Théa Fortin

Game hacking

whoami

- Chercheure cyber & consultante
- Graduée du collège communautaire du NB
- Net+, Sec+, CBBH, CPTS, PNPT, PJMT
- Développeure de challs au Hackfest

Qu'est-ce que le game hacking?

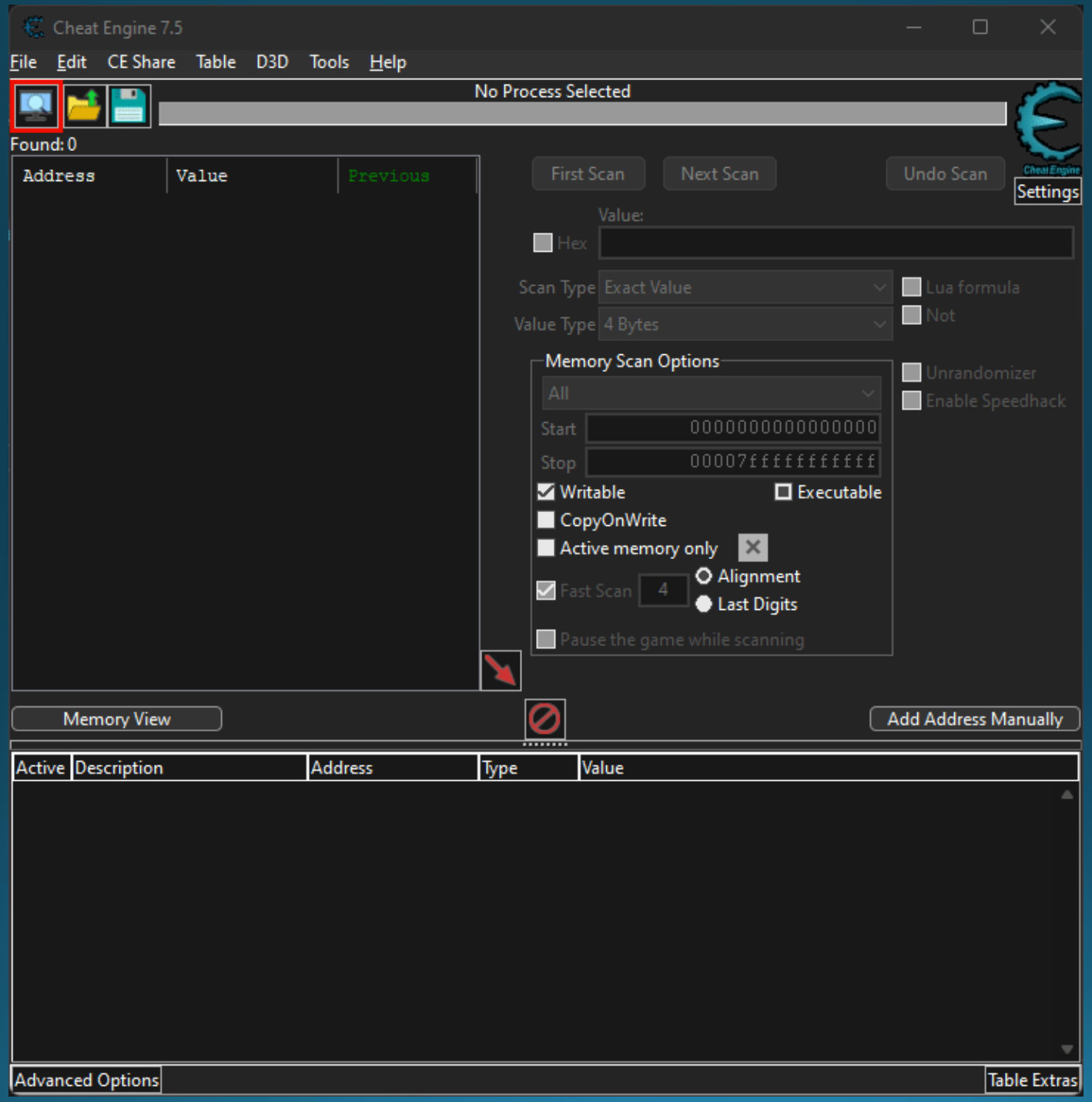
- Gagner un avantage injuste par des moyens involontaires
- Modding, Runtime Hooks, MitM, Modification mémoire…
- Aimbot, Godmode, infinite bullets…

Pourquoi faire du game hacking?

- S'applique à d'autres aspects de la cybersécurité
- Le piratage éthique de jeux vidéo est du vrais travail
- Contribu au développement de mods et de modding SDKs

Cheat Engine

- Créer par DarkByte au début des années 2000s
- Scanne, filtre et manipule la mémoire d'un processus


Cheat Engine 7.5
File
Edit
CE Share
Table
D3D
Tools
Help
No Process Selected
Found: 0
Address
Value
Previous
First Scan
Next Scan
Undo Scan
Settings
Value:
Hex
Scan Type
Exact Value
Value Type
4 Bytes
Lua formula
Not
Memory Scan Options
All
Start
0000000000000000
Stop
00007fffffffffff
Writable
Executable
CopyOnWrite
Active memory only
Fast Scan
4
Alignment
Last Digits
Pause the game while scanning
Unrandomizer
Enable Speedhack
Memory View
Add Address Manually
Active
Description
Address
Type
Value
Advanced Options
Table Extras

SuperTuxKart

Scanner et modifier de la mémoire

- Sélectionner le processus
- Faire un scan initial des valeurs cherchées
- Scanner pour les valeurs cherchées pour réduire les résultats jusqu'à ce que l'addresse cherchée soit trouvée
- Ajouter l'addresse a la cheat table et la modifier au besoin

Structures de données

- Défini des relations entre des variables appartenant à des data types individuels
- Chaque élément est stocké dans un bloque de mémoire contigu

```
struct Userstats{
float stamina;
int health;
double score;
}
```

Array of Bytes (AOB)

- Bloque de mémoire contiguë où chaque élément stocke un byte de donnée
- Représente souvent du bytecode
- Utile pour identifier des séquences spécifiques de code pointant à des variables cible
- Pointers

Insruction	Bytecode
mov eax 1	B8 01 00 00 00
add eax 2	83 C0 02
ret	C3

```
byte byteArray[] = {
  0xB8, 0x01, 0x00, 0x00, 0x00, // mov eax, 1
  0x83, 0xC0, 0x02 // add eax, 02
  0xC3 // ret
};
```

Scripting AOB

- Identifier les instructions accédant ou écrivant à la variable
- Créer un nouveau script d'injection AoB
- Modifier au besoin

Exercice

- Créer un script AOB pour gagner des vies infinis dans battle mode
- SuperTuxKart –> Singleplayer -> Battle

Aller plus loin…

- https://www.youtube.com/@StephenChapman
- https://www.youtube.com/@nathanbaggs/videos
- https://www.youtube.com/@MattKC

- Pwn island
- Hack the box game hacking challenges