Daily Work Assignment

Name :Lalit Joshi || Email: joshilalit2275@gmail.com

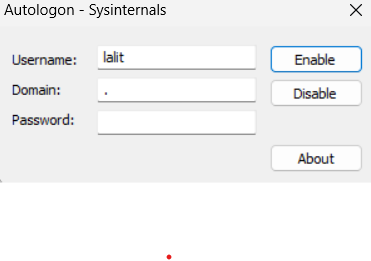
**TOPICS:**

**# Using Windows Tools for Debugging\_ LogonSessions,Autologon,Process Explorer ,Psexec,PSTools,RegMon,Whois,SysMon**

# 1. Autologon

• Purpose: Automatically logs in a user without requiring manual password entry.

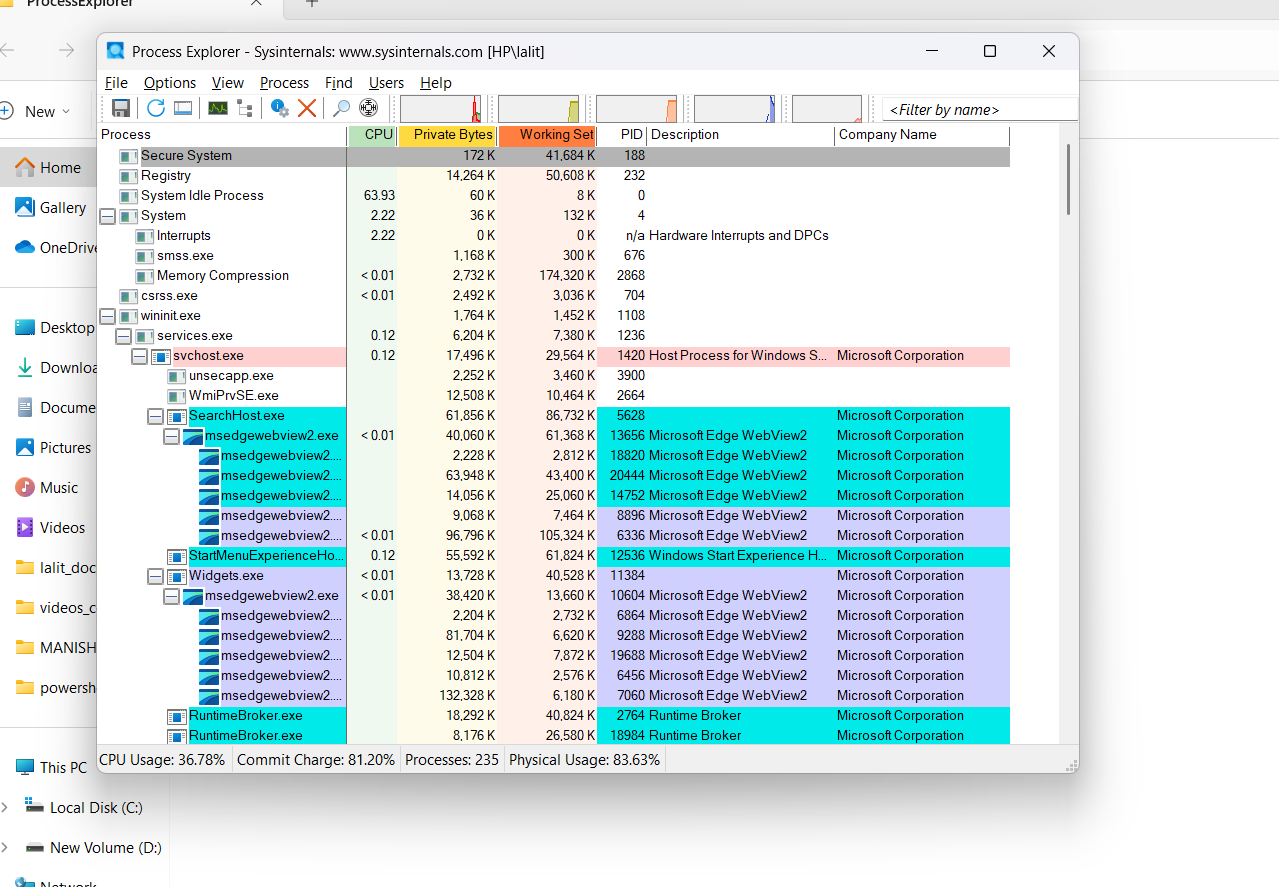
• How it works: Autologon stores the username and encrypted password in the Windows registry.

• Usage: Useful for kiosks, automated test systems, or VMs where automatic login is required.

# 2. Process Explorer

• Purpose: Advanced task manager for viewing detailed process and system information.

• How it works: Displays all running processes, their relationships, memory usage, and open handles.

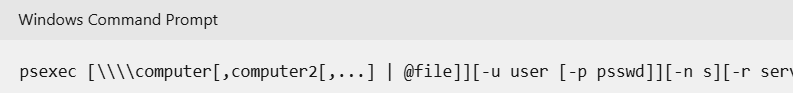
• Usage: Used for detecting malware, troubleshooting system slowdowns, or monitoring resource usage.

# 3. PsExec

• Purpose: Run processes on remote systems without manual login.

• How it works: Launches applications on remote systems using command-line interface.

• Usage: Helps in remote administration, automation, and executing remote scripts.



# 4. PSTools

• Purpose: A suite of command-line utilities for system administration tasks.

• How it works: Includes tools like PsLoggedOn, PsFile, PsList for remote monitoring and management.

• Usage: Ideal for administrators managing multiple systems remotely or locally.

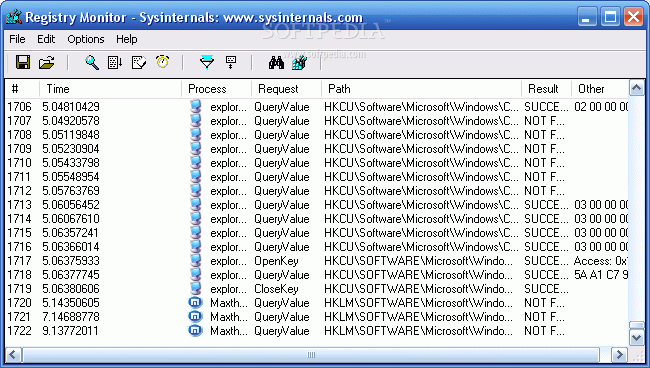


# 5. RegMon

• Purpose: Monitor Windows Registry activity in real time.

• How it works: Displays live registry reads/writes/deletes by applications or processes.

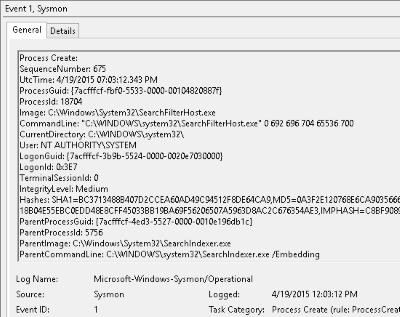
• Usage: Helpful in troubleshooting registry errors and understanding app behavior.



# 6. Sysmon

• Purpose: Provides detailed logging of system activity for security monitoring.

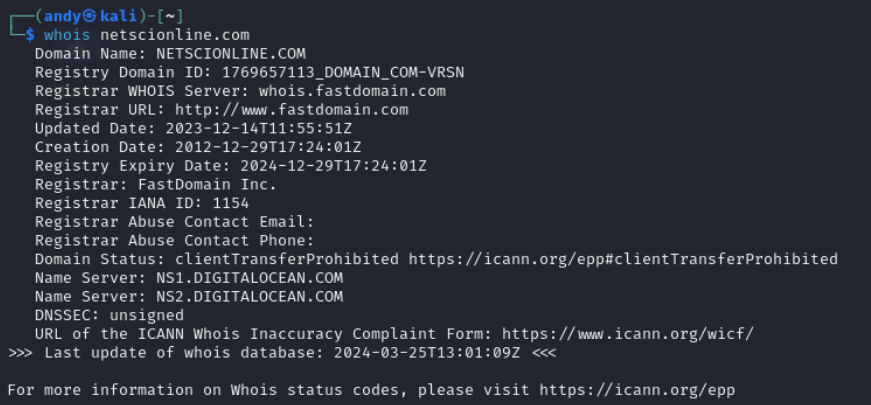
• How it works: Logs process creations, network connections, and file changes into the Windows event log.



# 7. Whois

• Purpose: Command-line tool to find information about domains and IP addresses.

• How it works: Queries public WHOIS servers to get domain registration and ownership data.

• Usage: Useful for checking domain ownership, identifying suspicious domains, and IT audits.

**# Active Setup and Versioning in Windows**

**Summary:**

**Active Setup** is a Windows feature that runs some setup tasks automatically for each user **when they log in**. It is commonly used by software installers to make sure every user on the computer gets the same setup experience (like registry keys, files, etc.).

To make this work, Windows uses two special places in the registry:

* **HKLM (HKEY\_LOCAL\_MACHINE):** This stores the *master settings* of the setup — like the app name, setup command (StubPath), and version.
* **HKCU (HKEY\_CURRENT\_USER):** This stores *user-specific settings* — it copies the data from HKLM when the user logs in.

**Working:**

1. When a user logs in, Windows **checks the version number** of the app in both places (HKLM and HKCU).
2. If the **HKLM version is newer** than the one in HKCU (or if the user is logging in for the first time), Windows **runs the setup command** (StubPath).
3. This allows settings, registry entries, or other user-level configurations to be applied automatically.

**Why Increment the Version?**

If you want the setup to **run again** (even for the same user), just increase the version number in the HKLM key. For example, change it from 1.0.0 to 1.0.1. This tells Windows that there is a new update, and it should re-run the setup for every user on next login.

**🧾 Example Registry Entry:**

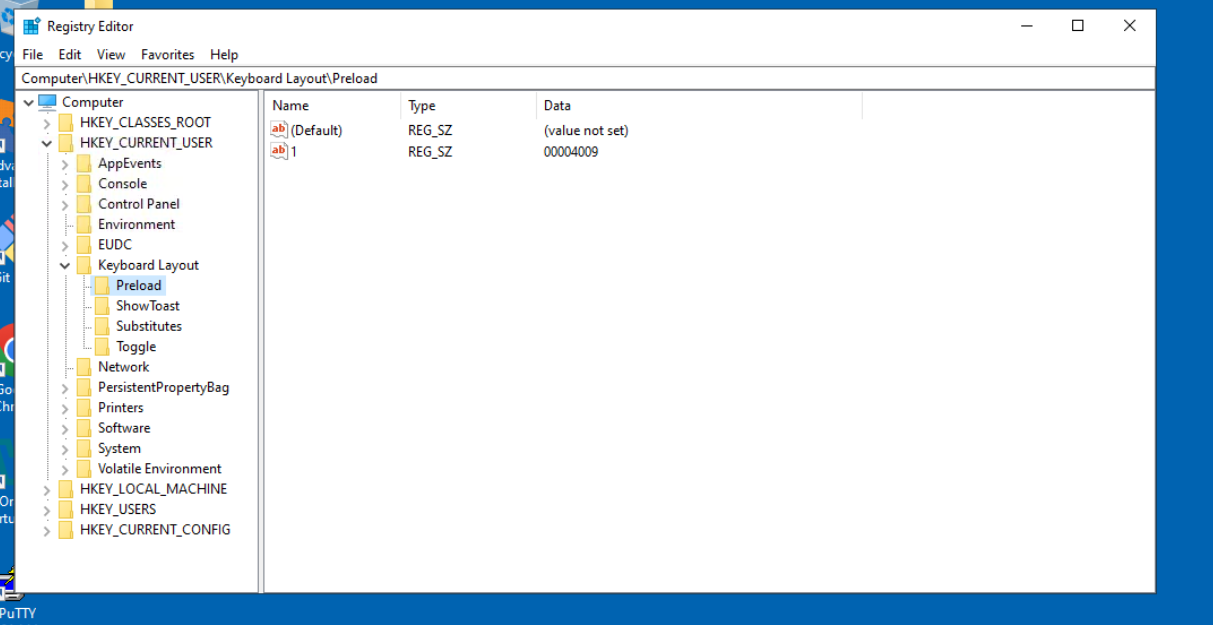
makefile

CopyEdit

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{GUID}

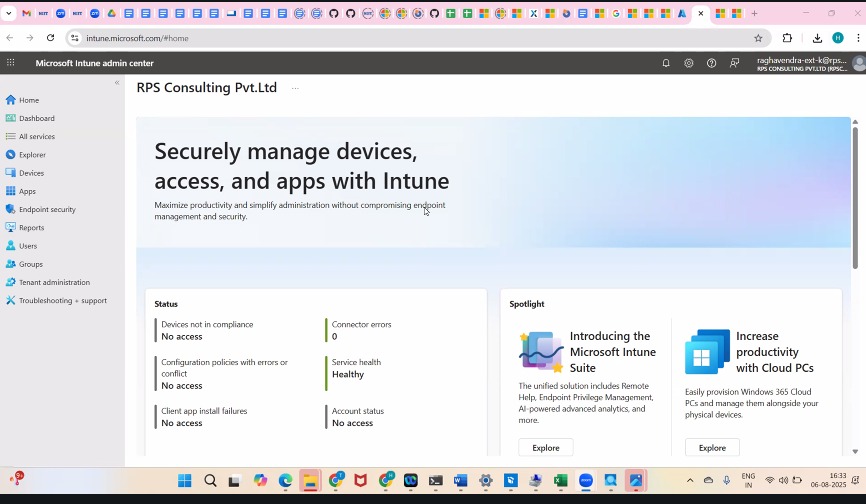
@ = "MyApp"

StubPath = "msiexec.exe /qb /i C:\Path\To\MyInstall.msi"

Version = "1,0,0"

**# 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.