evilprogrammer's mexican

https://crackmes.one/crackme/5d63011533c5d46f00e2c305

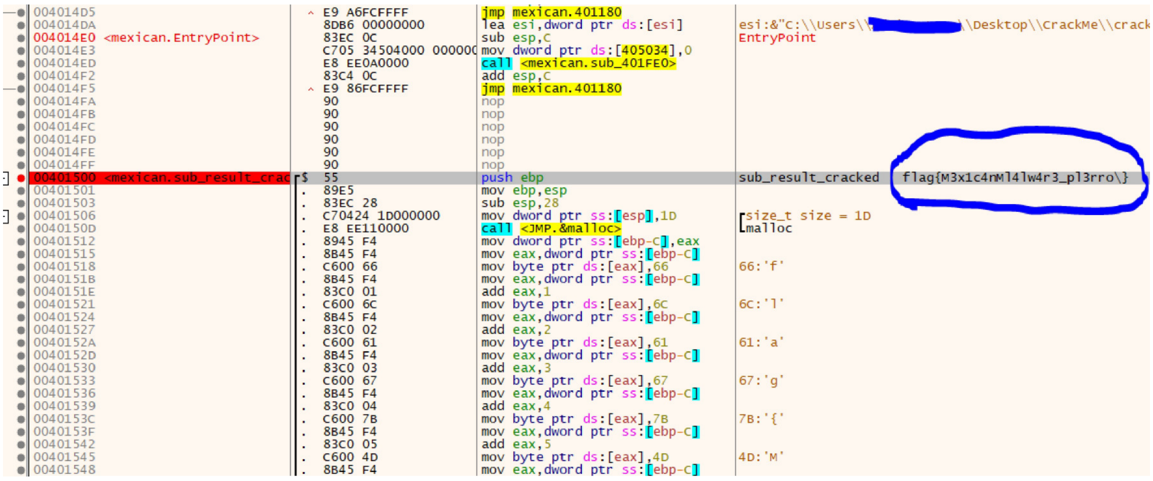
Crackme by b1h0 https://crackmes.one/user/b1h0

Date: 19/sep/2019

- Used **x64dbg** debugger.

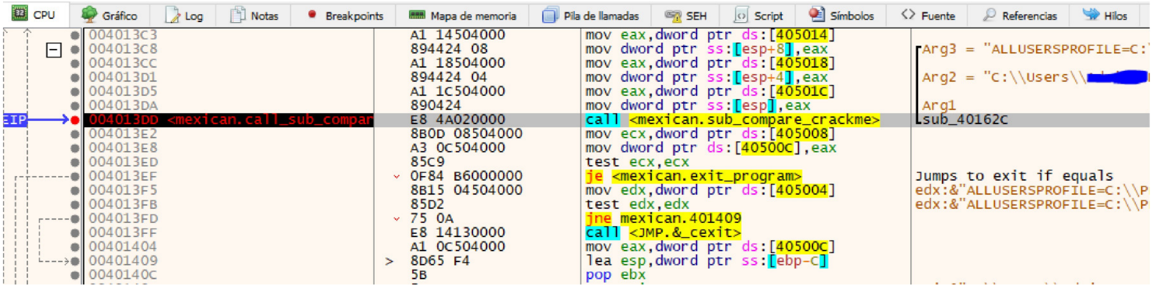
Some notes to get the flag and create the patch

- Once the **EntryPoint** is located, you can verify that at the address **0x00401500** a subroutine begins, which is the one shown in the *flag* text. We will call this subroutine: **sub_result_cracked**



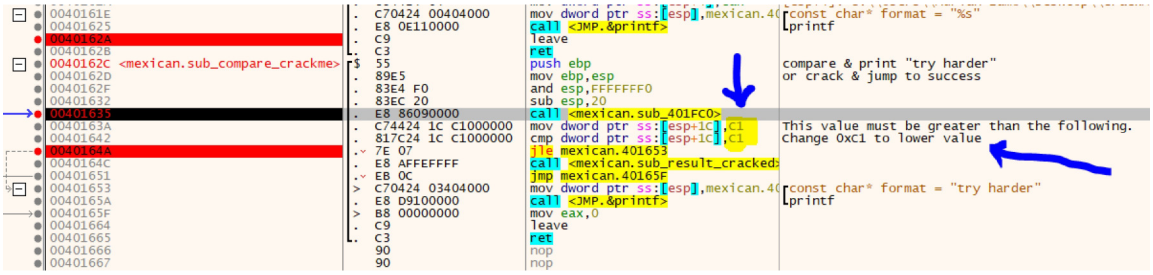
```
004014D5                             E9 A6FCFFFF        jmp mexican.401180
004014DA                             8DB6 00000000      lea esi,dword ptr ds:[esi]       esi:&"C:\\Users\\[redacted]\\Desktop\\CrackMe\\crack
004014E0 <mexican.EntryPoint>        83EC 0C            sub esp,C                        EntryPoint
004014E3                             C705 34504000 00000C mov dword ptr ds:[405034],0
004014ED                             E8 EE0A0000        call <mexican.sub_401FE0>
004014F2                             83C4 0C            add esp,C
004014F5                             E9 86FCFFFF        jmp mexican.401180
004014FA                             90                 nop
004014FB                             90                 nop
004014FC                             90                 nop
004014FD                             90                 nop
004014FE                             90                 nop
004014FF                             90                 nop
00401500 <mexican.sub_result_crac    55                 push ebp                         sub_result_cracked   flag{M3x1c4nMl4lw4r3_pl3rro\}
00401501                             89E5               mov ebp,esp
00401503                             83EC 28            sub esp,28
00401506                             C70424 1D000000    mov dword ptr ss:[esp],1D        size_t size = 1D
0040150D                             E8 EE110000        call <JMP.&malloc>               malloc
00401512                             8945 F4            mov dword ptr ss:[ebp-C],eax
00401515                             8B45 F4            mov eax,dword ptr ss:[ebp-C]
00401518                             C600 66            mov byte ptr ds:[eax],66         66:'f'
0040151B                             8B45 F4            mov eax,dword ptr ss:[ebp-C]
0040151E                             83C0 01            add eax,1
00401521                             C600 6C            mov byte ptr ds:[eax],6C         6C:'l'
00401524                             8B45 F4            mov eax,dword ptr ss:[ebp-C]
00401527                             83C0 02            add eax,2
0040152A                             C600 61            mov byte ptr ds:[eax],61         61:'a'
0040152D                             8B45 F4            mov eax,dword ptr ss:[ebp-C]
00401530                             83C0 03            add eax,3
00401533                             C600 67            mov byte ptr ds:[eax],67         67:'g'
00401536                             8B45 F4            mov eax,dword ptr ss:[ebp-C]
00401539                             83C0 04            add eax,4
0040153C                             C600 7B            mov byte ptr ds:[eax],7B         7B:'{'
0040153F                             8B45 F4            mov eax,dword ptr ss:[ebp-C]
00401542                             83C0 05            add eax,5
00401545                             C600 4D            mov byte ptr ds:[eax],4D         4D:'M'
00401548                             8B45 F4            mov eax,dword ptr ss:[ebp-C]
```

- Then later we can find in the address **0x004013dd** a call to the address **0x0040162c** which is the subroutine that we will call **sub_compare_crackme**. We establish a breakpoint there and then continue step by step.



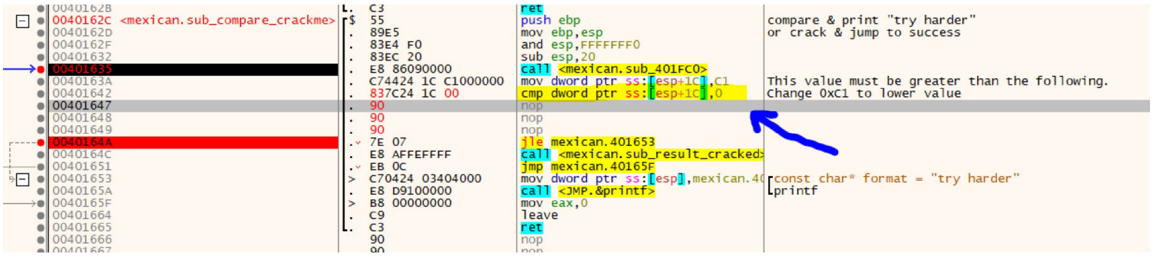
```
     004013C3                           A1 14504000        mov eax,dword ptr ds:[405014]
     004013C8                           894424 08          mov dword ptr ss:[esp+8],eax      Arg3 = "ALLUSERSPROFILE=C:
     004013CC                           A1 18504000        mov eax,dword ptr ds:[405018]
     004013D1                           894424 04          mov dword ptr ss:[esp+4],eax      Arg2 = "C:\\Users\\[redacted]
     004013D5                           A1 1C504000        mov eax,dword ptr ds:[40501C]
     004013DA                           890424             mov dword ptr ss:[esp],eax        Arg1
EIP  004013DD <mexican.call_sub_compar  E8 4A020000        call <mexican.sub_compare_crackme> sub_40162c
     004013E2                           8B0D 08504000      mov ecx,dword ptr ds:[405008]
     004013E8                           A3 0C504000        mov dword ptr ds:[40500C],eax
     004013ED                           85C9               test ecx,ecx
     004013EF                           0F84 B6000000      je <mexican.exit_program>         Jumps to exit if equals
     004013F5                           8B15 04504000      mov edx,dword ptr ds:[405004]     edx:&"ALLUSERSPROFILE=C:\\P
     004013FB                           85D2               test edx,edx                      edx:&"ALLUSERSPROFILE=C:\\P
     004013FD                           75 0A              jne mexican.401409
     004013FF                           E8 14130000        call <JMP.&_cexit>
     00401404                           A1 0C504000        mov eax,dword ptr ds:[40500C]
     00401409                           8D65 F4            lea esp,dword ptr ss:[ebp-C]
     0040140C                           5B                 pop ebx
```

- Finally at address **0x00401642** we find a comparison of the value **0xC1** with the value 0xC1. The key is that the two values have to be different, and in particular the first one greater than the second, therefore we change the first 0xC1 for a greater value, or the second 0xC1 for a smaller value.



```
0040161E                                 C70424 00404000    mov dword ptr ss:[esp],mexican.40  const char* format = "%s"
00401625                                 E8 0E110000        call <JMP.&printf>                 printf
0040162A                                 C9                 leave
0040162B                                 C3                 ret
0040162C <mexican.sub_compare_crackme>   55                 push ebp                           compare & print "try harder"
0040162D                                 89E5               mov ebp,esp                        or crack & jump to success
0040162F                                 83E4 F0            and esp,FFFFFFF0
00401632                                 83EC 20            sub esp,20
00401635                                 E8 86090000        call <mexican.sub_401FC0>
0040163A                                 C74424 1C C1000000 mov dword ptr ss:[esp+1C],C1       This value must be greater than the following.
00401642                                 817C24 1C C1000000 cmp dword ptr ss:[esp+1C],C1       Change 0xC1 to lower value
0040164A                                 7E 07              jle mexican.401653
0040164C                                 E8 AFFEFFFF        call <mexican.sub_result_cracked>
00401651                                 EB 0C              jmp mexican.40165F
00401653                                 C70424 03404000    mov dword ptr ss:[esp],mexican.40  const char* format = "try harder"
0040165A                                 E8 D9100000        call <JMP.&printf>                 printf
0040165F                                 B8 00000000        mov eax,0
00401664                                 C9                 leave
00401665                                 C3                 ret
00401666                                 90                 nop
00401667                                 90                 nop
```

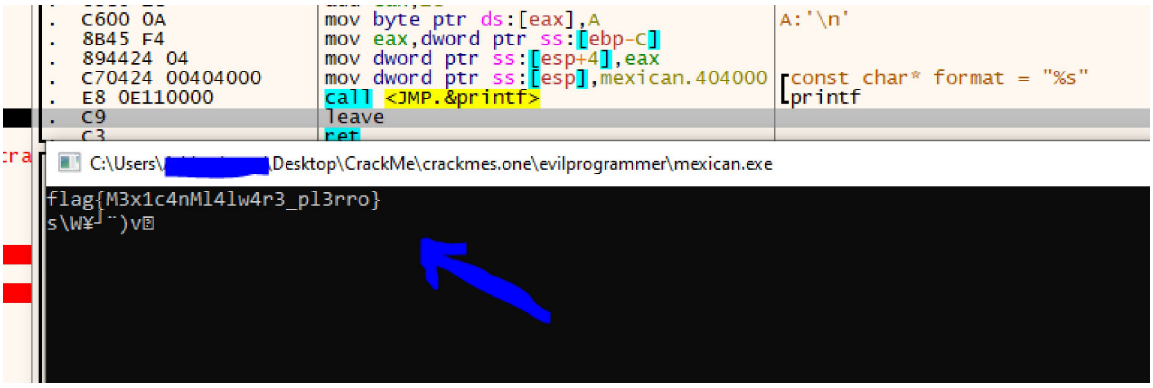
- So we change the *0xC1* value of the comparison line to a lower value. For example, **0 (zero)**



```
0040162B                                 C3                 ret
0040162C <mexican.sub_compare_crackme>   55                 push ebp                           compare & print "try harder"
0040162D                                 89E5               mov ebp,esp                        or crack & jump to success
0040162F                                 83E4 F0            and esp,FFFFFFF0
00401632                                 83EC 20            sub esp,20
00401635                                 E8 86090000        call <mexican.sub_401FC0>
0040163A                                 C74424 1C C1000000 mov dword ptr ss:[esp+1C],C1       This value must be greater than the following.
00401642                                 837C24 1C 00       cmp dword ptr ss:[esp+1C],0        Change 0xC1 to lower value
00401647                                 90                 nop
00401648                                 90                 nop
00401649                                 90                 nop
0040164A                                 7E 07              jle mexican.401653
0040164C                                 E8 AFFEFFFF        call <mexican.sub_result_cracked>
00401651                                 EB 0C              jmp mexican.40165F
00401653                                 C70424 03404000    mov dword ptr ss:[esp],mexican.40  const char* format = "try harder"
0040165A                                 E8 D9100000        call <JMP.&printf>                 printf
0040165F                                 B8 00000000        mov eax,0
00401664                                 C9                 leave
00401665                                 C3                 ret
00401666                                 90                 nop
00401667                                 90                 nop
```

The flag

- After the change, the flag message appears. Printed message: **flag**



```
C600 0A            mov byte ptr ds:[eax],A                  A:'\n'
8B45 F4            mov eax,dword ptr ss:[ebp-C]
894424 04          mov dword ptr ss:[esp+4],eax
C70424 00404000    mov dword ptr ss:[esp],mexican.404000    const char* format = "%s"
E8 0E110000        call <JMP.&printf>                       printf
C9                 leave
C3                 ret
```

C:\Users\[redacted]Desktop\CrackMe\crackmes.one\evilprogrammer\mexican.exe

```
flag{M3x1c4nMl4lw4r3_pl3rro}
s\W¥┘¨)v⊡
```

Note one curious thing. After displaying the flag, strange or random characters are still displayed. This is because the flag string does not end with **NULL '\0'**. It is likely that there is some part of the code that adds this value to the chain or it could also be that the programmer has forgotten this detail.

The Patch

The file for the patch is included with the name mexican-patch.1337

```
>mexican.exe
00001642:81->83
00001646:C1->00
00001647:00->90
00001648:00->90
00001649:00->90
```