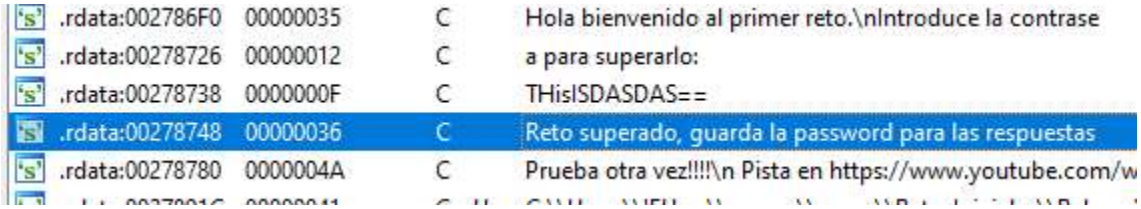
M7T1. Tarea 1

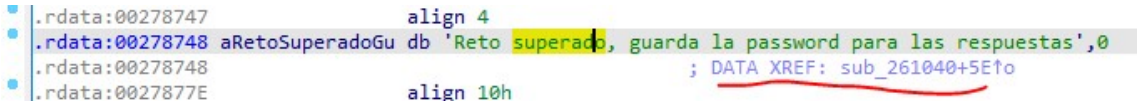
CrackMe0.exe:

Análisis con Ida Pro:

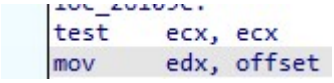
1. Buscamos las strings a ver que referencias nos encontramos.



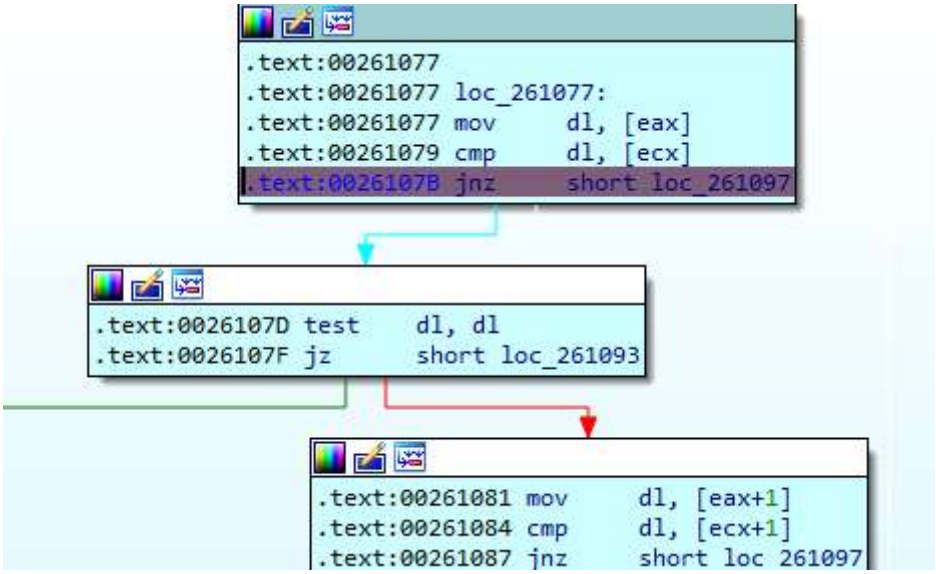
2. He seguido la referencia



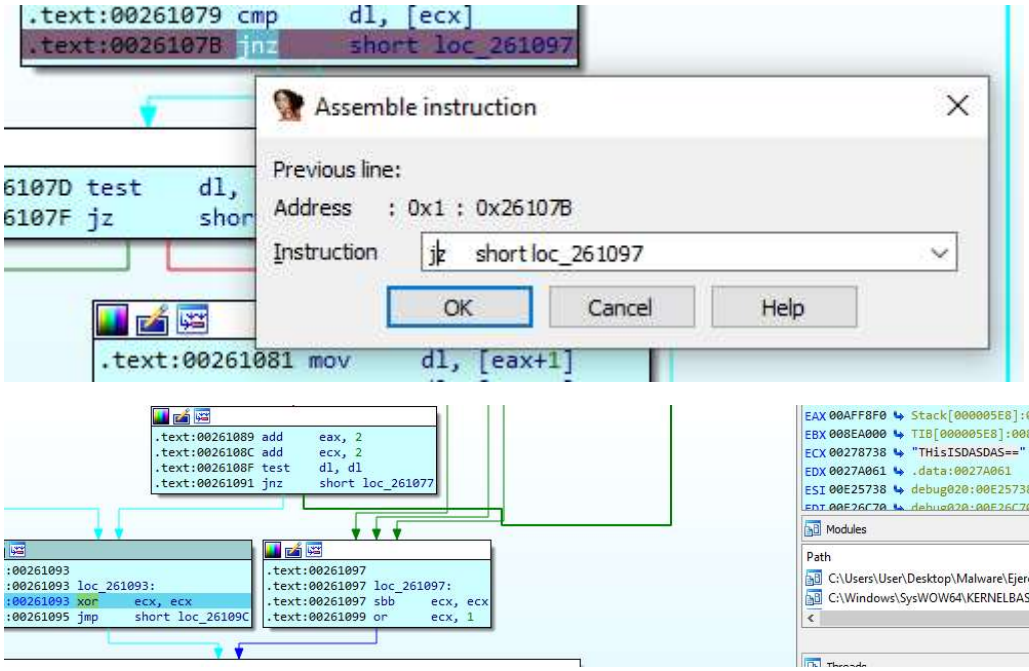
3. Esto nos lleva a encontrar que se realiza un test de ecx para comprobar la contraseña:



4. He puesto un breakpoint para revisar que camino sigue el programa al meter una contraseña incorrecta:



5. He editado el salto para ir por el camino deseado:



6. En el valor de ECX se visualiza la contraseña:

   “THisDASDAS==” es la password

   ** Era mas sencillo que todo esto ya que sale directamente en las strings **

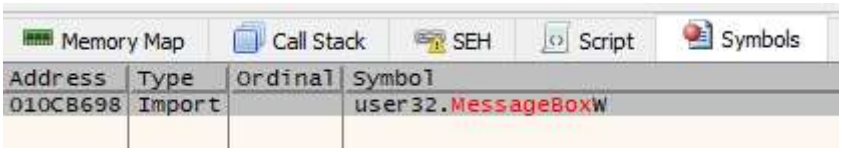
```
C:\Users\User\Desktop\Malware\Ejercicio1\Ejercicio1>CrackMe0.exe
Hola bienvenido al primer reto.
Introduce la contraseña para superarlo:THisISDASDAS==
Reto superado, guarda la password para las respuestas
```

CrackMe1.exe:

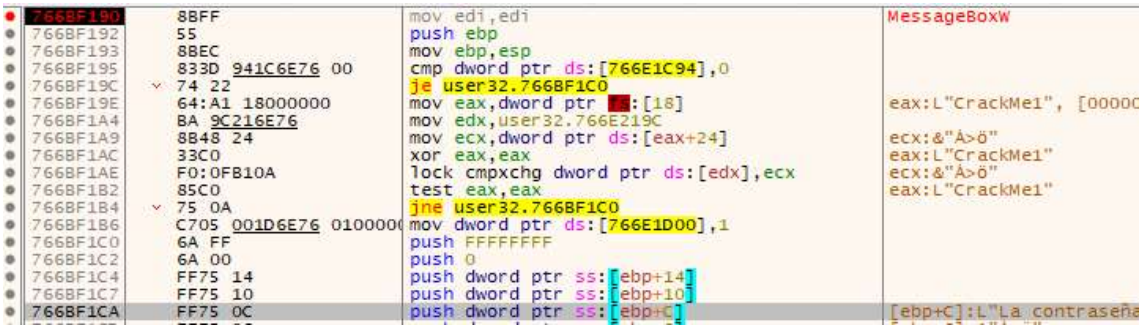
Análisis con XDBG (32bits):

1. He realizado un acercamiento diferente:

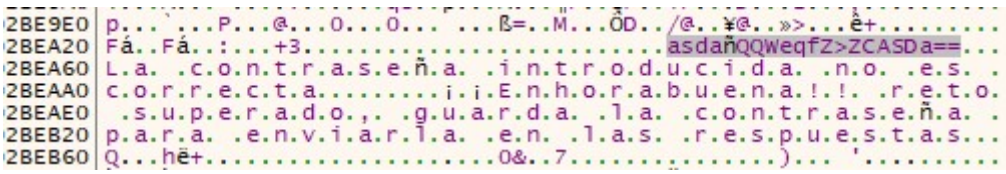
   Como en este programa al introducir una contraseña incorrecta sale un mensaje en una ventana, he comenzado buscando por referencias a la función MessageBox

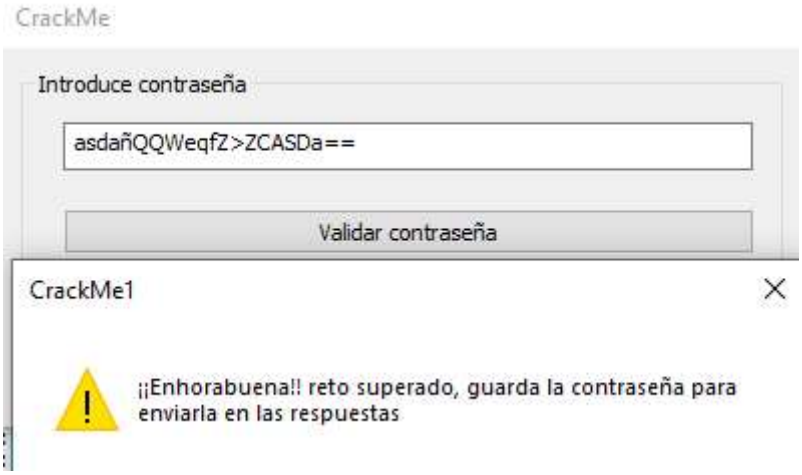


2. He colocado un breakpoint para ver que ocurre ahí:



3. Siguiendo los datos en el dump he dado con la contraseña: asdañQQWeqfZ>ZCASDa==





CrackMe2.exe:

Análisis intentedo de varias maneras, contraseña no encontrada.

He estado probado diferentes formas de analizar el fichero, con ida Pro, Cutter, etc y solamente he dado con este string: UEFTREFhZG1hbCEhMzQyLGxrYXNkYQ

Pero no es la contraseña.

```
.System.Security
.Cryptography.ge
t_Assembly...=U.
E.F.T.R.E.F.h.Z.
G.1.h.b.C.E.h.M.
z.Q.y.L.G.x.r.Y.
X.N.k.Y.Q...=.=.
.€.W.e.l.l.·.d.o
.n.e.!.!.!.·.r.e
```

CrackMe3.exe:

En este me ha ocurrido lo mismo. Lo he intentado de varias maneras, siguiendo varias pistas, funciones pero no lo he conseguido:

```
00007FFB1CF3641F    CC              int3
00007FFB1CF36420    41:B0 01        mov r8b,1                    gets
00007FFB1CF36423    48:83CA FF      or rdx,FFFFFFFFFFFFFFFF
00007FFB1CF36427  ^ E9 B0FCFFFF     jmp ucrtbase.7FFB1CF360DC
00007FFB1CF3642C    CC              int3
00007FFB1CF3642D    CC              int3
00007FFB1CF3642E    CC              int3
00007FFB1CF3642F    CC              int3
00007FFB1CF36430    CC              int3
00007FFB1CF36431    CC              int3
00007FFB1CF36432    CC              int3
00007FFB1CF36433    CC              int3
00007FFB1CF36434    CC              int3
00007FFB1CF36435    CC              int3
00007FFB1CF36436    CC              int3
00007FFB1CF36437    CC              int3
00007FFB1CF36438    CC              int3
00007FFB1CF36439    CC              int3
00007FFB1CF3643A    CC              int3
00007FFB1CF3643B    CC              int3
00007FFB1CF3643C    CC              int3
00007FFB1CF3643D    CC              int3
00007FFB1CF3643E    CC              int3
00007FFB1CF3643F    CC              int3
00007FFB1CF36440    45:33C0         xor r8d,r8d                  gets_s
00007FFB1CF36443  ^ E9 94FCFFFF     jmp ucrtbase.7FFB1CF360DC
00007FFB1CF36448    CC              int3
00007FFB1CF36449    CC              int3
```

CrackMe4.exe:

Análisis con Ida Pro:

1. Ha sido bastante sencillo ya que simplemente cargando el programa en Ida Pro, leyendo como comienza el programa, tenemos la contraseña:

   NEnLinuxGDB!!