**DIGISURAKSHA PARHARI FOUNDATION INTERNSHIP-2025**

**Week-1:POC on AutoLogons and LogonSessions Tools ID-257258**

**Name-Girija Shankar Sahoo Intern ID-444**

**AutoLogon : Introduction**

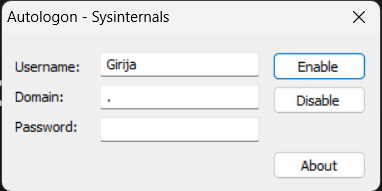
Autologon enables you to easily configure Windows built-in autologon mechanism. Instead of waiting for a user to enter their name and password, Windows used the credentials you enter with Autologon, which are encrypted in the Registry, to log on the Specified User automatically.

This tool is a free utility tool from Microsoft.

**Key Features Of AutoLogon:**

* Its core function is to bypass the manual login screen by automatically submitting stored credentials when Windows starts.
* The interface is so simple that is consist of just three fields “Username”, “Domain” and “Password”.
* When you enable AutoLogon, it does not store your password in plain text. The password is encrypted before being saved in the Windows Registry.
* For automation and scripting purposes, AutoLogon can be configured via the command line. This is a powerful feature for system administrators who need to deploy settings across multiple matchines. The Systax is -  
  [“autologon.exe <username> <domain> <password>”]
* It is very Light weight and portable.

**How to Use AutoLogon :**

* Download the executable file from “[Autologon - Sysinternals | Microsoft Learn](https://learn.microsoft.com/en-us/sysinternals/downloads/autologon)”.
* Run the Executable file.
* Write the Username, Domain
* Click Enable

**Drawbacks of AutoLogon:**

* While AutoLogon offers convenience, it is essential to be aware of the security risks involved. Although the password is encrypted in the Registry, a user with administrative privileges on the local machine can easily retrieve and decrypt it.

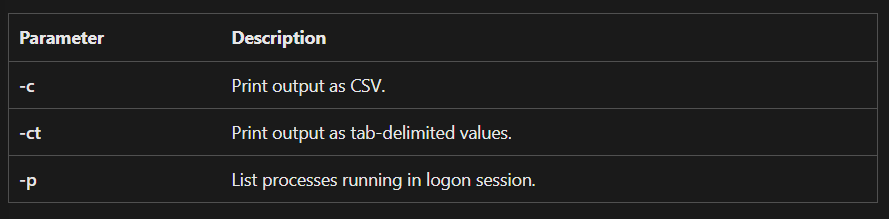
**Where can we use the AutoLogon features:**

1. Standalone machines in a secure location: For example, a computer in a locked office or a dedicated machine for a specific task where unauthorized physical access is highly unlikely.
2. **Kiosk systems:** Computers that are dedicated to a single application and are in a controlled environment.
3. **Test environments:** Where convenience for developers or testers outweighs the security risks.

**Logon Sessions :**

If you think that when you logon to a system there’s only one active logon session, this utility will surprise you. It list the currently active logon sessions and if you specify the -p option, the processes running in each session.

Usasge: logonsessions [-c[t]] [-p]



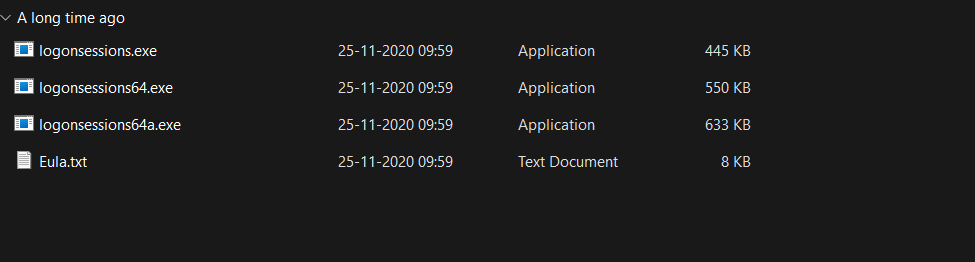
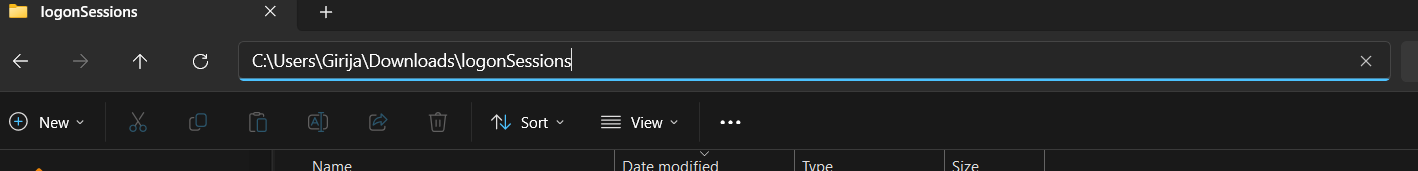
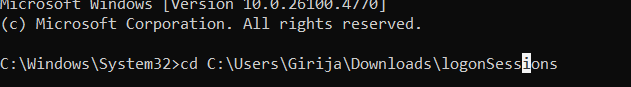
In the context of the Windows operating system, a **logon session** is a fundamental security concept that represents a single user's presence on a system. It is created after a user successfully authenticates their credentials and exists until the user logs off. Each logon session is a unique instance of a user's access and is critical for managing permissions and resources.

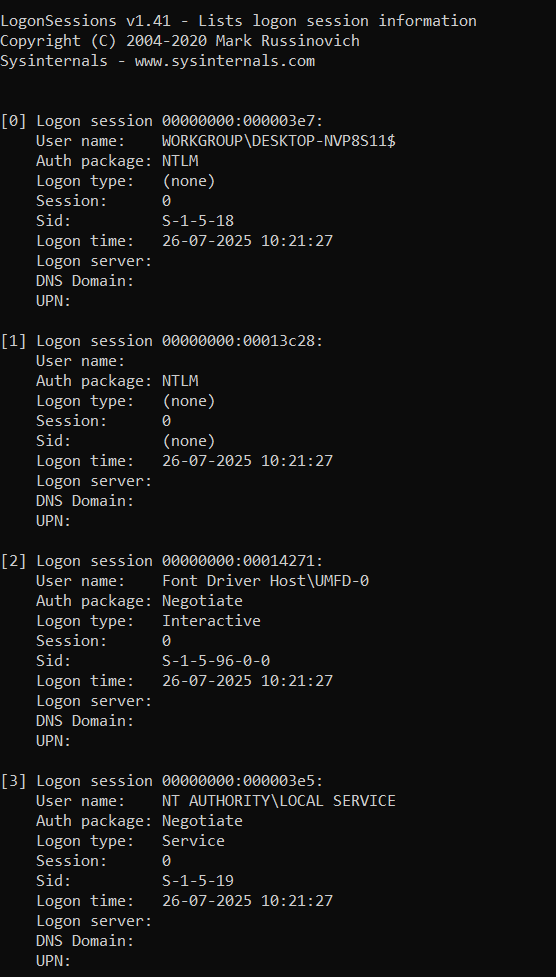
When a logon session begins, the Local Security Authority(LSA)- a protected subsystem in Windows – generates a crucial object called an access token. This token is the cornerstone of the logon session and acts as a digital ID cards for the user for the duration of their session.

The access token contains vital security information, including:

* User’s Security Identifier(SID): A unique value that identifies the user account.
* Group SIDs: SIDs for all the security groups the user account, such as the ability to shut down the system or change the system time.
* Logon ID : A locally unique identifier (LUID) that links the token back to the specific logon session.

**How to Use LogonSessions:**

1. Download LogonSessions from [LogonSessions - Sysinternals | Microsoft Learn](https://learn.microsoft.com/en-us/sysinternals/downloads/logonsessions)
2. Extract the zip file
3. Open Command promt or PowerShell in administrator mode.
4. Copy the file Directory
5. Change the Directory by using “cd [Directory]” 
6. Then Run the command “loginsessions.exe” 

**OUTPUT:-  
**

The output consist of logon session which is encrypted Hexadecimal Number, then comes the User name which is the name of the account associated with the Session, Auth Package refers to the protocols used for authentication of the account.  
  
Logon Type :

-Interactive: It refers to user

-Remote Interactive : User via RDP(Remote Desktop)

-Network : Access to resources from another machine.

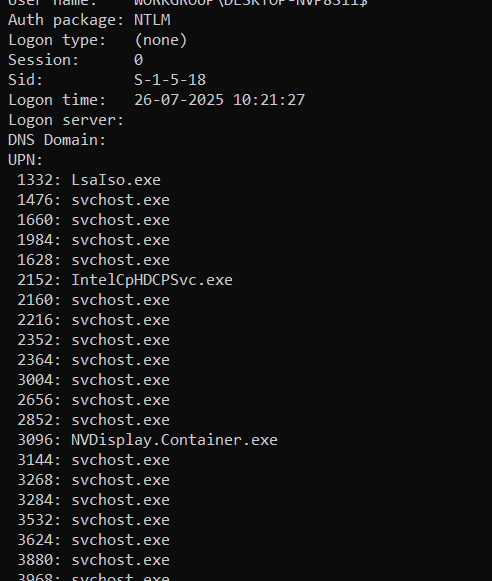
-Service : A Windows service startup

-Batch: A Scheduled Task Running

SID- The Security Identifier, a unique string that identifies the user

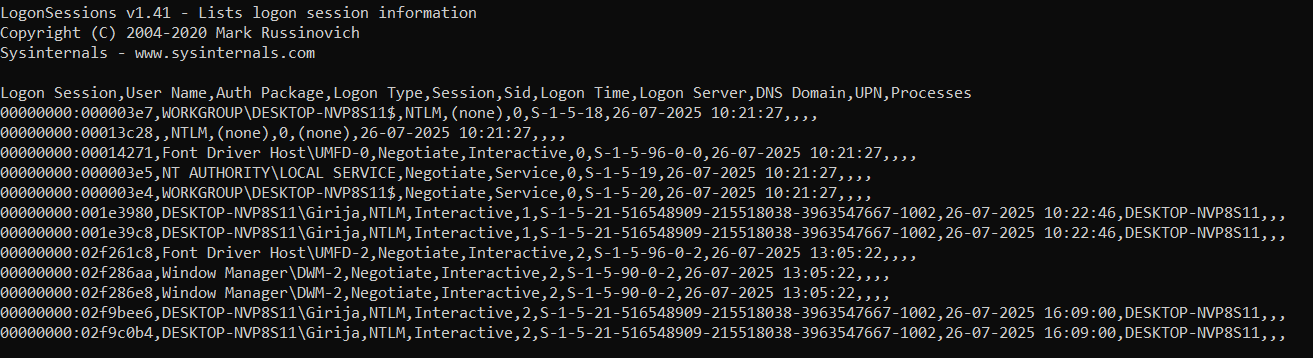
Use of -p

* Use the command “logonsessions.exe -p”



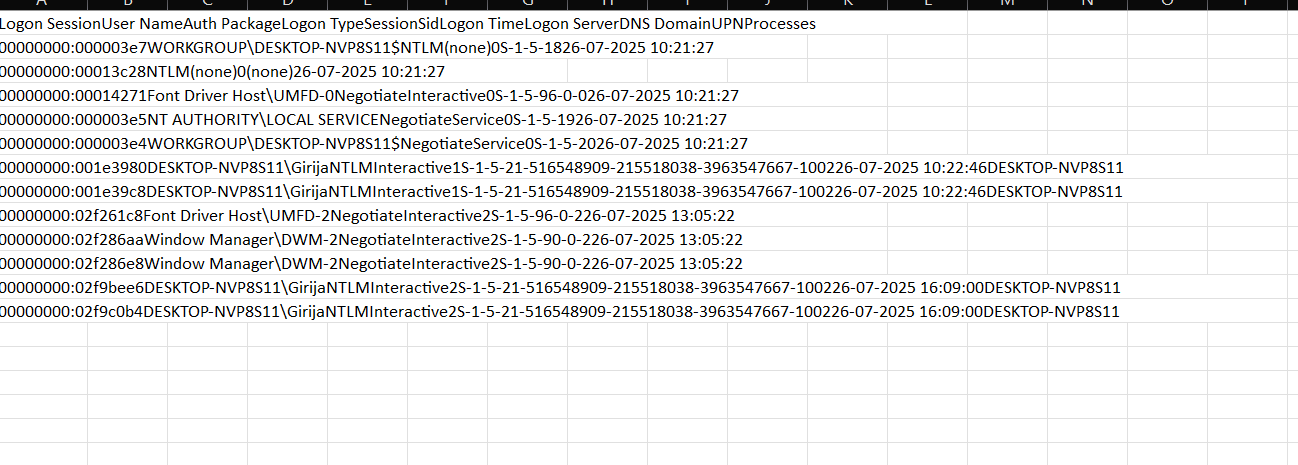
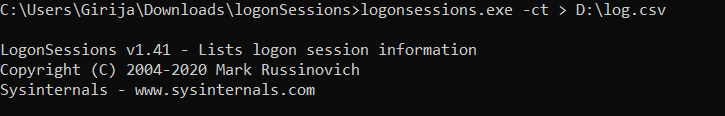
This command give you information about the Proccesses in each session

**USE OF -c:**

* Use the command “logonsessions.exe -c”
* This prints the output in csv. 

**USE OF -ct:**

* Use the command “logon sessions.exe -ct > a location”
* **Displays the output in CSV (Comma Separated Values) format, which can be easily redirected to a file and opened in a spreadsheet program like Excel.**



**CONCLUTION:**

This Proof of Concept successfully evaluated two key utilities from the Microsoft Sysinternals suite, AutoLogon and LogonSessions, to assess their functionality, interplay, and practical applications in a Windows environment. The findings confirm that while both tools are simple to use, they serve distinct and complementary purposes in system administration and security.

This POC concludes that while AutoLogon should be deployed with caution and only in controlled environments, a tool like LogonSessions is universally valuable