

Lab: SID

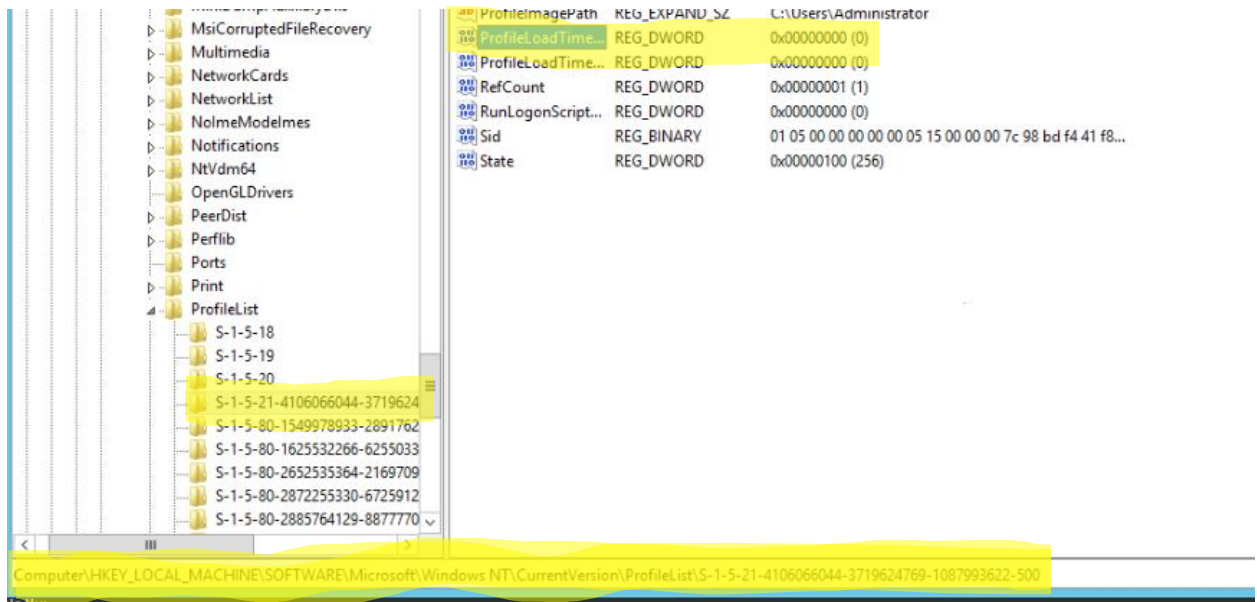
- This is worth 10 points and due tonight.
- Follow the usual naming convention. Place your answers on the separate tasks file and submit it. DO NOT use this file for submission.
- Please **zoom in** your screenshots.

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.

```
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
```

- 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

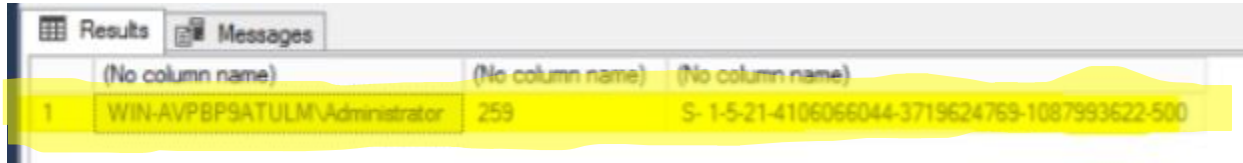
- Get the SID of the account you used for SQL Server login.
- A. SID: 0x0105000000000005150000007C98BDF441F8B4DD1677D940F4010000

SPID	LOGIN	SID
6	##MS_Policy\sql\executionLogi...	0xB5BA3F490770F14C9D037EB867C49F8F
7	WIN-AVPBP9ATULM\Administr...	0x0105000000000005150000007C98BDF441F8B4DD1677D940F4010000

- B. What is the role of the function “fn_SIDToString” in the above?

The role of the function is to change the SID integer value to a string value. "S-"

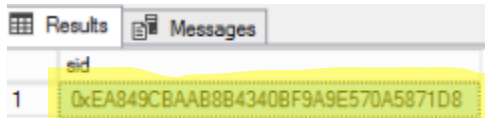
- C. Show in screenshots that the SID from SQL Server for the administrator login and that from Windows Server are the same. Compare the SIDs in a string format (not binary).



	(No column name)	(No column name)	(No column name)
1	WIN-AVPBPSATULM\Administrator	259	S-1-5-21-4106066044-3719624769-1087993622-500

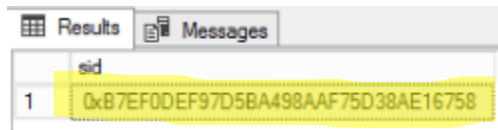
They are the same if you reference the screenshot above.

- D. SID: _____0xEA849CBAAB8B4340BF9A9E570A5871D8_____.



	sid
1	0xEA849CBAAB8B4340BF9A9E570A5871D8

- E. SID: _____0XB7EF0DEF97D5BA498AAF75D38AE16758_____.

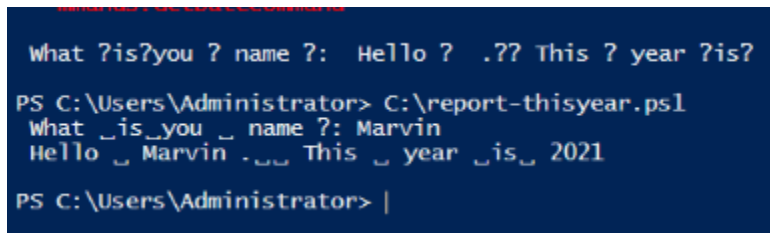


	sid
1	0XB7EF0DEF97D5BA498AAF75D38AE16758

- F. Are the SIDs of login `SIDTest` the same? Describe the reason why they are (not) the same?
They are not the same. The login record was deleted so the SID value changes when a new login record was created.

Task 3: Learn PowerShell Scripting

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



```
What is your name?: Hello .?? This year is?  
PS C:\Users\Administrator> C:\report-thisyear.ps1  
What is your name?: Marvin  
Hello Marvin .?? This year is 2021  
PS C:\Users\Administrator> |
```