

2019.02.21. CodeEngn Basic 20

Tree to Tree

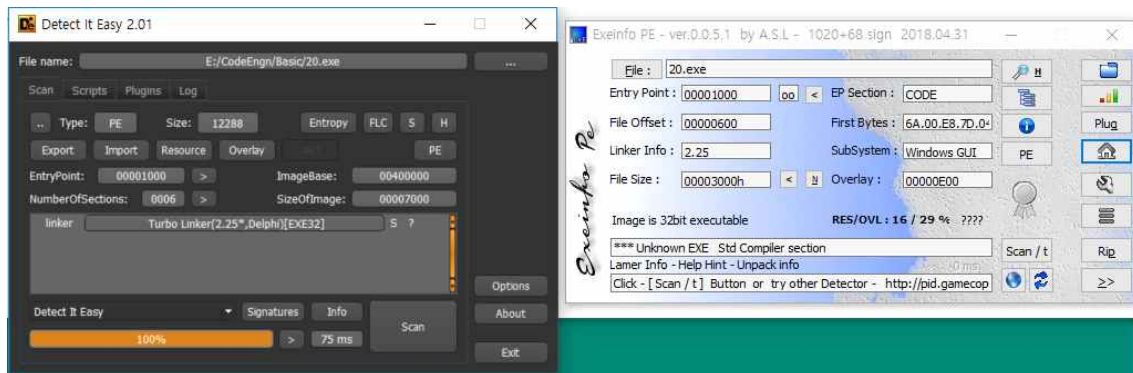
## Basic RCE L20

이 프로그램은 Key파일을 필요로 하는 프로그램이다.  
'Cracked by: CodeEngn!' 문구가 출력 되도록 하려면  
crackme3.key 파일안의 데이터는 무엇이 되어야 하는가  
Ex) 41424344454647  
(정답이 여러개 있는 문제로 인증시 맞지 않다고 나올 경우  
Contact로 연락주시면 확인 해드리겠습니다)

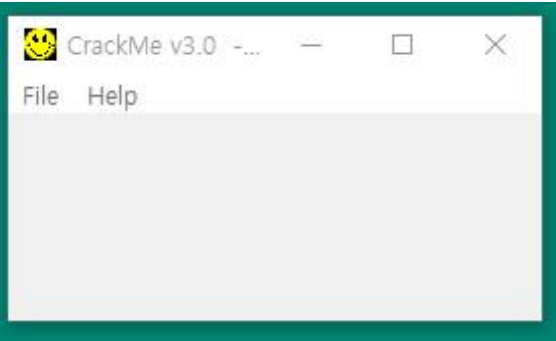
— Author: Cruehead / MiB  
— File Password: codeengn



Basic 마지막 문제 패킹이 되어있지 않음



그냥실행시켰을 때 파일을 열고 그런건 없음 자동실행이라고 예상



우선 문자열을 찾아보고

문자열
"CRACKME3.KEY"
"CrackMe v3.0"
"CrackMe v3.0"
"No need to disasm the code!"
"MENU"
"No need to disasm the code!"
"CrackMe v3.0"
"No need to disasm the code!"
"Now try the next crackme!"
"Cracked by: Now try the next crackme!"
"DLG_ABOUT"
"Good work cracker!"
"Cracked by: Now try the next crackme!"

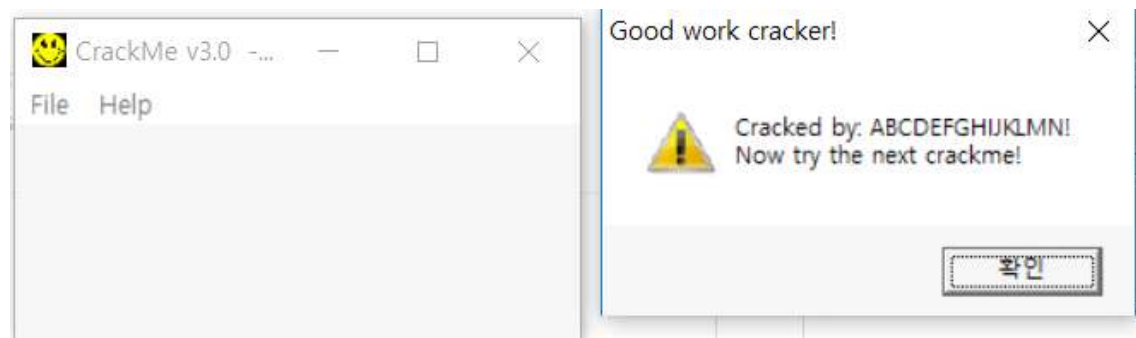
따라가다보니 파일이름은 CRACKME3.KEY

004020C8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 43	.....C
004020D8	52 41 43 4B	4D 45 33 2E	48 45 59 00	00 00 00 00	RACKME3.KEY.....
004020E8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	.....
004020F8	00 00 00 00	00 54 72 79	20 74 6F 20	63 72 61 63	.....Try to crac
00402108	6B 20 6D 65	21 00 43 72	61 63 6B 4D	65 20 76 33	k me!.CrackMe v3
00402118	2E 30 20 20	20 20 20 20	20 20 20 20	20 20 20 00	.0
00402128	4E 6F 20 6E	65 65 64 20	74 6F 20 64	69 73 61 73	No need to disas
00402138	6D 20 74 68	65 20 63 6F	64 65 21 00	4D 45 4E 55	m the code!.MENU
00402148	00 00 00 00	00 44 4C 47	5F 41 42 4F	55 54 00 47	.....DLG_ABOUT.G
00402158	6F 6F 64 20	77 6F 72 6B	20 63 72 61	63 68 65 72	ood work cracker
00402168	21 00 43 72	61 63 68 65	64 20 62 79	3A 20 20 20	!.Cracked by:
00402178	20 20 20 20	20 20 20 20	20 20 20 20	20 20 4E 6F	No
00402188	77 20 74 72	79 20 74 68	65 20 6E 65	78 74 20 63	w try the next c
00402198	72 61 63 6B	6D 65 21 00	00 00 00 00	00 00 00 00	rackme!.....
004021A8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	.....

계속 트레이싱 하다보니 조건문 3개만 넘기면 창을 띄울 수 있다.

문자열 출력 방식을 알기 위해 조건문을 간단한 우회로 넘기고 출력해보니

00401058	FF 35 F5 20 40 00	push dword ptr ds:[4020F5]	
00401061	E8 30 04 00 00	CALL <JMP.<readFile>	
00401066	83 3D A0 21 40 00 12	cmp dword ptr ds:[4021A0],12	
0040106D	74 C8	jle 20.401037	
0040106F	68 08 20 40 00	push 20.402008	402008: "ABCDEFGHIJKLMN"
00401074	E8 98 02 00 00	CALL 20.401311	
00401079	81 35 F9 20 40 00 78 56 34 1	xor dword ptr ds:[4020F9],12345678	
00401083	83 C4 04	add esp,4	
00401086	68 08 20 40 00	push 20.402008	402008: "ABCDEFGHIJKLMN"
00401088	E8 AC 02 00 00	CALL 20.40133C	
00401090	83 C4 04	add esp,4	
00401093	38 05 F9 20 40 00	cmp eax,dword ptr ds:[4020F9]	
00401099	0F 94 C0	sete al	
0040109C	50	push eax	
0040109D	84 C0	test al,al	
0040109F	74 96	jle 20.401037	
004010A1	68 0E 21 40 00	push 20.40210E	40210E: "CrackMe v3.0"
004010A6	E8 98 02 00 00	CALL 20.401346	
004010AB	83 C4 04	add esp,4	



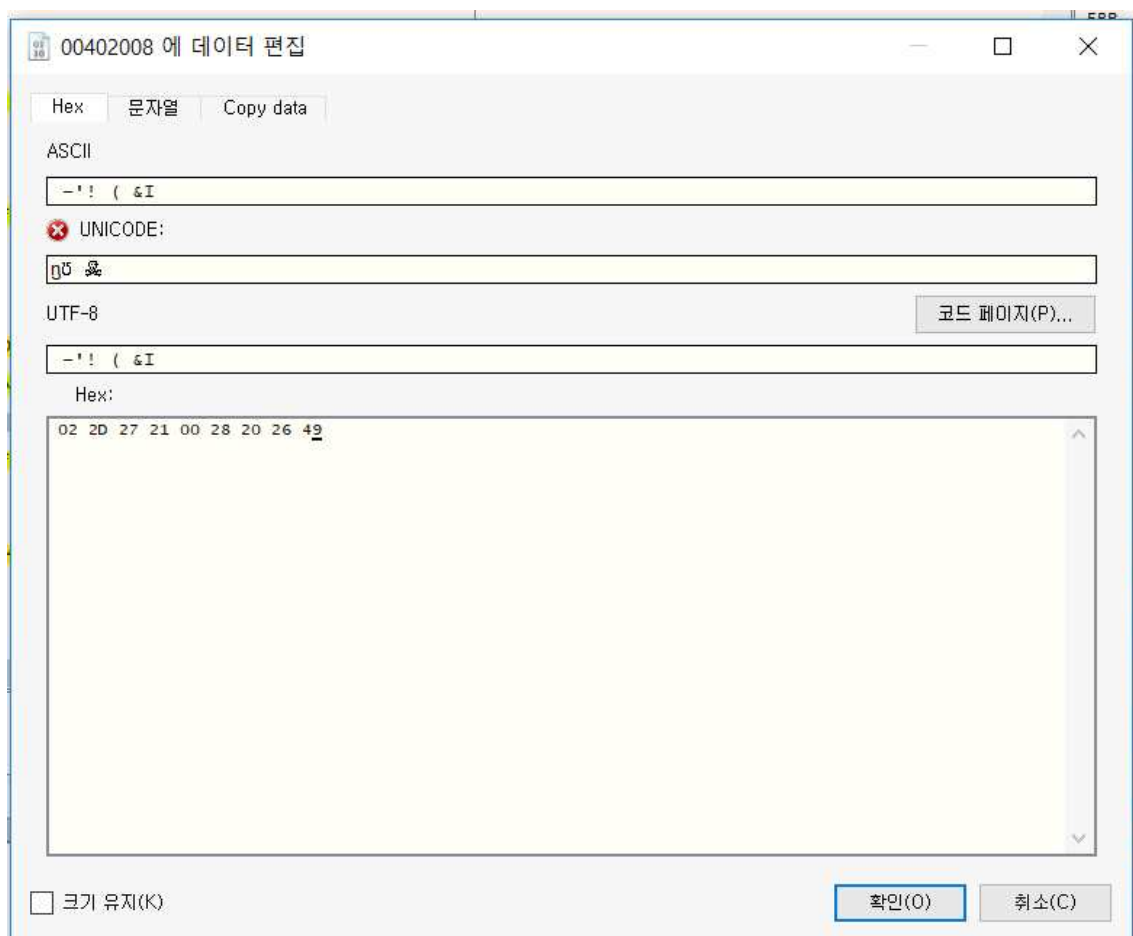
A~M까지 출력된다.

내부로 들어가보자

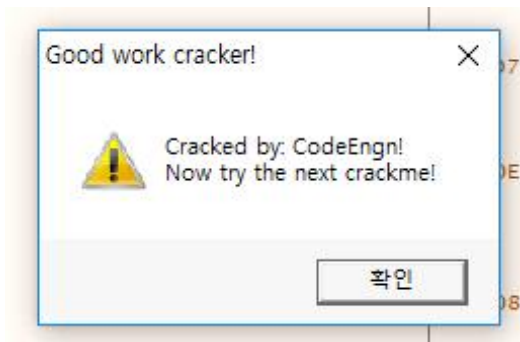
33 C9	xor ecx,ecx	
33 C0	xor eax,eax	
8B 74 24 04	mov esi,dword ptr ss:[esp+4]	
B3 41	mov bl,41	41: 'A'
8A 06	mov al,byte ptr ds:[esi]	
32 C3	xor al,bl	
8B 06	mov byte ptr ds:[esi],al	
46	inc esi	
FEC 3	inc bl	
01 05 F9 20 40 00	add dword ptr ds:[4020F9],eax	
3C 00	cmp al,0	
74 07	jle 20.401335	
FEC 1	inc cl	
80 FB 4F	cmp bl,4F	4F: 'O'
75 E6	jne 20.401318	
89 0D 49 21 40 00	mov dword ptr ds:[402149],ecx	
C3	ret	
8B 74 24 04	mov esi,dword ptr ss:[esp+4]	
83 C6 0E	add esi,E	
8B 06	mov eax,dword ptr ds:[esi]	
C3	ret	
8B 74 24 04	mov esi,dword ptr ss:[esp+4]	
83 C6 0D	add esi,D	
C7 06 20 2D 20 43	mov dword ptr ds:[esi],43202D20	
C7 46 04 72 61 63 6B	mov dword ptr ds:[esi+4],6B636172	
C7 46 08 65 64 21 21	mov dword ptr ds:[esi+8],21216465	
C3	ret	
8B 0D 49 21 40 00	mov ecx,dword ptr ds:[402149]	
8B 74 24 04	mov esi,dword ptr ss:[esp+4]	
8B 7C 24 08	mov edi,dword ptr ss:[esp+8]	
83 C7 0C	add edi,C	edi:EntryPoint
F3 A4	rep movsb	edi:EntryPoint



내부로 들어가서 조건을 보니 null을 만날때까지 문자 xor A++ 그리고 그 문자의 아스키코드를 중첩해서 더한다. 더한 값은 따로 저장



계산해보니022D27210028202649까지하면 딱 CodeEngn이 생성됨



이제 CRACKME3.KEY파일을 만들어서 해보니 조건문에 걸린다.

우선 파일크기가 18byte필요 지금까지 필요한값은 9byte

9byte가 더필요하다.

```

00401066 83 3D A0 21 40 00 12 cmp dword ptr ds:[4021A0],12
0040106D 75 C8 jne 20.401037

E8 98 02 00 00 call 20패치완,401311
81 35 F9 20 40 00 78 56 34 1 xor dword ptr ds:[4020F9],12345678
83 C4 04 add esp,4
68 08 20 40 00 push 20패치완,402008

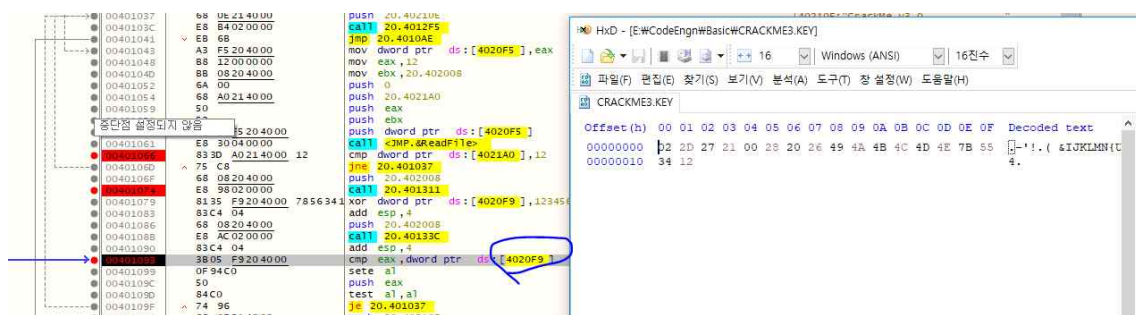
```

또 뒤에 4byte와 4020F9 (문자열을 만들며 hexa 값을 더한 값이 있는주소에 xor 123456788 한 값)를 비교함

```

004020E8 00 00 00 40 00
004020F8 FF 91 55 34 12

```



```

004020F9 7B 55 34 12

```

```

00401187 58 pop eax
00401188 3C 01 cmp al,1
0040118A 75 17 jne 20.4011A3
0040118C 68 86 21 40 00 push 20.402186

```

EAX	12345501
EBX	0040204A
ECX	00000000
EDX	00000000
EBP	0019FF94
ESP	0019FF84
ESI	0040211B
EDI	00401000

마지막에 한번 더 비교해주고 메시지창을 띄워준다.

022D27210028202649 + 잉여5byte + 7B553412

Clear