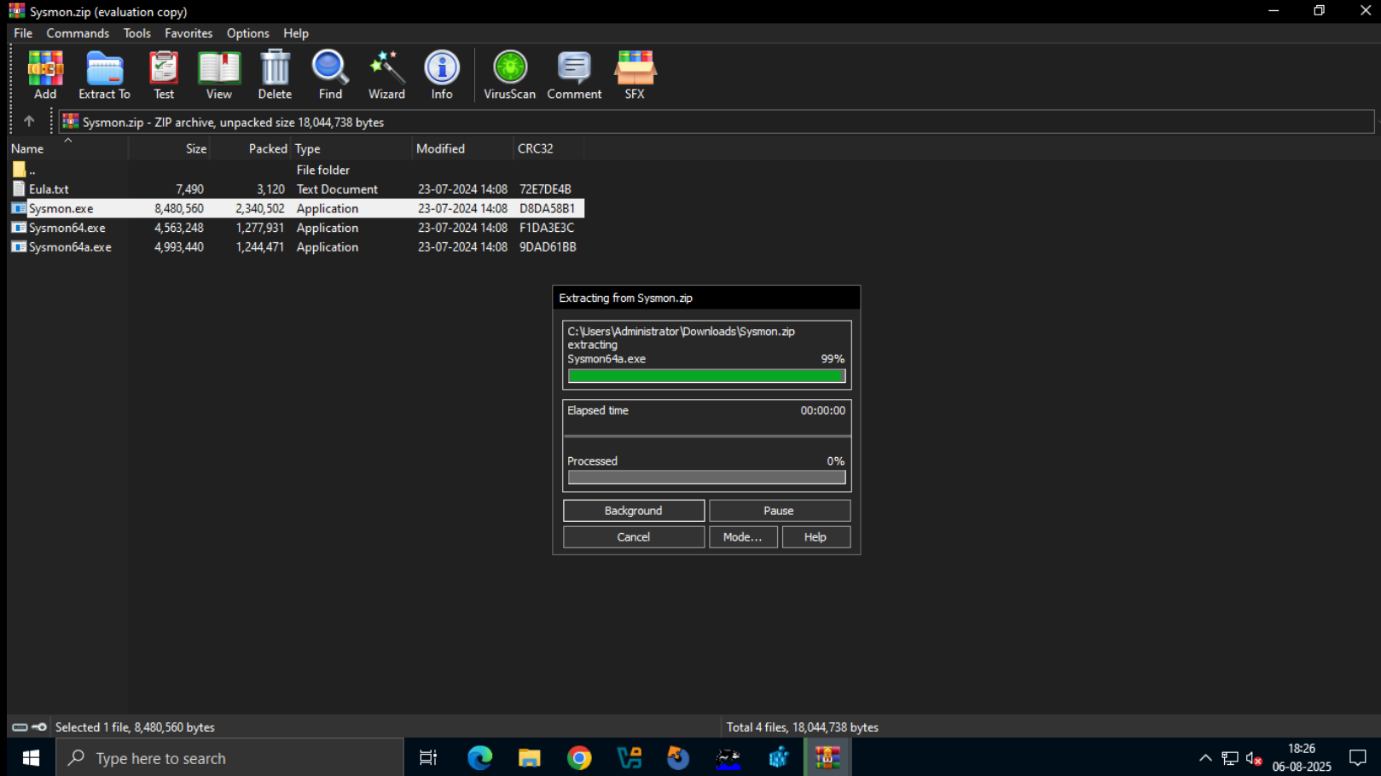






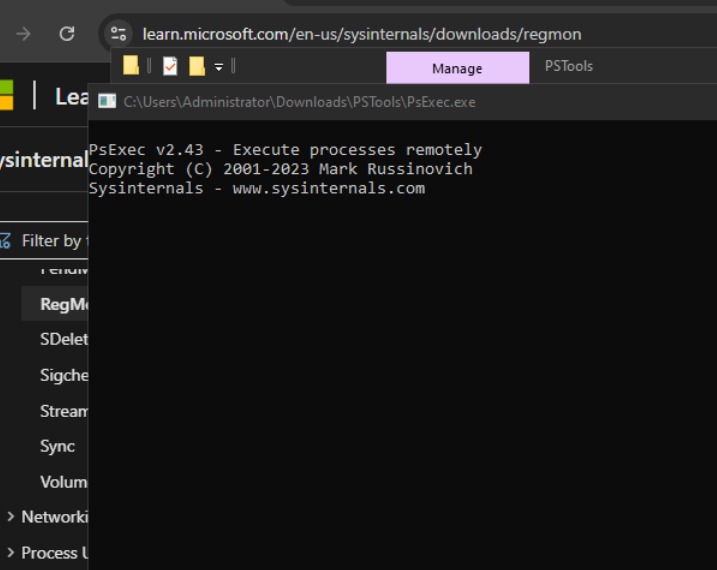
**6.Sysmon (System Monitor)**

It is a Windows system service and device driver that provides detailed and advanced logging of system activity to help with security monitoring and analysis. It captures events such as process creation, network connections, changes to file creation timestamps, and more. By generating rich event logs, Sysmon plays a critical role in intrusion detection, threat hunting, and forensic investigations. It is commonly used by security professionals to gain deep visibility into system behaviour and to detect suspicious or malicious activity.



**7.PsExec**

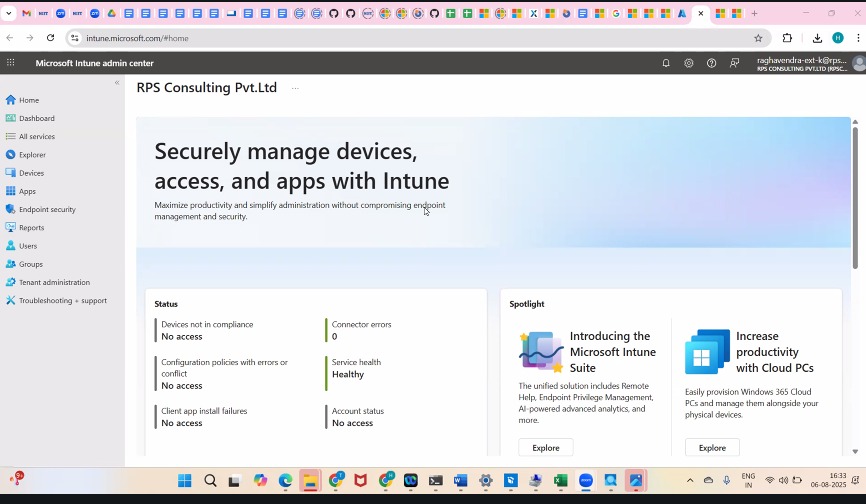
It is a powerful command-line utility from the PsTools suite that enables the execution of programs and commands on remote systems as if they were running locally. It allows administrators to launch processes on other computers without requiring physical access or remote desktop. PsExec is widely used for tasks such as remote system management, software deployment, patch installation, and troubleshooting. It simplifies administrative operations across multiple machines, making it an essential tool for IT professionals managing large networks.



**8.RegMon (Registry Monitor)** is a real-time monitoring tool for Windows that captures and displays all registry activity on a system. It tracks every read, write, and delete operation performed in the registry, showing which process initiated the action and what keys or values were accessed or modified. RegMon is especially useful for diagnosing registry-related problems, identifying unauthorized or suspicious applications that manipulate the registry, and investigating potential security threats or vulnerabilities in the system.

**Steps to create for Microsoft Inture portal**

**1.Sign In**  
Go to https://intune.microsoft.com and sign in with a Global Admin account.



2.**Assign Intune License**  
In Microsoft 365 Admin Center → Users → assign **Intune license** to users. **Set 3.MDM Authority**  
In Intune Admin Center → Tenant Administration → set **Microsoft Intune** as MDM authority.

4.**Enroll Devices**  
Go to **Devices → Enroll Devices**, set up platform-specific enrollments (Windows, Android, iOS).

5. **Create Policies**

* **Compliance Policy** (e.g., password rules, OS version)
* **Configuration Profile** (e.g., Wi-Fi, security, Defender settings)

6. **Add Apps**  
Go to **Apps → All Apps → Add**, upload or select apps, assign to users/devices.

7. **Monitor**  
Use the **Monitor** section to track device health, app deployments, and compliance.