République algérienne démocratique et populaire

Ministère de l'enseignement supérieur et de la recherche scientifique



Université de Blida-1-

Faculté des sciences et technologies

Département des mathématiques et informatique

**Rapport de projet C++**

CREER UN KEYLOGGER

**Réalisé par :**

REBAHI Nour El Houda

            2021/2022

1. C’est quoi un keylogger :

Il s’agit d’un système d’espionnage qui se charge d’enregistrer les frappes de touches de clavier cet enregistrement se fait dans un fichier

1. Utilisation des bibliothèques **:**

<cstdio> / <sstream>: pour effectuer des opérations de flux d'entrée/sortie du clavier

<map> : Les cartes sont les conteneurs associatifs qui stockent les paires clé-valeur triées

<time.h> :Fournit un ensemble de fonctions permettant la manipulation de dates, de temps et d'intervalles

1. Les étapes pour créer un keylogger :

**Etape1 :**

Est définir un Hook (crochet) qui permet de **modifier** ou même de **supprimer** un message avant qu'il atteigne l'application à laquelle il est destiné. On peut lire le contenu de chaque message que l'on intercepte de manière totalement transparente pour le reste du système.

**WH\_KEYBOARD :** le contrôle total sur le clavier

**SetWindowsHookEx :** une fonction qui permet de définir le type de Hook

**Etape2 :**

Est définir une fonction principale « Save » chargée d’inscrire dans le fichier log les touches du clavier on retrouve à l’intérieure d’autres fonction :

-Une pour détecter titre de la fenêtre active dans laquelle les touches sont tapées « GetWindowTextA »

- qui détectes les frappes du clavier dans le fichier .log

- qui mentionne le temps quand laquelle les frappes sont détectées

**Etape3 :**

Définir **Format** qui va nous permettre d’agir différemment selon la touche tapé qui nécessite plusieurs paramètres : 1.le code virtuel de la touche qui identifie la touche sur le clavier

2.le scan code de la touche identifiant la touche physiquement sur le clavier

3. un pointeur vers un tableau de 256 octets ce tableau est obtenu en appelant la fonction lastwindow

**Etape4:**

Cacher l’exécution du keylogger avec la fonction stealth qui cache la console qui utilise le parametre 0 a la fonction showWindow