

Para responder el reto correctamente, el software requiere más de una modificación en sus instrucciones:

Al ejecutar el programa por primera vez obtenemos:

```
C:\Documents and Settings\Admin\Desktop\crackme>crackme2.exe
I think you are missing something.

C:\Documents and Settings\Admin\Desktop\crackme>
```

Importamos a OllyDbg para su análisis:

Podemos ver que realiza una comprobación en el numero de parámetros.

<pre>0040120E ~ 74 25 JE SHORT crackme2.004012D5 00401210 - 83EC 08 SUB ESP,0x8 00401213 - 68 00304000 PUSH crackme2.00403000 00401218 - A1 E4504000 MOV EAX,DWORD PTR [(&svcr._ioh)] 0040121D - 83C0 40 ADD EAX,0x40 0040121E - 50 PUSH EAX 0040121F - E8 0A060000 CALL <JMP.&svcr.fprintf> 00401224 - 83C4 10 ADD ESP,0x10 00401229 - C745 F8 0100 MOV DWORD PTR [EBP-0x81,0x1] 0040122D - E9 C3000000 JMP crackme2.00401398 004012D5 > 8B45 0C MOV EAX,DWORD PTR [EBP+0xC]</pre>	<pre>format = "I think you are missing something." stream fprintf</pre>	<pre>Registers (FPU) EAX 00000000 ECX 0022FF00 EDX 7C90E514 ntdll.KiFastSystemCallRet EBX 7C90E514 ESP 0022FF00 EBP 0022FF00 ESI FFFFFFFF EDI 7C910228 ntdll.7C910228 EIP 00401210 crackme2.<ModuleEntryPoint></pre>
--	---	--

Ademas verifica que el exe se llame crackmeplease:

<pre>0040120E - 83EC 08 SUB ESP,0x8 00401210 - 68 24304000 PUSH crackme2.00403024 00401213 - FF30 PUSH DWORD PTR [EAX] 00401218 - E8 79060000 CALL <JMP.&svcr.streamp> 0040121D - 83C4 10 ADD ESP,0x10 0040121E - 85C0 TEST EAX,EAX 0040121F - 74 25 JE SHORT crackme2.00401313 00401224 - 83EC 08 SUB ESP,0x8 00401229 - 68 36304000 PUSH crackme2.00403036 0040122D - A1 E4504000 MOV EAX,DWORD PTR [(&svcr._ioh)] 00401231 - 83C0 40 ADD EAX,0x40 00401232 - 50 PUSH EAX 00401233 - E8 6C060000 CALL <JMP.&svcr.fprintf> 00401238 - 83C4 10 ADD ESP,0x10 0040123D - C745 F8 0200 MOV DWORD PTR [EBP-0x81,0x2] 00401241 - E9 85000000 JMP crackme2.00401398</pre>	<pre>s2 = "crackmeplease.exe" streamp format = "I have an identity problem." stream fprintf</pre>	<pre>C 0 ES 0023 32bit 0<FFFFFFFF> P 1 CS 001B 32bit 0<FFFFFFFF> A 0 SS 0023 32bit 0<FFFFFFFF> Z 1 DS 0023 32bit 0<FFFFFFFF> S 0 FS 0030 32bit 7FFDF000<FFF> I 0 GS 0000 NULL D 0 O 0 LastErr ERROR_ENVVAR_NOT_FOUND (00000000) EPL 00000246 (NO,NO,E,BE,NS,PE,GE,LE) STD empty -UNORM B944 01050104 0030006F STI empty +UNORM 006C 004F005C 0079006C STL empty +UNORM 006E 006F002E 00470042 STQ empty 0.0 STC empty 0.0 STB empty 0.0</pre>
---	---	---

Por ultimo, verifica que el argumento sea “I know the secret”.

<pre>00401316 - 83C0 04 ADD EAX,0x4 00401319 - 83EC 08 SUB ESP,0x8 0040131C - 68 53304000 PUSH crackme2.00403053 00401321 - FF30 PUSH DWORD PTR [EAX] 00401326 - E8 39060000 CALL <JMP.&svcr.streamp> 0040132B - 83C4 10 ADD ESP,0x10 0040132C - 85C0 TEST EAX,EAX 0040132D - 74 22 JE SHORT crackme2.00401351 0040132F - 83EC 08 SUB ESP,0x8 00401332 - 68 65304000 PUSH crackme2.00403065 00401337 - A1 E4504000 MOV EAX,DWORD PTR [(&svcr._ioh)] 0040133C - 83C0 40 ADD EAX,0x40 0040133D - 50 PUSH EAX 0040133E - E8 28060000 CALL <JMP.&svcr.fprintf> 00401343 - 83C4 10 ADD ESP,0x10 00401348 - C745 F8 0300 MOV DWORD PTR [EBP-0x81,0x3] 0040134D - EB 47 JMP SHORT crackme2.00401398 00401351 > C745 FC 0000 MOV DWORD PTR [EBP-0x41,0x0] 00401358 > 837D FC 21 CMP DWORD PTR [EBP-0x41,0x21] 0040135C ~ 77 23 JA SHORT crackme2.00401381</pre>	<pre>s2 = "I know the secret" streamp format = "Pardon? What did you say?" stream fprintf</pre>	<pre>C:\Users\Dell\Documents\Clases\Malware2016\Analisis de Malware FC 2016-2_Alumno s\Analisis de Malware FC 2016-2_Alumnos\Semana5 - 09May-13May\Iena5_Sub2.1.53y8 4 Bin\da011y_crackme2>crackmeplease.exe "I know the secret" We have a little secret: Chocolate</pre>
---	---	--

De ser asi, muestra el mensaje: “We hace a Little secret: Chocolate”.