[Exploitation/Windows] Ouvrir un shell NT authorité système

Introduction

Ce tuto vous permettra d'ouvrir un shell avec les droits systèmes.



Manuel

- Tout d'abord, téléchargez la suite **SysInternal** sur le site de Microsoft :

https://learn.microsoft.com/fr-fr/sysinternals/downloads/sysinternals-suite

- Vous pouvez extraire l'archive dans le dossier **C:\Windows\System32** pour avoir **PsExec** dans le path.
- Désormais, lancer un **cmd** en tant qu'administrateur et lancez la commande suivante :

```
PsExec.exe -s -i cmd.exe
```

Revision #4
Created 2023-11-14 11:07:19 UTC by Elieroc
Updated 2024-05-03 13:11:39 UTC by Elieroc