Lab 4 – SID, PowerShell

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.

CA.	Administrator: Command Prompt	_	×
C:\Users\Admin useraccout - f	istrator≻wmic useraccout get name,sid llias not found.		^
C:\llsevs\Admir	histrator/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		
MSSQLSERVERØ1	S-1-5-21-4106066044-3719624769-1087993622-1005		
MSSQLSERVER02	S-1-5-21-4106066044-3719624769-1087993622-1006		
MSSQLSERVERØ3	S-1-5-21-4106066044-3719624769-1087993622-1007		
MSSQLSERVERØ4	S-1-5-21-4106066044-3719624769-1087993622-1008		
MSSQLSERVER05	S-1-5-21-4106066044-3719624769-1087993622-1009		
MSSQLSERVERØ6	S-1-5-21-4106066044-3719624769-1087993622-1010		
MSSQLSERVER07	S-1-5-21-4106066044-3719624769-1087993622-1011		
MSSQLSERVERØ8	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	5-1-5-21-4106066044-3719624769-1087993622-1016		
MSSQLSERUER13	S-1-5-21-4106066044-3719624769-1087993622-1017		
MSSQLSERVER14	5-1-5-21-4106066044-3719624769-1087993622-1018		
ISSQLSERVER15	S-1-5-21-4106066044-3719624769-1087993622-1019		
ISSULSERVER16			~
1554LSERVER17	5-1-5-21-4106066044-3719624769-1087993622-1021		×.

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

lit Vi	ew Favorites Help					
	MCI32 MiniDumpAuxiliaryDlls MixoruptedFileRecovery Multimedia NetworkCards NetworkList NolmeModelmes Notifications NtVdm64 OpenGLDrivers PeerDist PeerDist	~	Name (Default) Flags ProfileAttempte ProfileAttempte ProfileImagePath ProfileLoadTime ProfileLoadTime RefCount RefCount RunLogonScript Sid	Type REG_SZ REG_DWORD REG_DWORD REG_EXPAND_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_BINARY	Data (value not set) 0x00000000 (0) 0x00000000 (0) C:\Users\Administrator 0x00000000 (0) 01 05 00 00 00 00 05 15 00 00 00 7c 98 bd f4 41 f8	
	Ports Print ProfileList S-1-5-18 S-1-5-19 S-1-5-20 S-1-5-20 S-1-5-20-1540978933-2891762758-20 S-1-5-80-1625532266-625503396-244 S-1-5-80-1625532266-625503396-244 S-1-5-80-265253330-672591203-888 S-1-5-80-2885764129-887777008-27 S-1-5-80-328513310-3392720605-11 S-1-5-80-347704410-376262199-21 S-1-5-80-3477044410-376262199-21	08 07: 41: 35: 88(≡ 16 794 10: 76	B State	REG_DWORD	0x00000100 (256)	
	III	>				

Task 2: Getting SID on SQL Server

Get the SID of the account you used for SQL Server login. A. SID for WIN-AVPBP9ATULM\Administrator: 0x01050000000005150000007C98BDF441F8B4DD1677D940F4010000

B. What is the role of the function "fn_SIDToString" in the above?

It takes a binary SID ('@BinSID') and converts the input into a string

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)

SELECT SUSER_NAME(), SUSER_SID(), dbo.fn_SIDToString(SUSER_SID()) Image: state	SQLQuery1	.sql - WIN-AVPBP9ATULM.master (WIN-AVPBP9ATULM\Adn	ninistrator (56))*
Results Messages (No column name) (No column name) Administrator 0x01050000000005150000007C98BDF441F884DD1677D9 S-1-5-21-4106066044-3719624769-1087993622	SELECT SU	<pre>SER_NAME(), SUSER_SID(), dbo.fn_SIDToString(SU</pre>	SER_SID())
Results Messages (No column name) (No column name) Administrator 0x01050000000005150000007C98BDF441F8B4DD1677D9 S-1-5-21-4106066044-3719624769-1087993622			
Results Image: Messages (No column name) (No column name) Administrator 0x01050000000005150000007C98BDF441F8B4DD1677D9 S-1-5-21-4106066044-3719624769-1087993622			
Results Image: Messages (No column name) (No column name) Administrator 0x01050000000005150000007C98BDF441F8B4DD1677D9 S-1-5-21-4106066044-3719624769-1087993622			
No. Nessages Results Image: Messages (No column name) (No column name) Administrator 0x01050000000005150000007C98BDF441F8B4DD1677D9 S-1-5-21-4106066044-3719624769-1087993622			
Results Results Messages (No column name) (No column name) Administrator 0x01050000000005150000007C98BDF441F8B4DD1677D9 S-1-5-21-4106066044-3719624769-1087993622			
(No column name) (No column name) \Administrator 0x01050000000005150000007C98BDF441F8B4DD1677D9 \$-1-5-21-4106066044-3719624769-1087993622			
\Administrator 0x010500000000005150000007C98BDF441F8B4DD1677D9 S-1-5-21-4106066044-3719624769-1087993622	Results	Messages	
	Results	Messages (No column name)	(No column name)
	Results	Messages (No column name) 0x0105000000000005150000007C98BDF441F8B4DD1677D9	(No column name) . S-1-5-21-4106066044-3719624769-1087993622
	Results	Messages (No column name) 0x0105000000000005150000007C98BDF441F8B4DD1677D9	(No column name) . <u>S-1-5-21-4106066044-3719624769-1087993622</u>
	Results	Messages (No column name) 0x0105000000000005150000007C98BDF441F8B4DD1677D9	(No column name) . S-1-5-21-4106066044-3719624769-1087993622
	Results Results	Messages (No column name) 0x0105000000000005150000007C98BDF441F8B4DD1677D9	(No column name) . S-1-5-21-4106066044-3719624769-1087993622
	Results Results	Messages (No column name) 0x0105000000000005150000007C98BDF441F8B4DD1677D9	(No column name) . S-1-5-21-4106066044-3719624769-1087993622

The SID of the administrator login from Windows Server (show the S-format)

0 GM	Administrator: Command Prompt	 ×
C:\Users\Admin	istrator)wmic_useraccout_get_name,sid	~
useraccout - H	llas not found.	=
C:\Users\Admin	istrator>wmic useraccount get name,sid	1000
Name		
Administrator	5-1-5-21-4106066044-3719624769-1087993622-500	
GIS483Hdmin		
GUEST MCCATCEDUEDA4	2-1-5-21-4100000044-3717024707-100773022-501 2-1-5-21-4100000044-3717024707-10073022-501	
MSSOLSERUER02	S-1-5-21-41060666044-3719624769-1087993622-1005	
MSSOLSERUER03	S-1-5-21-4106066044-3719624769-1087993622-1007	
MSSOLSERUER04	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	
ASSULSERVER13		
MCCOLCEDUED4	5-1-5-21-4106066044-3717624767-1087773622-1018	
MCCOL CEDUEDIC	5-1-5-21-4106066044-3717624767-1087773622-1017 c_1_c_91_4106066044-3717624769-1007093699-1090	
MCCOLCEDIED4 7	<u>5-1-5-21-41060606044-5717624767-1067773622-1020</u> c_1_5_21_41060666044-3719624769-1087993622-1020	V
Horoghoremotent 7	3 1 3 21 1100000011 3717021707 1007773022 1021	

They are the same

D. SID: 0xCBD189CBF1CE5E4BAE1310033D61F163

E. SID: 0XEE7C4ECFC463DE49BBD62A1C5E434372

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

They are not the same. SQL server generates a random new SID for security purposes whenever you create, drop, and recreate an account even if it's the same account.

Task 3: Learn PowerShell Scripting

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

