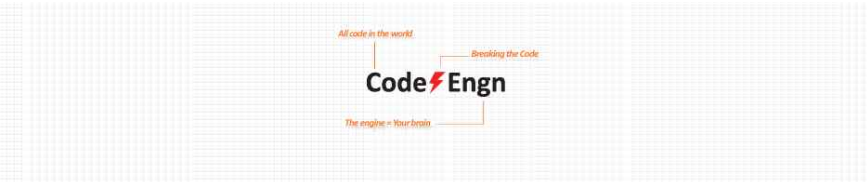
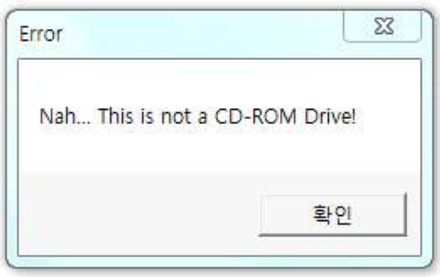
CodeEngn

Solving problems

basic levell



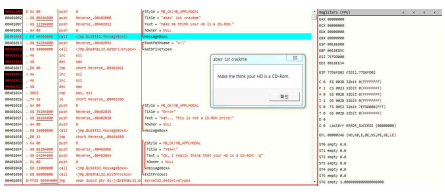
Nick : Cy_h
Email : h6lcker@gmail.com

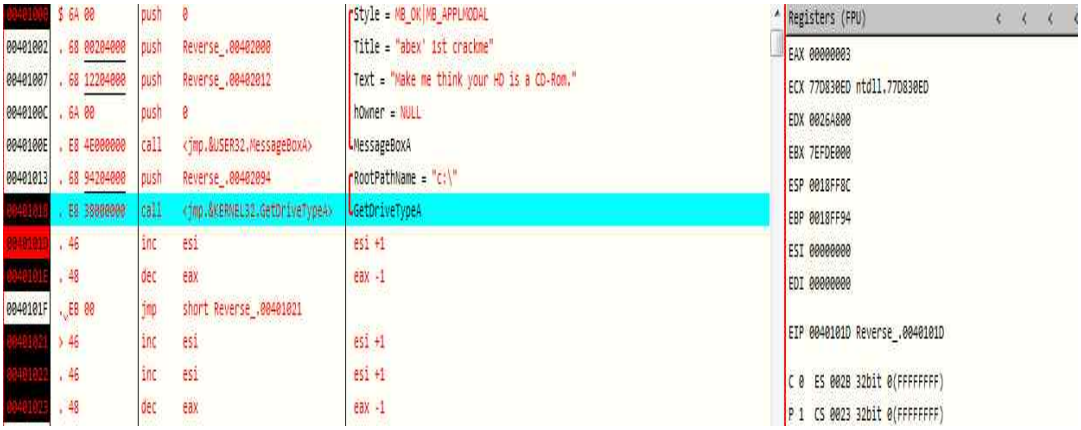


프로그램을 실행해보면 CD-ROM을 넣으라고 하고 Nah... This is not a CD-ROM Drive! 가 나옵니다.

추측을 해보자면 어떠한 조건을 충족시켜야 error 메시지를 출력하지를 않고 성공 메시지를 호출할것같습니다.

일단 첫 번째 API 가 호출됩니다.





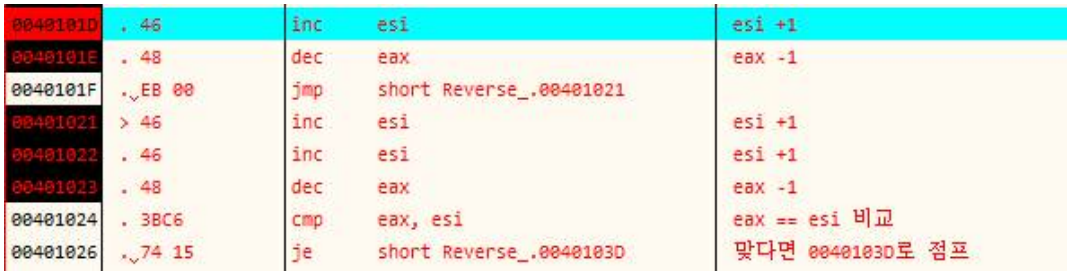
GetDrive 

Type() api를 호출합니다.

그리고 EAX 의 값이 3이 되었습니다.

eax 는 함수의 리턴 값 등등 연산 결과가 저장되는 레지스터입니다.

따라서, HDD를 CD-Rom으로 인식시키기 위해서는 GetDriveTypeA의 리턴값이 무엇이 되어야 하는가는 eax의 값이 리턴 값이 되는 것입니다.



여기서 보자면 esi 는 총 3번 증가하였고 (esi 초기값은 0임)
eax 는 2번 감소하였다 (eax 초기값은 3임)

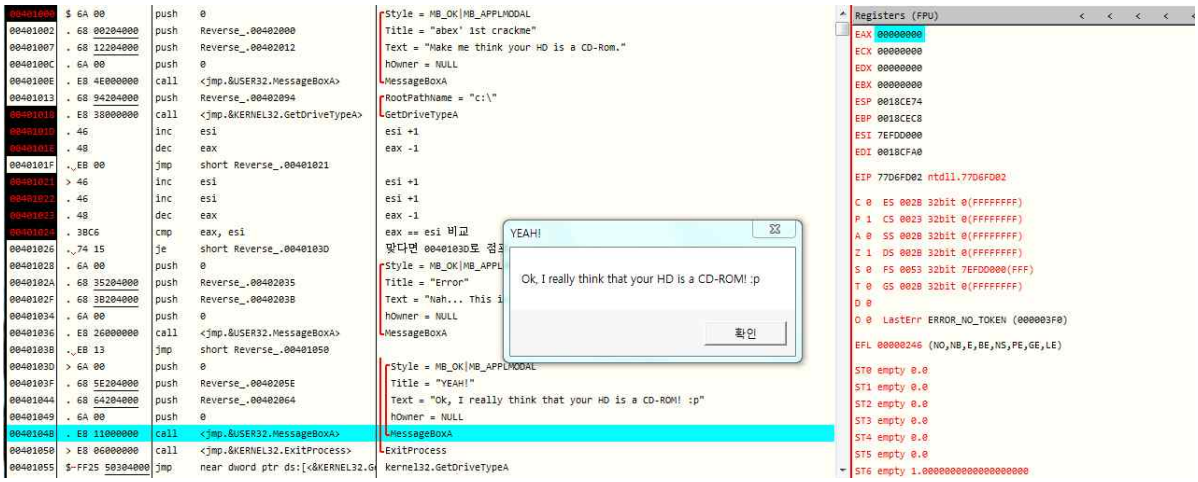
cmp 로 eax,esi 값이 같은지를 확인함. (eax == esi)

하지만 eax = 1 , esi = 3

비교해봐도 같지가 않다 즉, 같아 질려면 eax 는 5 가 되어야한다.

eax = 5 일 때를 eax 에 대입해서 결과를 보면


Registers (FPU)
EAX 00000003
ECX 77D830ED ntdll.77D830ED
EDX 005DA800
EBX 7EFDE000
ESP 0018FF8C
EBP 0018FF94
ESI 00000003
EDI 00000000


00401000 $ 6A 00 push 0 Style = MB_OK|MB_APPLMODAL
00401002 . 68 00204000 push Reverse_.00402000 Title = "abex' 1st crackme"
00401007 . 68 12204000 push Reverse_.00402012 Text = "Make me think your HD is a CD-Rom."
0040100C . 6A 00 push 0 hOwner = NULL
0040100E . E8 4E000000 call <jmp.&USER32.MessageBoxA> MessageBoxA
00401013 . 68 94204000 push Reverse_.00402094 RootPathName = "c:\"
00401018 . E8 38000000 call <jmp.&KERNEL32.GetDriveTypeA> GetDriveTypeA
0040101D . 46 inc esi esi +1
0040101E . 48 dec eax eax -1
0040101F . EB 00 jmp short Reverse_.00401021
00401021 > 46 inc esi esi +1
00401022 . 46 inc esi esi +1
00401023 . 48 dec eax eax -1
00401024 . 3BC6 cmp eax, esi eax == esi 비교
00401026 . 74 15 je short Reverse_.0040103D 맞다면 0040103D로 점프
00401028 . 6A 00 push 0 Style = MB_OK|MB_APPL
0040102A . 68 35204000 push Reverse_.00402035 Title = "Error"
0040102F . 68 3B204000 push Reverse_.0040203B Text = "Nah... This i
00401034 . 6A 00 push 0 hOwner = NULL
00401036 . E8 26000000 call <jmp.&USER32.MessageBoxA> MessageBoxA
0040103B . EB 13 jmp short Reverse_.00401050
0040103D > 6A 00 push 0 Style = MB_OK|MB_APPLMODAL
0040103F . 68 5E204000 push Reverse_.0040205E Title = "YEAH!"
00401044 . 68 64204000 push Reverse_.00402064 Text = "Ok, I really think that your HD is a CD-ROM! :p"
00401049 . 6A 00 push 0 hOwner = NULL
0040104B . E8 11000000 call <jmp.&USER32.MessageBoxA> MessageBoxA
00401050 > E8 06000000 call <jmp.&KERNEL32.ExitProcess> ExitProcess
00401055 $-FF25 50304000 jmp near dword ptr ds:[<&KERNEL32.G kernel32.GetDriveTypeA
YEAH!
Ok, I really think that your HD is a CD-ROM! :p
확인
Registers (FPU)
EAX 00000000
ECX 00000000
EDX 00000000
EBX 00000000
ESP 0018CE74
EBP 0018CEC8
ESI 7EFDD000
EDI 0018CFA0
EIP 77D6FD02 ntdll.77D6FD02
C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 1 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 7EFDD000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0 LastErr ERROR_NO_TOKEN (000003F0)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 1.0000000000000000000

flag : 5