

: Name이 CodeEngn일때 Serial을 구하시오



ReWrit's Crackme#5

* This is my 5th crackme. *
* i hope you will enjoy it. *

Enter your Name:

00401597	8045 C4	LEA EAX, DWORD PTR SS:[EBP-3C]	
0040159A	0110	ADD DWORD PTR DS:[EAX], EDX	
0040159C	8B45 C0	MOV EAX, DWORD PTR SS:[EBP-40]	
0040159F	3B45 C4	CMP EAX, DWORD PTR SS:[EBP-3C]	
004015A2	0F85 94000000	JNZ 16.0040163C	
004015A8	C7424 F5FFFF	MOV DWORD PTR SS:[ESP], -0B	
004015AF	E8 8CF60000	CALL <JMP.&KERNEL32.GetStdHandle>	GetStdHandle
004015B4	83EC 04	SUB ESP, 4	
004015B7	C74424 04 0000	MOV DWORD PTR SS:[ESP+4], 00	

EAX와 스택영역의 EBP-3C의 4바이트 공간 값을 비교하고, 이 값이 같아야 성공메세지로 가게 된다.

반대로 0040163C 는

00401637	.E9 EA000000	JMP 16.00401726	
0040163C	> C70424 F5FFFF	MOV DWORD PTR SS:[ESP],-0B	
00401643	. C745 90 010000	MOV DWORD PTR SS:[EBP-70],1	
0040164A	. E8 F1F50000	CALL <JMP.&KERNEL32.GetStdHandle>	GetStdHandle
0040164F	. 83EC 04	SUB ESP,4	
00401652	. C74424 04 0C00	MOV DWORD PTR SS:[ESP+4],0C	
0040165A	. 890424	MOV DWORD PTR SS:[ESP],EAX	
0040165D	. E8 EEF50000	CALL <JMP.&KERNEL32.SetConsoleTextAttri	SetConsoleTextAtt
00401662	. 83EC 08	SUB ESP,8	
00401665	. C74424 04 A8B	MOV DWORD PTR SS:[ESP+4],16.0043B1A8	
0040166D	. C70424 C03344	MOV DWORD PTR SS:[ESP],16.004433C0	
00401674	. E8 B78C0200	CALL 16.0042A330	
00401679	. C74424 04 FF0	MOV DWORD PTR SS:[ESP+4],16.004400FF	ASCII " Wrong pas
00401681	. C70424 C03344	MOV DWORD PTR SS:[ESP],16.004433C0	
00401688	. E8 4BAD0300	CALL 16.0043C3D8	
0040168D	. C74424 04 110	MOV DWORD PTR SS:[ESP+4],16.00440111	ASCII " =/"

에러메세지 바로 위에 존재한다는 것을 알 수 있다.



CMP와 JNZ에 각각 BP를 걸고 실행했고, 이름과 패스워드를 입력하였다.

Registers (FPU)			
EAX	00000457		
ECX	00000000		
EDX	E4B88080		
EBX	00004000		
ESP	0070FE70		
EBP	0070FF28		
ESI	00401220	16.<ModuleEntryPoint>	
EDI	00401220	16.<ModuleEntryPoint>	
EIP	0040159F	16.0040159F	
C 0	ES 002B	32bit 0(FFFFFFFF)	
P 0	CS 0023	32bit 0(FFFFFFFF)	
A 0	SS 002B	32bit 0(FFFFFFFF)	
Z 0	DS 002B	32bit 0(FFFFFFFF)	
S 1	FS 0053	32bit 321000(FFF)	
T 0	GS 002B	32bit 0(FFFFFFFF)	
O 0			
	LastErr	ERROR_SUCCESS (00000000)	

EAX값이 1111의 16진수 값 457 이므로, 1111을 입력한다는 것을 알 수 있다.

즉 NAME이 CodeEngn일 때의 패스워드 값은 "스택영역의 EBP-3C주소의 4바이트 값"이라는 것을 알 수 있다.

```
004015E6 | . C70424 C03344 | MOV DWORD PTR SS:[ESP]  
004015ED | . E8 F6000300 | CALL 16.0043C3D8  
Stack SS:[0070FEEC]=E4C60D97  
EAX=00000457
```

EBP-3C 는 0070FEEC이고, 이 값이 E4C60D97이라는 것을 올리디버거에서 알려주고 있다.
E4C60D97은 4바이트 값도 맞기 때문에, 이게 답이라는 것을 알 수 있다! 이 외에도 밑에
HEX가 나와있는 곳에서 CTRL+G를 눌러 0070FEEC를 집어넣으면 확인이 가능하다.



굿잡 ! 이라는 성공 메시지가 나온다.