Introduction au GameHacking

Électif ESGI - 4A 2024 / 2025

whoami

Simon ‘astalios’ DE BROU

ESGI Alumni

Administrator @ Hacklab ESGI

Security and Network Engineer @ ACKnowledge

discord : astalios

Calendrier de Cours

Jeudi 31/10 - Presentation generale du domaine, structure du cours, révisions des bases, Cheat Engine pt 1

Vendredi 29/11 - Cheat Engine pt 2, ReClass pt 1

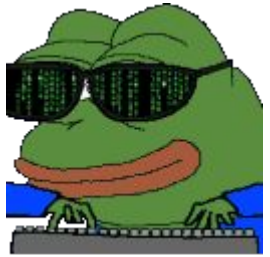
Vendredi 20/12 - External Hack pt 1, ReClass pt 2

Vendredi 17/01 - External Hack pt 2, Internal Hack pt 1

Vendredi 07/02 - Internal Hack pt 2, DLL Injection

Mercredi 05/03 - Examen

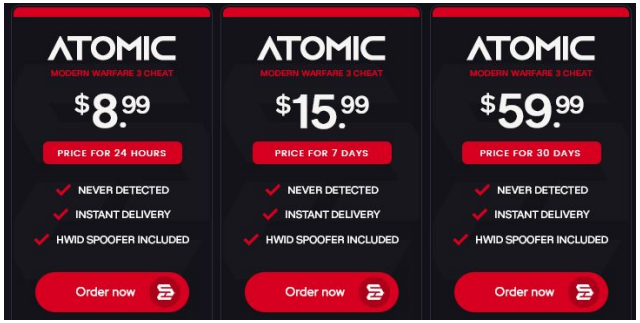
Table des Matières

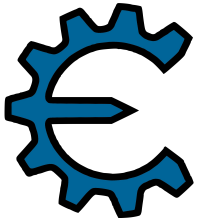


Le GameHacking

Le sujet est très large

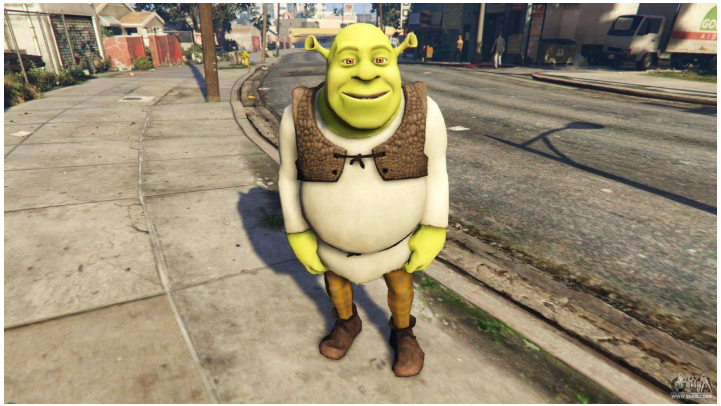
- Pour certains c’est simplement tricher dans un jeu vidéo
  - Donne un avantage conséquent et injuste contre les autres joueurs
  - Domaine très lucratif





Cheat engine, le scanner de mémoire le plus populaire dans le domaine du GameHacking

Le GameHacking



Nexus mods, la référence dans la communauté modding

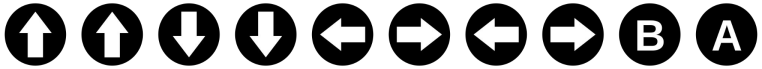
- Pour d’autre ça modifie l’expérience du jeu
  - Modder son jeu est une forme de hacking
    - Ajout de nouveaux **assets**, modification des textures
  - Débloquer le menu développeur
    - Accéder à des features cachées

Le GameHacking

- Cracker des Jeux
  - Développement des crack no-cd
  - Rétro-Ingénierie pour développer des **keygen** (générateur de clef)
  - Contournement (bypass) des **DRM** (Digital Rights Management)

Notons cependant que ces méthodes citées ci-dessus sont applicable de manière plus générale à l'univers du développement logiciel

Point Histoire



Un peu de contexte historique

- Années 80 : à l'époque, l'un des seuls moyens de tricher reposait dans les codes de triches intégrés par les développeurs.
  - *Par exemple le légendaire code Konami*
- Début des années 90, arrivée du *GameGenie,* une des premières cartouches "3rd Party" (de contrefaçon)
- Fin 90, la naissance du modding de jeux
  - https://gamehacking.org/ est une référence !
- De la fin des années 90 à Aujourd'hui, le gamehacking tel qu'on le connaît aujourd'hui :
  - Aimbot, ESP, god-mode, Infinite Ammo, no-recoil, etc.

Comment Lutter ?

On développe des outils anti-triche.

Un outil anti-triche est au jeu vidéo ce qu'un **XDR** est à un poste informatique:

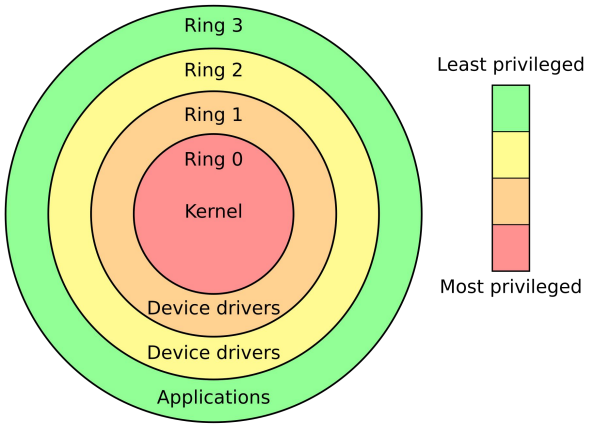
- Regarder les actions utilisateurs
- Analyser en temps réel si des applications tierces ne scannent pas les processus ou tentent de modifier l'outil ou le jeu surveillé
- Passer en revue les données envoyées par le joueur
    - C'est comme ça qu'on détectait les tricheurs à l'époque d'unreal tournament dans les années 90

État de l’art des AntiCheat

La majorité des produits anti-triche nécessitent aujourd’hui des appareils **DMA**.

Quelques AntiCheats réputés:

- Vanguard, FaceIt, EasyAntiCheat.
  - Ce sont des **Kernel AntiCheat**.
    - Ce qui signifie qu’ils sont chargés au noyau de l’ordinateur, en tant que driver ou service.
    - Ce sont des produits très bas niveau, avec un contrôle très pointu sur l’appareil de l’utilisateur.
    - Placé très proche du **ring 0**



Ring kernel - niveau de privilège, aujourd’hui Vanguard est dans le ring 0, discord dans le ring 3

État de l’art des AntiCheat

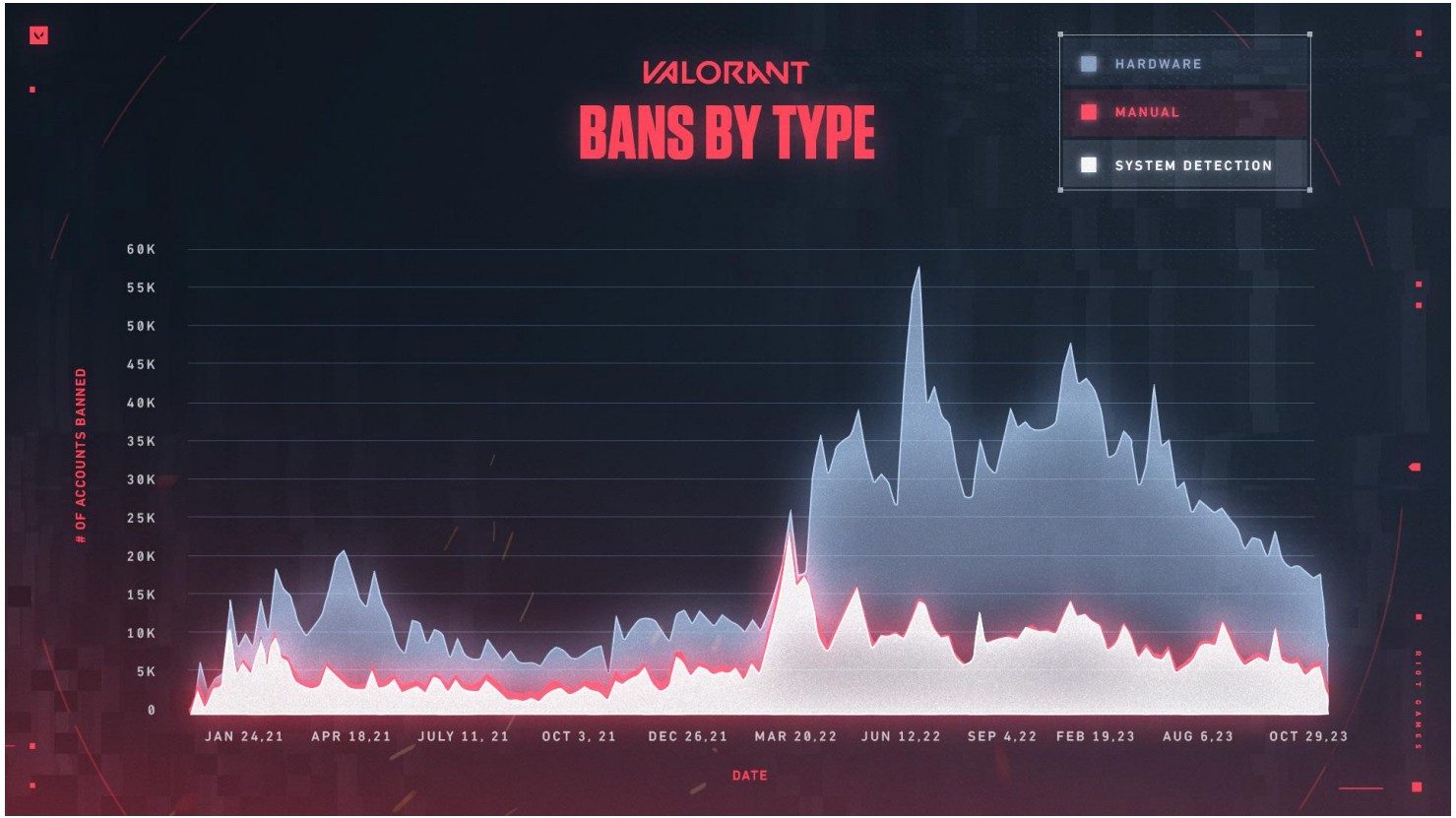
Vanguard :

- Considéré par Internet comme le meilleur AntiCheat actuel.
  - Dans la réalité, c’est parce qu’il est présent sur très peu de jeux :
    - *League of Legends, TFT, Valorant, etc.*

La course est extrêmement rude, et sont souvent en retard par rapport aux méthodes de contournement anti-triche.

Certaines méthodes utilisées pour tricher aujourd’hui font fureur dans le domaine de la cybersécurité pour attaquer certains systèmes, au niveau du contournement des détections mises en places sur les machines.

État de l’art des AntiCheat



Point Définitions

Ce qu’on a vu :

Hacking - Ensemble des techniques et des méthodes pour explorer, manipuler ou contourner quelque chose, souvent pour comprendre son fonctionnement.

DRM - Digital Right Management, terme utilisé pour les mécanismes anticopie

keygen - Générateur de Clefs produits

no-cd Crack - Crack pour se passer du DVD / CD

XDR - Extended Detection and Response - Solution de cybersécurité qui combine plusieurs sources de détection.

DMA - Direct Memory Access - Outil Physique se branchant sur un ordinateur permettant l’analyse et l’ édition en temps réelle de la mémoire sur l’ordinateur, les Cheat DMA sont donc des cartes qui ont été programmées pour s’injecter sur le poste et y altérer le fonctionnement du jeu pour tricher.

Les Pointeurs

- Variable qui stocke l’adresse mémoire d’une autre variable
- Dans le monde du Game Hacking on va manipuler directement la mémoire, a terme on pourra aussi noter des gains de performance.

Pour des besoins d’analogie, on va penser que chaque case mémoire, est une maison au sein de l’ordinateur.

Les Pointeurs

```
bob = 21;
tom = bob;
alice = &bob;
```

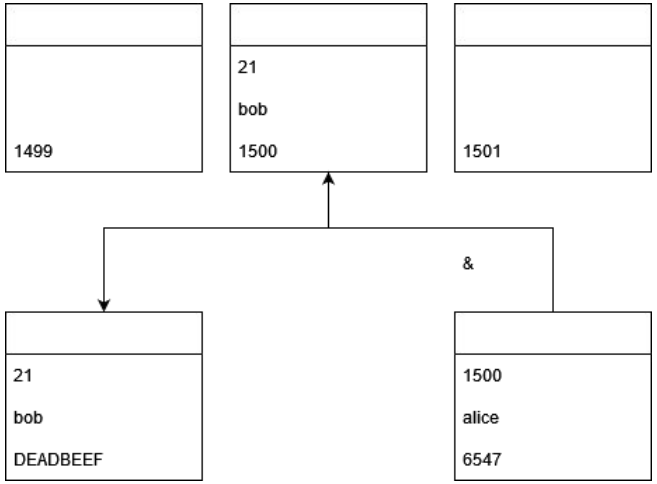
alice habite au 6547

bob habite au 1500

tom habite au DEADBEEF

alice a enregistré l'adresse de bob, 1500

tom à enregistré l'âge (la valeur) de bob, 21 ans



Les Pointeurs

```
bob = 21;
alice = &bob;
sam = *alice;
```

alice habite au 6547

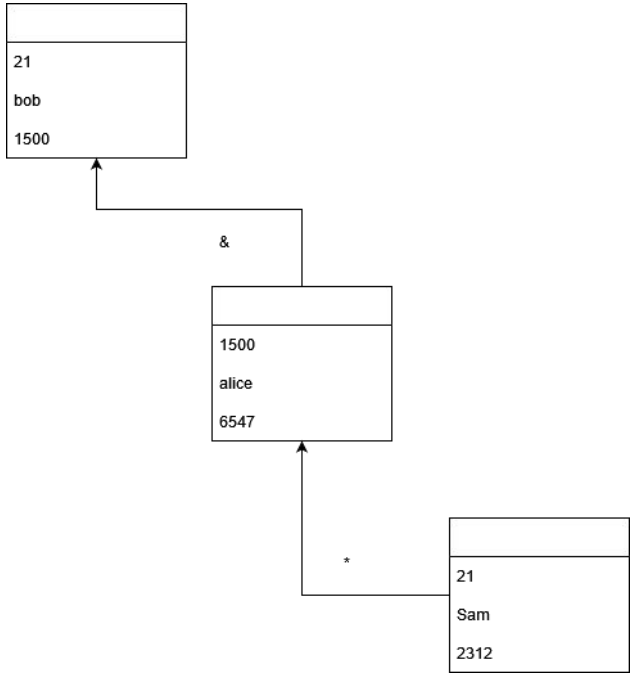
bob habite au 1500

sam habite au 2312

alice a enregistré l’adresse de bob, 1500

sam demande à alice la valeur qu’elle stocke chez elle, et elle lui dit 1500, sam va donc aller à l'adresse 1500, chez bob, et va prendre la valeur qu’il a stocké chez lui.

Attention a prendre en compte que si bob change de valeur, sam, lui ne changera pas de valeur tant qu’il aura pas été mis à jour.



Les Pointeurs

les pointeurs se déclarent comme suit :

```
int *alice;
```
mais
```
int *alice, bob;
```

ça ne crée pas deux pointeurs, il faudra faire comme suit :

```
int *alice, *bob;
```

Des exemples un peu plus complets :

```
int bob = 21;
int *alice;
alice = &bob;
```

Si on complexifie la donne :

```
int bob = 21;
int *alice, *sam;
alice = bob;
sam = *alice;
```

ce qu'on doit comprendre :

On crée deux pointeurs, alice, sam. Alice va ranger dans sa maison, l'adresse de bob. Mais sam, lui va enregistrer la valeur de bob, qu'il a obtenu de alice.

Les Pointeurs

petit exercice :

```
int a = 5, b = 10;
int *p1, *p2;
p1 = &a;
p2 = &b;
*p1 = 10;
p1 = p2;
*p1 = 20;
printf("a = %d\n", a);
printf("b = %d\n", b);
```

Les Pointeurs

petit exercice, correction :

a = 10
b = 20

Registres assembleur

Registres généraux

Ces registres servent à stocker des données temporaires et des résultats d'opérations :

x86 (32 bits) : **EAX**, **EBX**, **ECX**, **EDX**

x86-64 (64 bits) : **RAX**, **RBX**, **RCX**, **RDX** (extensions des versions 32 bits)

Registres assembleur

Registres d'index et de pointeurs

Ils facilitent la manipulation des adresses mémoire :

Pointeur de base : **EBP** (32 bits), **RBP** (64 bits)

Pointeur de pile : **ESP** (32 bits), **RSP** (64 bits)

Index de source : **ESI** (32 bits), **RSI** (64 bits)

Index de destination : **EDI** (32 bits), **RDI** (64 bits)

Cheat Engine

Outil Surpuissant, il sert à:

- Scanner la mémoire
- Modifier les valeurs
- Scripting, et modification de l’assembleur
- Débug, analyse en temps réel
- Création de “Trainers”

Cheat Engine

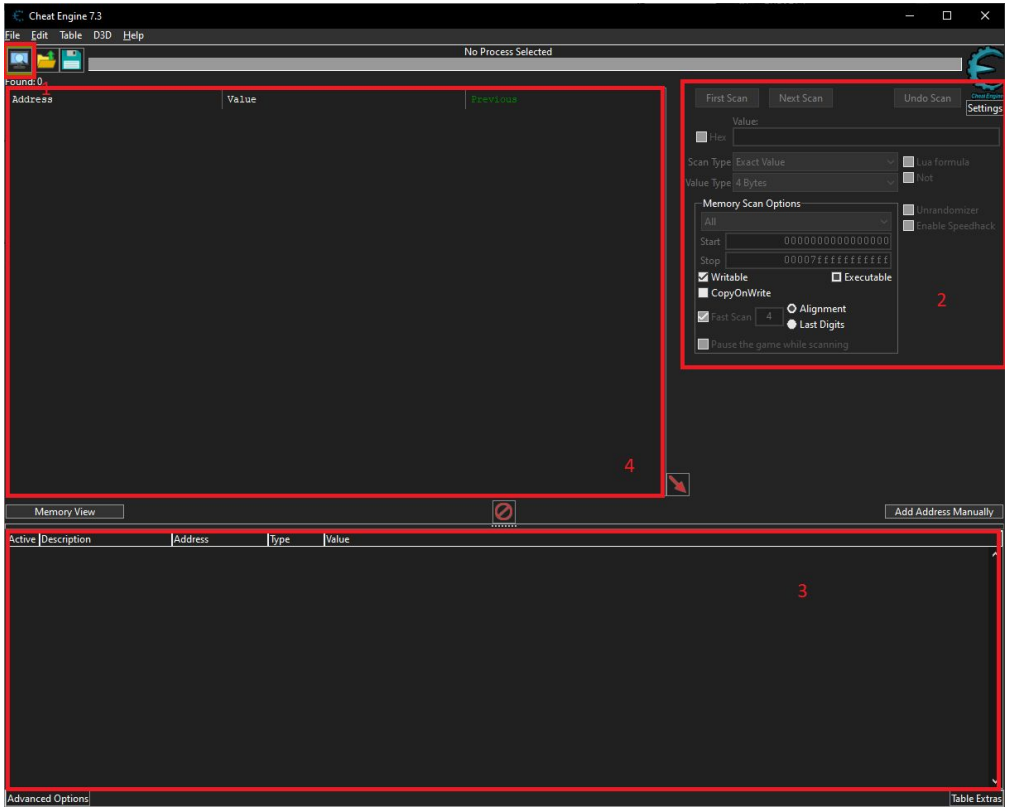
Son Interface

1 - Sélection du processus

2 - Interface de Recherche

3 - Zone d’enregistrement des variables

4 - Affichage des recherches



Cheat Engine - Get Health Address

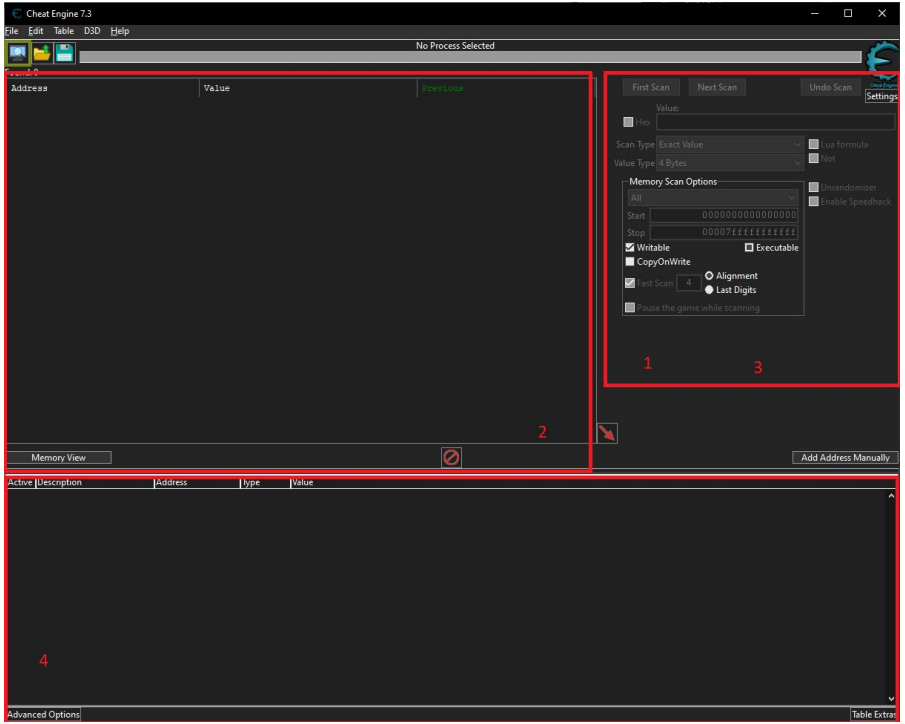
Récupérer les points de vie

1 - Dans la barre de recherche value, entrer 100, les points de vie du joueur, cliquez sur first scan

2 - Interface de Recherche

3 - Zone d’enregistrement des variables

4 - Affichage des recherches



Calendrier de Cours

Jeudi 31/10 - Presentation generale du domaine, structure du cours, révisions des bases, Cheat Engine

Vendredi 29/11 - Cheat Engine pt 2, ReClass pt 1

Vendredi 20/12 - External Hack pt 1, ReClass pt 2

Vendredi 17/01 - External Hack pt 2, Internal Hack pt 1

Vendredi 07/02 - Internal Hack pt 2, DLL Injection

Mercredi 05/03 - Examen

Calendrier de Cours

Jeudi 31/10 - Presentation generale du domaine, structure du cours, révisions des bases, Cheat Engine

Vendredi 29/11 - Cheat Engine pt 2, ReClass pt 1

Vendredi 20/12 - External Hack pt 1, ReClass pt 2

Vendredi 17/01 - External Hack pt 2, Internal Hack pt 1

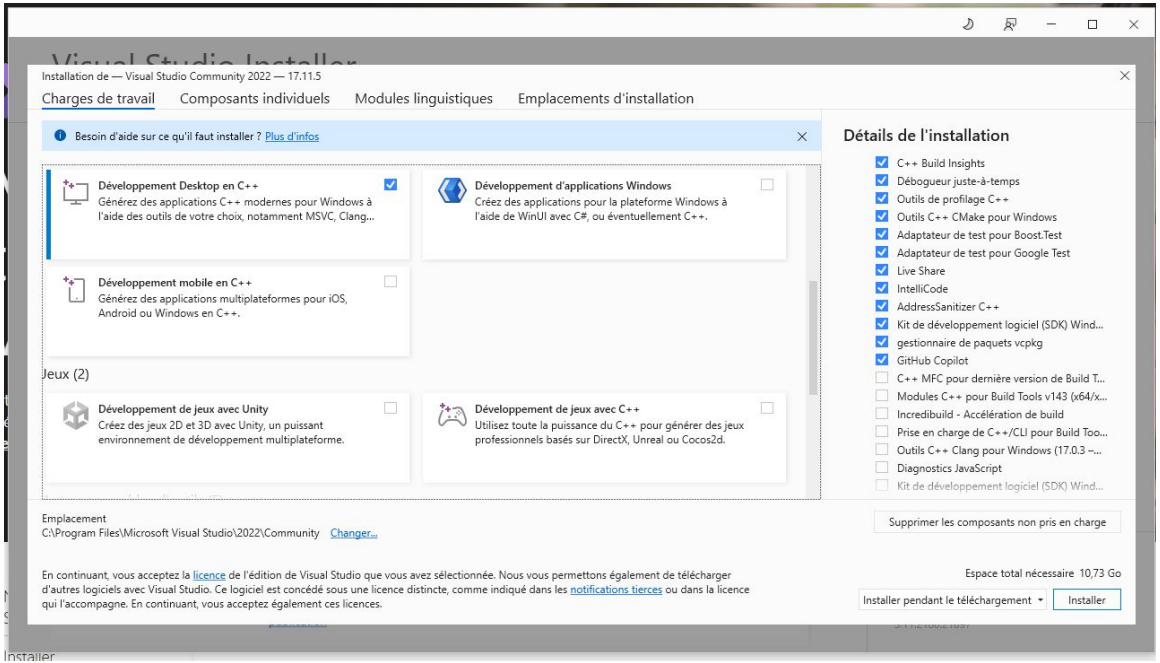
Vendredi 07/02 - Internal Hack pt 2, DLL Injection

Mercredi 05/03 - Examen

Installation de Visual Studio - Community

- *Disponible sur le site de microsoft.*
- Choix des composants de base a l’installation de VS
- Quelques parametrages a mettre en place
- Demarrage d’un nouveau projet

Installation de Visual Studio - Community



C'est long, ça prend 10 go d'installation

Calendrier de Cours

Jeudi 31/10 - Presentation generale du domaine, structure du cours, révisions des bases, Cheat Engine

Vendredi 29/11 - Cheat Engine pt 2, ReClass pt 1

Vendredi 20/12 - External Hack pt 1, ReClass pt 2

Vendredi 17/01 - External Hack pt 2, Internal Hack pt 1

Vendredi 07/02 - Internal Hack pt 2, DLL Injection

Mercredi 05/03 - Examen

Calendrier de Cours

Jeudi 31/10 - Presentation generale du domaine, structure du cours, révisions des bases, Cheat Engine

Vendredi 29/11 - Cheat Engine pt 2, ReClass pt 1

Vendredi 20/12 - External Hack pt 1, ReClass pt 2

Vendredi 17/01 - External Hack pt 2, Internal Hack pt 1

Vendredi 07/02 - Internal Hack pt 2, DLL Injection

Mercredi 05/03 - Examen