Poor Windows

Auteur	Catégorie	Niveau
Cécile	Forensic	Facile

Énoncé :

Intro

J'ai voulu jouer à un mini-jeu envoyé par l'un de mes amis mais quand j'ai cliqué sur l'exécutable, mon PC a crashé. Peux tu me donner le nom de l'executable qui a fait planté mon PC grace au dump que j'ai récupéré ? Le format du flag est **NHM2l{nomdufichiersanslextension}**.

Pièce Jointe

Un fichier MEMORY.DMP

Préparation du challenge

Objectif

Comprendre la logique du forensic et les étapes à suivre.

Flag

NHM2l{c3stnullw1nd0ws}

Démarche

Après avoir créé une machine windows, on créé un petit fichier .bat contenant un script qui fait crasher la machine et on récupère ensuite un dump mémoire pour l'analyser.

Le script utilisé est le suivant :

```
@echo off
:crash
start
goto crash
```

> + **System**
> - **EventData**
>
> | | |
> |---|---|
> | **param1** | 0xc0000022 (0x0000000000000000, 0x0000000000000000, 0x0000000000000000, 0x0000000000000000) |
> | **param2** | C:\Windows\MEMORY.DMP |
> | **param3** | 90051ebe-ae56-4696-b6f5-1f063403149d |

L'ordinateur a redémarré après une vérification d'erreur. La vérification d'erreur était : 0xc0000022 (0×0000000000000000, 0×0000000000000000, 0×0000000000000000, 0×0000000000000000). Un vidage a été enregistré dans : C:\Windows\MEMORY.DMP. ID de rapport : 90051ebe-ae56-4696-b6f5-1f063403149d.

Résolution :

Solution débutant ++ :

On se renseigne sur ce qu'est un fichier .dmp :
Il s'agit d'un fichier de vidage mémoire créé lorsqu'un système d'exploitation plante ou rencontre une erreur critique.
ils peuvent contenir des informations sur l'état de la mémoire, les fichiers ouverts, etc ....

On fait un file sur le fichier pour en apprendre un peu plus sur lui :

```
file MEMORY.DMP      ◖ ✔ ◗ 5s
MEMORY.DMP: MS Windows 64bit crash dump, 4992030524978970960 pages
```

Il semble très long (4992030524978970960 pages).

On essaye d'utiliser strings mixé avec grep pour chercher les lignes ou il y a .exe :

```
strings MEMORY.DMP | grep '.exe'
```

Et en parcourant les nombreux résultats on tombe sur un fichier qui ressemble à un flag :

```
d.exe /c vssadmin
serv.exe\:c,
hellexecuteas.
x_exe_pa
C:\Users\harrypotter\Desktop\c3stnullw1nd0ws.exe
mmap.exe
smR1asm.exe
obj.exe
smR1lp.exe
ec.exe
\Device\HarddiskVolume3\Users\harrypotter\Desktop\c3stnullw1nd0ws.exe
\Device\HarddiskVolume3\Windows\System32\Fondue.exe
Applications\notepad.exe_.DMP
Applications\notepad.exe_.hta
```