AD SQL Logins unrolled leveraging PowerShell

Jared Kirkpatrick

✉ kirk1880@me.com

ABOUT ME

Member of PASS since 1999

Presenter for several SQL Saturdays

5 X 140.6 Ironman Finisher | 21 X 70.3

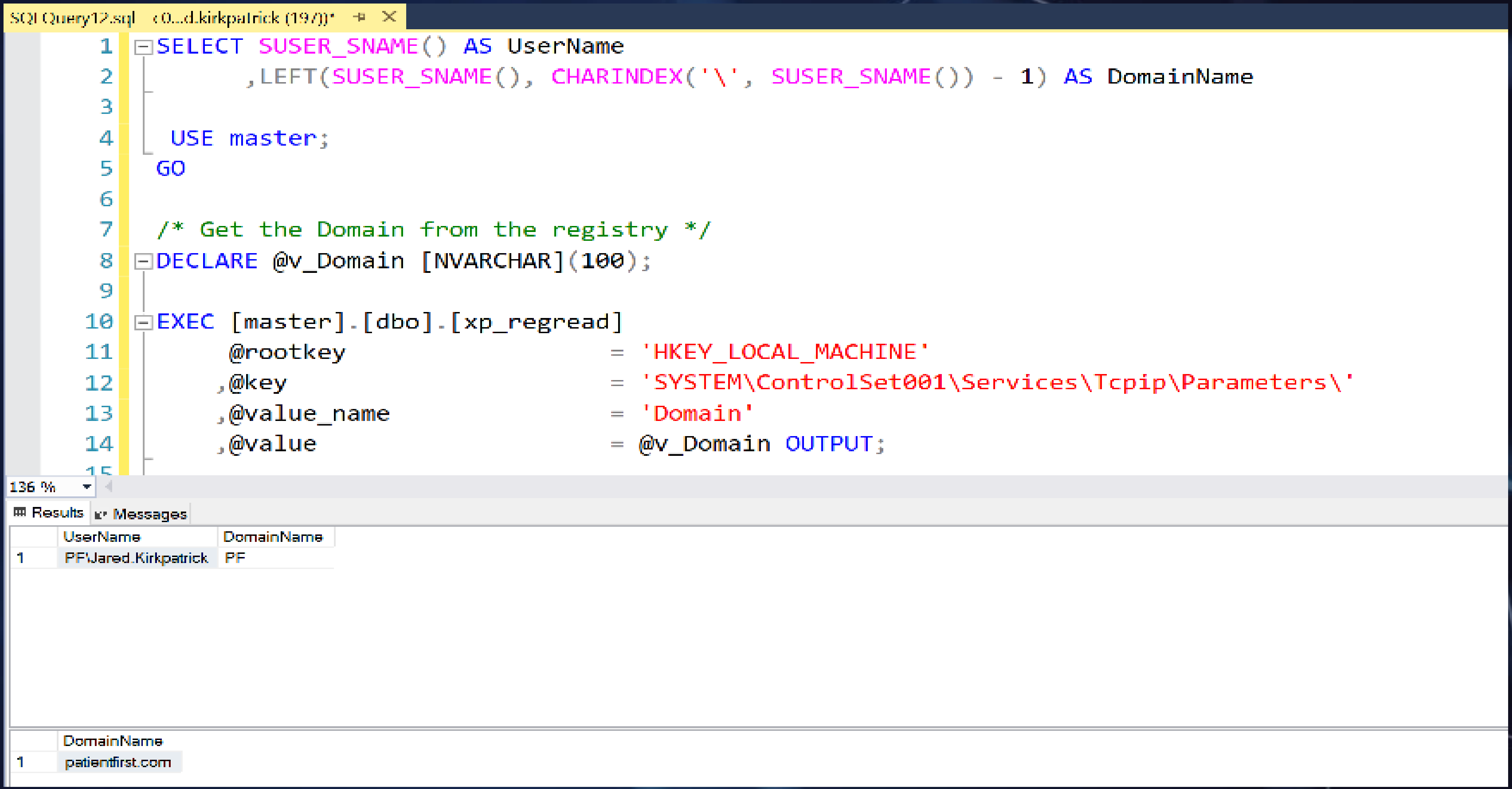
12 Gran Fondo / 100 Mile Bike Race

Agenda

- Different Type of Logins
- Windows AD Groups, Domains, and Aliases
- Extended Stored Procedures
- Global Groups vs Local Groups
- PowerShell Solution
- Results

What are the different Security Logins Available?

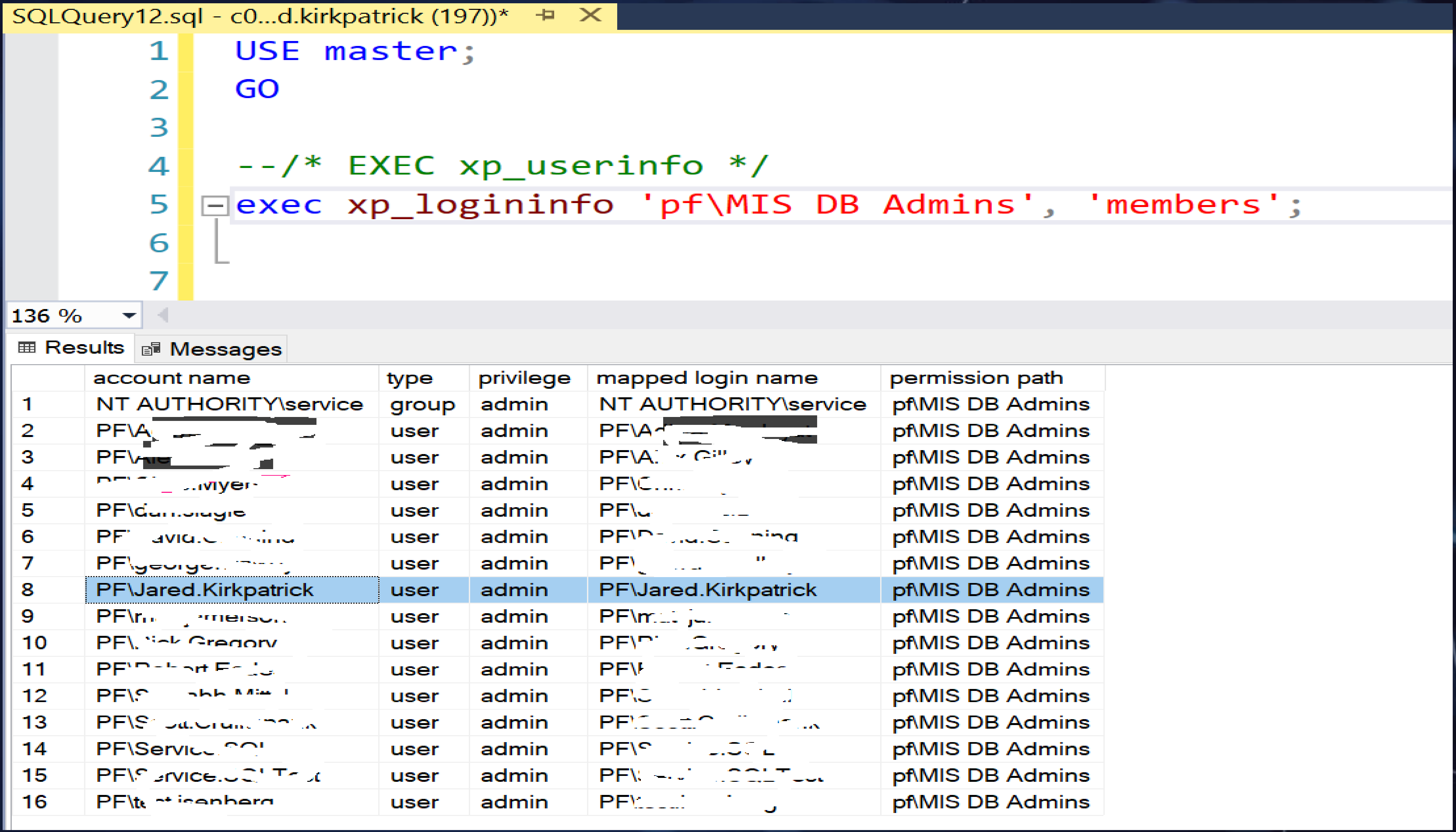
1. SQL Server Authentication
2. Windows Authentication and Group Authentication
3. Azure Active Directory (AAD) Authentication
4. Certificate-Based Authentication
5. Multi-Factor Authentication (MFA)



```
SELECT SUSER_SNAME() AS UserName
      ,LEFT(SUSER_SNAME(), CHARINDEX('\', SUSER_SNAME()) - 1) AS DomainName

 USE master;
GO

/* Get the Domain from the registry */
DECLARE @v_Domain [NVARCHAR](100);

EXEC [master].[dbo].[xp_regread]
     @rootkey                      = 'HKEY_LOCAL_MACHINE'
    ,@key                          = 'SYSTEM\ControlSet001\Services\Tcpip\Parameters\'
    ,@value_name                   = 'Domain'
    ,@value                        = @v_Domain OUTPUT;
```

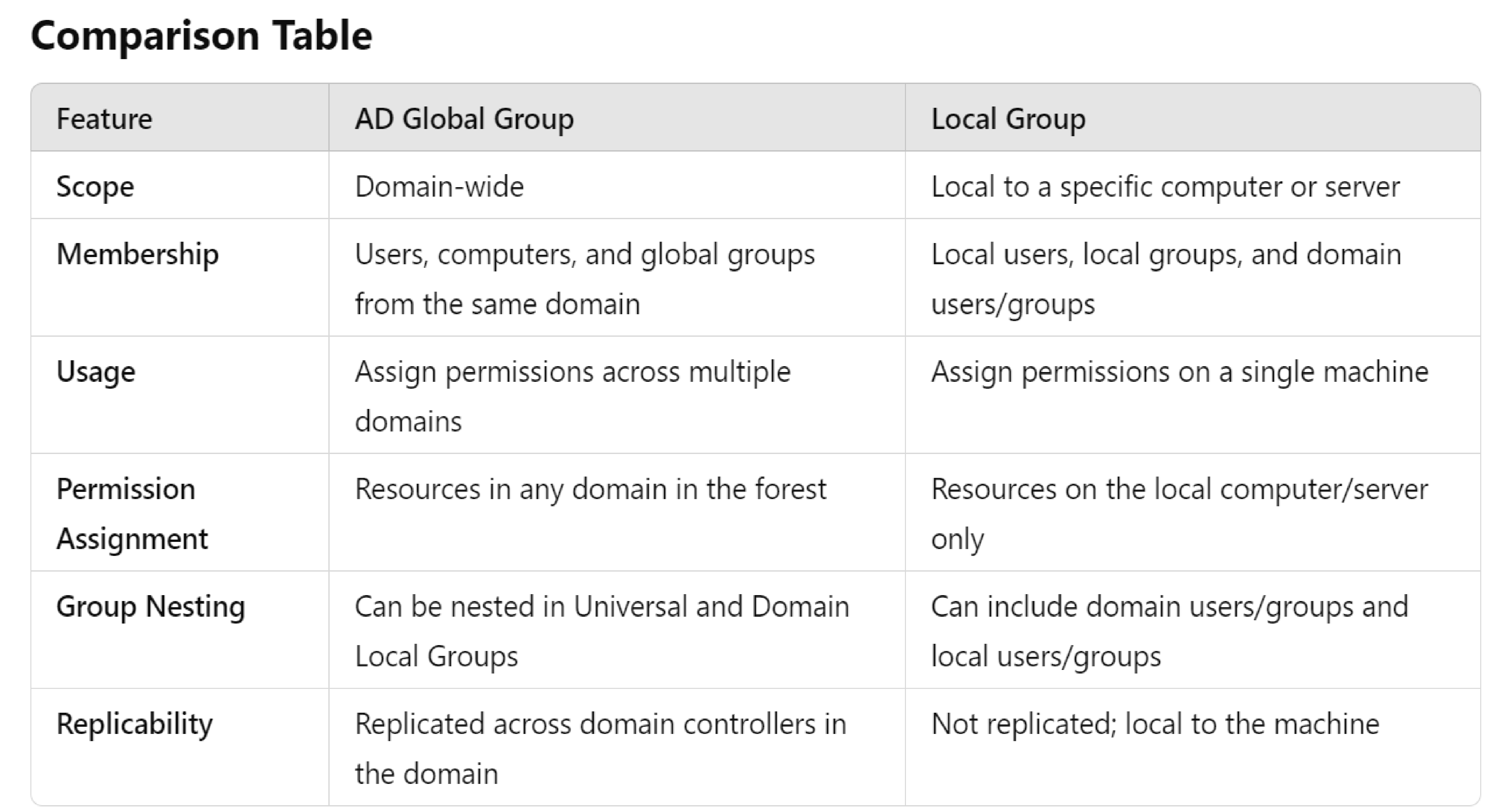
	UserName	DomainName
1	PF\Jared.Kirkpatrick	PF

	DomainName
1	patientfirst.com



```sql
USE master;
GO

--/* EXEC xp_userinfo */
exec xp_logininfo 'pf\MIS DB Admins', 'members';
```

	account name	type	privilege	mapped login name	permission path
1	NT AUTHORITY\service	group	admin	NT AUTHORITY\service	pf\MIS DB Admins
2	[redacted]	user	admin	[redacted]	pf\MIS DB Admins
3	[redacted]	user	admin	[redacted]	pf\MIS DB Admins
4	[redacted]	user	admin	[redacted]	pf\MIS DB Admins
5	[redacted]	user	admin	[redacted]	pf\MIS DB Admins
6	[redacted]	user	admin	[redacted]	pf\MIS DB Admins
7	[redacted]	user	admin	[redacted]	pf\MIS DB Admins
8	PF\Jared.Kirkpatrick	user	admin	PF\Jared.Kirkpatrick	pf\MIS DB Admins
9	[redacted]	user	admin	[redacted]	pf\MIS DB Admins
10	[redacted]	user	admin	[redacted]	pf\MIS DB Admins
11	[redacted]	user	admin	[redacted]	pf\MIS DB Admins
12	[redacted]	user	admin	[redacted]	pf\MIS DB Admins
13	[redacted]	user	admin	[redacted]	pf\MIS DB Admins
14	[redacted]	user	admin	[redacted]	pf\MIS DB Admins
15	[redacted]	user	admin	[redacted]	pf\MIS DB Admins
16	[redacted]	user	admin	[redacted]	pf\MIS DB Admins



Comparison Table

Feature	AD Global Group	Local Group
Scope	Domain-wide	Local to a specific computer or server
Membership	Users, computers, and global groups from the same domain	Local users, local groups, and domain users/groups
Usage	Assign permissions across multiple domains	Assign permissions on a single machine
Permission Assignment	Resources in any domain in the forest	Resources on the local computer/server only
Group Nesting	Can be nested in Universal and Domain Local Groups	Can include domain users/groups and local users/groups
Replicability	Replicated across domain controllers in the domain	Not replicated; local to the machine

Jared.Kirkpatrick

GG_DBE

Dev/Test/QA
LG_DBE_Sysadmin

Production Systems
LG_DBE_Read

Jared.Kirkpatrick_Admin

GG_DBE_
Admin

GG_SQL_
Admin

All Systems
LG_SQL_Sysadmin

PowerShell Script SvrLogins.psl

1) Pass in a SQL Instance Parameter = $SQLInstance

2) Create a Function to connect to a SQL Server and Exec a query that return Logins

3) Filter the Results to remove the Domain Name

4) Loop through the filtered Results for Each Domain Group

5) Leverage the PowerShell AD Functions to get members from each of the groups

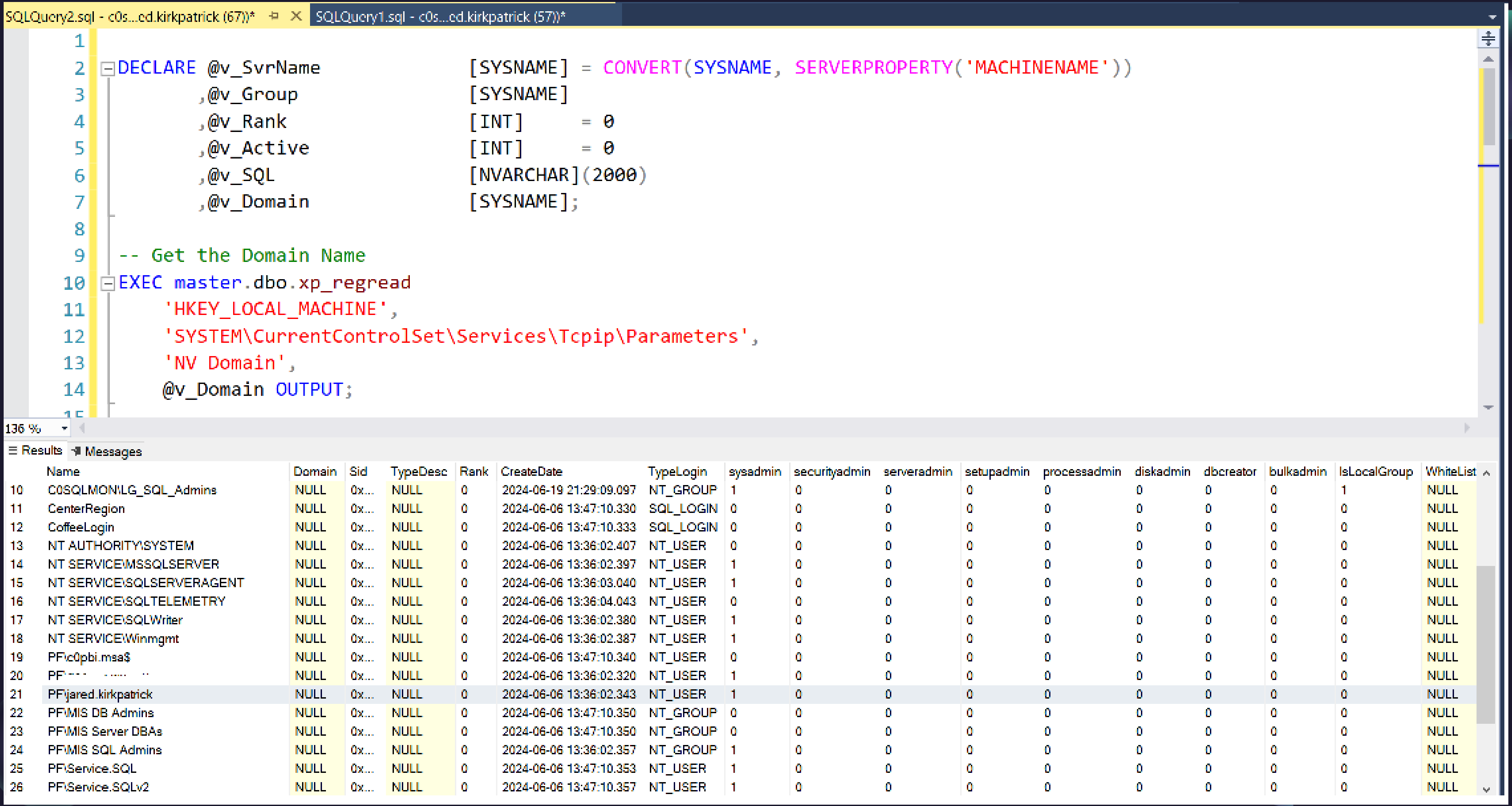
6) Add the mambers/nested groups to the original result set with an incrementing rank

7) Create a datatable object for the final results and insert the base result set where rank = 0

8) Loop through the remaining results and get the parent group as well as the very first group of the login

9) Add the record to the final result data table

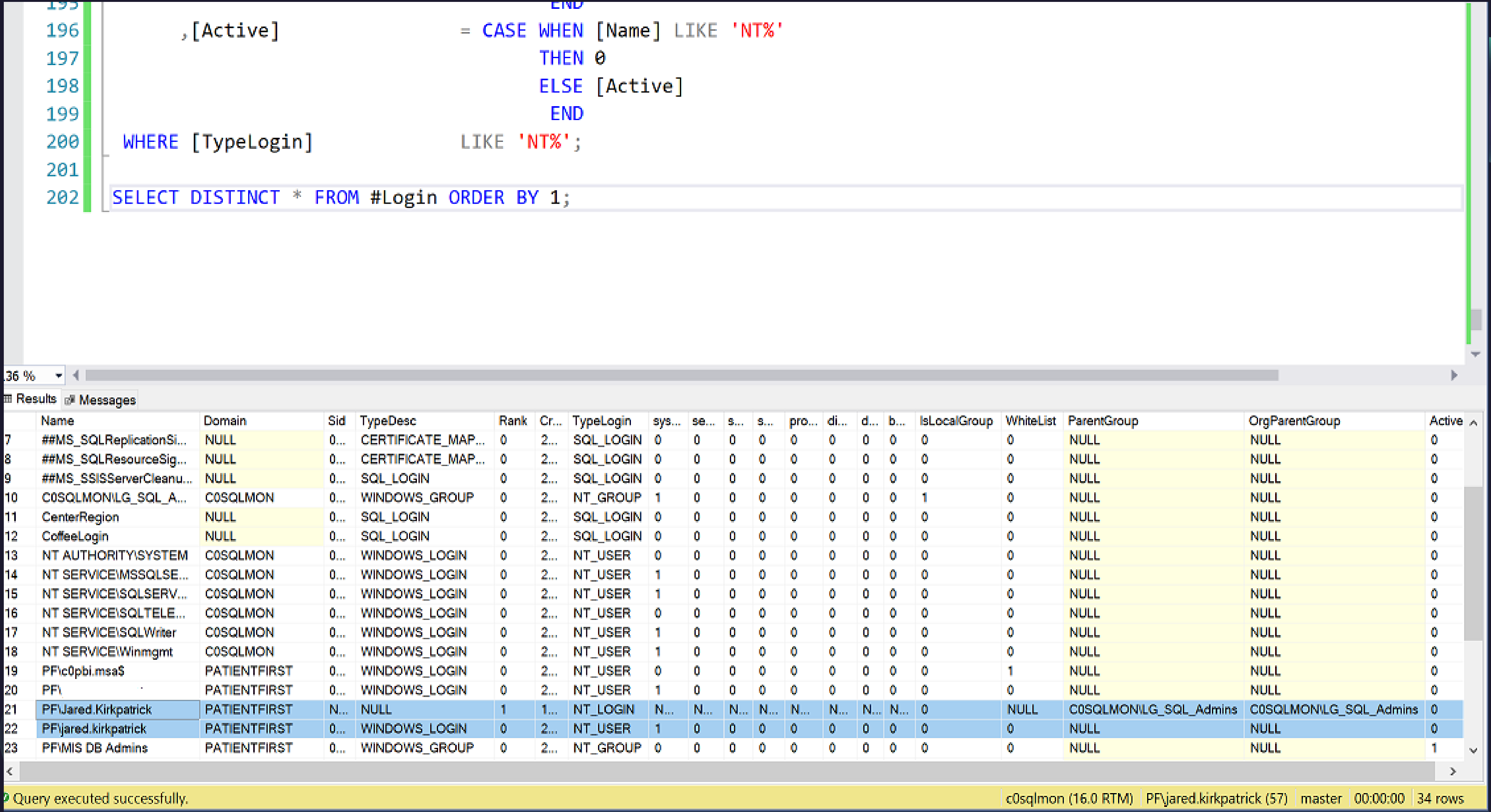
10) Take the $PSScriptRoot, scrub out a filename, and save the results as a CSV.



SQLQuery2.sql - c0s...ed.kirkpatrick (67))*
SQLQuery1.sql - c0s...ed.kirkpatrick (57))*
136 %
Results
Messages

```sql

DECLARE @v_SvrName              [SYSNAME] = CONVERT(SYSNAME, SERVERPROPERTY('MACHINENAME'))
        ,@v_Group               [SYSNAME]
        ,@v_Rank                [INT]     = 0
        ,@v_Active              [INT]     = 0
        ,@v_SQL                 [NVARCHAR](2000)
        ,@v_Domain              [SYSNAME];

-- Get the Domain Name
EXEC master.dbo.xp_regread
    'HKEY_LOCAL_MACHINE',
    'SYSTEM\CurrentControlSet\Services\Tcpip\Parameters',
    'NV Domain',
    @v_Domain OUTPUT;
```

	Name	Domain	Sid	TypeDesc	Rank	CreateDate	TypeLogin	sysadmin	securityadmin	serveradmin	setupadmin	processadmin	diskadmin	dbcreator	bulkadmin	IsLocalGroup	WhiteList
10	C0SQLMON\LG_SQL_Admins	NULL	0x...	NULL	0	2024-06-19 21:29:09.097	NT_GROUP	1	0	0	0	0	0	0	0	1	NULL
11	CenterRegion	NULL	0x...	NULL	0	2024-06-06 13:47:10.330	SQL_LOGIN	0	0	0	0	0	0	0	0	0	NULL
12	CoffeeLogin	NULL	0x...	NULL	0	2024-06-06 13:47:10.333	SQL_LOGIN	0	0	0	0	0	0	0	0	0	NULL
13	NT AUTHORITY\SYSTEM	NULL	0x...	NULL	0	2024-06-06 13:36:02.407	NT_USER	0	0	0	0	0	0	0	0	0	NULL
14	NT SERVICE\MSSQLSERVER	NULL	0x...	NULL	0	2024-06-06 13:36:02.397	NT_USER	1	0	0	0	0	0	0	0	0	NULL
15	NT SERVICE\SQLSERVERAGENT	NULL	0x...	NULL	0	2024-06-06 13:36:03.040	NT_USER	1	0	0	0	0	0	0	0	0	NULL
16	NT SERVICE\SQLTELEMETRY	NULL	0x...	NULL	0	2024-06-06 13:36:04.043	NT_USER	0	0	0	0	0	0	0	0	0	NULL
17	NT SERVICE\SQLWriter	NULL	0x...	NULL	0	2024-06-06 13:36:02.380	NT_USER	1	0	0	0	0	0	0	0	0	NULL
18	NT SERVICE\Winmgmt	NULL	0x...	NULL	0	2024-06-06 13:36:02.387	NT_USER	1	0	0	0	0	0	0	0	0	NULL
19	PF\c0pbi.msa$	NULL	0x...	NULL	0	2024-06-06 13:47:10.340	NT_USER	0	0	0	0	0	0	0	0	0	NULL
20	PF[redacted]	NULL	0x...	NULL	0	2024-06-06 13:36:02.320	NT_USER	1	0	0	0	0	0	0	0	0	NULL
21	PF\jared.kirkpatrick	NULL	0x...	NULL	0	2024-06-06 13:36:02.343	NT_USER	1	0	0	0	0	0	0	0	0	NULL
22	PF\MIS DB Admins	NULL	0x...	NULL	0	2024-06-06 13:47:10.350	NT_GROUP	0	0	0	0	0	0	0	0	0	NULL
23	PF\MIS Server DBAs	NULL	0x...	NULL	0	2024-06-06 13:47:10.350	NT_GROUP	0	0	0	0	0	0	0	0	0	NULL
24	PF\MIS SQL Admins	NULL	0x...	NULL	0	2024-06-06 13:36:02.357	NT_GROUP	1	0	0	0	0	0	0	0	0	NULL
25	PF\Service.SQL	NULL	0x...	NULL	0	2024-06-06 13:47:10.353	NT_USER	1	0	0	0	0	0	0	0	0	NULL
26	PF\Service.SQLv2	NULL	0x...	NULL	0	2024-06-06 13:47:10.357	NT_USER	1	0	0	0	0	0	0	0	0	NULL



```sql
                                          END
        ,[Active]                       = CASE WHEN [Name] LIKE 'NT%'
                                          THEN 0
                                          ELSE [Active]
                                           END
 WHERE [TypeLogin]                   LIKE 'NT%';

SELECT DISTINCT * FROM #Login ORDER BY 1;
```

	Name	Domain	Sid	TypeDesc	Rank	Cr...	TypeLogin	sys...	se...	s...	s...	pro...	di...	d...	b...	IsLocalGroup	WhiteList	ParentGroup	OrgParentGroup	Active
7	##MS_SQLReplicationSi...	NULL	0...	CERTIFICATE_MAP...	0	2...	SQL_LOGIN	0	0	0	0	0	0	0	0	0	0	NULL	NULL	0
8	##MS_SQLResourceSig...	NULL	0...	CERTIFICATE_MAP...	0	2...	SQL_LOGIN	0	0	0	0	0	0	0	0	0	0	NULL	NULL	0
9	##MS_SSISServerCleanu...	NULL	0...	SQL_LOGIN	0	2...	SQL_LOGIN	0	0	0	0	0	0	0	0	0	0	NULL	NULL	0
10	C0SQLMON\LG_SQL_A...	C0SQLMON	0...	WINDOWS_GROUP	0	2...	NT_GROUP	1	0	0	0	0	0	0	0	1	0	NULL	NULL	0
11	CenterRegion	NULL	0...	SQL_LOGIN	0	2...	SQL_LOGIN	0	0	0	0	0	0	0	0	0	0	NULL	NULL	0
12	CoffeeLogin	NULL	0...	SQL_LOGIN	0	2...	SQL_LOGIN	0	0	0	0	0	0	0	0	0	0	NULL	NULL	0
13	NT AUTHORITY\SYSTEM	C0SQLMON	0...	WINDOWS_LOGIN	0	2...	NT_USER	0	0	0	0	0	0	0	0	0	0	NULL	NULL	0
14	NT SERVICE\MSSQLSE...	C0SQLMON	0...	WINDOWS_LOGIN	0	2...	NT_USER	1	0	0	0	0	0	0	0	0	0	NULL	NULL	0
15	NT SERVICE\SQLSERV...	C0SQLMON	0...	WINDOWS_LOGIN	0	2...	NT_USER	1	0	0	0	0	0	0	0	0	0	NULL	NULL	0
16	NT SERVICE\SQLTELE...	C0SQLMON	0...	WINDOWS_LOGIN	0	2...	NT_USER	0	0	0	0	0	0	0	0	0	0	NULL	NULL	0
17	NT SERVICE\SQLWriter	C0SQLMON	0...	WINDOWS_LOGIN	0	2...	NT_USER	1	0	0	0	0	0	0	0	0	0	NULL	NULL	0
18	NT SERVICE\Winmgmt	C0SQLMON	0...	WINDOWS_LOGIN	0	2...	NT_USER	1	0	0	0	0	0	0	0	0	0	NULL	NULL	0
19	PF\c0pbi.msa$	PATIENTFIRST	0...	WINDOWS_LOGIN	0	2...	NT_USER	0	0	0	0	0	0	0	0	0	1	NULL	NULL	0
20	PF\	PATIENTFIRST	0...	WINDOWS_LOGIN	0	2...	NT_USER	1	0	0	0	0	0	0	0	0	0	NULL	NULL	0
21	PF\Jared.Kirkpatrick	PATIENTFIRST	N...	NULL	1	1...	NT_LOGIN	N...	N...	N...	N...	N...	N...	N...	N...	0	NULL	C0SQLMON\LG_SQL_Admins	C0SQLMON\LG_SQL_Admins	0
22	PF\jared.kirkpatrick	PATIENTFIRST	0...	WINDOWS_LOGIN	0	2...	NT_USER	1	0	0	0	0	0	0	0	0	0	NULL	NULL	0
23	PF\MIS DB Admins	PATIENTFIRST	0...	WINDOWS_GROUP	0	2...	NT_GROUP	0	0	0	0	0	0	0	0	0	0	NULL	NULL	1

Query executed successfully.

c0sqlmon (16.0 RTM) | PF\jared.kirkpatrick (57) | master | 00:00:00 | 34 rows

PowerShell Script SvrLogins.psl

1) Pass in a SQL Instance Parameter = $SQLInstance

2) Create a Function to connect to a SQL Server and Exec a query that return Logins

3) Filter the Results to remove the Domain Name

4) Loop through the filtered Results for Each Domain Group

5) Leverage the PowerShell AD Functions to get members from each of the groups

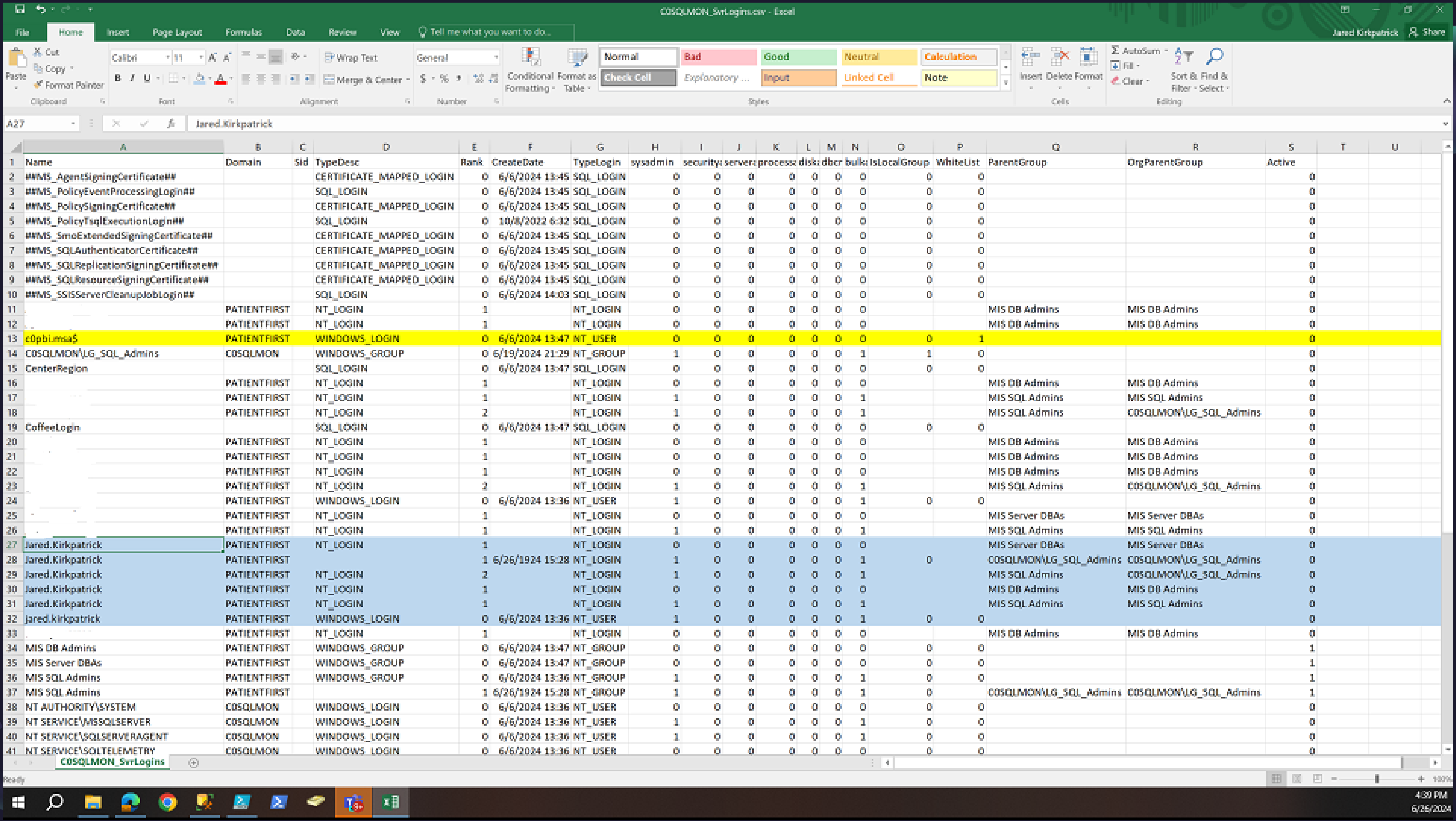
6) Add the mambers/nested groups to the original result set with an incrementing rank

7) Create a datatable object for the final results and insert the base result set where rank = 0

8) Loop through the remaining results and get the parent group as well as the very first group of the login

9) Add the record to the final result data table

10) Take the $PSScriptRoot, scrub out a filename, and save the results as a CSV.



A27 Jared.Kirkpatrick

	Name	Domain	Sid	TypeDesc	Rank	CreateDate	TypeLogin	sysadmin	security:	server:	process:	disk:	dbcr	bulk:	IsLocalGroup	WhiteList	ParentGroup	OrgParentGroup	Active
2	##MS_AgentSigningCertificate##			CERTIFICATE_MAPPED_LOGIN	0	6/6/2024 13:45	SQL_LOGIN	0	0	0	0	0	0	0	0	0			0
3	##MS_PolicyEventProcessingLogin##			SQL_LOGIN	0	6/6/2024 13:45	SQL_LOGIN	0	0	0	0	0	0	0	0	0			0
4	##MS_PolicySigningCertificate##			CERTIFICATE_MAPPED_LOGIN	0	6/6/2024 13:45	SQL_LOGIN	0	0	0	0	0	0	0	0	0			0
5	##MS_PolicyTsqlExecutionLogin##			SQL_LOGIN	0	10/8/2022 6:32	SQL_LOGIN	0	0	0	0	0	0	0	0	0			0
6	##MS_SmoExtendedSigningCertificate##			CERTIFICATE_MAPPED_LOGIN	0	6/6/2024 13:45	SQL_LOGIN	0	0	0	0	0	0	0	0	0			0
7	##MS_SQLAuthenticatorCertificate##			CERTIFICATE_MAPPED_LOGIN	0	6/6/2024 13:45	SQL_LOGIN	0	0	0	0	0	0	0	0	0			0
8	##MS_SQLReplicationSigningCertificate##			CERTIFICATE_MAPPED_LOGIN	0	6/6/2024 13:45	SQL_LOGIN	0	0	0	0	0	0	0	0	0			0
9	##MS_SQLResourceSigningCertificate##			CERTIFICATE_MAPPED_LOGIN	0	6/6/2024 13:45	SQL_LOGIN	0	0	0	0	0	0	0	0	0			0
10	##MS_SSISServerCleanupJobLogin##			SQL_LOGIN	0	6/6/2024 14:03	SQL_LOGIN	0	0	0	0	0	0	0	0	0			0
11	[redacted]	PATIENTFIRST		NT_LOGIN	1		NT_LOGIN	0	0	0	0	0	0	0			MIS DB Admins	MIS DB Admins	0
12	[redacted]	PATIENTFIRST		NT_LOGIN	1		NT_LOGIN	0	0	0	0	0	0	0			MIS DB Admins	MIS DB Admins	0
13	c0pbi.msa$	PATIENTFIRST		WINDOWS_LOGIN	0	6/6/2024 13:47	NT_USER	0	0	0	0	0	0	0	0	1			0
14	C0SQLMON\LG_SQL_Admins	C0SQLMON		WINDOWS_GROUP	0	6/19/2024 21:29	NT_GROUP	1	0	0	0	0	0	1	1	0			0
15	CenterRegion			SQL_LOGIN	0	6/6/2024 13:47	SQL_LOGIN	0	0	0	0	0	0	0	0	0			0
16	[redacted]	PATIENTFIRST		NT_LOGIN	1		NT_LOGIN	0	0	0	0	0	0	0			MIS DB Admins	MIS DB Admins	0
17	[redacted]	PATIENTFIRST		NT_LOGIN	1		NT_LOGIN	1	0	0	0	0	0	1			MIS SQL Admins	MIS SQL Admins	0
18	[redacted]	PATIENTFIRST		NT_LOGIN	2		NT_LOGIN	1	0	0	0	0	0	1			MIS SQL Admins	C0SQLMON\LG_SQL_Admins	0
19	CoffeeLogin			SQL_LOGIN	0	6/6/2024 13:47	SQL_LOGIN	0	0	0	0	0	0	0	0	0			0
20	[redacted]	PATIENTFIRST		NT_LOGIN	1		NT_LOGIN	0	0	0	0	0	0	0			MIS DB Admins	MIS DB Admins	0
21	[redacted]	PATIENTFIRST		NT_LOGIN	1		NT_LOGIN	0	0	0	0	0	0	0			MIS DB Admins	MIS DB Admins	0
22	[redacted]	PATIENTFIRST		NT_LOGIN	1		NT_LOGIN	0	0	0	0	0	0	0			MIS DB Admins	MIS DB Admins	0
23	[redacted]	PATIENTFIRST		NT_LOGIN	2		NT_LOGIN	1	0	0	0	0	0	1			MIS SQL Admins	C0SQLMON\LG_SQL_Admins	0
24	[redacted]	PATIENTFIRST		WINDOWS_LOGIN	0	6/6/2024 13:36	NT_USER	1	0	0	0	0	0	1	0	0			0
25	[redacted]	PATIENTFIRST		NT_LOGIN	1		NT_LOGIN	0	0	0	0	0	0	0			MIS Server DBAs	MIS Server DBAs	0
26	[redacted]	PATIENTFIRST		NT_LOGIN	1		NT_LOGIN	1	0	0	0	0	0	1			MIS SQL Admins	MIS SQL Admins	0
27	Jared.Kirkpatrick	PATIENTFIRST		NT_LOGIN	1		NT_LOGIN	0	0	0	0	0	0	0			MIS Server DBAs	MIS Server DBAs	0
28	Jared.Kirkpatrick	PATIENTFIRST			1	6/26/1924 15:28	NT_LOGIN	1	0	0	0	0	0	1	0		C0SQLMON\LG_SQL_Admins	C0SQLMON\LG_SQL_Admins	0
29	Jared.Kirkpatrick	PATIENTFIRST		NT_LOGIN	2		NT_LOGIN	1	0	0	0	0	0	1			MIS SQL Admins	C0SQLMON\LG_SQL_Admins	0
30	Jared.Kirkpatrick	PATIENTFIRST		NT_LOGIN	1		NT_LOGIN	0	0	0	0	0	0	0			MIS DB Admins	MIS DB Admins	0
31	Jared.Kirkpatrick	PATIENTFIRST		NT_LOGIN	1		NT_LOGIN	1	0	0	0	0	0	1			MIS SQL Admins	MIS SQL Admins	0
32	jared.kirkpatrick	PATIENTFIRST		WINDOWS_LOGIN	0	6/6/2024 13:36	NT_USER	1	0	0	0	0	0	1	0	0			0
33	[redacted]	PATIENTFIRST		NT_LOGIN	1		NT_LOGIN	0	0	0	0	0	0	0			MIS DB Admins	MIS DB Admins	0
34	MIS DB Admins	PATIENTFIRST		WINDOWS_GROUP	0	6/6/2024 13:47	NT_GROUP	0	0	0	0	0	0	0	0	0			1
35	MIS Server DBAs	PATIENTFIRST		WINDOWS_GROUP	0	6/6/2024 13:47	NT_GROUP	0	0	0	0	0	0	0	0	0			1
36	MIS SQL Admins	PATIENTFIRST		WINDOWS_GROUP	0	6/6/2024 13:36	NT_GROUP	1	0	0	0	0	0	1	0	0			1
37	MIS SQL Admins	PATIENTFIRST			1	6/26/1924 15:28	NT_GROUP	1	0	0	0	0	0	1	0		C0SQLMON\LG_SQL_Admins	C0SQLMON\LG_SQL_Admins	1
38	NT AUTHORITY\SYSTEM	C0SQLMON		WINDOWS_LOGIN	0	6/6/2024 13:36	NT_USER	0	0	0	0	0	0	0	0	0			0
39	NT SERVICE\MSSQLSERVER	C0SQLMON		WINDOWS_LOGIN	0	6/6/2024 13:36	NT_USER	1	0	0	0	0	0	1	0	0			0
40	NT SERVICE\SQLSERVERAGENT	C0SQLMON		WINDOWS_LOGIN	0	6/6/2024 13:36	NT_USER	1	0	0	0	0	0	1	0	0			0
41	NT SERVICE\SQLTELEMETRY	C0SQLMON		WINDOWS_LOGIN	0	6/6/2024 13:36	NT_USER	0	0	0	0	0	0	0	0	0			0