Global Information Security Society for Professionals of Pakistan

Topic: Microsoft Sysinternals: What Is It?

Speaker: Syed Hasan (DFIR)

What Is Microsoft's Sysinternals?

- Suite of tools
- Assist in administration, management, monitoring, and many other tasks on a Windows environment
- Freeware comprising over 70+ free tools
- Developed by Mark Russinovich and Bryce Cogwell at Winternals Software
- Acquired by Microsoft in 2006 and renamed to "Sysinternals"
- Available for downloads at Microsoft's TechNet website

Must-know Tools from Sysinternals

- ProcessExplorer
- Procmon
- Sysmon
- AutoRuns
- PsExec
- TcpView
- PsLoggedOn, LogonSessions
- sDelete
- Sigcheck
- Streams

ProcessExplorer

- Provides detailed information about workings of applications in a Windows environment
- Processes, handles, threads, DLLs, etc.
- Resource consumption on a Windows system
- View in-memory strings of processes
- View security privileges assigned to Processes
- Check process hash on VirusTotal
- Alternative of Windows Task Manager

ProcMon or “Process Monitor”

- System-wide monitoring tool
- Capture real-time filesystem, registry, and process activity on a system
- Capture processes, image paths, command line, user and session IDs, and much more
- Powerful filtering capabilities (non-destructive)
- Excellent for troubleshooting, dynamic malware analysis, and malware hunting

Sysmon or “System Monitor”

- Advanced monitoring of a Windows system
- Registered as a System Service and Device Driver (boot start) on a system
- Identify malware, intrusions, and breaches within a network
- Log process creations, network communication, file modification, and DLLs
- Install Sysmon with a configuration file (good profiles are available on GitHub)
- A new channel is created for Sysmon under “Applications and Services Logs”
- Forward events to a centralized logging system for better monitoring

AutoRuns

- Find all auto-start applications or services in a Windows environment
- Covers more sources beyond typical utilities
- Optional feature to hide (signed) Microsoft auto-start binaries
- Available in GUI and as a command-line service (Autorunssc)
- Allows deletion of entries along with an option to disable them
- Supports VirusTotal checks

PsExec

- Remote execution utility
- 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
- A favorite for many threat groups as well!
- Example command:
  - Psexec \\192.168.0.109 –u Hasan –p P@assword123 ipconfig
    - This will return the output of 'ipconfig' on the specified host if permissions are granted

TcpView

- Enumerate all TCP/UDP endpoints on a workstation in detail
- Covers almost the same output as ‘netstat’ but in a presentable format
- Close unrecognized connections from the GUI
- Command-line version: tcpvcon

PsLoggedOn, LogonSessions

- PsLoggedOn can help identify local and remote logons (resource shares) on a system
- Allows user-based searching in environment for all logons
- LogonSessions returns a list of active logon sessions
- Also has the capabilities to return processes from each session
- Useful in Forensic investigations to identify active logons on a system

SDelete or “Secure Delete”

- Technically, data isn’t deleted when you press “Delete” but marked as free
- Forensic tools can still recover data from the filesystem
- Ensure secure deletion of files by using SDelete
- Used for handling of classified information
- Also utilized by threat actors to wipe malware after execution
- Detailed working is available on Microsoft’s SDelete documentation

Sigcheck

- Find versions, timestamps, and signature details of files
- Find unsigned files on the file system
- Submit files to VirusTotal
- Example commands:
  - Sigcheck.exe –u –vt C:\Windows\System32
    - Search for unsigned files and search them against VT's database

Streams

- Analyze Alternate Data Streams (ADS) of files
- Delete streams from files
- Streams are commonly utilized by malware authors to hide suspicious commands

Thank you.