

## Lab – SID

- This is worth 10 points and due tonight.
- Follow the usual naming convention.
- Please **zoom in** your screenshots.

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

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

S-1-5-21-646919476-1537115703-3374233482-500

```

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

C:\Windows\system32>wmic useraccount get name,sid
Name SID
Administrator S-1-5-21-646919476-1537115703-3374233482-500
Guest S-1-5-21-646919476-1537115703-3374233482-501

C:\Windows\system32>
  
```

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

S-1-5-21-646919476-1537115703-3374233482-500

### Task 2: Getting SID on SQL Server

Get the SID of the account you used for SQL Server login.

A. SID: \_\_\_\_\_.

0x010500000000000051500000034358F2637869E5B8AB71EC9F4010000

S-1-5-21-646919476-1537115703-3374233482-500

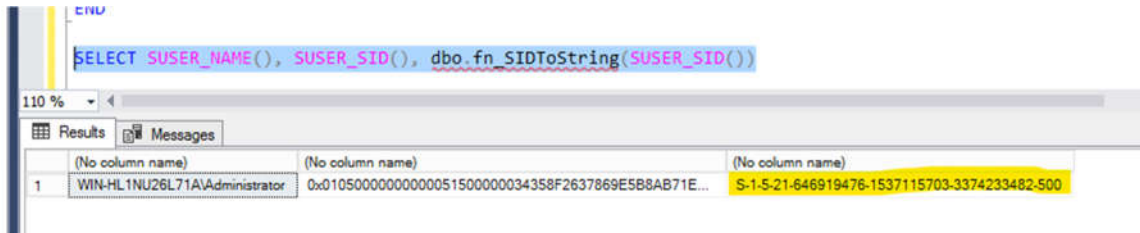
13	##MS_SQLAuthenticatorCertificate##	103	0x01060000000000009010000009C2489DA5896119E5966619B7C4599A48A60E095	C	CERTIFICATE_MAPPED_LC
14	##MS_PolicySigningCertificate##	105	0x010600000000000090100000D869A47D58180CB1AA6465F30AD19B9A8ABB2C83	C	CERTIFICATE_MAPPED_LC
15	##MS_SmoExtendedSigningCertificate##	106	0x01060000000000009010000008A55BB60CE89D5ABFF5EB0A0B0E2995ABEB7B983	C	CERTIFICATE_MAPPED_LC
16	##MS_PolicyTsqlExecutionLogin##	257	0xB5BA3F49077DF14C95D37EBB67C49F8F	S	SQL_LOGIN
17	WIN-7CO68DHNIT\Administrator	259	0x010500000000000051500000034358F2637869E5B8AB71EC9F4010000	U	WINDOWS_LOGIN
18	NT SERVICE\SQLWriter	260	0x0106000000000000550000000732B9753646EF90356745CB675C3AA6CD6B4D28B	U	WINDOWS_LOGIN
19	NT SERVICE\Winmgmt	261	0x01060000000000005500000005A048DFF9C7430AB450D4E7477A2172AB4170F4	U	WINDOWS_LOGIN
20	NT Service\MSSQLSERVER	262	0x0106000000000000550000000E20F4FE7B15874E48E19026478C2DC9AC307B83E	U	WINDOWS_LOGIN
21	NT AUTHORITY\SYSTEM	263	0x01010000000000000512000000	U	WINDOWS_LOGIN

B. What is the role of the function “fn\_SIDToString” in the above?

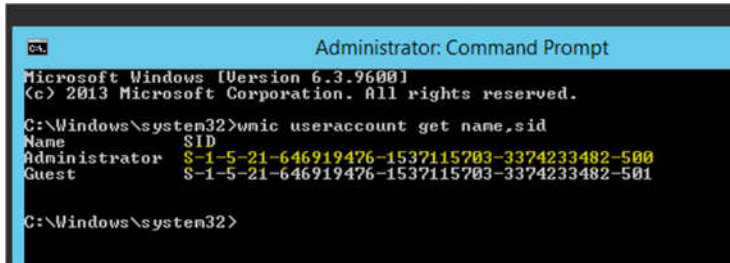
Converts a SID stored in Hexadecimal format to a string format that starts with “S-”

C. Compare the SID from SQL Server for the administrator login with that from Windows Server for the administrator. Show the two screenshots. Use the SIDs in a string format (that is, in the S- format, not in Hex). Are they the same?

The SID of the administrator login from SQL Server (show the S-format)  
S-1-5-21-646919476-1537115703-3374233482-500

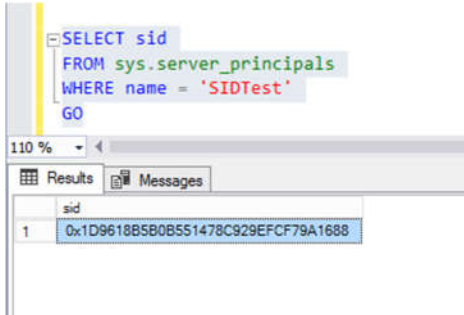


The SID of the administrator login from Windows Server (show the S-format)  
S-1-5-21-646919476-1537115703-3374233482-500



D. SID: \_\_\_\_\_.

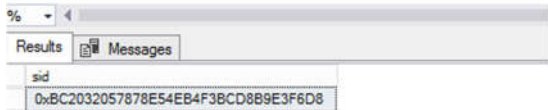
0x1D9618B5B0B551478C929EFCF79A1688



E. SID: \_\_\_\_\_.

0xBC2032057878E54EB4F3BCD8B9E3F6D8

```
CREATE LOGIN SIDTest WITH PASSWORD = ' Pa$$w0rd'
GO
SELECT sid
FROM sys.server_principals
WHERE name = 'SIDTest'
GO
```



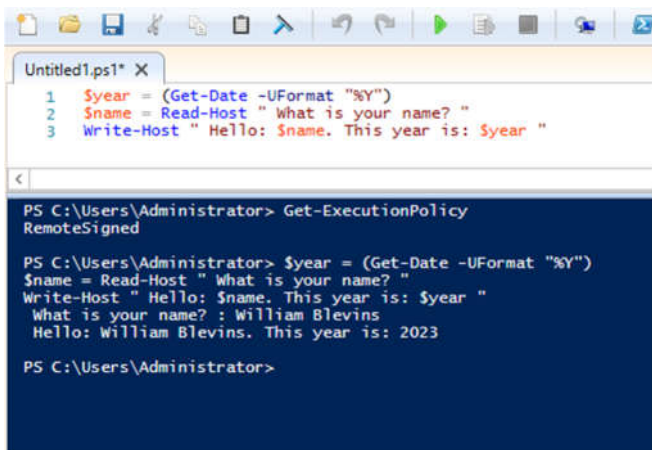
sid
0xBC2032057878E54EB4F3BCD8B9E3F6D8

F. Are the SIDs of login `SIDTest` the same? Describe the reason why they are (not) the same?

They are not the same. A unique SID was assigned when the first `SIDTest` was created. When that account was dropped, the unique SID was removed as well. When the second account was created, Windows assigned a second unique SID to the account, even though the name matches. It is a separate account with a separate SID.

### Task 3: Learn PowerShell Scripting

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



```
1 $year = (Get-Date -UFormat "%Y")
2 $name = Read-Host " What is your name? "
3 Write-Host " Hello: $name. This year is: $year "
```

```
PS C:\Users\Administrator> Get-ExecutionPolicy
RemoteSigned

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? : William Blevins
Hello: William Blevins. This year is: 2023

PS C:\Users\Administrator>
```