**Name**: Harsh Kumar

**Email**: [hs150harsh@gmail.com](mailto:hs150harsh@gmail.com)

***Assignment -2***

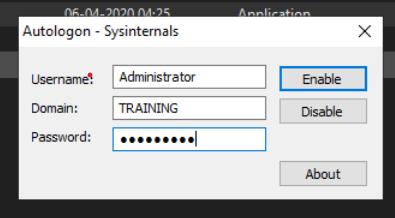
***Using Windows tools for Debugging LogonSessions, Autologon, Process Explorer , Psexec, PSTools, RegMon, Whois, SysMon***

*SysInternals tools are valuable for troubleshooting and security analysis on Windows system. It is legendary suite of Advanced System Utilities. It’s a go-to toolkit for IT pros, developers, and power users who want to diagnose, troubleshoot, and monitor Windows systems at a deep level.*

*Here is a detailed look at each tool:*

***1. Autologon***

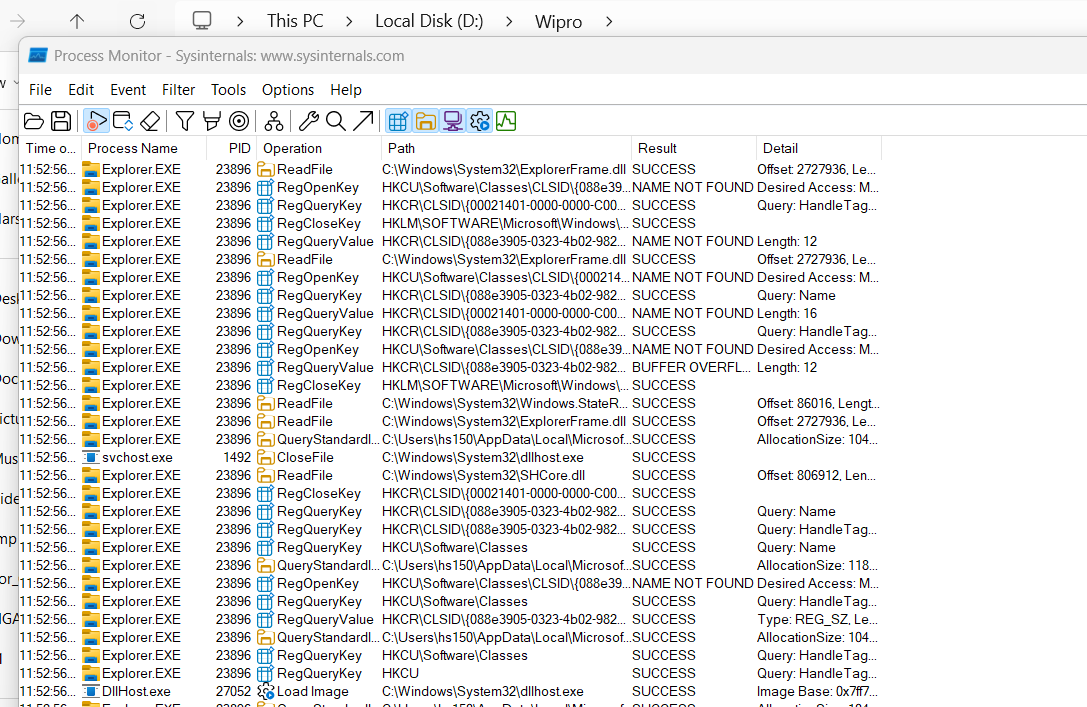
* ***Purpose:*** *Automates the Windows login process.*
* ***Functionality:*** *Provides a graphical user interface to configure registry settings, enabling automatic logon for a specified user using stored credentials.*
* ***Typical Use Cases:*** *Ideal for headless systems, kiosk setups, or automated testing environments where manual login is impractical.*

** *A screenshot of a computer error

AI-generated content may be incorrect.*

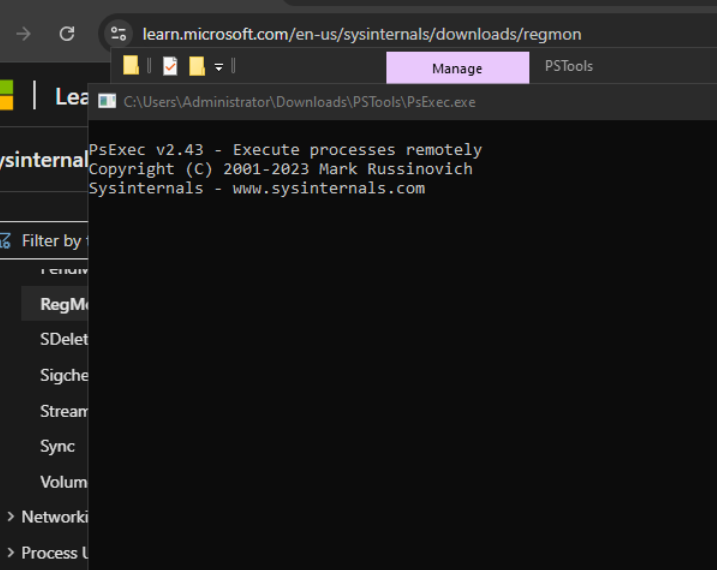
***2. Process Explorer***

* ***Purpose:*** *Advanced tool for monitoring and managing running processes.*
* ***Functionality:*** *Offers real-time, in-depth details about active processes, including memory usage, handles, threads, and open files.*
* ***Typical Use Cases:*** *Essential for troubleshooting applications, identifying performance issues, and investigating potential malware activity.*

**

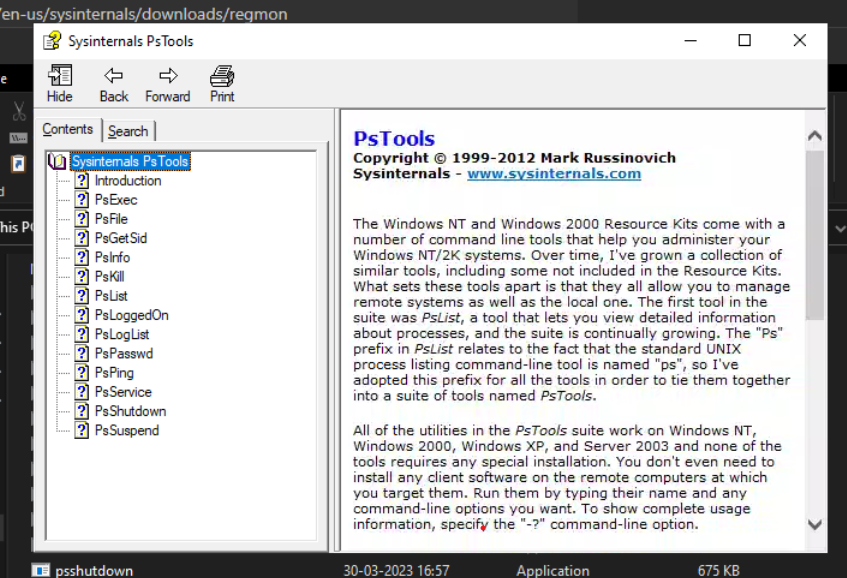
***3. PsExec***

* ***Purpose:*** *Facilitates remote execution of commands and applications.*
* ***Functionality:*** *Allows administrators to launch programs or run command-line utilities on remote systems as if they were being executed locally.*
* ***Typical Use Cases:*** *Remote administration, software deployment, patch management, and troubleshooting across systems.*

**

***4. PSTools Suite***

* ***Purpose:*** *Collection of lightweight command-line utilities for Windows system administration.*
* ***Functionality:*** *Includes tools like PsLoggedOn, PsFile, and PsList, which provide insights into user sessions, open files, process lists, and more.*
* ***Typical Use Cases:*** *Broad administrative tasks on both local and remote computers.*

**

***5. RegMon***

* ***Purpose:*** *Real-time registry monitoring utility.*
* ***Functionality:*** *Tracks registry reads, writes, deletes, and other activities live as they occur.*
* ***Typical Use Cases:*** *Troubleshooting registry problems, identifying changes made by applications, and investigating security issues.*

***REGMON SUPPORT ENDED SO I CAN’T USE IT ANYMORE***

***6. Sysmon***

* ***Purpose:*** *System service and driver for advanced system monitoring and auditing.*
* ***Functionality:*** *Logs detailed information about process creation, network connections, and file modifications to the Windows event log.*
* ***Typical Use Cases:*** *Security monitoring, intrusion detection, forensic investigations, and compliance auditing.*

***7. Whois***

* ***Purpose:*** *Queries and retrieves registration details for domain names and IP addresses.*
* ***Functionality:*** *Uses the command line to access Whois databases and return domain ownership and registration information.*
* ***Typical Use Cases:*** *Network troubleshooting, validating domain ownership, and assessing domain availability.*

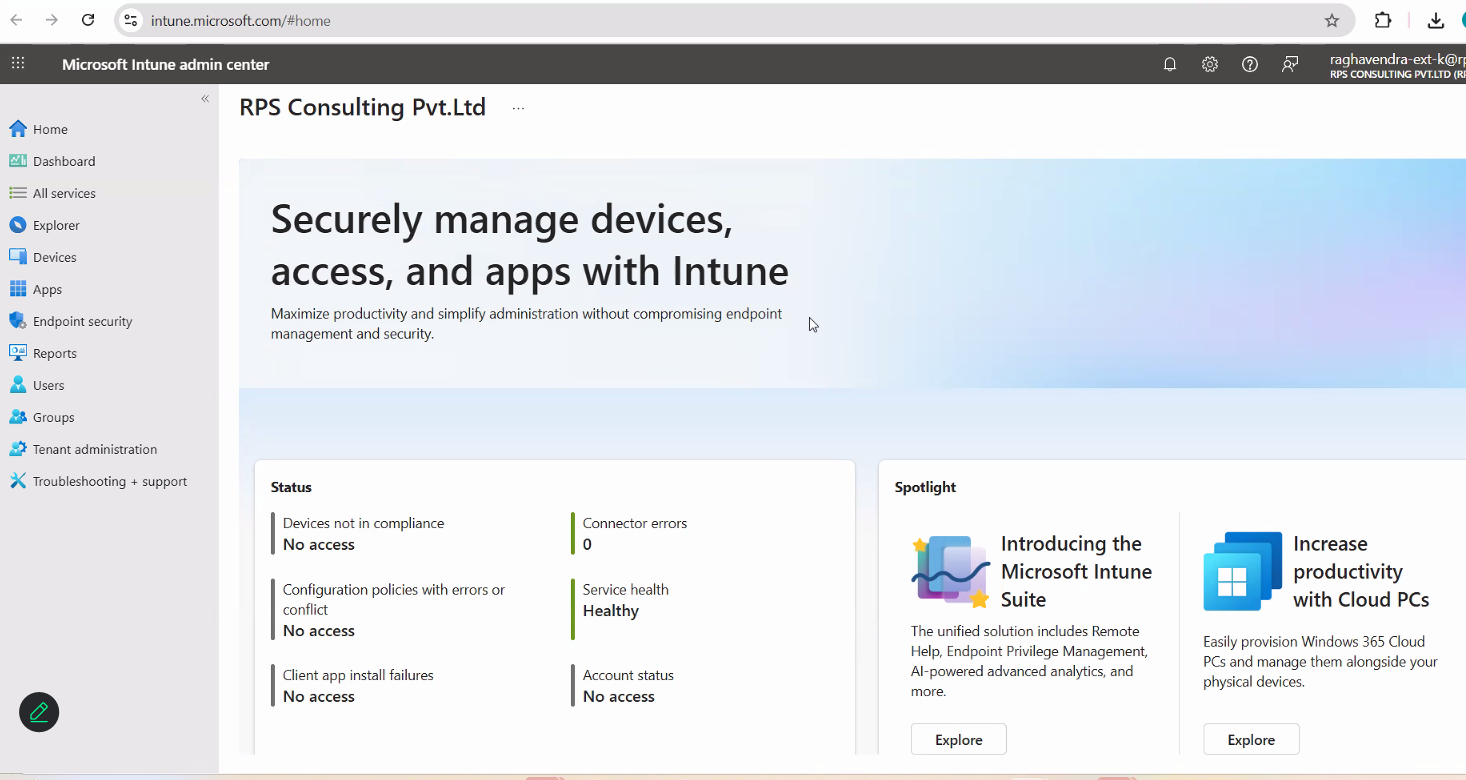
***Microsoft Intune***

* *Microsoft Intune, a pivotal cloud-based service for mobile device management (MDM) and mobile application management (MAM)*
* *It enables organizations to manage both the devices employees use to access company data and the applications they use in their day-to-day work.*
* *It integrates seamlessly with Azure Active Directory and Azure Information Protection, offering a holistic approach to device, application, and data management.*

***Steps to create a Microsoft Intune account***

1. *Set up Microsoft Intune*
2. Sign up for Microsoft Intune
3. Configure a custom domain name for your Intune tenant
4. Add users to Intune
5. Create groups in Intune
6. Manage licenses
7. Manage Roles and grant admin permissions for Intune
8. Set the mobile device management authority
9. Customize the Intune company portal

**This is how it will look after setting up**

****