

*CodeEngn basic RCE 1

: HDD를 CD-Rom으로 인식시키기 위해서는 GetDriveTypeA의 리턴값이 무엇이 되어야 하는가

코드엔진 베이직 1번을 풀기 위해서는 ollydbg를 다운받아야 한다.

구글에 ollydbg를 검색하고 공식 웹사이트에서 .zip 파일을 다운로드하고 압축을 풀면 올리디버가 설치 가능하다.

우선 코드엔진에서 다운로드 받은 zip파일을 풀면 실행파일이 하나 존재한다. 해당 실행파일을 더블클릭하면 "make me think your HD is a CD-ROM"이라고 나오고, 확인을 누르면 CD-ROM이 아니라고 나온다.

올리디버를 실행해 file-open을 눌러 해당 exe파일을 열어보았다.

00401000	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
00401002	68 00204000	PUSH 01.00402000	Title = "aben' 1st crackme"
00401004	68 12204000	PUSH 01.00402012	Text = "make me think your HD is a CD-Rom."
00401006	6A 00	PUSH 0	hOwner = NULL
00401008	E8 4E000000	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
00401010	68 94204000	PUSH 01.00402094	RootPathName = "c:\\"
00401012	E8 38000000	CALL <JMP.&KERNEL32.GetDriveTypeA>	GetDriveTypeA
00401014	46	INC ESI	
00401016	48	DEC EAX	
00401018	EB 00	JMP SHORT 01.00401021	
00401020	46	INC ESI	
00401022	46	INC ESI	
00401024	48	DEC EAX	
00401026	3BC6	CMPL EAX,ESI	
00401028	74 15	JMP SHORT 01.0040103D	
00401030	6A 00	PUSH 0	Title = "Error"
00401032	68 35204000	PUSH 01.00402035	Text = "Nah... This is not a CD-ROM Drive!"
00401034	68 3B204000	PUSH 01.0040203B	hOwner = NULL
00401036	6A 00	PUSH 0	MessageBoxA
00401038	E8 26000000	CALL <JMP.&USER32.MessageBoxA>	
0040103A	EB 13	JMP SHORT 01.00401050	
0040103C	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
0040103E	68 5E204000	PUSH 01.0040205E	Title = "YEAH!"
00401040	68 64204000	PUSH 01.00402064	Text = "Ok, I really think that your HD is a CD-ROM! :p"
00401042	6A 00	PUSH 0	hOwner = NULL
00401044	E8 11000000	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
00401046	EB 08	JMP SHORT 01.00401050	
00401048	E8 06000000	CALL <JMP.&KERNEL32.ExitProcess>	ExitProcess
0040104A	FF25 50304000	JMP DWORD PTR DS:[&KERNEL32.GetDriveTypeA]	KERNEL32.GetDriveTypeA
0040104C	FF25 54304000	JMP DWORD PTR DS:[&KERNEL32.ExitProcess]	KERNEL32.ExitProcess
0040104E	FF25 5C304000	JMP DWORD PTR DS:[&USER32.MessageBoxA]	USER32.MessageBoxA
00401050	00	DB 00	
00401052	00	DB 00	
00401054	00	DB 00	
00401056	00	DB 00	
00401058	00	DB 00	
0040105A	00	DB 00	
0040105C	00	DB 00	
0040105E	00	DB 00	
00401060	00	DB 00	
00401062	00	DB 00	
00401064	00	DB 00	
00401066	00	DB 00	
00401068	00	DB 00	
0040106A	00	DB 00	
0040106C	00	DB 00	
0040106E	00	DB 00	
00401070	00	DB 00	
00401072	00	DB 00	

주목해야 할 함수는 GetDriveType이다.

이 함수는 현재 파일이 위치하고 있는 드라이브 타입에 따라 상수값을 리턴해준다. HDD의 경우에는 3을 리턴, CD-ROM인 경우에는 5를 리턴한다.

해설

위 그림에서 0040101D 부터 살펴보면 INC 와 DEC 가 쪽 나오고 있는데, INC는 +1을 의미하고, DEC는 -1을 의미한다.

EAX는 -2가 될것이고, ESI는 +3이 될것이다.

근데 여기서 현재 위치하고 있는 디스크가 HDD이기 때문에 EAX의 값은 3이므로 -2를 해주게 되면 1이 나오게 된다.

CMP: 2개의 값을 비교

JE: CMP 명령에서 비교한 결과가 같으면 지정된 주소로 점프

JE 명령에서 지정된 주소는 바로 성공 메시지가 나오는 주소이기 때문에,

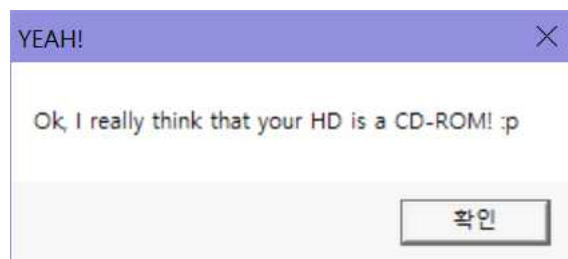
이 문제의 목표는 EAX=ESI라고 할 수 있다.

EAX=1, ESI=3이므로 두 값을 비교하면 다르기 때문에 성공 메시지로 가라는 JE 명령을 지나치게 되는 것이다.

그럼 해주어야 할 것은 EAX에 +2를 해주어야 한다

(그래야 HDD에 있지만 CD-ROM으로 인식하기 때문)

나같은 경우는 어셈블리어를 수정했는데, JE명령을 JMP명령으로 바꿔서 해당 명령어를 만나면 비교와 상관없이 바로 성공메세지 주소로 가도록 수정하였다.



성공 !!!*^.^*

+다음에는 ESI의 값은 무엇이며 EAX의 값을 바꾸려면 어떻게 해야하는지 알아보자(레지스터)