

ESTUDIO DE PROTECCIONES BASICO PARA PRINCIPIANTES

(También llamado cracking)

Impartido por Ratón (Nivel principiante)

Nota

Cada capitulo ira acompañado de su crackme correspondiente.No facilitare paginas de donde bajarse herramientas ni enlaces a paginas de crackers, la intención es que busquéis en Internet todo lo necesario. Seguro que encontráis mas paginas de herramientas, tutoriales y utilidades relacionadas con este tema que las que yo pueda deciros.

Con esto solo quiero fomentar vuestro interés, además se que la búsqueda os proporcionara gratas sorpresas.

A todos un saludo.

Capitulo 7

Victima

Crackme3 de Joe Cracker (así se hace un crackme, si señor!!!)

Para mayores de 18 años

Herramientas

Olly Debugger.

DeDe.

Instinto

Objetivo

Conocer otro tipo de protección.

Repasar lo visto anteriormente

Pasar un rato entretenidos (como premio por soportar el capitulo anterior este capitulo será sencillo)

Al ataque

Lo examinamos con Peid y nos dice que esta hecho en Delphi y sin proteccion.

Nos aparece la primera ventana del crackme y disfrutamos de ella leyendo toda la parrafada

Más que nada para que os deis cuenta de que pasado un tiempo el programa se cierra

Abrámoslo con DeDe

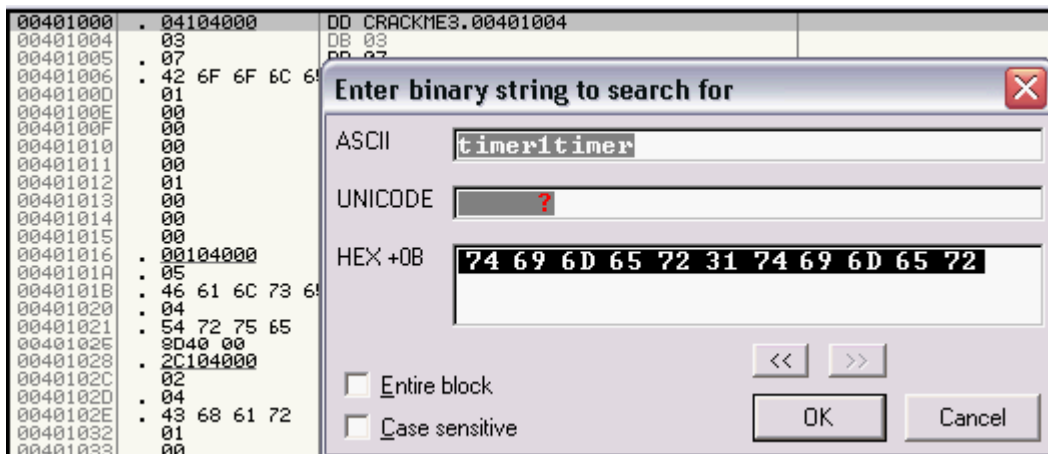
En el form principal vemos algo que llama la atención: el Timer

Seguro que tiene algo que ver con el cierre de la ventana, apuntemos su dirección

TPrincipal		
Events	Controls	<input type="checkbox"/> Show classes having no published m
Event	RVA	Hint
Registrar1Click	0046AF50	0016
Acercade1Click	0046AF00	0015
Label7Click	0046AFA0	0012
FormCreate	0046B00C	0011
Inform2Click	0046B138	0013
queClick	0046B188	000F
Saludos2Click	0046B1D8	0014
Button2Click	0046B228	0013
Timer1Timer	0046B27C	0012
Button3Click	0046B2B4	0013
_PROC_0046B2C0	0046B2C0	FFFF
_PROC_0046B300	0046B300	FFFF
_PROC_0046B308	0046B308	FFFF
_PROC_0046B3A2	0046B3A2	FFFF

Miremos el crackme en Olly

Buscamos la cadena timer1timer (Control + B)



Caemos en la dirección **0046AE92** que es donde esta la cadena y para seguirla subimos a la dirección **0046AE8D**

Desde hache pulsamos la tecla enter o click derecho Follow

0046AE8C	00	DB 00
0046AE8D	7C B2 46 00	DD CRACKME3.0046B27C
0046AE91	0B	DB 0B
0046AE92	54 69 6D 65 72	ASCII "Timer1Timer"
0046AE9D	13	DB 13
0046AE9F	00	DB 00

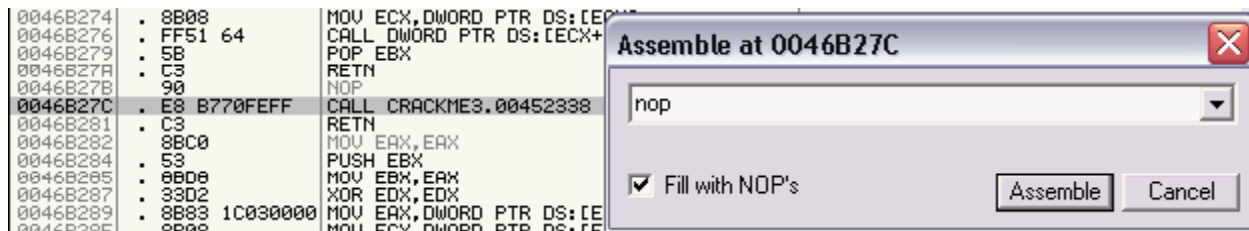
y llegamos al call que genera el timer, el reloj que hace que se cierre el programa pasado un cierto tiempo

0046B279	5B	POP EBX
0046B27A	C3	RETN
0046B27B	90	NOP
0046B27C	E8 B7 70 FE FF	CALL CRACKME3.00452338
0046B281	C3	RETN
0046B282	8B C0	MOV EAX, EAX
0046B284	53	PUSH EBX
0046B285	8B D8	MOV EBX, EAX
0046B287	33 02	XOR EDX, EDX

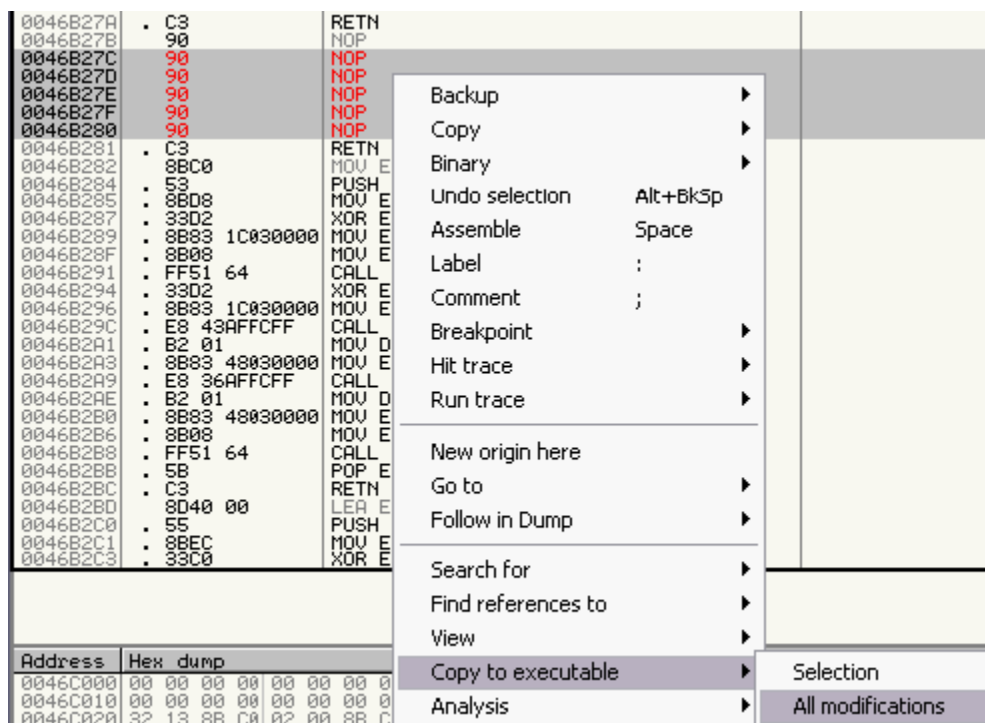
Que haremos para evitar el funcionamiento del reloj ¿?

Usaremos la instrucción NOP (no operation), si dejamos el call inoperativo a lo mejor el reloj ya no funciona

Fijaros que esta marcada la opción fill with nops y así Olly se ocupa del cambiar lo que haga falta



Sombreamos todo lo que cambiamos y guardamos como siempre



Probamos el crackme un par de minutos y vemos que acertamos

Vamos a por el número de registro

Mirando el crackme con DeDe

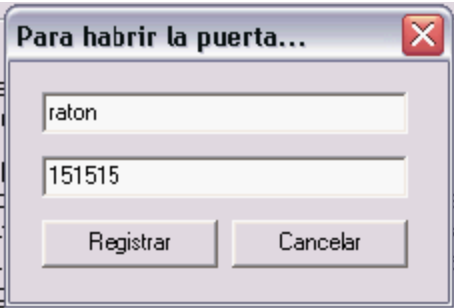
Tened en cuenta que existen dos botones con el nombre registrar aparte de la opción del menú

Este es el que aparece al abrir el crackme

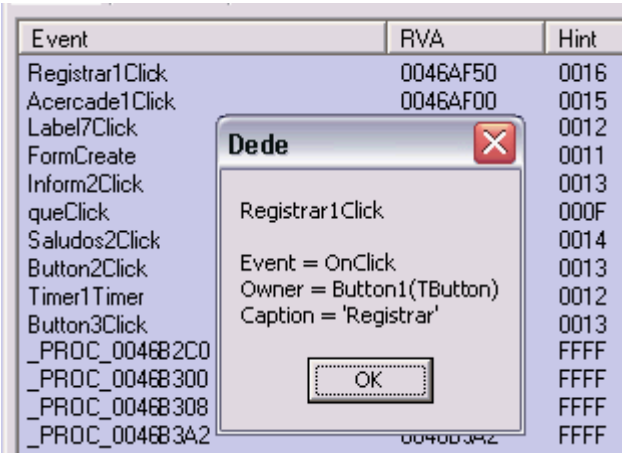
<http://www.iespana.es/OllyDBG>

Registrar

Y este que es el que nos interesa



Este no nos interesa pues es el del formulario principal del programa lo deducimos pues esta en el form principal

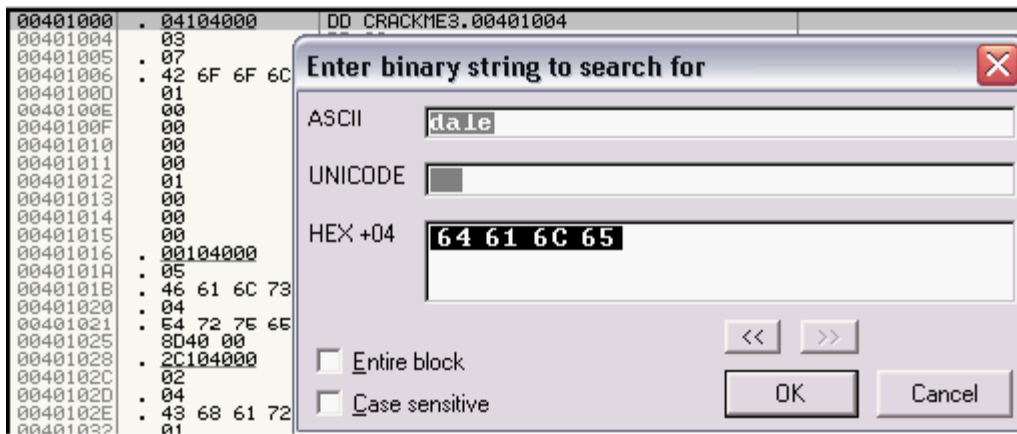


Este es el que buscamos, lo oculta Joe bajo el nombre Dale para despistarnos y esta en el form register del programa y se llama Dale

A estas alturas supongo que sabréis diferenciar entre el nombre y el caption



Olly de nuevo y a buscar el nombre del botón



Encontramos Dale click

Hacemos como con timer 2 líneas más arriba y enter para seguirlo

0046B47F	10	DB 10
0046B480	00	DB 00
0046B481	08B44600	DD CRACKME3.0046B4D8
0046B485	09	DB 09
0046B486	44 61 6C 65 4	ASCII "DaleClick"
0046B48F	11	DB 11
0046B490	00	DB 00
0046B491	0CB64600	DD CRACKME3.0046B6DC

Aparecemos aquí, que es donde se registra cuando pulsamos sobre el botón Dale (con el caption register)

Hemos buscado el evento OnClick del boton dale

Ponemos un BP con F2

0046B4D5	00	DB 00
0046B4D6	00	DB 00
0046B4D7	90	NOF
0046B4D8	55	PUSH EBP
0046B4D9	8BEC	MOV EBP,ESP
0046B4DB	33C9	XOR ECX,ECX
0046B4DD	51	PUSH ECX
0046B4DE	51	PUSH ECX
0046B4DF	51	PUSH ECX

Pulsamos F9, nos vamos a la ventana de registro e introducimos nombre y serial y Olly para en el BP

0046B4D5	00	DB 00
0046B4D6	00	DB 00
0046B4D7	90	NOF
0046B4D8	55	PUSH EBP
0046B4D9	8BEC	MOV EBP,ESP
0046B4DB	33C9	XOR ECX,ECX
0046B4DD	51	PUSH ECX
0046B4DE	51	PUSH ECX
0046B4DF	51	PUSH ECX

Con F8 vamos examinando poco a poco bajando línea a línea y vamos observando nuestro nombre aparecer de vez en cuando pero lo que nos interesa es esta zona, en 0046b5A2 vemos que hay algo parecido ha un archivo *.ini

Vamos a cambiar el sentido de los saltos a ver que sucede

0046B58F	. F7F9	IDIV ECX	
0046B591	. 8B00	MOV EDX,EAX	
0046B593	. 2B03	SUB EDX,EBX	
0046B595	✓75 02	JNZ SHORT CRACKME3.0046B599	
0046B597	. 8BC3	MOV EAX,EBX	
0046B599	> 8D141B	LEA EDX,DWORD PTR DS:[EBX+EBX]	
0046B59C	. 03D8	ADD EBX,EAX	
0046B59E	. 3BD3	CMP EDX,EBX	
0046B5A0	✓75 49	JNZ SHORT CRACKME3.0046B5EB	
0046B5A2	. B9 58B64600	MOV ECX,CRACKME3.0046B658	ASCII "C:/cm3jc.ini"
0046B5A7	. B2 01	MOV DL,1	
0046B5A9	. A1 60A44200	MOV EAX,DWORD PTR DS:[42A460]	
0046B5AE	. E8 5DEFFBFF	CALL CRACKME3.0042A510	
0046B5B3	. A3 74ED4600	MOV DWORD PTR DS:[46ED74],EAX	
0046B5B8	. 8D55 E8	LEA EDX,DWORD PTR SS:[EBP-18]	
0046B5BB	. 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
0046B5BE	. 8B80 F8020000	MOV EAX,DWORD PTR DS:[EAX+2F8]	
0046B5C4	. E8 FBACFCFF	CALL CRACKME3.004362C4	
0046B5C9	. 8B45 E8	MOV EAX,DWORD PTR SS:[EBP-18]	
0046B5CC	. 50	PUSH EAX	
0046B5CD	. B9 70B64600	MOV ECX,CRACKME3.0046B670	ASCII "to"
0046B5D2	. BA 7CB64600	MOV EDX,CRACKME3.0046B67C	ASCII "Regist"
0046B5D7	. A1 74ED4600	MOV EAX,DWORD PTR DS:[46ED74]	
0046B5DC	. 8B18	MOV EBX,DWORD PTR DS:[EAX]	
0046B5DE	. FF53 04	CALL DWORD PTR DS:[EBX+4]	
0046B5F1	. 01 74ED4600	MOV EBX,DWORD PTR DS:[46ED74]	

Probé los 2 saltos y al cambiar este 0046B5A0 y registrarme con nombre y serial falso y reiniciar el programa como me pide el crackme

0046B58F	. F7F9	IDIV ECX	
0046B591	. 8B00	MOV EDX,EAX	
0046B593	. 2B03	SUB EDX,EBX	
0046B595	✓75 02	JNZ SHORT CRACKME3.0046B599	
0046B597	. 8BC3	MOV EAX,EBX	
0046B599	> 8D141B	LEA EDX,DWORD PTR DS:[EBX+EBX]	
0046B59C	. 03D8	ADD EBX,EAX	
0046B59E	. 3BD3	CMP EDX,EBX	
0046B5A0	✓74 49	JE SHORT CRACKME3.0046B5EB	
0046B5A2	. B9 58B64600	MOV ECX,CRACKME3.0046B658	ASCII "C:/cm3jc.ini"
0046B5A7	. B2 01	MOV DL,1	
0046B5A9	. A1 60A44200	MOV EAX,DWORD PTR DS:[42A460]	
0046B5AE	. E8 5DEFFBFF	CALL CRACKME3.0042A510	

Veo que cambió el caption del botón y puedo por fin ver la puerta abierta (aunque no es lo único que esta abierto)

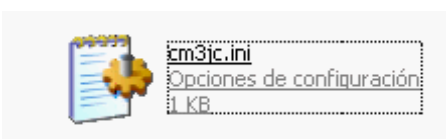


Desde ahora en adelante ya no tendré que registrar más el programa cada vez que quiera ver la sorpresa

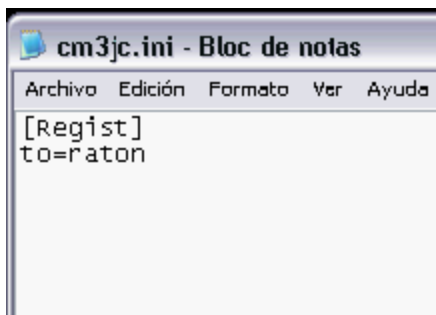
Esto ocurre por lo siguiente

Si recordáis habíamos visto en un tramo del código algo que parecía un archivo *.ini, pues bien en ese tramo del código se da una orden para escribir algo en un archivo llamado cm3jc.ini

Que nos guarda en el disco duro (C en mi caso)



Si lo abrimos con el bloc



El crackme al ejecutarse toma referencia de este archivo para saber si estamos registrados o no, al alterar el salto [0046B5A0](#) obligamos al crackme a escribir el archivo *.ini que nos da por registrados

Si lo borramos del disco duro el crackme volverá a decirnos que no estamos registrados

Esto que vemos en este capítulo es parecido a lo que vimos en los capítulos 4 y 5

Por hoy nada mas ya dije que este era un capítulo de descanso después del anterior

Si alguien se anima a encontrar el número de serie valido para su nombre y hacer un tuto de cómo se hizo podría añadirse como complemento a este capítulo.

Gracias

A todas las personas que colaboran desde el foro de HackxCrack para llevar adelante el curso, tanto los que colaboran aportando sus conocimientos como complemento al curso como a los que postean sus dudas para que aprendamos todos y por supuesto a los moderadores del mismo

A todos los crackers y programadores de los cuales he aprendido y sigo aprendiendo.

A los creadores de crackmes

En especial y sin menospreciar a nadie a [Ricardo Narvaja](#) por su aportación y su trabajo sobre el estudio de las protecciones y sus tutoriales en castellano y a [Makkakko](#) por sus tutoriales con Olly Debugger (Recomendados 100%) y por supuesto a [Shoulck](#) por la ayuda desinteresada que me esta prestando a costa de algo tan preciado como su tiempo.

A ti que me estas leyendo