


# codeengn-basic-L01 풀이

리버싱 문제풀이 / Wonlf / 2022. 3. 11. 09:47

Basic RCE L01

HDD를 CD-Rom으로 인식시키기 위해서는 GetDriveTypeA의 리턴값이 무엇이 되어야 하는가

— Author: abex  
— File Password: codeengn



abex' 1st crackme

Make me think your HD is a CD-Rom.

확인

Error

Nah... This is not a CD-ROM Drive!

확인

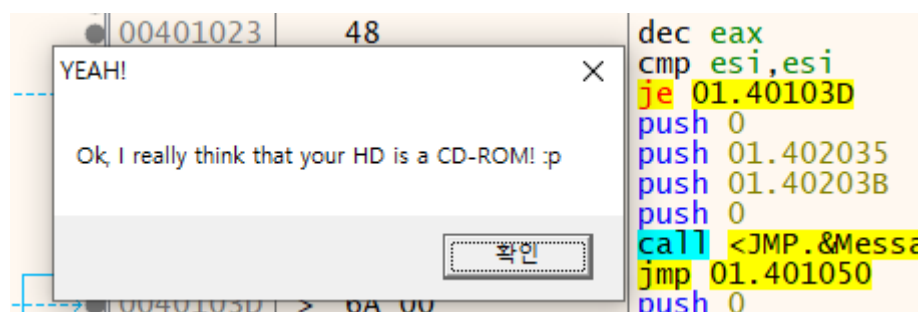
실행하면 메시지 박스가 나오고, 확인을 누르면 CD-ROM드라이브가 아니라고 거부 당하는 메시지가 뜨네요

x64dbg로 열어서 저 메시지들이 있는 구문을 살펴보겠습니다.

push 0	EntryPoint
push 01.402000	402000:"abex' 1st crackme"
push 01.402012	402012:"Make me think your HD is a CD-Rom."
push 0	
call <JMP.&MessageBoxA>	
push 01.402094	402094:"c:\\\"
call <JMP.&GetDriveTypeA>	이 함수가 반환하는 값은 eax = 3
inc esi	esi = esi + 1
dec eax	eax = eax - 1
jmp 01.401021	
inc esi	esi = esi + 1
inc esi	esi = esi + 1
dec eax	eax = eax - 1
cmp esi,esi	eax와 ecx를 비교하고
je 01.40103D	같으면 통과구문으로 점프
push 0	
push 01.402035	402035:"Error"
push 01.40203B	40203B:"Nah... This is not a CD-ROM Drive!"
push 0	
call <JMP.&MessageBoxA>	
jmp 01.401050	
push 0	
push 01.40205E	40205E:"YEAH!"
push 01.402064	402064:"Ok, I really think that your HD is a CD-ROM! :p"
push 0	
call <JMP.&MessageBoxA>	
call <JMP.&ExitProcess>	
jmp dword ptr ds:[<&GetDriveTypeA	JMP.&GetDriveTypeA
jmp dword ptr ds:[<&ExitProcess	JMP.&ExitProcess
jmp dword ptr ds:[<&MessageBoxA	JMP.&MessageBoxA

eax와 ecx를 비교하여 같다면 무조건 통과되는 것이니 cmp eax, esi 부분을 cmp eax, esi 로 바꿔주어 통과로 점프

그럼 통과 메시지가 출력된다.



그렇다면 정작 이 문제의 플래그인 CD-ROM으로 인식되게 하려면 eax가 얼마가 되어야 할까.

inc esi가 총 3 번있고 dec eax가 총 2번 있으니 esi의 값은 +3이 되어있고 eax의 값은 처음이었던 3에서 -2가 되어있다

eax값과 esi의 값이 연산 후 같게 되려면 GetDriveTypeA함수를 실행한 후 eax의 값이 5이어야 한다.

맞나 확인해보려 마이크로소프트 공식 문서를 뒤져봅니다.

---

드라이브\_CDROM

5

드라이브는 CD-ROM 드라이브입니다.

---

정답이네요. 플

래그는 {5}