

2019.03.02. CodeEngn Advance 2


Tree to Tree

Advance RCE L02

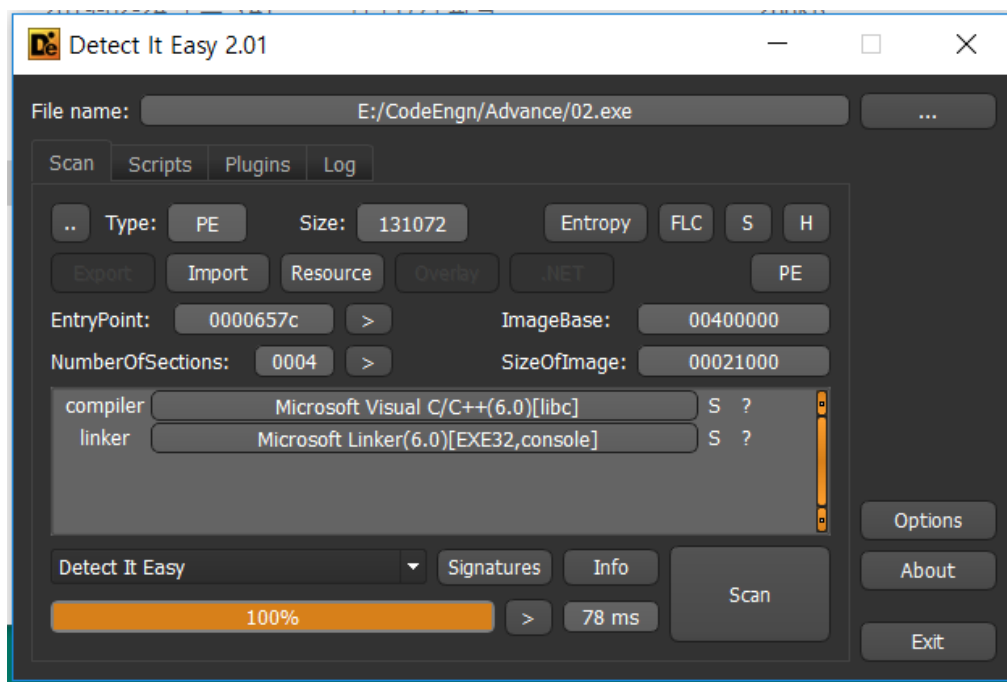
정답은 무엇인가

— Author: Noble

— File Password: codeengn



심플하게 정답은 무엇인가??

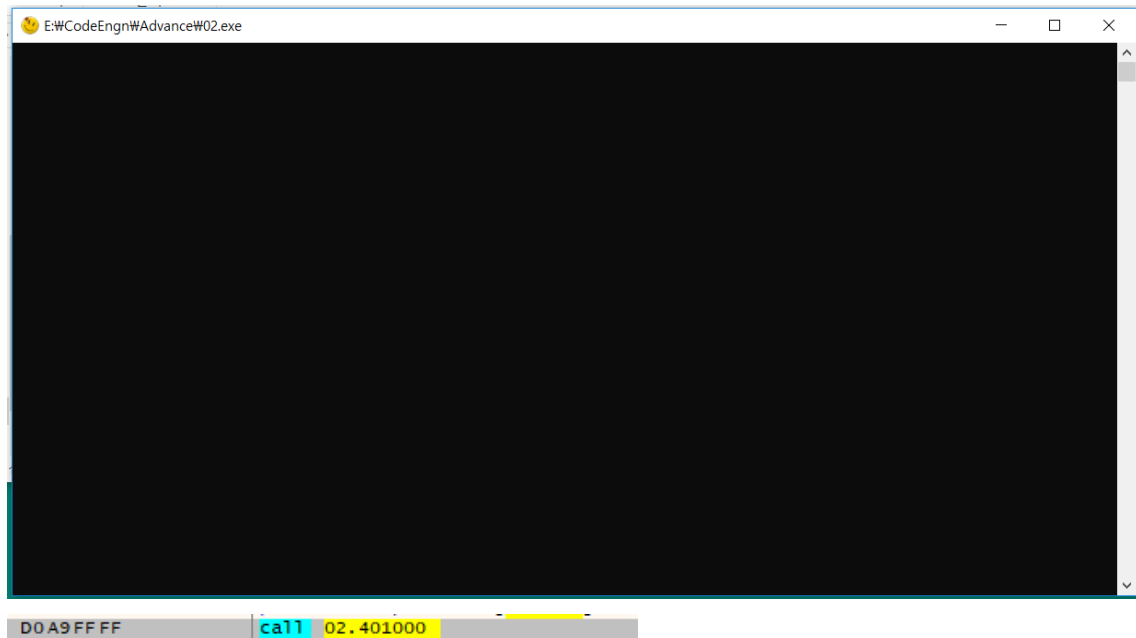


별다른 패킹이 되어있지 않다.

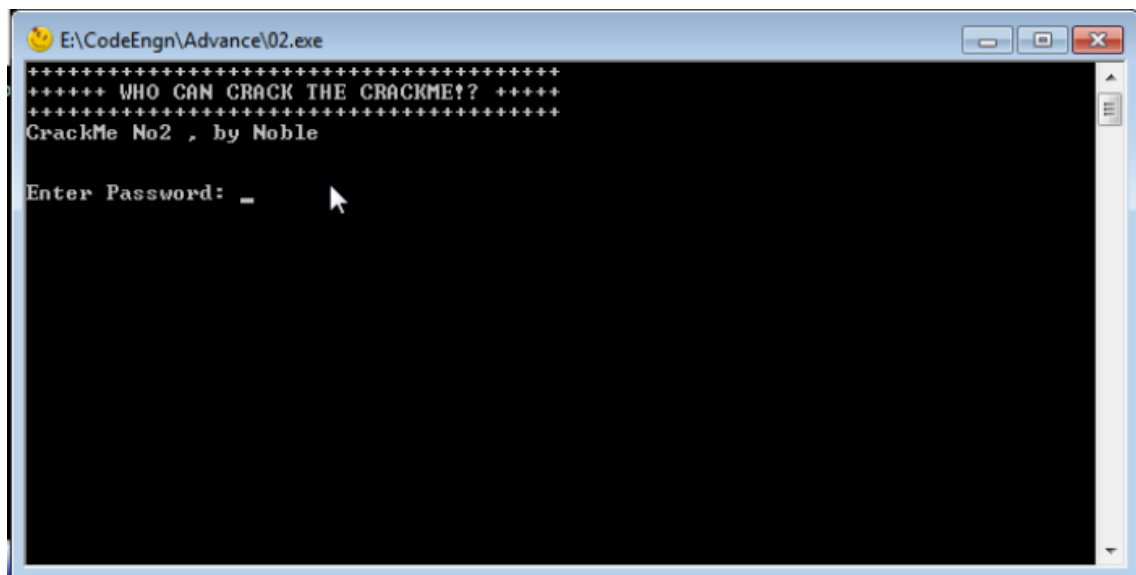
근데 윈도우10 환경에서 실행시켰을 때 아무런 글귀도 나오지 않음...

문자열을 뒤져보니 WHO CAN CRACK THE CRACKME!라는 글귀들을 찾았는데

문자열이 출력되지 않아서 윈도우 10환경에서 계속 트레이싱해보니 어떤 DLL파일을 찾으려고 계속 빙빙돌아 실행이안된다.



가상머신으로 window7환경에서 실행시켜보니 나타나서 윈도우7환경에서 리버싱을 다시 시작했다.



나타난 문자열열 중 Enter Password:가 출력되는 부분에 breakpoint를 설정후에 문자열을 받는 함수를 찾음.

00401285	68 30424100	push 02.414230	414230:"Enter Password: "
0040128A	68 40844100	push 02.418440	
0040128F	AA	stosb	
004012C0	E8 B80A0000	call 02.401D80	
004012C5	808C24 F8030000	lea ecx,dword ptr ss:[esp+3F8]	
004012C6	51	push ecx	
004012C7	68 D0844100	push 02.4184D0	
004012D2	E8 390D0000	call 02.402010	문자열 입력

004012C5	808C24 F8030000	lea ecx,dword ptr ss:[esp+3F8]	
004012C6	51	push ecx	
004012C7	68 D0844100	push 02.4184D0	
004012D2	E8 390D0000	call 02.402010	
004012D3	83C4 10	add esp,10	
004012E0	009424 88070000	lea edx,dword ptr ss:[esp+3F8]	
004012E1	68 D0144000	push 02.401400	
004012E6	68 40144000	push 02.401440	
004012EB	6A 64	push 64	
004012ED	6A 10	push 10	
004012EE	52	push edx	
004012F0	E8 B0460000	call 02.4059A5	
004012F5	C78424 D0000000 00000000	mov dword ptr ss:[esp+000]	
00401300	809C24 8C070000	lea ebx,dword ptr ss:[esp+3F8]	
00401307	C74424 10 64000000	mov dword ptr ss:[esp+10]	
0040130F	808C24 F0030000	lea edi,dword ptr ss:[esp+3F8]	
00401316	83C9 FF	or ecx,FFFFFFFF	
00401319	33C0	xor eax,eax	
0040131B	6A 01	push 1	
0040131D	F2AE	repne scasb	
0040131F	F701	not ecx	
00401321	49	dec ecx	
00401322	8BE9	mov ebp,ecx	
00401324	804B FC	lea ecx,dword ptr ds:[ebp-4]	
00401327	55	push ebp	
00401328	E8 C3060000	call 02.4019F0	
0040132D	84C0	test al,al	
0040132F	74 24	jz 02.401355	
00401331	8B3B	mov edi,dword ptr ds:[ebp]	
00401333	8BD0	mov ecx,edi	

그 후에 call문에 breakpoint들을 걸고 프로세스가 종료되는 call함수를 찾아보니

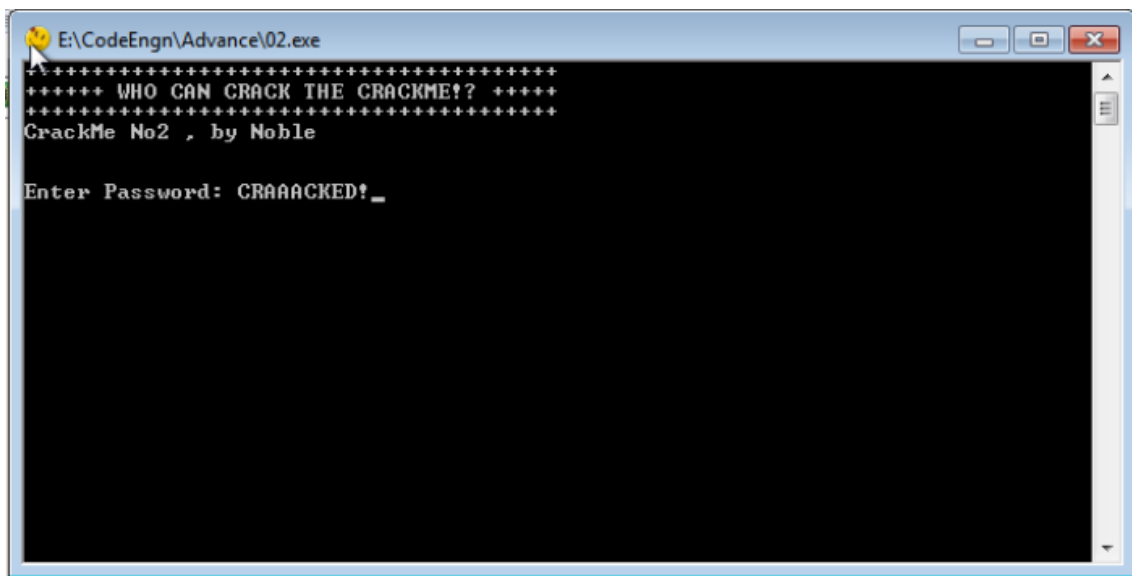
00401363	E8 1F460000	call 02.405987	
00401368	33D2	xor edx,edx	
0040136A	B9 64000000	mov ecx,64	64: 'd'
0040136F	F7F1	div ecx	
00401371	33FF	xor edi,edi	
00401373	8D4C24 14	lea ecx,dword ptr ss:[esp+14]	
00401377	57	push edi	
00401378	C1E2 04	shl edx,4	
0040137B	8DB414 8C070000	lea esi,dword ptr ss:[esp+edx+78C]	
00401382	8A9414 8C070000	mov dl,byte ptr ss:[esp+edx+78C]	
00401389	885424 18	mov byte ptr ss:[esp+18],dl	
0040138D	E8 7E050000	call 02.401910	
00401392	A1 FC104100	mov eax,dword ptr ds:[4110FC]	eax: "abcde"
00401398	8D4C24 14	lea ecx,dword ptr ss:[esp+14]	eax: "abcde"
0040139B	50	push eax	
0040139C	57	push edi	
0040139D	56	push esi	
0040139E	E8 6D030000	call 02.401710	
004013A3	8B4424 18	mov eax,dword ptr ss:[esp+18]	
004013A7	C68424 D00D0000 01	mov byte ptr ss:[esp+DD0],1	
004013AF	3BC7	cmp eax,edi	eax: "abcde"
004013B1	75 05	jnz 02.4013B8	
004013B3	B8 F8104100	mov eax,02.4110F8	eax: "abcde"
004013B8	8D4C24 24	lea ecx,dword ptr ss:[esp+24]	eax: "abcde"
004013BC	50	push eax	
004013BD	51	push ecx	
004013BE	8D9424 EC050000	lea edx,dword ptr ss:[esp+5EC]	
004013C5	FFD2	call edx	
004013C7	83C4 08	add esp,8	
004013CA	E8 07EA0000	call 02.40FDD6	

call edx부분 구문실행시키면 프로세스가 종료된다.

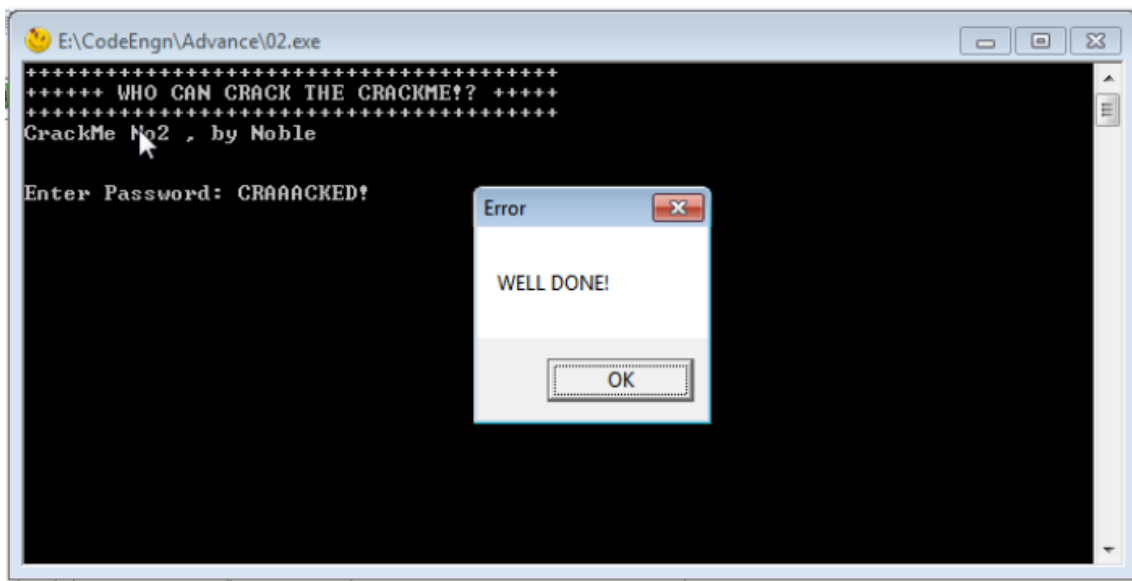
call edx문 안으로 들어가서 명령어들을 보니 문자열 hello를 하나하나 잘라서 비교하는 어셈블리어가 보임

80BD 1CFFFFFF	lea edi,dword ptr ss:[ebp-E4]		
B9 39000000	mov ecx,39	39: '9'	
B8 CCCCCCCC	mov eax,CCCCCCCC	eax: "hell"	
F3:AB	rep stosd		
A1 08604000	mov eax,dword ptr ds:[406008]	eax: "hell"	
33C5	xor eax,ebp		
8945 FC	mov dword ptr ss:[ebp-4],eax		
8B45 0C	mov eax,dword ptr ss:[ebp+C]		
0FB8E08	movsx ecx,byte ptr ds:[eax]	eax: "hell"	
83F9 43	cmp ecx,43	43: 'C'	
0FB8E08	jne 18F88A		
8B45 0C	mov eax,dword ptr ss:[ebp+C]		
0FB8E48 01	movsx ecx,byte ptr ds:[eax+1]	eax+1: "ell"	
83F9 52	cmp ecx,52	52: 'R'	
0FB8E08	jne 18F88A		
8B45 0C	mov eax,dword ptr ss:[ebp+C]		
0FB8E48 02	movsx ecx,byte ptr ds:[eax+2]	eax+2: "ll"	
83F9 41	cmp ecx,41	41: 'A'	
0FB8E08	jne 18F88A		
8B45 0C	mov eax,dword ptr ss:[ebp+C]		
0FB8E48 03	movsx ecx,byte ptr ds:[eax+3]		
83F9 41	cmp ecx,41	41: 'A'	
0FB8E08	jne 18F88A		
8B45 0C	mov eax,dword ptr ss:[ebp+C]		
0FB8E48 04	movsx ecx,byte ptr ds:[eax+4]		
83F9 41	cmp ecx,41	41: 'A'	
0FB8E08	jne 18F88A		
8B45 0C	mov eax,dword ptr ss:[ebp+C]		
0FB8E48 05	movsx ecx,byte ptr ds:[eax+5]		
83F9 43	cmp ecx,43	43: 'C'	
0FB8E08	jne 18F88A		
8B45 0C	mov eax,dword ptr ss:[ebp+C]		
0FB8E48 06	movsx ecx,byte ptr ds:[eax+6]		
83F9 4B	cmp ecx,4B	4B: 'K'	
0FB8E08	jne 18F88A		
8B45 0C	mov eax,dword ptr ss:[ebp+C]		
0FB8E48 07	movsx ecx,byte ptr ds:[eax+7]		
83F9 45	cmp ecx,45	45: 'E'	
0FB8E08	jne 18F88A		
0018F803	8B45 0C	mov eax,dword ptr ss:[ebp+C]	
0018F806	0FB8E48 08	movsx ecx,byte ptr ds:[eax+8]	
0018F80A	83F9 44	cmp ecx,44	44: 'D'
0018F80D	75 7B	jne 18F88A	
0018F80F	8B45 0C	mov eax,dword ptr ss:[ebp+C]	
0018F812	0FB8E48 09	movsx ecx,byte ptr ds:[eax+9]	
0018F816	83F9 21	cmp ecx,21	21: ' '!'
0018F819	75 6F	jne 18F88A	
0018F81B	8B45 0C	mov eax,dword ptr ss:[ebp+C]	
0018F81E	0FB8E48 0A	movsx ecx,byte ptr ds:[eax+A]	
0018F822	85C9	test ecx,ecx	
0018F824	74 13	je 18F839	
0018F826	8BF4	mov esi,esp	
0018F828	6A 01	push 1	
0018F82A	8B45 08	mov eax,dword ptr ss:[ebp+8]	
0018F82D	8B48 08	mov ecx,dword ptr ds:[eax+8]	
0018F830	FFD1	call ecx	

문자열들을 다합치면 CRAAAKED! 라는 문자열을 발견할수 있다.



입력하니 바로 종료되지 않고



WELL DONE!이라는 문자가 들어있는 MessageBox가 나타난다.

Clear