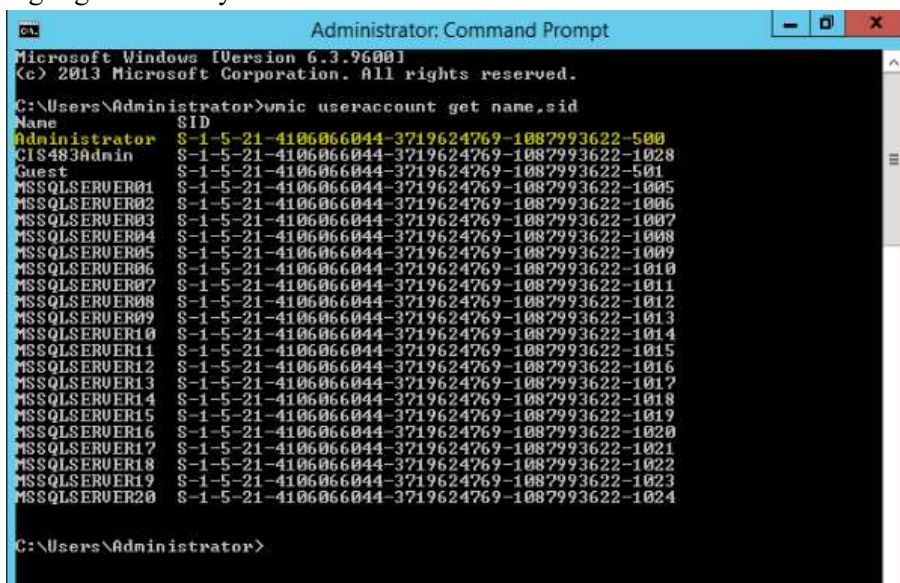


## Lab: SID

- This is worth 10 points and due tonight.
- Follow the usual naming convention. Place your answers on the separate tasks file and submit it. DO NOT use this file for submission.
- Please **zoom in** your screenshots.

### Task 1: Getting SID, SAT in Windows

- Obtain the SID of the current login with **WMIC** command. Attach a screenshot for the SID and highlight it in red/yellow.

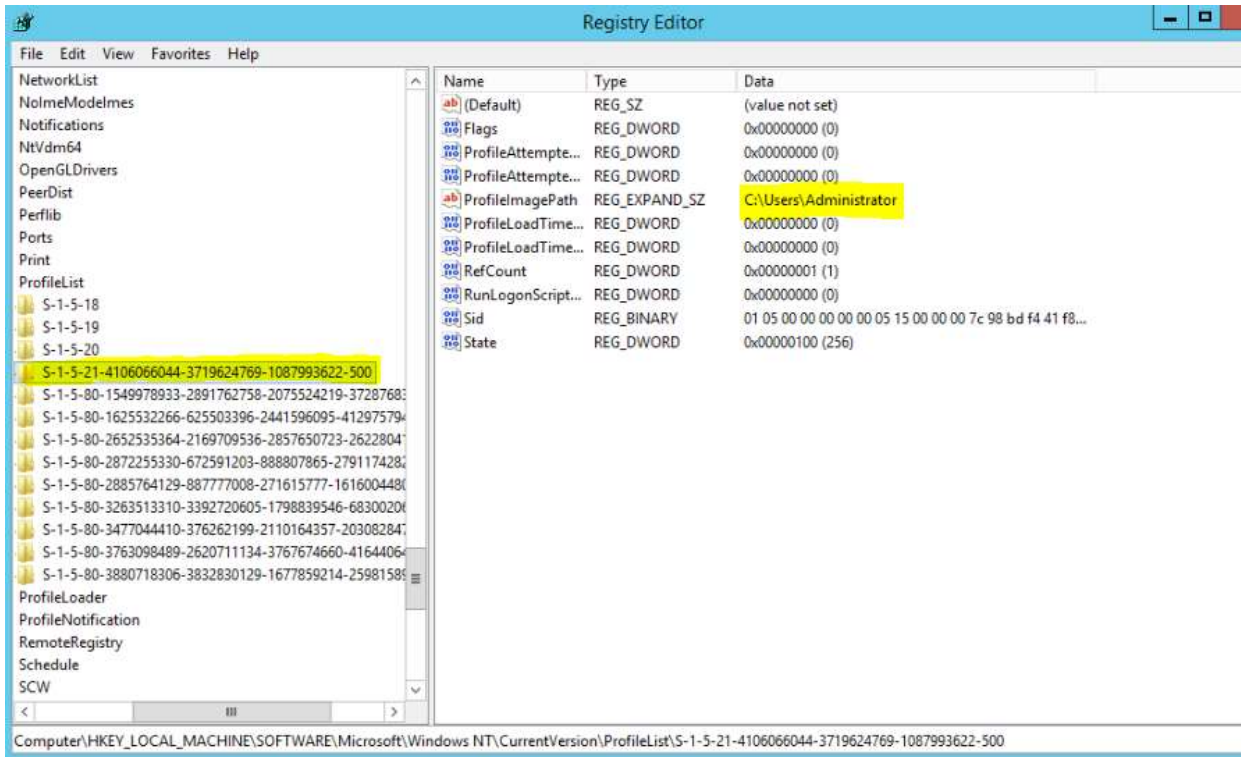


```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>wmic useraccount get name,sid
Name                SID
Administrator      S-1-5-21-4106066044-3719624769-1087993622-500
CIS483Admin         S-1-5-21-4106066044-3719624769-1087993622-1028
Guest               S-1-5-21-4106066044-3719624769-1087993622-501
MSSQLSERVER01       S-1-5-21-4106066044-3719624769-1087993622-1005
MSSQLSERVER02       S-1-5-21-4106066044-3719624769-1087993622-1006
MSSQLSERVER03       S-1-5-21-4106066044-3719624769-1087993622-1007
MSSQLSERVER04       S-1-5-21-4106066044-3719624769-1087993622-1008
MSSQLSERVER05       S-1-5-21-4106066044-3719624769-1087993622-1009
MSSQLSERVER06       S-1-5-21-4106066044-3719624769-1087993622-1010
MSSQLSERVER07       S-1-5-21-4106066044-3719624769-1087993622-1011
MSSQLSERVER08       S-1-5-21-4106066044-3719624769-1087993622-1012
MSSQLSERVER09       S-1-5-21-4106066044-3719624769-1087993622-1013
MSSQLSERVER10       S-1-5-21-4106066044-3719624769-1087993622-1014
MSSQLSERVER11       S-1-5-21-4106066044-3719624769-1087993622-1015
MSSQLSERVER12       S-1-5-21-4106066044-3719624769-1087993622-1016
MSSQLSERVER13       S-1-5-21-4106066044-3719624769-1087993622-1017
MSSQLSERVER14       S-1-5-21-4106066044-3719624769-1087993622-1018
MSSQLSERVER15       S-1-5-21-4106066044-3719624769-1087993622-1019
MSSQLSERVER16       S-1-5-21-4106066044-3719624769-1087993622-1020
MSSQLSERVER17       S-1-5-21-4106066044-3719624769-1087993622-1021
MSSQLSERVER18       S-1-5-21-4106066044-3719624769-1087993622-1022
MSSQLSERVER19       S-1-5-21-4106066044-3719624769-1087993622-1023
MSSQLSERVER20       S-1-5-21-4106066044-3719624769-1087993622-1024

C:\Users\Administrator>
```

- Obtain the SID of the current login in the Registry. Attach a screenshot for the SID and highlight it in red/yellow.



## Task 2: Getting SID in SQL Server

- Get the SID of the account you used for SQL Server login.
- A. SID: 0x010500000000000005150000007C98BDF441F8B4DD1677D940F4010000.
- B. What is the role of the function “fn\_SIDToString” in the above? The role of the function “fn\_SIDToString” retrieves the SID from the local machine, parses it from a hexadecimal into a string, and then returns the string.
- C. Show in screenshots that the SID from SQL Server for the administrator login and that from Windows Server are the same. Compare the SIDs in a string format (not binary).

SQLQuery1.sql - Win...Administrator (54)) \* - X

```
SELECT *
FROM sys.server_principals
```

100 %

Results Messages

	principal_id	sid
12 mSigningCertificate...	102	0x01060000000000009010000006614898B406FF993D488BA0385EE027AC97C
13 atorCertificate##	103	0x0106000000000000901000000EE747B84C5199C269923E3E59D30D25EB79
14 Certificate##	105	0x0106000000000000901000000DCAED0CCB132F656A0E972C008CD036658f
15 SigningCertificate##	106	0x01060000000000009010000002FB3F79B3304FFA24B6CE32B888FA353904f
16 utionLogin##	257	0xB5BA3F49077DF14C95D37EBB67C49F8F
17 \Administrator	259	0x010500000000000005150000007C98BDF441F8B4DD1677D940F4010000

SQLQuery1.sql - Win...Administrator (54)) \* - X

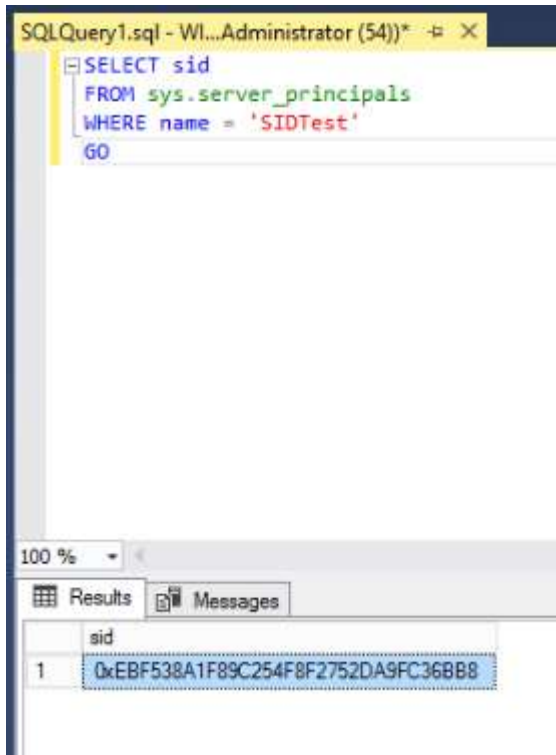
```
SELECT SUSER_NAME(), SUSER_SID(), dbo.fn_SIDToString(SUSER_SID())
```

100 %

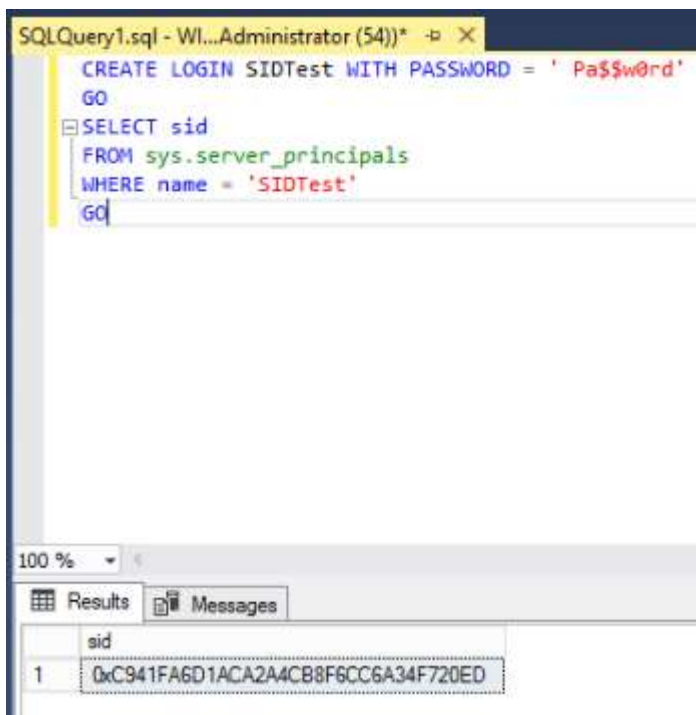
Results Messages

	(No column name)	(No column name)
1	WIN-AVPBP9ATULM\Administrator	0x010500000000000005150000007C98BDF441F8B4DD1677D940F4010000

- D. SID: 0xEBF538A1F89C254F8F2752DA9FC36BB8



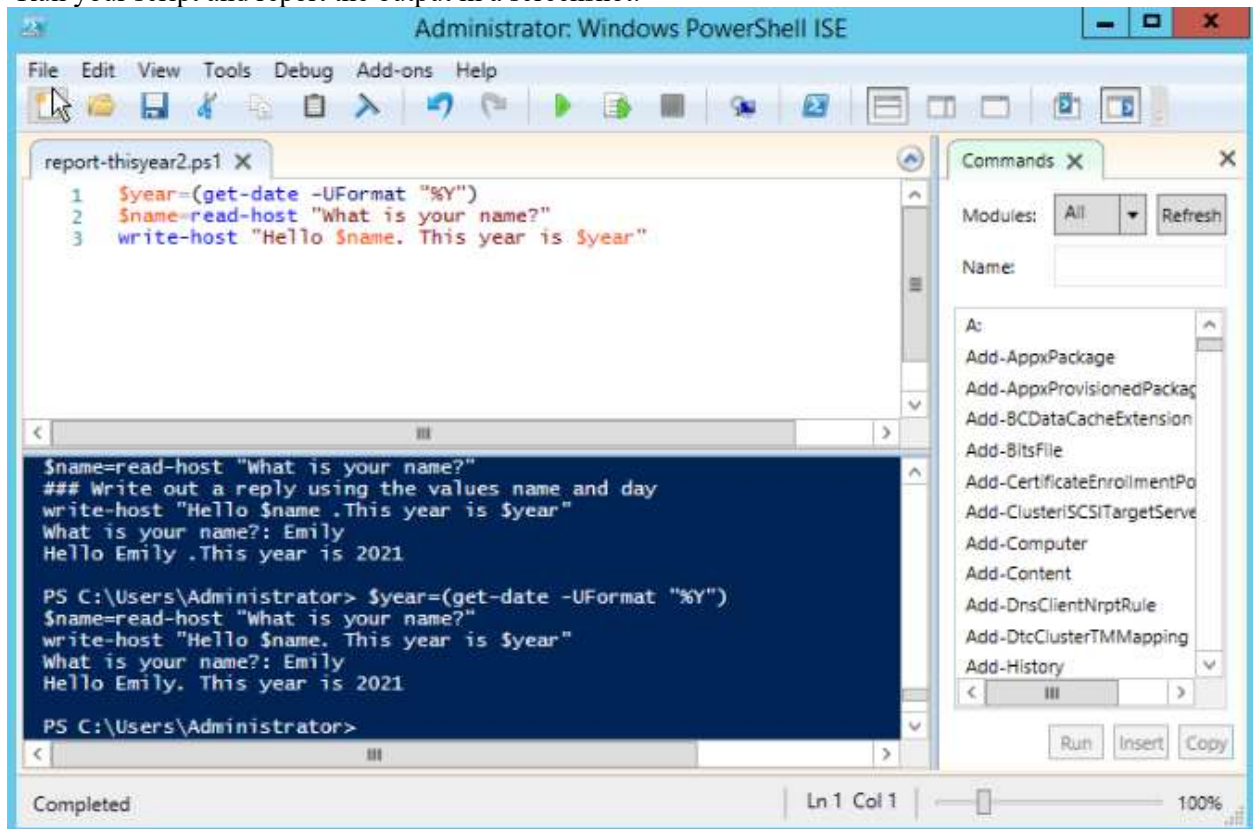
- E. SID: 0xC941FA6D1ACA2A4CB8F6CC6A34F270ED



- F. Are the SIDs of login `SIDTest` the same? Describe the reason why they are (not) the same? No, they are not the same because we used a password the second time.

### Task 3: Learn PowerShell Scripting

- Run your script and report the output in a screenshot.



The screenshot displays the Windows PowerShell ISE interface. The main editor window shows a script named `report-thisyear2.ps1` with the following content:

```
1 $year=(get-date -UFormat "%Y")
2 $name=read-host "What is your name?"
3 write-host "Hello $name. This year is $year"
```

The console window below the script shows the execution of the script. It prompts the user for their name, which is entered as "Emily". The script then outputs the message "Hello Emily. This year is 2021".

```
$name=read-host "What is your name?"
## Write out a reply using the values name and day
write-host "Hello $name. This year is $year"
What is your name?: Emily
Hello Emily. This year is 2021

PS C:\Users\Administrator> $year=(get-date -UFormat "%Y")
$name=read-host "What is your name?"
write-host "Hello $name. This year is $year"
What is your name?: Emily
Hello Emily. This year is 2021

PS C:\Users\Administrator>
```

The status bar at the bottom indicates "Completed" and "Ln 1 Col 1".