Digisuraksha Cyber Security Internship

Name : Nikhil Saini

Intern id: 440

## **Tool Name**: PsLoddedOn

## **History: Tool Name**

**PsLoggedOn** is part of the **Sysinternals PsTools Suite**, developed by **Mark Russinovich** and **Bryce Cogswell**. Originally created to assist system administrators in monitoring Windows environments, the tool has become a standard in live forensic analysis, enabling analysts to identify active user sessions, both local and remote.

## **Description:**

**PsLoggedOn** is a command-line tool that displays users currently logged into a system either **locally** or **through resource shares** (SMB sessions). It helps system admins and forensic investigators understand who is actively using or accessing a system at any given point in time.

## **What Is This Tool About?**

**PsLoggedOn** is designed to show which users are logged into a system and how — either locally (via keyboard/mouse) or remotely (via shared resources such as SMB or administrative shares). This information is essential in **incident response**, **live forensics**, and **lateral movement detection**.

## **Key Characteristics / Features:**

1. Lightweight executable (no installation)
2. Shows local logins and network-based access (SMB)
3. Part of Sysinternals Suite
4. CLI-based, easy scripting support
5. Works with Windows NT and above
6. Remote scan (via IP/hostname)
7. Minimal system resource usage
8. Supports auditing of user presence during red-team attacks
9. Does not require agent installation on target system
10. Fast execution and instant results

## **Types / Modules Available:**

* **Local Scan**: Lists users logged on locally.
* **Remote Scan**: Lists users logged into a remote system via:
  + Network shares (SMB)
  + Remote desktop sessions (if active)

## **How to Setup:**

### **▶ On Windows 11:**

1. Download the Sysinternals Suite
2. Extract the contents to: C:\SysinternalsSuite
3. Open cmd.exe as Administrator
4. Run the tool by applying below command on cmd:

cd C:\SysinternalsSuite  
PsLoggedOn.exe  
PsLoggedOn.exe \\<Remote-IP>

### **▶ On Kali Linux (for testing remote access):**

1. Ensure SMB client is installed:
2. On terminal Run Below command to install smbclient

sudo apt install smbclient

1. Access shared folders on Windows:

smbclient -L //192.168.29.44 -U Nikhil --option="client min protocol=SMB2"

smbclient //192.168.29.44/test -U Nikhil

## **How Will This Tool Help?**

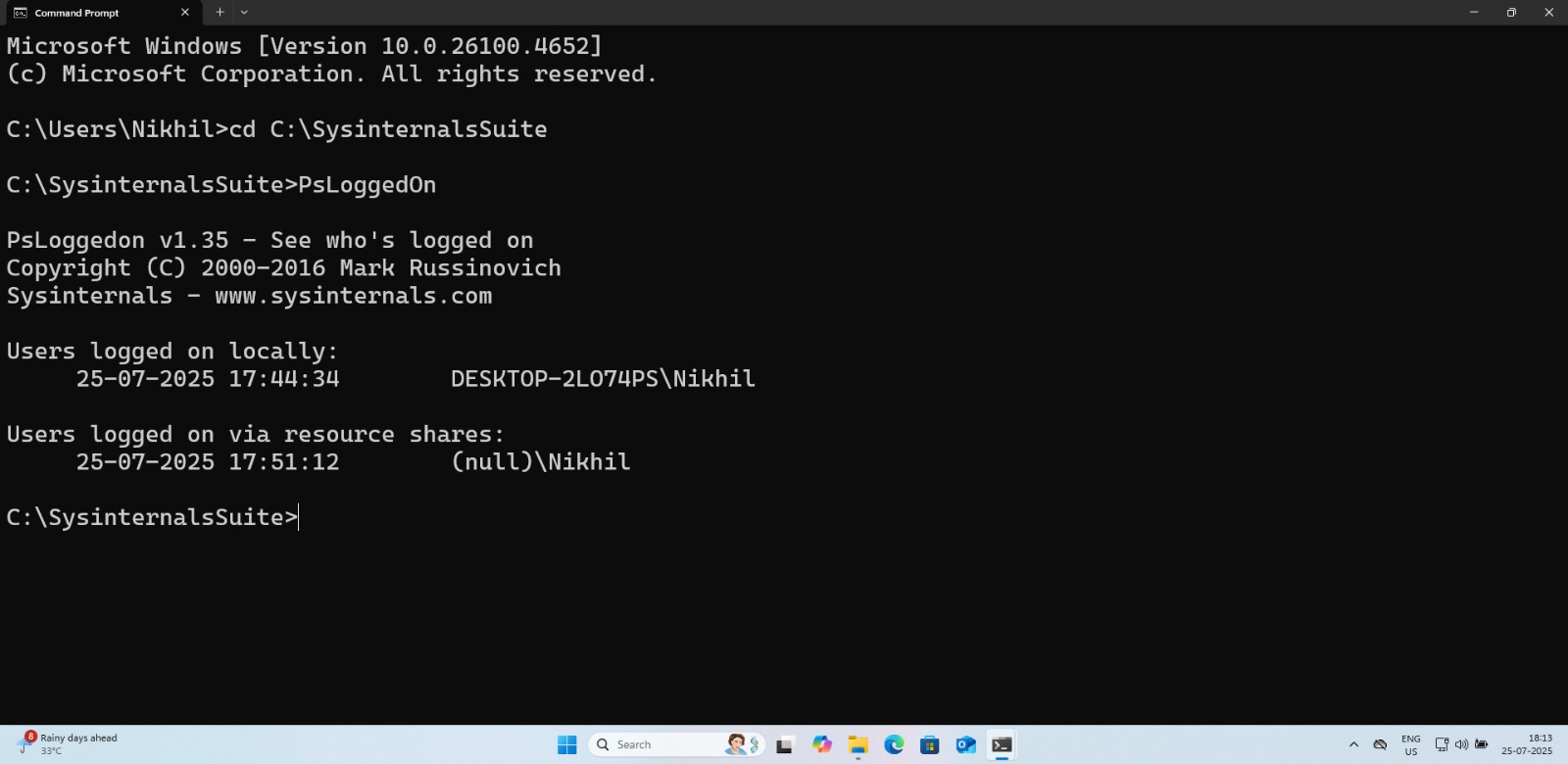
* Detects if unauthorized users are logged in
* Verifies remote sessions over SMB
* Identifies interactive logins versus remote access
* Helps with **incident response**, **red team monitoring**, and **forensic evidence collection**
* Complements lateral movement tracking tools (e.g., SMB relay detection)

## **Proof of Concept (PoC):**

### **Scenario:**

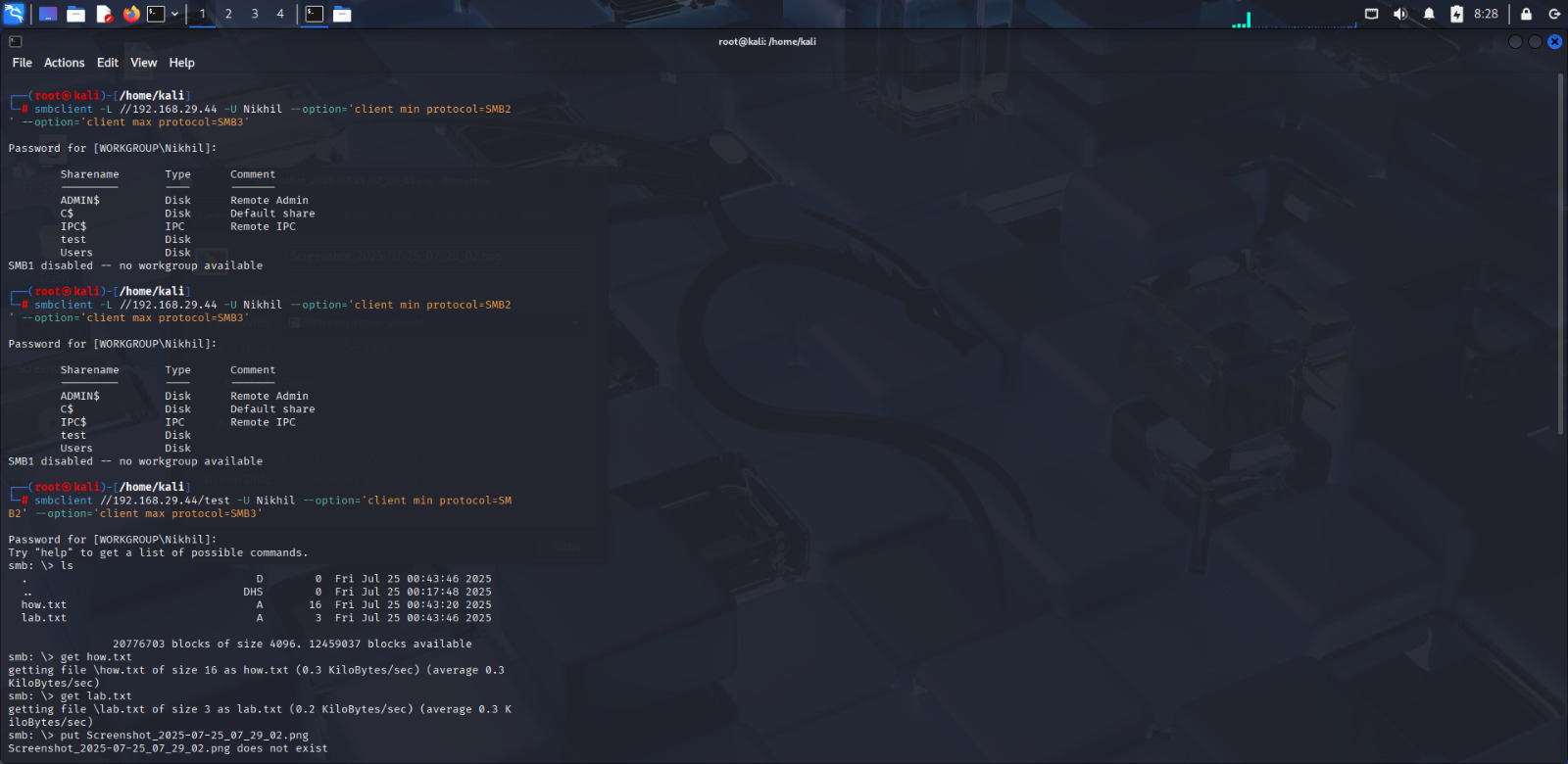
* Kali initiates SMB access to Windows 11 machine
* Windows logs access under “Users logged on via resource shares”

### **Windows cmd Input:**



**Kali Linux Command:**

smbclient -L //192.168.29.44 -U Nikhil --option="client min protocol=SMB2"

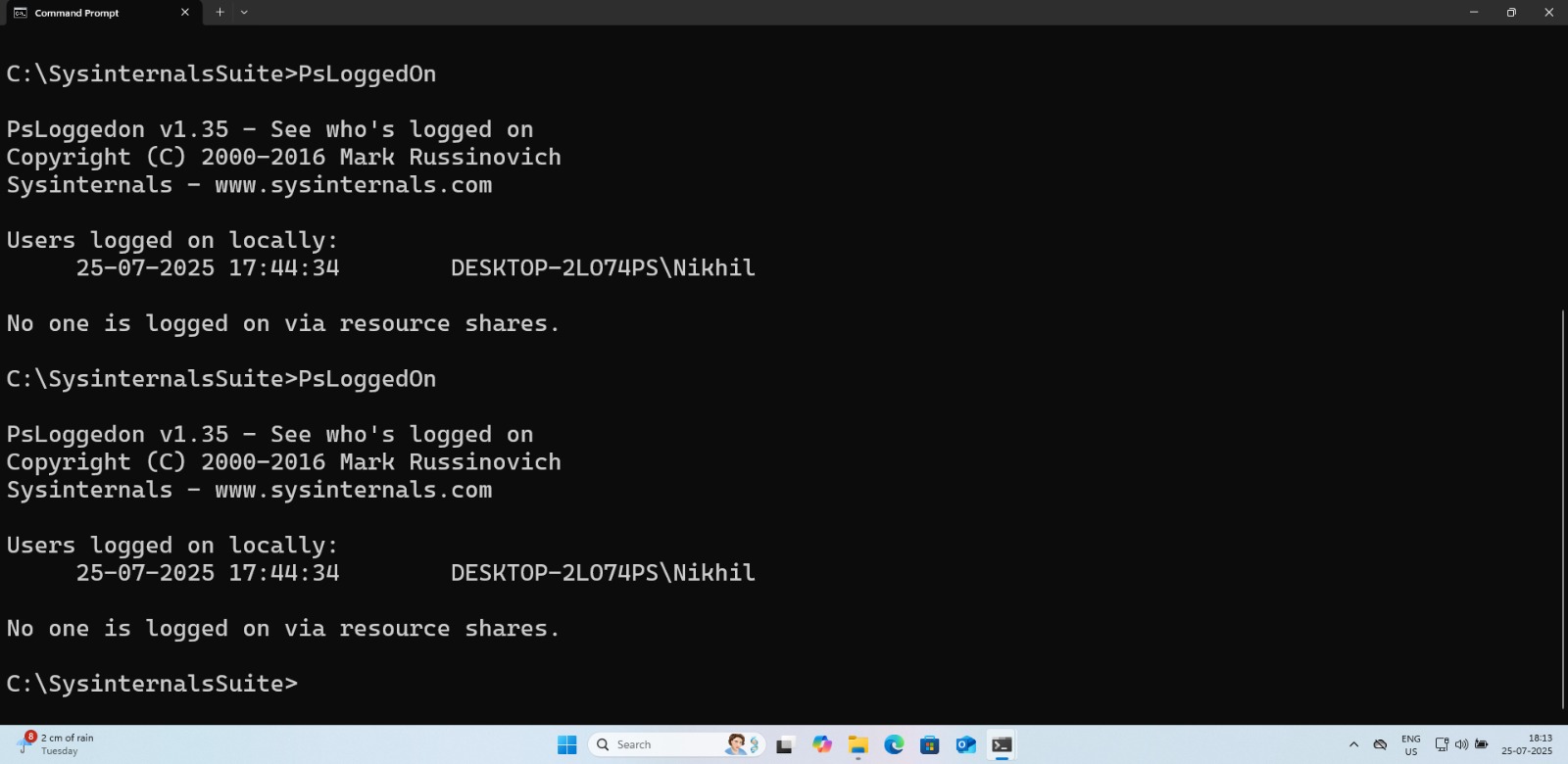


### **Windows CMD Output:**

PsLoggedOn

Users logged on locally: DESKTOP-2LO74PS\Nikhil

Users logged on via resource shares: WORKGROUP\Nikhil



## **Summary:**

1. CLI-based tool for user session auditing
2. Part of the Microsoft Sysinternals Suite
3. Detects both local and remote logins
4. No installation needed
5. Works from local or remote context
6. Shows users via SMB share activity
7. Requires administrative privilege for remote queries
8. Outputs real-time results
9. Useful in forensics, IR, and IT admin work
10. Lightweight, fast, and portable
11. Ideal for lateral movement tracing
12. CLI-only interface (good for scripting)
13. Can integrate with other PsTools
14. Maintained by Microsoft
15. Trusted tool in enterprise environments

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

* During **live incident response** to verify active sessions
* While investigating **unauthorized SMB access**
* When checking for **remote persistence or backdoor logins**
* During red team/blue team exercises
* In forensic triage after detecting anomalies

## **When to Use During Investigation:**

* During or right after a breach
* When analyzing potential lateral movement
* While collecting volatile system information
* When verifying which accounts were active during a compromise
* For validating if shared credentials are actively in use

## **Best Person to Use This Tool & Required Skills:**

### **Best User:**

* SOC Analysts
* Incident Responders
* Digital Forensics Experts
* System Administrators

### **Required Skills:**

* Familiarity with Windows internals
* Basic command-line usage
* Understanding of SMB and network share protocols
* Privilege management in Windows
* Forensic investigation fundamentals

## **Flaws / Suggestions to Improve:**

|  |  |
| --- | --- |
| **Flaw** | **Suggestion** |
| No session duration info | Add timestamps and duration tracking |
| No logging/export capability | Allow results to be exported to CSV/JSON |
| Basic output only | Provide rich metadata like source IP/user type |
| Requires Admin for remote | Introduce limited-info mode without admin rights |

## **Good About the Tool:**

* Free and maintained by Microsoft
* Fast and lightweight
* Portable and easy to run
* No dependencies or installation needed
* Excellent integration with other Sysinternals tools
* Real-time insights during live forensic sessions
* Highly useful in red-team/blue-team scenarios
* Perfect for security and IT operations environments