Date: May 10, 2022 (Eastern Daylight Time)

SysInternals Suite - Guide

Description:

Microsoft Sysinternals is essentially a suite of tools which help in administration, management, monitoring and many other tasks on a Windows environment. It is a freeware comprising of 70+ tools. It was developed by Mark Russinovich and Bryce Cogwell at Winternal Software, before Microsoft acquired it in 2006 and renamed it to SysInternals Suite.

Important Tools of SysInternals:

These are few of the most popular tools of Sysinternals.

1. ProcessExplorer:

   Provides detailed information about workings of applications in a Windows environment including but not limited to: processes, threads, handles, Dynamic Link Libraries, etc. Also shows the resource consumption on a Windows System, can view in-memory strings, view security priviledges of processes.
   A better and more holistic alternative to Task Manager.

2. Procmon:

   Process Monitor (ProcMon), is a system wide monitoring tool. Can capture real time snapshots of the file system, registry activity and process activity. Can capture user and session id's, image paths, cmd activity, etc. Powerful tool for malware analysis.

3. Sysmon:

   System Monitor (SysMon) is used for advanced monitoring of a Windows System. Registered as a System Service and Device Driver (bootstart) on a system. Identifies malware, intrusions, and breaches within a network. Logs process creations, network communication ,file modification, and DLL's. Configuration file can be bespoke per use case.

4. AutoRuns:

   Finds all auto start applications or services in a Windows environment. Covers more sources beyond typical utilities. Available in GUI and as a command-line service (Autorunssc). Allows deletion of entries along with an option to disable them. Supports Virus Total checks.

5. PsExec:

   It is a Remote execution utility. Has the ability to launch interactive command prompts and execute programs. Creates a service and named pipe, PsExecSvc, on the remote system. Requires SMB, File and Print sharing, and the Admin share on the remote system.
   Syntax: Psexec \\192.168.0.109 –u Name –p P@assword123 ipconfig
   This will return the output of 'ipconfig' on the specified host if permissions are granted.

Date: May 10, 2022 (Eastern Daylight Time)

Other Useful Tools:

6. TcpView : Enumerate all TCP/UDP endpoints on a workstation in detail
7. PsLoggedOn, LogonSessions : Helps identify local and remote log ons.
8. sDelete : Secure Delete
9. Sigcheck : Finds file signature
10. Streams: Analyze ADS (Alternate Data Streams) of Files and deletes streams from file. Streams are commonly used to hide malicious commands.

Installation:

Steps:

1. Go to https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite
2. Download and save file
3. Right click on downloaded .zip and click on extract
4. Extract folder contents to any location in C: drive, preferably in Program Files, as a folder named SysInternals

Optional Step:

Copy path of the extracted folder SysInternals and then save it to an environment variable. This will make it possible to access SysInternals Tools from the command line.

Usage:

1. Debugging Applications
2. Dynamic Malware Analysis
3. Securely Auditing PCs
4. Malware Hunting
5. Analyze, Diagnose and Optimize Windows.
6. Windows Security