14.5.2.—Enumerar instrucciones

Dentro de una función dada, podemos querer enumerar cualquier instrucción. El siguiente script cuenta el número de instrucciones contenidas en la función identificada por la posición del cursor:

```
//include obligado
#include <idc.idc>

//funcion main obligada
 static main() {

    //declaramos variables
    auto funcion, final, cuenta, instruccion;

    //Toma el atributo de una función, en este caso la funcion que le proporciona
    //ScreenEA () la cual proporcionaque la direccion donde esta el cursor posicionado,
    //el atributo es la direccion de inicio de dicha funcion
    funcion = GetFunctionAttr(ScreenEA(), FUNCATTR_START);

    //Desviacion de flujo si cumple nos da información de la funcion
    if (funcion != -1) {

       //Toma el atributo de una funcion,en este caso el final de la funcion
       final = GetFunctionAttr(funcion, FUNCATTR_END);

       //Iniciamos variable cuenta
       cuenta = 0;

       //Iniciamos variable instruccion
       instruccion = funcion;

       //Creamos un bucle que itera hasta el final de la función
       while (instruccion < final) {

           //cada iteración es una instrucción que se va totalizando en cuenta
          cuenta++;

          //Con FindCode nos va dando la instrucción, iterando hacia direccion
          //inferior y buscando la siguiente
          instruccion = FindCode(instruccion, SEARCH_DOWN | SEARCH_NEXT);
       }

       //Nos muestra un dialogo con la información
       Warning("%s contiene %d instrucciones\n", Name(funcion), cuenta);
    }

    //Desviación de flujo con if, se ejecuta si en la direccion del cursor no hay
    //funcion.
    else {

       //Nos muestra un dialogo con la información
       Warning("No existe funcion en la ubicacion %x", ScreenEA());
    }
 }
```

La funcion **main** se inicia utilizando **GetFunctionAttr** para determinar la dirección de inicio de la función contenida en la dirección donde está situado el cursor, la cual nos es proporcionada por la función **ScreenEA ( ).**

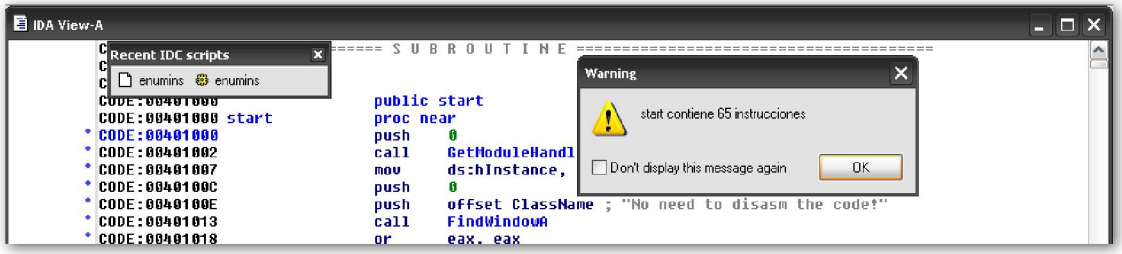
```
funcion = GetFunctionAttr(ScreenEA(), FUNCATTR_START);
    if (funcion != -1) {
```

Si en la dirección existe el principio de una función, se ejecutará el siguiente paso

```
final = GetFunctionAttr(funcion, FUNCATTR_END);
       cuenta = 0;
       instruccion = funcion;
       while (instruccion < final) {
          cuenta++;
```

en la cual se determina la dirección final de la función utilizando otra vez **GetFunctionAttr**. Una vez tenemos delimitada la función, se ejecuta un bucle para iterar sucesivamente por las instrucciones de la función utilizando la funcionalidad de búsqueda de la función **FindCode**. En este ejemplo se utiliza la función **Warning** para mostrar el resultado, lo cual es una advertencia más obvia que hacerlo en la ventana de mensajes de IDA.

Como en el ejemplo anterior una vez realizado tomamos nuestro script al cual llamaremos **enumins.idc** y lo colocamos en la carpeta **idc** de IDA. Cargamos nuestro CRACKME.EXE y con la acción **File > IDC file** lo ejecutamos y seguidamente podemos ver las dos opciones de información que nos puede mostrar dicho script, si hay función o si no hay función.



Performance Bigundill@