

CodeEngn basic RCE L07

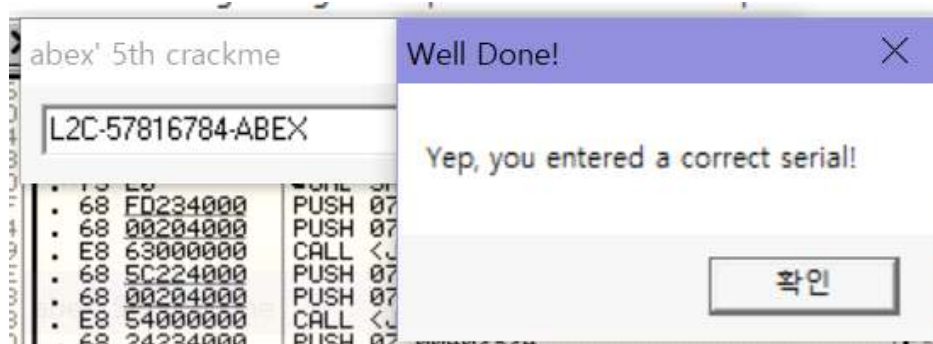
: 컴퓨터 C 드라이브의 이름이 CodeEngn 일경우 시리얼이 생성될때 CodeEngn은 '3어떤것'으로 변경되는가



시리얼을 구해야 한다.

004010B6	. 8305 50224000	ADD DWORD PTR DS:[40225D],1	
004010B0	. 8305 5E224000	ADD DWORD PTR DS:[40225E],1	
004010C4	. 8305 5F224000	ADD DWORD PTR DS:[40225F],1	
004010C8	. FECA	DEC DL	
004010CD	. ^75 E0	JNZ SHORT 07.004010AF	
004010CF	. 68 FD234000	PUSH 07.004023FD	
004010D4	. 68 00204000	PUSH 07.00402000	
004010D9	. E8 63000000	CALL <JMP.&KERNEL32.lstrcatA>	[StringToAdd = "L2C-5781"
004010DE	. 68 5C224000	PUSH 07.0040225C	ConcatString = "L2C-57816784-ABEX"
004010E3	. 68 00204000	PUSH 07.00402000	lstrcatA
004010E8	. E8 54000000	CALL <JMP.&KERNEL32.lstrcatA>	[StringToAdd = "6784-ABEX"
004010ED	. 68 24234000	PUSH 07.00402324	ConcatString = "L2C-57816784-ABEX"
004010F2	. 68 00204000	PUSH 07.00402000	lstrcatA
004010F7	. E8 51000000	CALL <JMP.&KERNEL32.lstrcatA>	[String2 = "123"
004010FC	. 33F8 00	CMPEB EAX,0	String1 = "L2C-57816784-ABEX"
004010FF	. ^74 16	JE SHORT 07.00401117	lstrcatA
00401101	. 6A 00	PUSH 0	
00401103	. 68 34244000	PUSH 07.00402434	[Style = MB_OK;MB_APPLMODAL
00401108	. 68 3B244000	PUSH 07.0040243B	Title = "Error!"
0040110D	. FF75 08	PUSH DWORD PTR SS:[EBP+8]	Text = "The serial you entered is not correct!"
00401110	. E8 56000000	CALL <JMP.&USER32.MessageBoxA>	hOwner
00401115	. ^EB 16	JMP SHORT 07.0040112D	MessageBoxA
00401117	. > 6A 00	PUSH 0	
00401119	. 68 06244000	PUSH 07.00402406	[Style = MB_OK;MB_APPLMODAL
0040111E	. 68 11244000	PUSH 07.00402411	Title = "Well Done!"
00401123	. FF75 08	PUSH DWORD PTR SS:[EBP+8]	Text = "Yep, you entered a correct serial!"
00401126	. E8 40000000	CALL <JMP.&USER32.MessageBoxA>	hOwner
0040112B	. ^EB 00	JMP SHORT 07.0040112D	MessageBoxA
0040112D	. > 6A 00	PUSH 0	
0040112F	. FF75 08	PUSH DWORD PTR SS:[EBP+8]	Result = 0
00401132	. E8 22000000	CALL <JMP.&USER32.EndDialog>	hWnd
00401137	. C9	LEAVE	EndDialog
00401138	. C2 1000	RETN 10	
0040113B	. \$-FF25 6C304000	JMP DWORD PTR DS:[<&KERNEL32.GetModuleH	KERNEL32.GetModuleHandler
00401141	. \$-FF25 75304000	JMP DWORD PTR DS:[<&KERNEL32.GetModuleH	KERNEL32.GetModuleHandler

에러메세지 내용이 있는 부분을 찾았고, 위에 있는 알 수 없는 문자열이 수상해 보여서 exe를 실행시켜 123이라는 숫자를 넣어보았더니, 두개의 문자열이 이어진게 시리얼 값이라고 추측이 된다.



++근데 코드엔진 문제에서 원하는 답은 c드라이브 변경 시 어떻게 되는지를 물었는데,
저는 쫄보라서 이름을 변경해보지 못했어요... 노트북 안에 있는 내용들 날아갈까봐...
검색해보니 만약 codeengn으로 드라이브 이름을 변경했다면 두 문자열사이에 codeengn이
추가되어서 L2C-5781codeengn6784-ABEX 로 나온다고 합니다 ! :)