VAIBHAV RATAN Intern ID- 441

🛠️ Tool Name: PsInfo

📄 Description:

PsInfo is a command-line utility developed by Microsoft Sysinternals that gathers and displays detailed information about a Windows system, including OS version, uptime, installed hotfixes, memory, disk, network configuration, and more.

📌 What Is This Tool About?

PsInfo is used for system diagnostics and quick asset discovery. It's useful in incident response and audits to rapidly profile system configurations and health.

⭐ Key Characteristics / Features:

1. Displays system uptime and install date
2. Lists memory and processor details
3. Shows disk volume information
4. Displays installed hotfixes and service packs
5. Shows networking info (IP, MAC, etc.)
6. Lists system boot time
7. Outputs directly to console or file
8. Runs remotely using PsExec
9. Lightweight and fast
10. No installation required
11. Part of the Sysinternals Suite
12. Digital signature verified
13. Supports CSV output for automation

14. Works on all Windows versions
15. Can be used in batch scripts

🔧 **Types / Modules Available:**

- CLI binary (psinfo.exe)
- Switches for targeting remote systems
- Filtering options (-s, -d, -h, etc.)
- Output formatting (-c for CSV)

🎯 **How Will This Tool Help?**

- Fast collection of system-level info during IR
- Helps in identifying compromised hosts
- Useful for profiling endpoints in bulk
- Enables forensic triage without GUI
- Supports automation in scripts

🖼️ **Proof of Concept (PoC) Images:**

```
C:\Users\Asus>psinfo.exe

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

System information for \\TUF-A15:
Uptime:                    0 days 1 hour 42 minutes 16 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:
Registered owner:          Asus
IE version:                9.0000
System root:               C:\WINDOWS
Processors:                16
Processor speed:           3.0 GHz
Processor type:            AMD Ryzen 7 7435HS
Physical memory:           16202 MB
Video driver:              NVIDIA GeForce RTX 3050 Laptop GPU
```

📜 **15-Liner Summary:**

1. CLI tool to collect Windows system info
2. Lists OS version, memory, hotfixes
3. Shows disk, uptime, and boot time
4. Includes network configuration
5. No installation required
6. Portable and scriptable
7. Part of Sysinternals Suite
8. Great for IR and audits
9. Supports remote use with PsExec
10. Output in table or CSV
11. Very fast and lightweight
12. Useful in forensics and IT asset checks
13. Works across Windows OS
14. Minimal resource usage
15. Microsoft-signed binary

⏱️ **Time to Use / Best Case Scenarios:**

- Initial incident triage
- Profiling systems in a network
- Baseline system info during audits
- Lightweight footprint scans

🕵️ When to Use During Investigation:

- First step in IR when approaching a machine
- During enumeration of affected systems
- To collect system facts for case reports
- When analyzing rogue/misconfigured endpoints

👨‍💻 Best Person to Use & Required Skills:

Best User: SOC Analyst / IR Specialist / IT Auditor
Skills Needed:

- Basic Windows CLI usage
- Familiarity with system internals
- Understanding system artifacts (hotfixes, memory, etc.)
- Batch scripting skills (for automation)

🧩 Flaws / Suggestions to Improve:

- No GUI interface
- Does not export directly to PDF
- Can’t parse WMI in depth
- No Linux version
- Add JSON output for better integration
- Include user login history if possible

✅ Good About the Tool:

- Fast, portable, and free
- No install required

- Works well on all Windows systems
- Simple output
- Reliable for bulk endpoint scanning
- Great for scripting and integration