

M7T1. Tarea 1

CrackMe0.exe:

Análisis con Ida Pro:

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

.rdata:002786F0	00000035	C	Hola bienvenido al primer reto.\nIntroduce la contrase
.rdata:00278726	00000012	C	a para superarlo:
.rdata:00278738	0000000F	C	THisISDASDAS==
.rdata:00278748	00000036	C	Reto superado, guarda la password para las respuestas
.rdata:00278780	0000004A	C	Prueba otra vez!!!!\n Pista en https://www.youtube.com/w

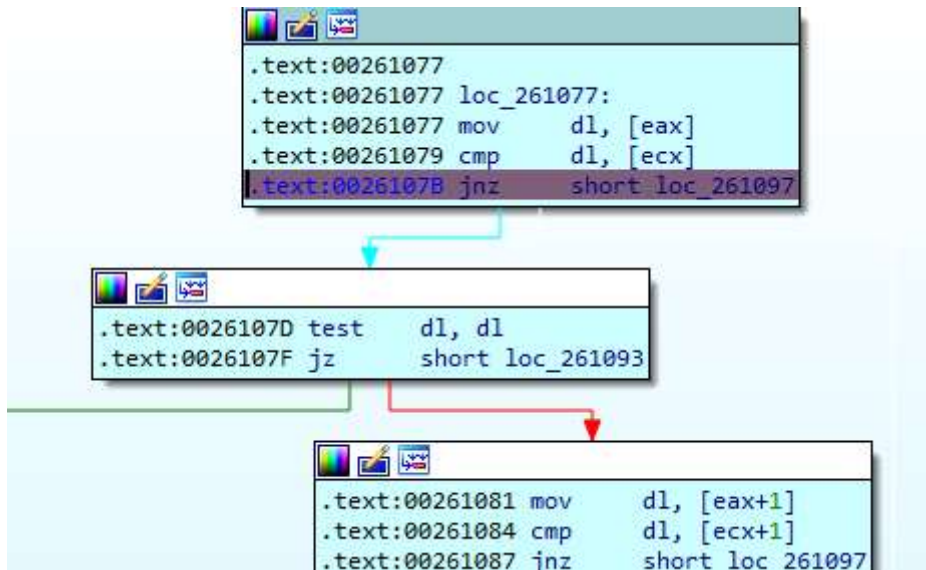
2. He seguido la referencia

```
.rdata:00278747 align 4
.rdata:00278748 aRetoSuperadoGu db 'Reto superado, guarda la password para las respuestas',0
.rdata:00278748 ; DATA XREF: sub_261040+5Eto
.rdata:0027877E align 10h
```

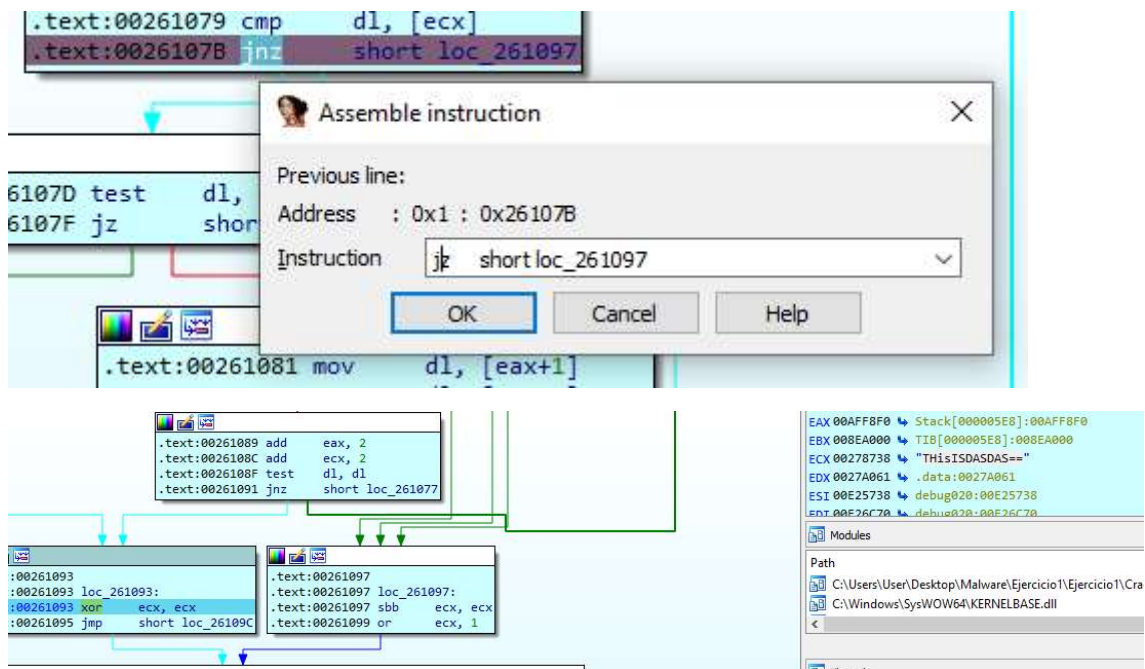
3. Esto nos lleva a encontrar que se realiza un test de ecx para comprobar la contraseña:

```
loc_261097:
test    ecx, ecx
mov     edx, offset
```

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

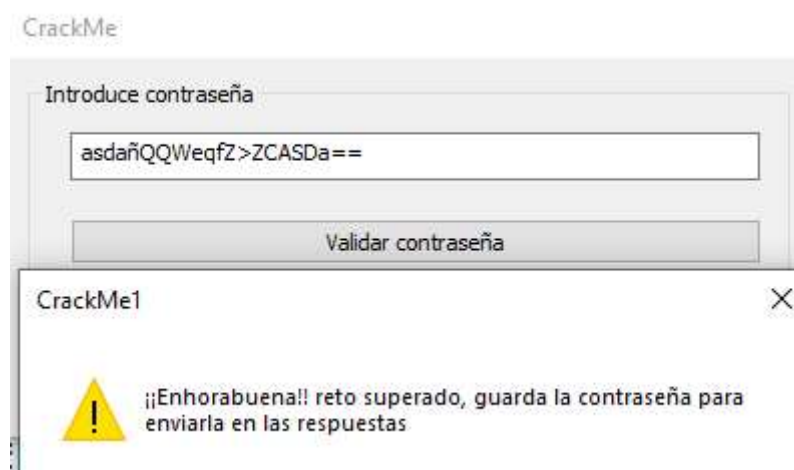
Memory Map	Call Stack	SEH	Script	Symbols
Address	Type	Ordinal	Symbol	
010CB698	Import		user32.MessageBoxW	

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

766BF190	88FF	mov edi,edi	MessageBoxW
766BF192	55	push ebp	
766BF193	88EC	mov ebp,esp	
766BF195	833D 941C6E76 00	cmp dword ptr ds:[766E1C94],0	
766BF19C	74 22	je user32.766BF1C0	
766BF19E	64:A1 18000000	mov eax,dword ptr [18]	eax:L"CrackMe1", [00000000]
766BF1A4	BA 9C216E76	mov edx,user32.766E219C	
766BF1A9	8B48 24	mov ecx,dword ptr ds:[eax+24]	ecx:&"A>0"
766BF1AC	33C0	xor eax,eax	eax:L"CrackMe1"
766BF1AE	F0:0FB10A	lock cmpxchg dword ptr ds:[edx],ecx	ecx:&"A>0"
766BF1B2	85C0	test eax,eax	eax:L"CrackMe1"
766BF1B4	75 0A	jne user32.766BF1C0	
766BF1B6	C705 001D6E76 01000000	mov dword ptr ds:[766E1D00],1	
766BF1C0	6A FF	push FFFFFFFF	
766BF1C2	6A 00	push 0	
766BF1C4	FF75 14	push dword ptr ss:[ebp+14]	
766BF1C7	FF75 10	push dword ptr ss:[ebp+10]	
766BF1CA	FF75 0C	push dword ptr ss:[ebp+0C]	[ebp+C]:L"La contraseña"

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

```
2BE9E0 p...P...@...0...0...B=.M...0D.../@...%@...»>...è+...
2BEA20 Fá. Fá. :...+3...asdañQQWeqfZ>ZCASDa==
2BEA60 L.a.c.o.n.t.r.a.s.e.ñ.a.i.n.t.r.o.d.u.c.i.d.a.n.o.e.s.
2BEAA0 c.o.r.r.e.c.t.a...i.i.E.n.h.o.r.a.b.u.e.n.a!!..r.e.t.o.
2BEAE0 .s.u.p.e.r.a.d.o.,.g.u.a.r.d.a.l.a.c.o.n.t.r.a.s.e.ñ.a.
2BEB20 p.a.r.a.e.n.v.i.a.r.l.a.e.n.l.a.s.r.e.s.p.u.e.s.t.a.s.
2BEB60 Q...hè+...0&.7...)
```



CrackMe2.exe:

Análisis intentado 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!!

