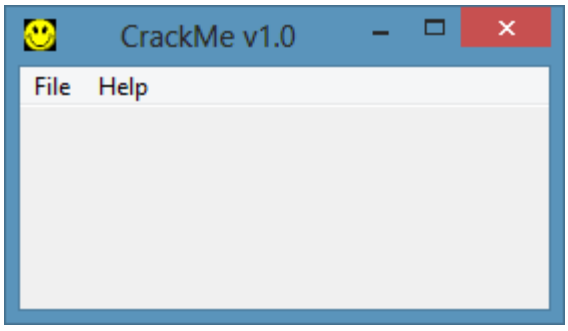
Keygen para el CrackMe#01 de Cruehead

Haciendo el KeyGen de un clásico



By deurus
08/09/2014

ÍNDICE

Equipo utilizado:

S.O: Windows 7 x32 /Windows 8 x64

Depurador: Ollydbg 1.10 (32bits) con plugins

Analizador: PEiD 0.95

1. Introducción

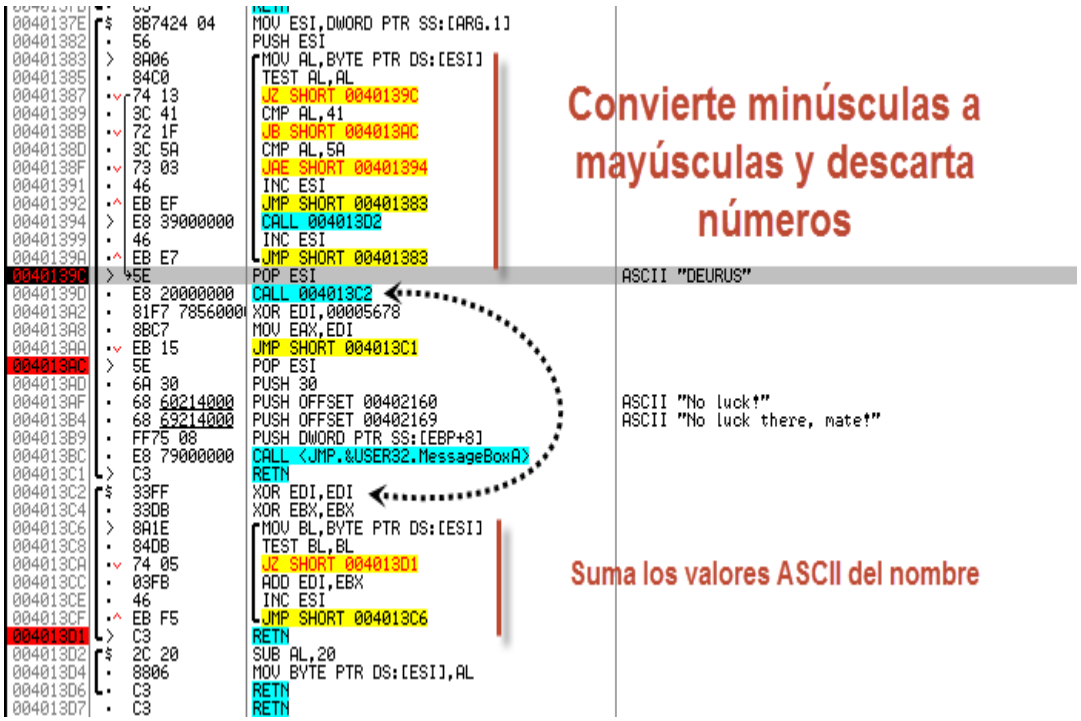
Esta es la primera entrega de tres en las que vamos a ver tres crackmes que todo reverser debería hacer. Son la serie del autor Cruehead. Aunque los hice hace ya muchos años, he decidido documentarlos para que el lector que empieza pueda deleitarse. En este caso se trata del típico Nombre / Serial.

2. El algoritmo

El algoritmo de este crackme es lo más sencillo que nos podemos encontrar.

Abrimos el crackme con **Olly** y buscamos en las "string references" el mensaje de error. Pinchamos sobre él y en la parte superior enseguida vemos 2 calls muy interesantes.

Veamos que hace con el **nombre**.

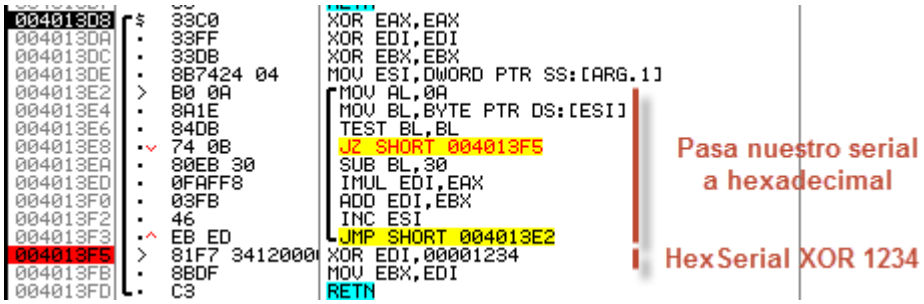


Para “deurus” pondría todo en mayúsculas, sumaría su valor ascii y le haría **XOR 0x5678**.

Ejemplo:

deurus –> DEURUS –> 0x44+0x45+0x55+0x52+0x55+0x53 = 0x1D8 XOR 0x5678 = **0x57A0**

Veamos que hace con el **serial introducido**.

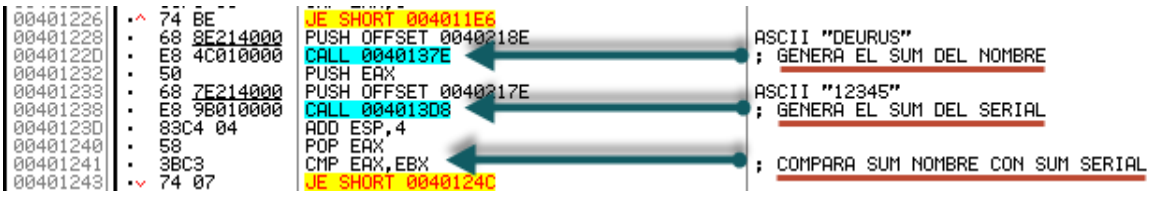


Convierte nuestro **serial** a hexadecimal y le hace **XOR 0x1234**.

Ejemplo:

Serial = 12345 –> 0x3039 XOR 0x1234 = **0x220D**

Una vez que tenemos el **SUMNombre** y el **SUMSerial** los compara. Lo vemos en **CMP EAX, EBX**.



En resumen, si a nuestro **SUMNombre** le hacemos **XOR 0x5678** y **XOR 0x1234** ya tenemos el serial bueno.

Ejemplo:

deurus –> DEURUS –> 0x44+0x45+0x55+0x52+0x55+0x53 = 0x1D8 **XOR 0x5678** = 0x57A0 **XOR 0x1234** = **0x4594**

0x4594 = **17812** = Nuestro serial bueno.

3. KeyGen

```
char Nombre[20];
GetWindowText(hwndEdit1, Nombre, 20);
char Serial[20];
int len = strlen(Nombre);
int suma = 0;
boolean error = false;
   for(int i = 0; i <= len; i = i + 1)
   {
      suma += toupper(Nombre[i]);
   }
suma = suma^0x444C; //444C == 5678 xor 1234
wsprintf(Serial,"%d",suma);
SetWindowText(hwndEdit2, TEXT(Serial));
```

4. Enlaces

- Crackme
- Keygen

5. Repositorio

- https://deurus.info/archivos/crackmes/Crackme_cruehead_1.0.rar