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:

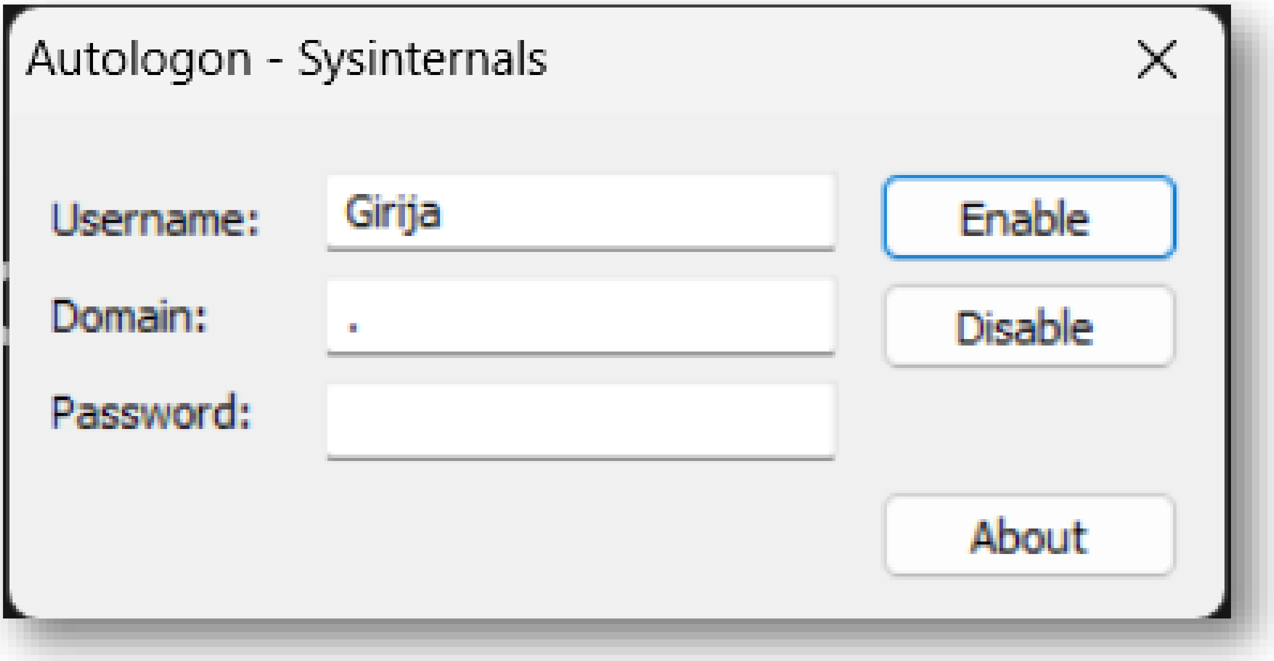
- Its core function is to bypass the manual login screen by automatically submitting stored credentials when Windows starts.
- The interface is so simple that is consist of just three fields “Username”, “Domain” and “Password”.
- When you enable AutoLogon, it does not store your password in plain text. 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".
- Run the Executable file.
- Write the Username, Domain



Username: Girija
Domain: .
Password:

- 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.

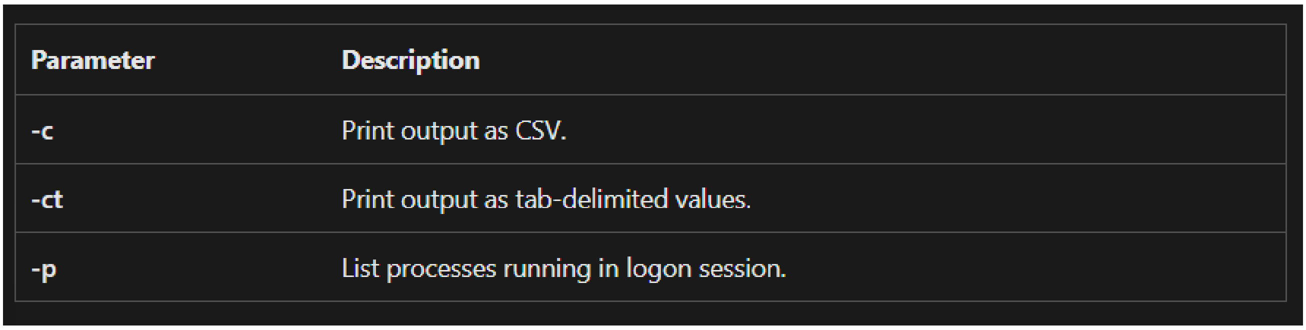
Where can we use the AutoLogon features:

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]



Parameter	Description
-c	Print output as CSV.
-ct	Print output as tab-delimited values.
-p	List processes running in logon session.

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.

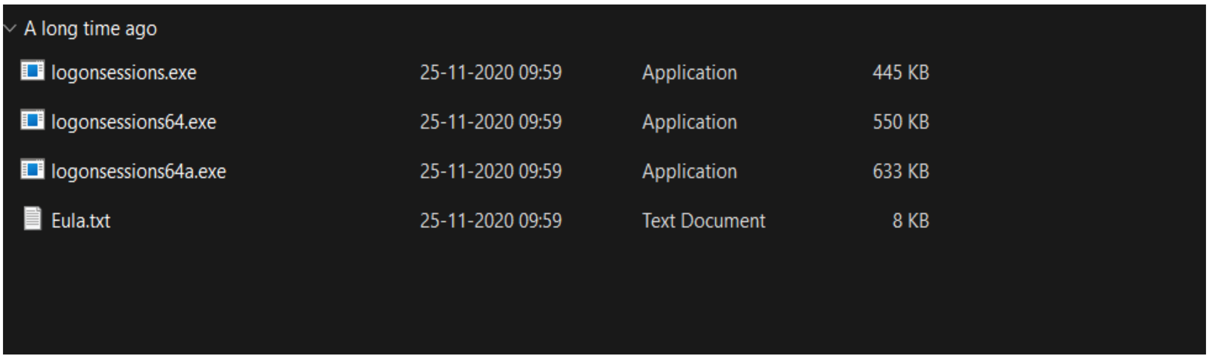
When a logon session begins, the Local Security Authority(LSA)- a protected subsystem in Windows – generates a crucial object called an access token. This token is the cornerstone of the logon session and acts as a digital ID cards for the user for the duration of their session.

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.

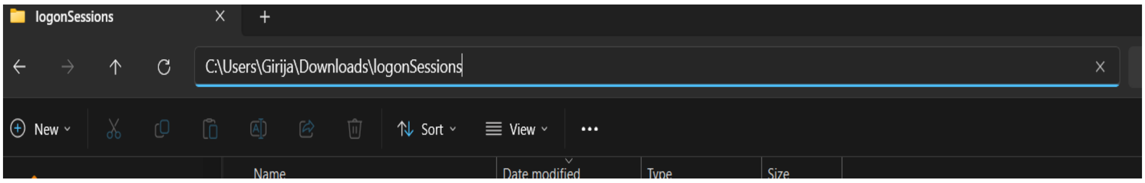
How to Use LogonSessions:

1. Download LogonSessions from [LogonSessions - Sysinternals | Microsoft Learn]()
2. Extract the zip file



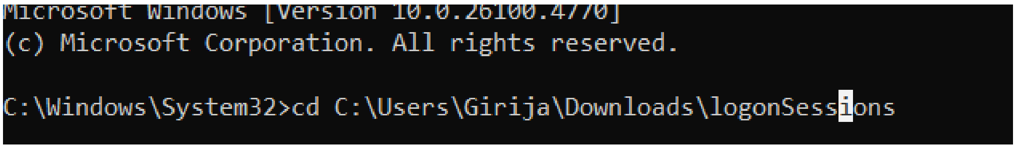
```
A long time ago
logonsessions.exe      25-11-2020 09:59   Application      445 KB
logonsessions64.exe    25-11-2020 09:59   Application      550 KB
logonsessions64a.exe   25-11-2020 09:59   Application      633 KB
Eula.txt               25-11-2020 09:59   Text Document      8 KB
```

3. Open Command promt or PowerShell in administrator mode.
4. Copy the file Directory



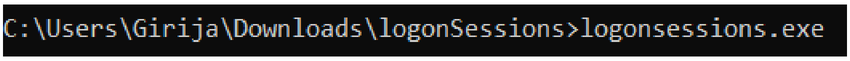
```
C:\Users\Girija\Downloads\logonSessions
```

5. Change the Directory by using “cd [Directory]”



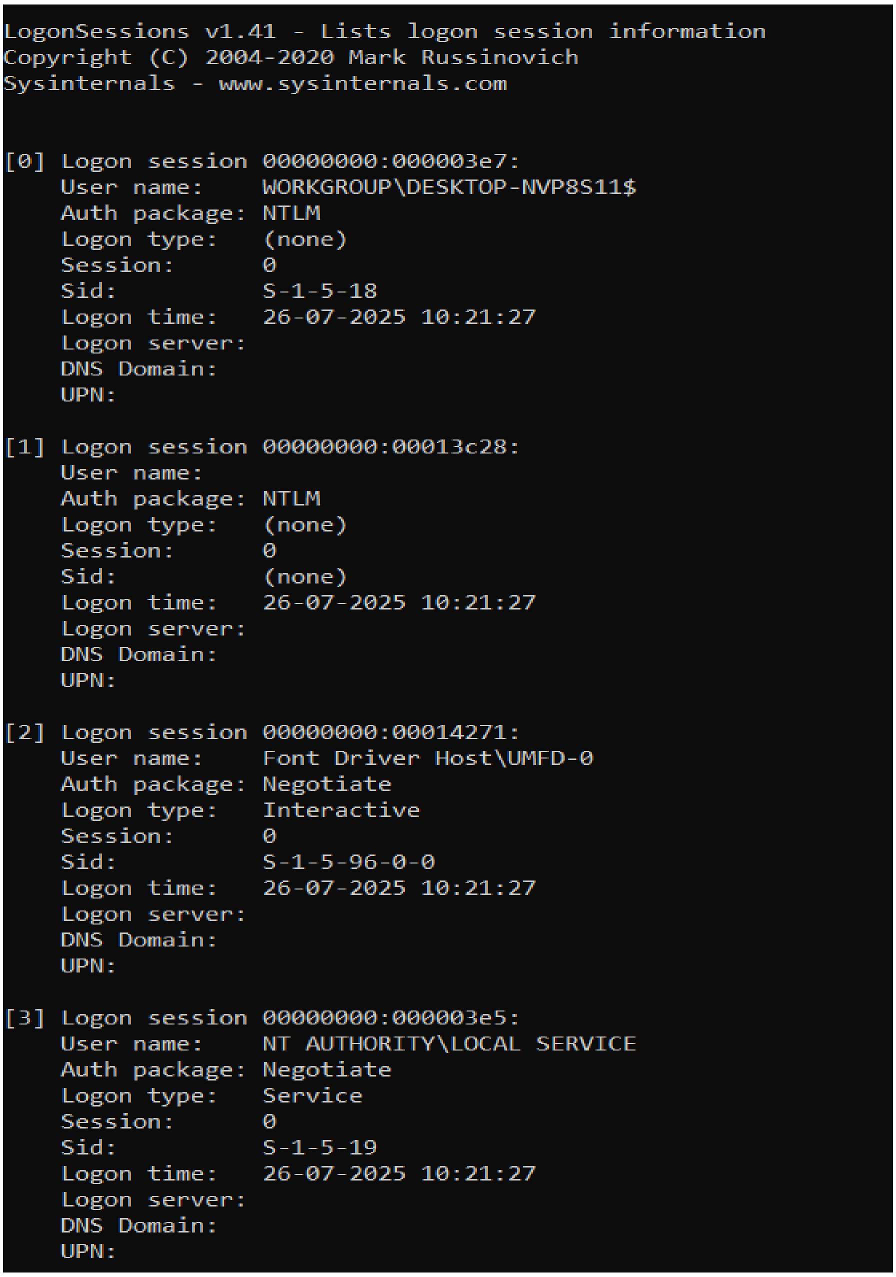
```
Microsoft Windows [Version 10.0.26100.4770]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd C:\Users\Girija\Downloads\logonSessions
```

6. Then Run the command “loginsessions.exe”



```
C:\Users\Girija\Downloads\logonSessions>logonsessions.exe
```

OUTPUT:-



```
LogonSessions v1.41 - Lists logon session information
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com


[0] Logon session 00000000:000003e7:
    User name:    WORKGROUP\DESKTOP-NVP8S11$
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          S-1-5-18
    Logon time:   26-07-2025 10:21:27
    Logon server:
    DNS Domain:
    UPN:

[1] Logon session 00000000:00013c28:
    User name:
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          (none)
    Logon time:   26-07-2025 10:21:27
    Logon server:
    DNS Domain:
    UPN:

[2] Logon session 00000000:00014271:
    User name:    Font Driver Host\UMFD-0
    Auth package: Negotiate
    Logon type:   Interactive
    Session:      0
    Sid:          S-1-5-96-0-0
    Logon time:   26-07-2025 10:21:27
    Logon server:
    DNS Domain:
    UPN:

[3] Logon session 00000000:000003e5:
    User name:    NT AUTHORITY\LOCAL SERVICE
    Auth package: Negotiate
    Logon type:   Service
    Session:      0
    Sid:          S-1-5-19
    Logon time:   26-07-2025 10:21:27
    Logon server:
    DNS Domain:
    UPN:
```

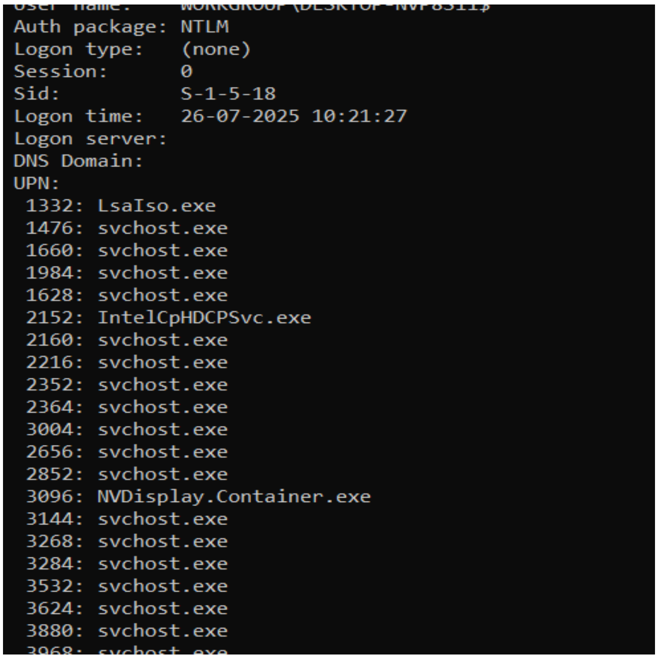
The output consist of logon session which is encrypted Hexadecimal Number, then comes the User name which is the name of the account associated with the Session, Auth Package refers to the protocols used for authentication of the account.

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”

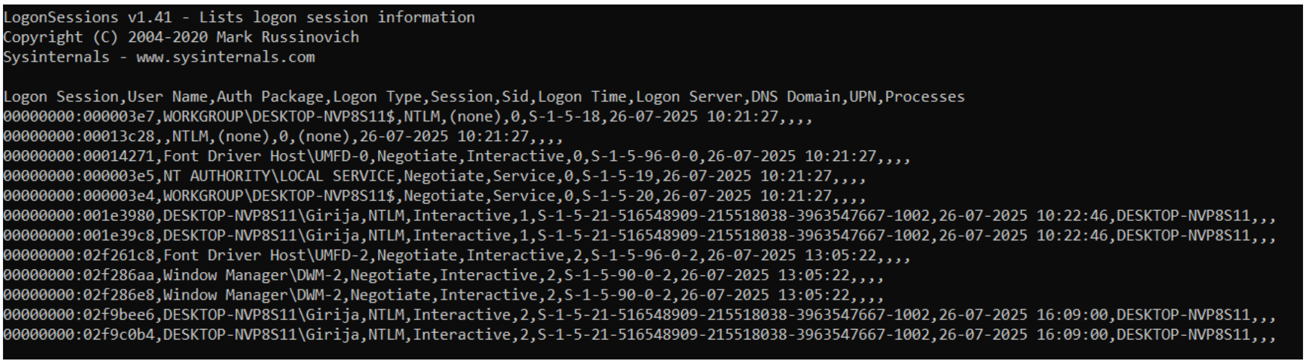


```
User name:     WORKGROUP\DESKTOP-NVP8311$
Auth package: NTLM
Logon type:   (none)
Session:      0
Sid:          S-1-5-18
Logon time:   26-07-2025 10:21:27
Logon server:
DNS Domain:
UPN:
 1332: LsaIso.exe
 1476: svchost.exe
 1660: svchost.exe
 1984: svchost.exe
 1628: svchost.exe
 2152: IntelCpHDCPSvc.exe
 2160: svchost.exe
 2216: svchost.exe
 2352: svchost.exe
 2364: svchost.exe
 3004: svchost.exe
 2656: svchost.exe
 2852: svchost.exe
 3096: NVDisplay.Container.exe
 3144: svchost.exe
 3268: svchost.exe
 3284: svchost.exe
 3532: svchost.exe
 3624: svchost.exe
 3880: svchost.exe
 3968: svchost.exe
```

This command give you information about the Proccesses in each session

<u>USE OF -c:</u>

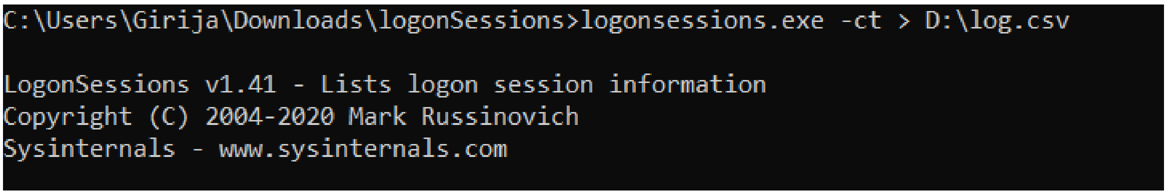
- Use the command “logonsessions.exe -c”
- This prints the output in csv.



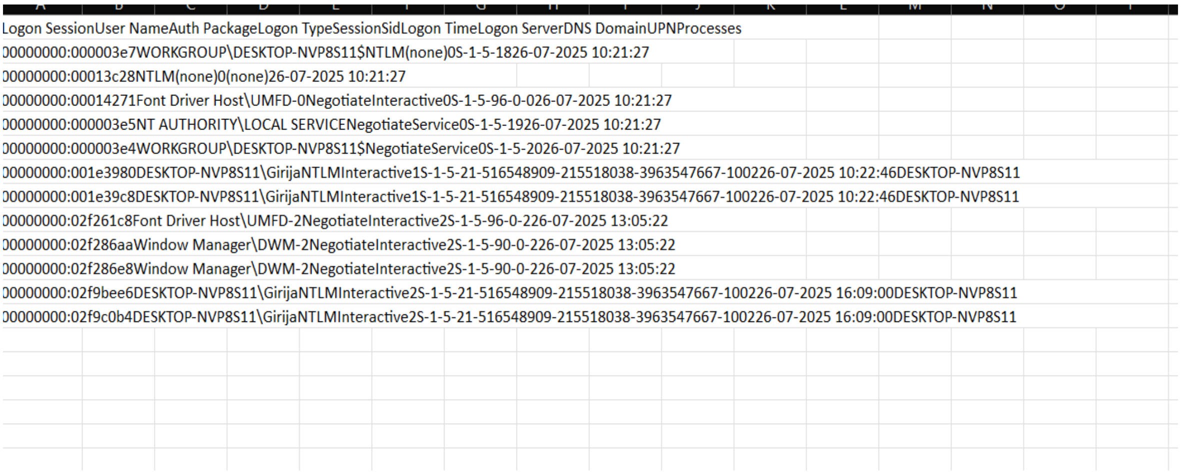
```
LogonSessions v1.41 - Lists logon session information
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

Logon Session,User Name,Auth Package,Logon Type,Session,Sid,Logon Time,Logon Server,DNS Domain,UPN,Processes
00000000:000003e7,WORKGROUP\DESKTOP-NVP8S11$,NTLM,(none),0,S-1-5-18,26-07-2025 10:21:27,,,,
00000000:00013c28,,NTLM,(none),0,(none),26-07-2025 10:21:27,,,,
00000000:00014271,Font Driver Host\UMFD-0,Negotiate,Interactive,0,S-1-5-96-0-0,26-07-2025 10:21:27,,,,
00000000:000003e5,NT AUTHORITY\LOCAL SERVICE,Negotiate,Service,0,S-1-5-19,26-07-2025 10:21:27,,,,
00000000:000003e4,WORKGROUP\DESKTOP-NVP8S11$,Negotiate,Service,0,S-1-5-20,26-07-2025 10:21:27,,,,
00000000:001e3980,DESKTOP-NVP8S11\Girija,NTLM,Interactive,1,S-1-5-21-516548909-215518038-3963547667-1002,26-07-2025 10:22:46,DESKTOP-NVP8S11,,,
00000000:001e39c8,DESKTOP-NVP8S11\Girija,NTLM,Interactive,1,S-1-5-21-516548909-215518038-3963547667-1002,26-07-2025 10:22:46,DESKTOP-NVP8S11,,,
00000000:02f261c8,Font Driver Host\UMFD-2,Negotiate,Interactive,2,S-1-5-96-0-2,26-07-2025 13:05:22,,,,
00000000:02f286aa,Window Manager\DWM-2,Negotiate,Interactive,2,S-1-5-90-0-2,26-07-2025 13:05:22,,,,
00000000:02f286e8,Window Manager\DWM-2,Negotiate,Interactive,2,S-1-5-90-0-2,26-07-2025 13:05:22,,,,
00000000:02f9bee6,DESKTOP-NVP8S11\Girija,NTLM,Interactive,2,S-1-5-21-516548909-215518038-3963547667-1002,26-07-2025 16:09:00,DESKTOP-NVP8S11,,,
00000000:02f9c0b4,DESKTOP-NVP8S11\Girija,NTLM,Interactive,2,S-1-5-21-516548909-215518038-3963547667-1002,26-07-2025 16:09:00,DESKTOP-NVP8S11,,,
```

<u>USE OF -ct:</u>

- Use the command “logon sessions.exe -ct > a location”
- **<u>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.</u>**



```
C:\Users\Girija\Downloads\logonSessions>logonsessions.exe -ct > D:\log.csv

LogonSessions v1.41 - Lists logon session information
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com
```



```
Logon SessionUser NameAuth PackageLogon TypeSessionSidLogon TimeLogon ServerDNS DomainUPNProcesses
00000000:000003e7WORKGROUP\DESKTOP-NVP8S11$NTLM(none)0S-1-5-1826-07-2025 10:21:27
00000000:00013c28NTLM(none)0(none)26-07-2025 10:21:27
00000000:00014271Font Driver Host\UMFD-0NegotiateInteractive0S-1-5-96-0-026-07-2025 10:21:27
00000000:000003e5NT AUTHORITY\LOCAL SERVICENegotiateService0S-1-5-1926-07-2025 10:21:27
00000000:000003e4WORKGROUP\DESKTOP-NVP8S11$NegotiateService0S-1-5-2026-07-2025 10:21:27
00000000:001e3980DESKTOP-NVP8S11\GirijaNTLMInteractive1S-1-5-21-516548909-215518038-3963547667-100226-07-2025 10:22:46DESKTOP-NVP8S11
00000000:001e39c8DESKTOP-NVP8S11\GirijaNTLMInteractive1S-1-5-21-516548909-215518038-3963547667-100226-07-2025 10:22:46DESKTOP-NVP8S11
00000000:02f261c8Font Driver Host\UMFD-2NegotiateInteractive2S-1-5-96-0-226-07-2025 13:05:22
00000000:02f286aaWindow Manager\DWM-2NegotiateInteractive2S-1-5-90-0-226-07-2025 13:05:22
00000000:02f286e8Window Manager\DWM-2NegotiateInteractive2S-1-5-90-0-226-07-2025 13:05:22
00000000:02f9bee6DESKTOP-NVP8S11\GirijaNTLMInteractive2S-1-5-21-516548909-215518038-3963547667-100226-07-2025 16:09:00DESKTOP-NVP8S11
00000000:02f9c0b4DESKTOP-NVP8S11\GirijaNTLMInteractive2S-1-5-21-516548909-215518038-3963547667-100226-07-2025 16:09:00DESKTOP-NVP8S11
```

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