

19.02.16 CodeEngn Basic RCE L11

Tree to Tree

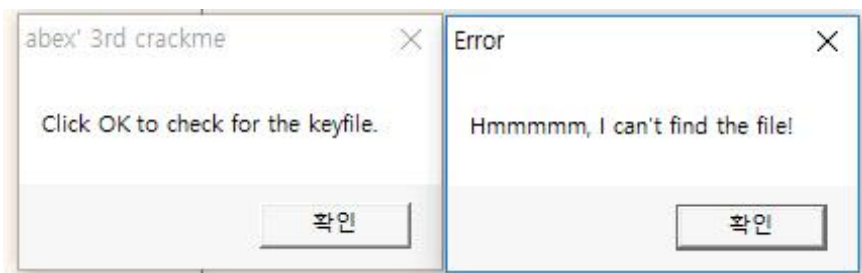
Basic RCE L11

OEP를 찾으시오. Ex) 00401000 / Stolenbyte 를 찾으시오.
Ex) FF35CA204000E84D000000 정답인증은 OEP+ Stolenbyte
Ex) 00401000FF35CA204000E84D000000

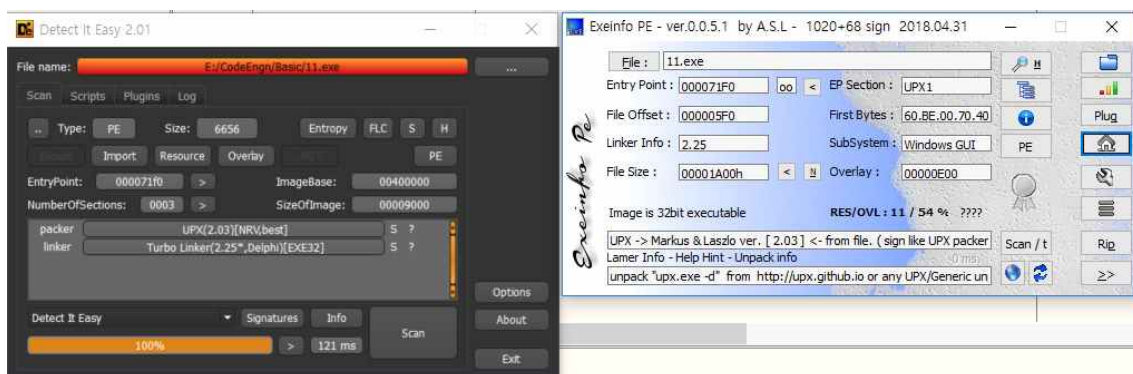
— Author: abex
— File Password: codeengn



Stolienbyte를 찾아보자



실행했을 때 나오는 창



UPX 2.0버전으로 pack되어있음

pushad breakpoint

주소	Module/Label/Exception	상태	디스어셈블리
004071F0	<11.exe.EntryPoint>	One-time	pushad

실행 후 popad 찾으러 감.
밑으로 쭉내려서 popad에 breakpoint걸고 실행

→ 0040736E	6A 00	push 0	
00407370	68 00 20 40 00	push 11.402000	402000:"abex' 3rd crackme"
00407375	68 12 20 40 00	push 11.402012	402012:"Click OK to check for the keyfile"
0040737A	8D 44 24 80	lea eax, dword ptr [esp-80]	
→ 0040737E	6A 00	push 0	
00407380	39 C4	cmp esp, eax	
00407382	75 FA	jne 11.40737E	
00407384	83 EC 80	sub esp, FFFFFFFF80	
00407387	E9 80 9C FFFF	jmp 11.40100C	

실행시켰을 때 나오는 문자열들이 push되는 모습
Stolenbyte 6A0068002040006812204000

0040100C	6A 00	push 0	미지P
0040100E	E8 8C 00 00 00	call <JMP.&MessageBoxA>	
00401013	6A 00	push 0	
00401015	68 80 00 00 00	push 80	
0040101A	6A 03	push 3	
0040101C	6A 00	push 0	
0040101E	6A 00	push 0	
00401020	68 00 00 00 80	push 80000000	
00401025	68 B9 20 40 00	push 11.4020B9	4020B9:"abex.12c"
0040102A	E8 5E 00 00 00	call <JMP.&createFileA>	
0040102F	A3 CA 20 40 00	mov dword ptr ds:[4020CA], eax	
00401034	93 F8 FF	cmp eax, FFFFFFFF	
00401037	74 3C	je 11.401075	
00401039	6A 00	push 0	
0040103B	FF 35 CA 20 40 00	push dword ptr ds:[4020CA]	
00401041	E8 4D 00 00 00	call <JMP.&GetFileSize>	

OEP 0040100C - C(opset) = 00401000
004010006A0068002040006812204000
Clear