### **Windows Enumeration using Sysinternals Tools**

Agasthya P CH.EN.U4CYS22004

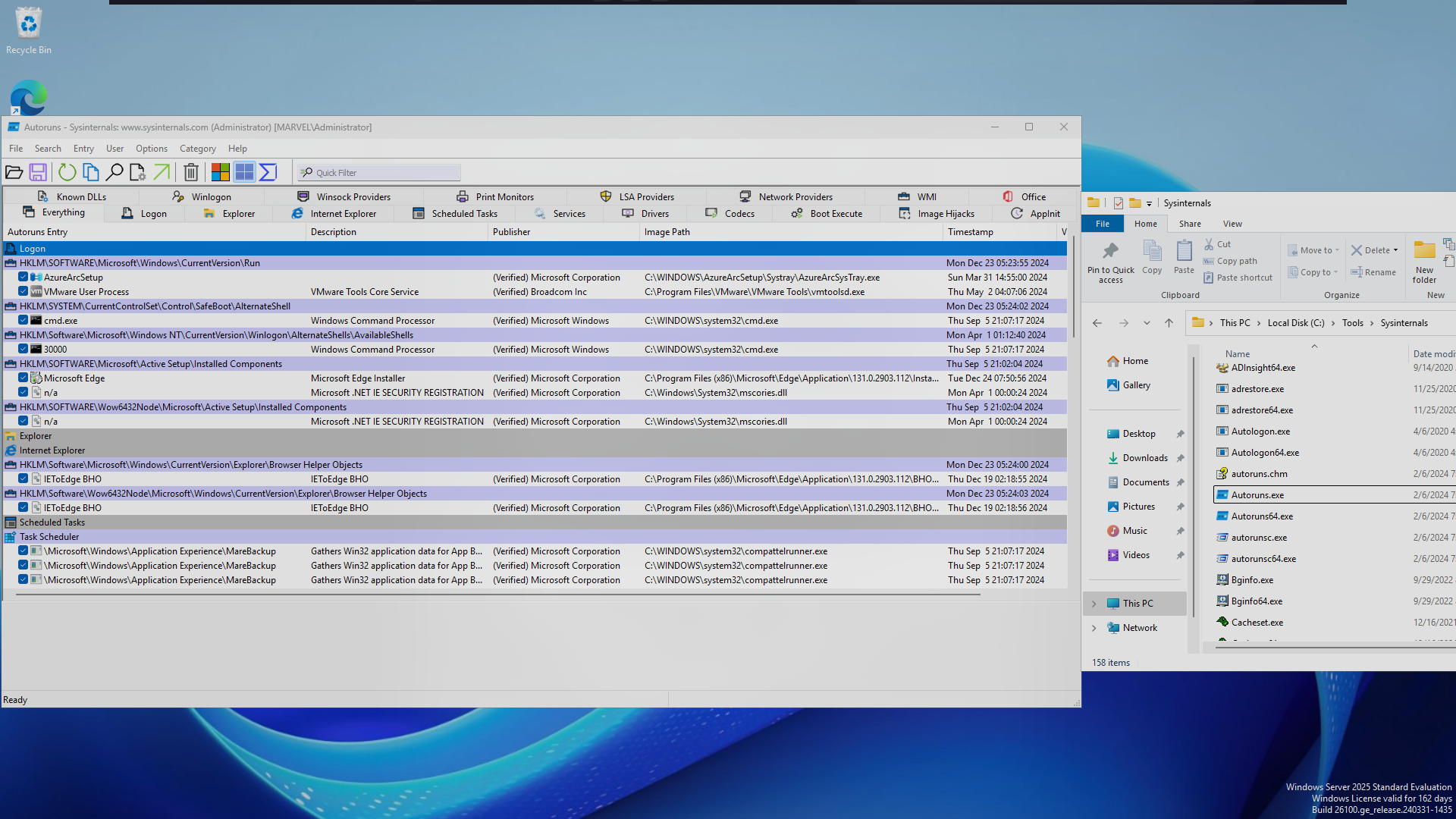
#### **Tools Overview**

Sysinternals Suite is a collection of advanced utilities to manage, diagnose, troubleshoot, and monitor Windows systems. For this experiment, we will use:

1. **Process Explorer** (Process Category)
2. **TCPView** (Network Category)

#### **Installation Steps**

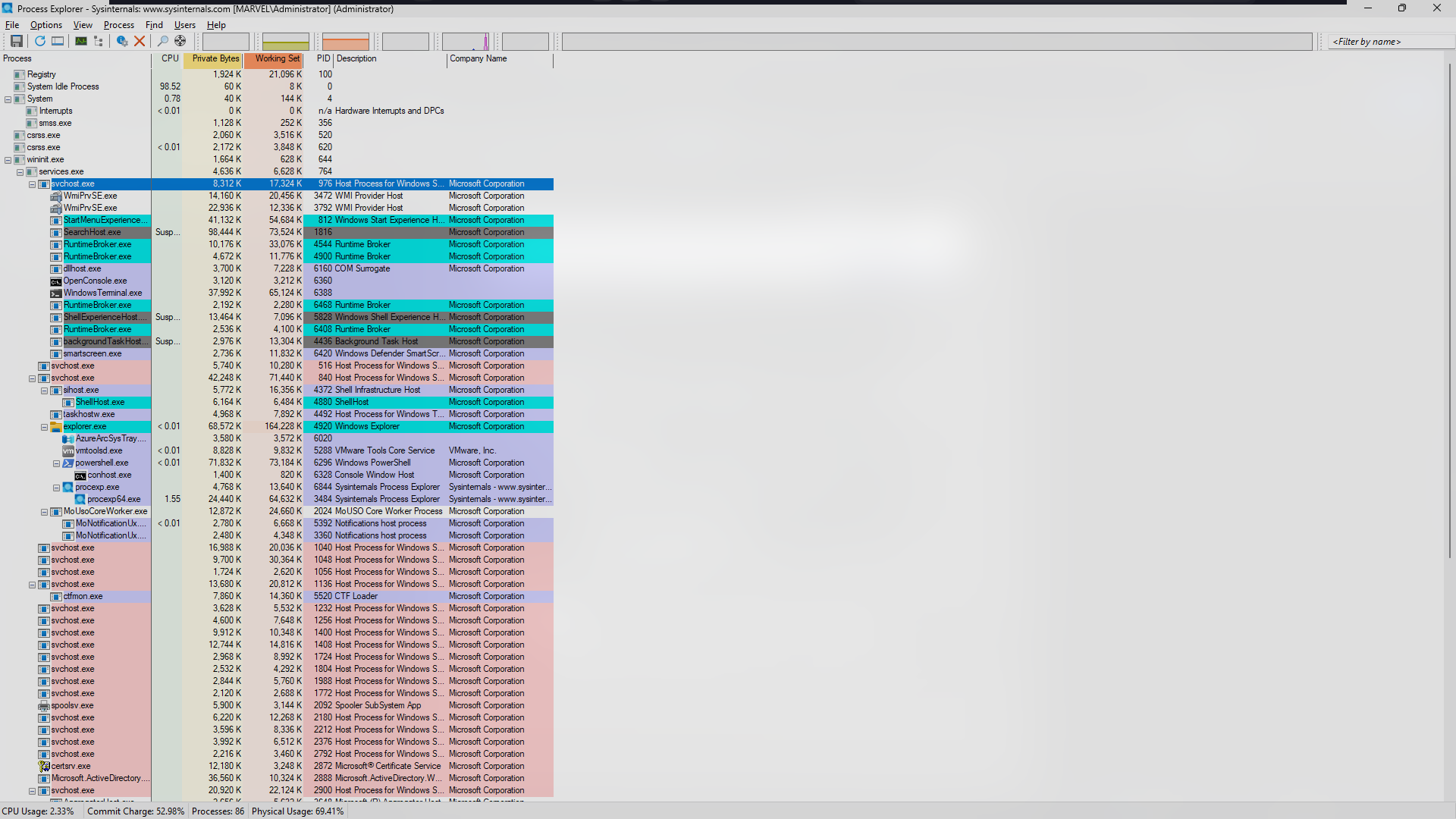
1. Download Sysinternals Suite from the official Microsoft website: <https://learn.microsoft.com/en-us/sysinternals/downloads/>
2. Extract the downloaded ZIP file to a desired folder (e.g., C:\Sysinternals).
3. Open the folder and run the tools as needed (most tools require administrator privileges).



#### **Usage**

##### **1. Process Explorer**

* **Purpose**: Displays detailed information about processes running on a system.
* **How to Use**:
  + Navigate to the extracted Sysinternals folder and run procexp.exe.
  + Grant administrator permissions if prompted.
  + Analyze running processes, including:
    - Parent-child relationships.
    - Memory and CPU usage.
    - DLLs loaded by a process.
    - Kill unwanted processes by right-clicking and selecting Kill Process.



##### **2. TCPView**

* **Purpose**: Monitors TCP and UDP endpoints on the system.
* **How to Use**:
  + Navigate to the Sysinternals folder and run tcpview.exe.
  + Review active network connections, including:
    - Local and remote addresses.
    - Connection states (LISTENING, ESTABLISHED, etc.).
    - Protocol type (TCP/UDP).
  + Identify suspicious connections and terminate them by right-clicking and selecting Close Connection.

