TP AISE — Révision

Exercice : SUID

Récupérer le code ci-dessous, le compiler et le placer dans un répertoire. Faites en sorte que ce répertoire soit la propriété **exclusive** de root (par exemple, dans le doute, faites un autre utilisateur). Ajouter dans ce répertoire un fichier « .secret » qui contient des (faux) mots de passe par exemple.

- Lancer le code depuis votre espace utilisateur, ça marche ?
- Attacher la permission SUID au binaire généré
- Lancer à nouveau le code, ça marche ?
- Trouvez une vulnérabilité et exploitez-là (**recompilation interdite**)

```c
#include <stdlib.h>
int main(int argc, char **argv){
{
    system("ls ./.secret");
    return 0;
}
```

Exercice : Stack Overflow

Exploitez la vulnérabilité du code ci-dessous pour appeler la fonction hook lorsque la fonction main termine:

```c
#include <string.h>
#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>

/* -fno-stack-protector -no-pie -Wl,-z,relro,-z,now,-z,noexecstack */

void hook(){
    char *argv[] = { "/bin/bash", "-p", NULL };
    execve(argv[0], argv, NULL);
}

int main(int argc, char **argv){

    char buffer[32];
    int len, i;

    scanf("%s", buffer);
    len = strlen(buffer);

    printf("Hello %s\n", buffer);

    return 0;
}
```

Exercice : Dessin de l'ensemble de Mandelbrot

Le français Benoit Mandelbrot présente la notion de rugosité dans cette vidéo. Nous allons nous intéresser à la fractale qui porte son nom. Cet objet de curiosité est d'une infinie complexité bien que nous allons voir, il nait d'un simple formule répétée à l'infini. Pour appréhender ce « méta-exercice », nous allons découper le travail en plusieurs parties.

Sous-exercice 1: dessiner

L'un des problème parallèle les plus simple porte sur le traitement d'images, nous cherchons donc à générer des images en C. Le but de ce premier exercice est de construire une bibliothèque de dessin basée sur un format simple : Portable Pixmap. Nous vous invitons à lire la documentation, notamment le format (ASCII ou binaire ?)

Sous-exercice 2: Ensemble de Mandelbrot

L'ensemble de Mandelbrot est défini de manière récursive, pour tout point du plan complexe, comme suit:

- `Z(0) = 0`
- `Z(n+1) = Z(n)^2 + C`

Ce qui est bien avec un complexe, c'est qu'il peut facilement se représenter sur un plan 2D (=image), le « x » servant les réels, le « y » servant les imaginaires. Il suffit alors de connaître, pour chaque point complexe du plan, le « poids » à afficher. Dans le cas de l'ensemble de Mandelbrot, on choisira le nombre de termes nécessaires pour rendre la suite divergente. Autrement dit, plus il y a d'itérations pour un nombre, plus son poids augmente. Quelques tuyaux qui pourraient vous aider:

- La suite diverge (=sort de l'ensemble) lorsque son module est supérieur à 2
- Les complexes existe en C: `man complex`

Have fun :)