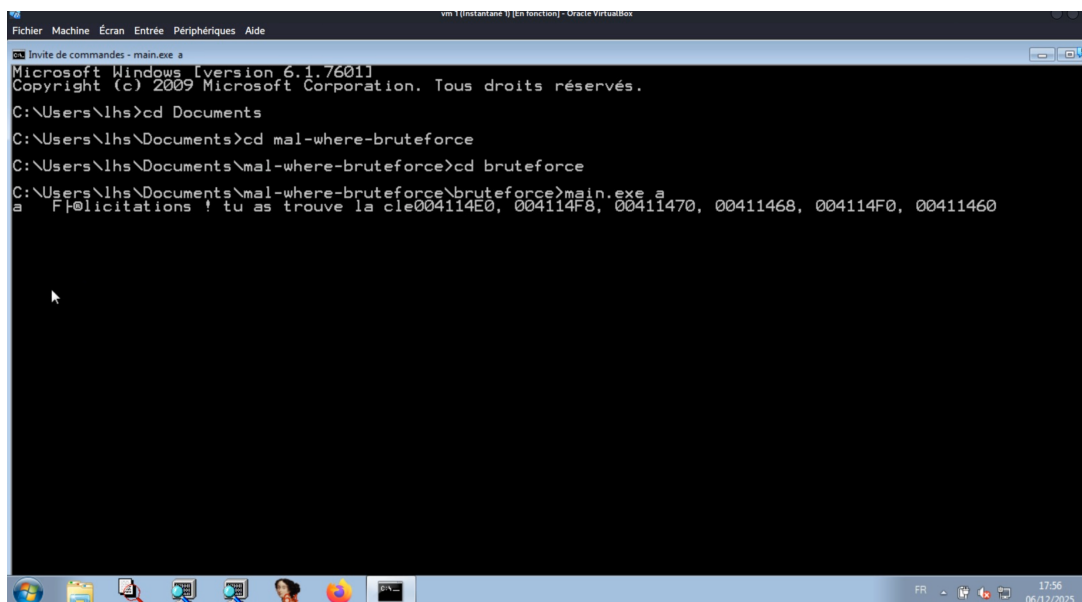


Affichage furtif et fuite d'adresse mémoire

Localisation: 0x004052BC, 0x0040530C Fonction: ?

Type: ? Sévérité: Moyenne

Screenshot



Analyse

En exécutant le fichier `main.exe` de manière légitime (en respectant les contraintes de taille, avec la chaîne `a` par exemple), le programme affiche pendant moins d'une seconde la chaîne de caractère suivante : `a Félicitations ! tu as trouve la cle04114E0, 004114F8, 00411470, 00411468, 004114F0, 00411460`. En cherchant dans le résultat de `strings main.exe` on trouve la chaîne partielle `licitations !` et la chaîne `%p, %p, %p, %p, %p, %p`, ainsi en cherchant dans les données brutes avec IDA on peut remonter au code assembleur suivant :

Code Assembleur : Fuite d'adresse mémoire

```
1  mov     [esp+518h+hWnd], eax
2  mov     [esp+518h+lpRect], edx
3  call    __moddi3
4  mov     [ebp+var_54], eax
5  mov     [esp+518h+x1], offset strlen
6  mov     [esp+518h+hdcSrc], offset free
7  mov     [esp+518h+cy], offset malloc
8  mov     [esp+518h+wDest], offset memcpy
9  mov     [esp+518h+y], offset loc_4114F8
10 mov     [esp+518h+lpRect], offset printf
11 mov     [esp+518h+hWnd], offset aPPPPPP ; "%p, %p, %p, %p, %p, %p"
12 mov     [ebp+var_44C], 4
13 call    printf
```

Analyse

Ce code appelle la fonction `printf` et affiche les adresses mémoire des fonctions suivantes :

- `strlen`
- `free`
- `malloc`
- `memcpy`
- `loc_4114F8`
- `printf`