

# [Code\_Engn] Basic RCE L01

🕒 생성일	@2022년 11월 29일 오전 11:21
🏷 태그	Rev

## Basic RCE L01

HDD를 CD-Rom으로 인식시키기 위해서는 GetDriveTypeA의 리턴값이 무엇이 되어야 하는가

— Author: abex

— File Password: codeengn



00401000	6A 00	push 0	EntryPoint
00401002	68 00204000	push 01.402000	402000:"abex' 1st crackme"
00401007	68 12204000	push 01.402012	402012:"Make me think your HD is a CD-Rom."
0040100C	6A 00	push 0	
0040100E	E8 4E000000	call <JMP.&MessageBoxA>	
00401013	68 94204000	push 01.402094	402094:"c:\\\"
00401018	E8 38000000	call <JMP.&GetDriveTypeA>	
0040101D	46	inc esi	esi:EntryPoint
0040101E	48	dec eax	
0040101F	EB 00	jmp 01.401021	
00401021	46	inc esi	esi:EntryPoint
00401022	46	inc esi	esi:EntryPoint
00401023	48	dec eax	
00401024	3BC6	cmp eax,esi	esi:EntryPoint
00401026	74 15	je 01.40103D	
00401028	6A 00	push 0	
0040102A	68 35204000	push 01.402035	402035:"Error"
0040102F	68 38204000	push 01.402038	402038:"Nah... This is not a CD-ROM Drive!"
00401034	6A 00	push 0	
00401036	E8 26000000	call <JMP.&MessageBoxA>	
00401038	EB 13	jmp 01.401050	
0040103D	6A 00	push 0	
0040103F	68 5E204000	push 01.40205E	40205E:"YEAH!"
00401044	68 64204000	push 01.402064	402064:"Ok, I really think that your HD is a CD-ROM! :p"
00401049	6A 00	push 0	
0040104B	E8 11000000	call <JMP.&MessageBoxA>	
00401050	E8 06000000	call <JMP.&ExitProcess>	
00401055	FF25 50304000	jmp dword ptr ds:[<&GetDriveTypeA>]	JMP.&GetDriveTypeA
00401058	FF25 54304000	jmp dword ptr ds:[<&ExitProcess>]	JMP.&ExitProcess
00401061	FF25 5C304000	jmp dword ptr ds:[<&MessageBoxA>]	JMP.&MessageBoxA
00401067	0000	add byte ptr ds:[eax],a]	

GetDriveTypeA에 브레이크 포인트를 걸고 실행시켜보았다.

● 0040100E	E8 4E000000	call <JMP.&MessageBoxA>	
● 00401013	68 94204000	push 01.402094	402094:"c:\\\"
● 00401018	E8 38000000	call <JMP.&GetDriveTypeA>	
● 0040101D	46	inc esi	esi:EntryPoint
● 0040101E	48	dec eax	
● 0040101F	✓ EB 00	jmp 01.401021	
● 00401021	46	inc esi	esi:EntryPoint
● 00401022	46	inc esi	esi:EntryPoint
● 00401023	48	dec eax	
● 00401024	38C6	cmp eax,esi	esi:EntryPoint
● 00401026	✓ 74 15	je 01.40103D	

끝나고 레지스터를 보면 EAX에는 3이 들어있고, ESI에는 0이 들어있는걸 볼 수 있다.

EAX	00000003
EBX	0023D000
ECX	00490000
EDX	00490000
EBP	0019FF80
ESP	0019FF74
ESI	00401000
EDI	00401000

그리고 cmp구문전 까지 실행시키면 레지스터안에 값들이 아래 처럼 변해있다.

EAX	00000001
EBX	0023D000
ECX	00490000
EDX	00490000
EBP	0019FF80
ESP	0019FF74
ESI	00401003
EDI	00401000

EAX : 3 → 1 | ESI : 0 → 3

이 두값이 같아야 CDROM으로 인식하니 GetDriveTypeA의 리턴값은 5가 되어야 한다.