🔧 Tools POC – PsSuspend & PsTools

🧑 Intern Details

- **Name:** Atul Singh Chandel
- **Intern ID:** 442

🛠 Tool Name

PsSuspend & PsTools

📚 History

PsTools is a powerful suite of system utilities developed by **Mark Russinovich** under **Sysinternals**, now maintained by **Microsoft**. These tools provide command-line utilities for managing local and remote Windows systems.
PsSuspend, one of the tools, allows temporary suspension of any running process, preserving its state in memory without killing it.

📄 Description

The PsTools suite enables system administrators and security professionals to interact with system-level processes.
PsSuspend freezes a process without termination, making it valuable for live incident response and memory analysis. It is often used in conjunction with tasklist, taskkill, and other process management tools.

📌 What Is This Tool About?

- **PsSuspend** suspends a process (by name or PID) without affecting its memory.
- It is used for **forensics**, **threat isolation**, and **system troubleshooting**.
- PsTools offers a broader range of system-level commands for remote control and automation.

⭐ Key Characteristics / Features

- Portable – no installation required
- Suspend process without termination
- Requires Administrator privileges
- Fully command-line interface (CLI)

- Works on Windows 7–11 and Server OS
- Compatible with remote systems
- Useful for malware isolation and live memory analysis
- Supports process filtering by name or PID
- Often used by SOC teams
- Integrated into automation and scripting workflows
- Minimal resource consumption
- Verified and signed by Microsoft
- CLI output is script-friendly
- No .NET or PowerShell dependencies
- Trusted in DFIR (Digital Forensics & Incident Response)

🔧 Types / Modules Available in PsTools

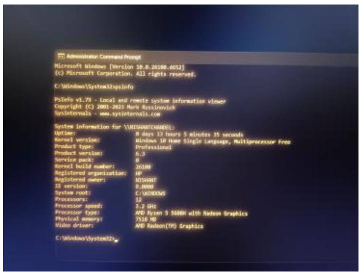
- **PsExec** – Remote process execution
- **PsSuspend** – Suspend running processes
- **PsList** – List running processes
- **PsKill** – Terminate processes
- **PsInfo** – System information
- **PsShutdown** – Remote shutdown/restart
- **PsLoggedOn** – Check logged-on users
- **PsService** – Control system services

🎯 How Will This Tool Help?

- Suspend potentially malicious processes **without losing evidence**
- Reduce system load during triage
- Maintain the state of malware for memory analysis
- Use during forensic acquisition or RAM dump
- Automate containment via batch or PowerShell

🖼 Proof of Concept (PoC) Images

📸 Screenshots below show real-world usage:



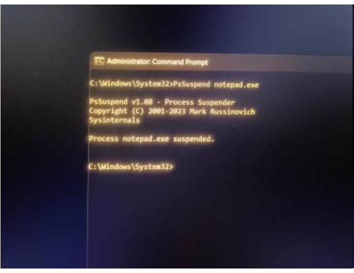
```
Microsoft Windows [Version 10.0.26100.4652]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>psinfo

PsInfo v1.79 - Local and remote system information viewer
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

System information for \\NISHANTCHANDEL:
Uptime:                    0 days 13 hours 5 minutes 35 seconds
Kernel version:            Windows 10 Home Single Language, Multiprocessor Free
Product type:              Professional
Product version:           6.3
Service pack:              0
Kernel build number:       26100
Registered organization:   HP
Registered owner:          NISHANT
IE version:                9.0000
System root:               C:\WINDOWS
Processors:                12
Processor speed:           3.2 GHz
Processor type:            AMD Ryzen 5 5600H with Radeon Graphics
Physical memory:           7510 MB
Video driver:              AMD Radeon(TM) Graphics

C:\Windows\System32>
```

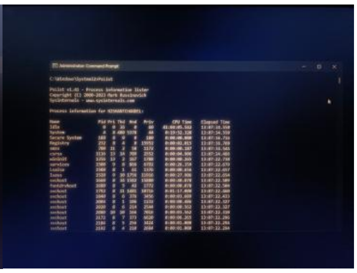


```
C:\Windows\System32>PsSuspend notepad.exe

PsSuspend v1.08 - Process Suspender
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals

Process notepad.exe suspended.


C:\Windows\System32>
```



```
C:\Windows\System32>PsList

PsList v1.41 - Process information lister
Copyright (C) 2000-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for NISHANTCHANDEL:

Name                Pid Pri Thd  Hnd   Priv        CPU Time    Elapsed Time
Idle                  0   0  20    0     60   41:00:05.502    13:07:18.550
System                4   8 480 5378     44    0:19:52.328    13:07:34.550
Secure System       160   8   9    0    180    0:00:00.000    13:07:16.718
Registry            232   8   4    0  15951    0:00:01.015    13:07:16.709
smss                708  11   2   58   1172    0:00:00.187    13:07:16.565
csrss              1136  13  14  708   2552    0:00:04.906    13:07:14.460
wininit            1156  13   2  167   1708    0:00:00.265    13:07:12.718
services           1500   9   8  806   6792    0:00:28.358    13:07:12.670
LsaIso             1568   8   1   61   1376    0:00:00.016    13:07:12.657
lsass              1528   9  10 1758  11956    0:00:27.906    13:07:12.654
svchost            1660   8  16 1502  15080    0:00:08.078    13:07:12.509
fontdrvhost        1680   8   5   42   1772    0:00:00.078    13:07:12.500
svchost            1792   8  11 1401  18716    0:01:17.000    13:07:12.488
svchost            1040   8   6  376   3456    0:00:03.609    13:07:12.433
svchost            2084   8   1  106   1132    0:00:00.406    13:07:12.327
svchost            2020   8   6  214   2544    0:00:00.562    13:07:12.327
svchost            2080  10  10  266   7052    0:00:03.562    13:07:12.330
svchost            2172   8   7  373   6620    0:00:00.265    13:07:12.296
svchost            2184   8   9  294   3024    0:00:01.000    13:07:12.286
svchost            2182   8   4  218   2084    0:00:01.000    13:07:12.284
```

1. **PsList** – Listing running processes
2. **PsSuspend** – Suspending a target process
3. **PsInfo** – Gathering system information

(Embed screenshots in final document PDF/DOCX when generating)

🧾 15-Liner Summary

1. Part of PsTools suite by Microsoft
2. CLI-based utility
3. Suspends processes by name or PID
4. Preserves state without killing
5. Works locally or remotely
6. Portable – no install needed
7. Useful in DFIR and SOC
8. Minimal footprint
9. Compatible with all Windows systems
10. Works with other tools like tasklist/taskkill
11. Does not resume processes
12. Trusted in enterprise environments
13. Batch/script integration friendly
14. Lightweight & secure
15. Maintained by Microsoft Sysinternals

⏱️ Time to Use / Best Case Scenarios

- During malware containment
- Before capturing memory dumps
- While analyzing suspicious processes

- In real-time incident response
- During post-breach analysis

🕵️ When to Use During Investigation

- Live memory forensics
- Process state preservation
- Ransomware or APT containment
- Pausing unauthorized or unknown processes
- Testing malware in sandboxed environments

👨‍💻 Best Person to Use & Skills Required

Best User: SOC Analyst / Incident Responder / Forensics Expert
Required Skills:

- Command-line proficiency
- Windows process and memory knowledge
- Familiarity with forensic tools and analysis
- Administrative privileges on system

🧩 Flaws / Suggestions to Improve

- No resume support for suspended processes
- No logging features or GUI interface
- Could benefit from live memory integration
- Often flagged by antivirus (due to misuse potential)
- No notification or rollback system

✅ Good About the Tools

- Fast and lightweight
- Microsoft trusted utility
- Easy to use in automated incident response
- Works on almost all Windows systems
- Very useful in live malware handling