

Advance RCE L08

Key 값이 5D88-53B4-52A87D27-1D0D-5B09 일때 Name은 무엇인가

힌트 : Name은 두자리인데.. 알파벳일수도 있고 숫자일수도 있고..

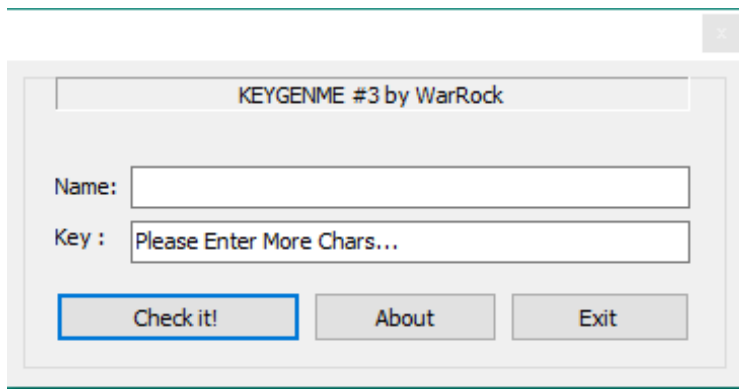
정답인증은 Name의 MD5 해쉬값(대문자)

— Author: WarRock

— File Password: codeengn

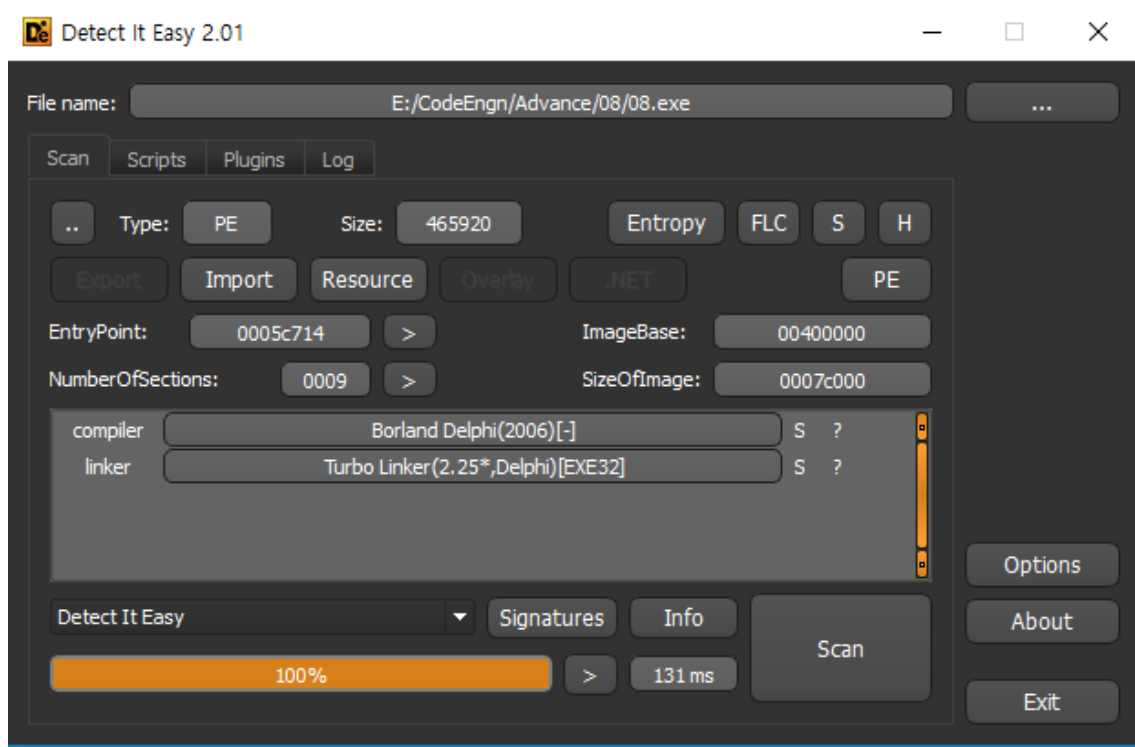


Name을 알아보자



그냥 Check it을 누르니
더많은 문자열을 입력하라고 나온다.

패킹이 따로 되어있지 않다.



Check it 했을 때 나오는 문자열 Please Enter More Chars..로 본문을 찾아냄

0045BB27	7D 15	JG 08.45B83E	
0045BB29	EA 18BC4500	mov edx,08.45BC18	45BC18:"Please Enter More Chars..."
0045BB2E	8B83 74030000	mov eax,dword ptr ds:[ebx+374]	
0045BB34	E8 6BE5FDFF	CALL 08.43A0A4	
0045BB39	E9 91000000	JMP 08.45B8CF	
0045BB3E	8D55 F4	lea edx,dword ptr ss:[ebp-C]	
0045BB41	8B83 68030000	mov eax,dword ptr ds:[ebx+368]	
0045BB47	E8 28E5FDFF	CALL 08.43A074	
0045BB4C	8B45 F4	mov eax,dword ptr ss:[ebp-C]	
0045BB4F	8945 F8	mov dword ptr ss:[ebp-B],eax	
0045BB52	8B45 F8	mov eax,dword ptr ss:[ebp-B]	
0045BB55	85C0	test eax,eax	
0045BB57	74 05	JE 08.45B85E	
0045BB59	83E8 04	sub eax,4	
0045BB5C	8B00	mov eax,dword ptr ds:[eax]	
0045BB5E	83F8 1E	cmp eax,1E	
0045BB61	7E 12	JLE 08.45B875	
0045BB63	BA 3CB84500	mov edx,08.45BC3C	45BC3C:"Please Enter Not More Than 30 Chars..."
0045BB68	8B83 74030000	mov eax,dword ptr ds:[ebx+374]	
0045BB6E	E8 31E5FDFF	CALL 08.43A0A4	
0045BB73	EB 5A	JMP 08.45B8CF	
0045BB75	8D55 F0	lea edx,dword ptr ss:[ebp-10]	
0045BB78	8B83 74030000	mov eax,dword ptr ds:[ebx+374]	
0045BB7E	E8 F1E4FDFF	CALL 08.43A074	
0045BB83	8B45 F0	mov eax,dword ptr ss:[ebp-10]	
0045BB86	50	push eax	
0045BB87	8D55 E8	lea edx,dword ptr ss:[ebp-18]	
0045BB8A	8B83 68030000	mov eax,dword ptr ds:[ebx+368]	
0045BB90	E8 DFE4FDFF	CALL 08.43A074	
0045BB95	8B45 E8	mov eax,dword ptr ss:[ebp-18]	
0045BB98	8D55 EC	lea edx,dword ptr ss:[ebp-14]	
0045BB9B	E8 B0FCFFFF	CALL 08.45B850	
0045BB9E	8B55 EC	mov edx,dword ptr ss:[ebp-14]	
0045BBA0	58	pop eax	
0045BBA3	58	CALL 08.404C3C	
0045BBA4	E8 9390FAFF	JNE 08.45B8C5	
0045BBA9	75 1A	push 40	
0045BBAB	6A 40	mov ecx,08.45BC64	45BC64:"Good Boy!!!"
0045BBAD	B9 64BC4500	mov edx,08.45BC70	45BC70:"Well done!"
0045BBB2	BA 70BC4500	mov eax,dword ptr ds:[45E9C0]	
0045BBB7	A1 C0E94500	mov eax,dword ptr ds:[eax]	
0045BBBC	8B00		
0045BBBE	E8 B5D0FFFF	CALL 08.45BC78	
0045BBC3	EB 0A	JMP 08.45B8CF	

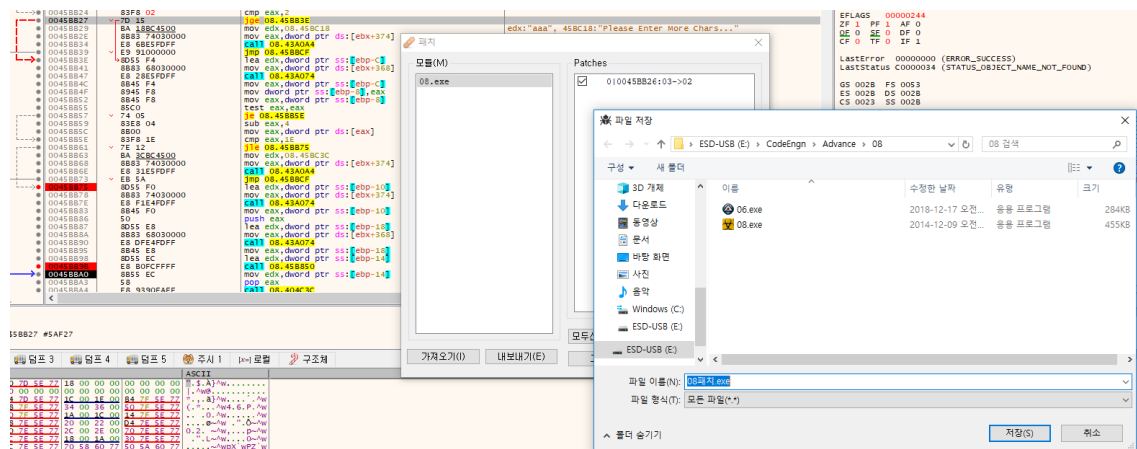
name에 aaa를 준뒤 트레이싱 해보니
비트로 엄청 장난친다.

```
mov ebx,dword ptr ss:[ebp-4]
movzx esi,byte ptr ds:[ebx+ecx-1]
add esi,edx
imul esi,esi,772
mov edx,esi
imul edx,esi
add esi,edx
or esi,esi
imul esi,esi,474
add esi,esi
mov edx,esi
inc ecx
dec eax
jne 08.45B89D
```

우선 위에 어셈블리어를 분석하여 알고리즘으로 만들었다.

1. 첫글짜와 772 곱
2. 곱한거 ^2
3. 1번 + 2번
4. 3번 * 474
5. 4번 *2

Name에 문자의 길이는 최소 3인데 2글자도 받을 수 있도록 패치



aa를 넣어서 시리얼 값을 보고

0045BB8A	8B85 68030000	mov eax,dword ptr ds:[ebx+368]	
0045BB8B	85 DF44DFDF	call 08函数.43A074	
0045BB95	8845 E8	mov eax,dword ptr ss:[ebp-18]	[ebp-18]: "aa"
0045BB98	8D55 EC	lea edx,dword ptr ss:[ebp-14]	[ebp-14]: "7A69-7DD8-4898F8F2-1846-8F71"
0045BB99	E8 B0FCFFFF	call 08函数.458B50	
0045BBA0	8845 EC	mov edx,dword ptr ss:[ebp-14]	[ebp-14]: "7A69-7DD8-4898F8F2-1846-8F71"
0045BBA3	58	pop eax	
0045BBA4	85 9390FAFF	call 08函数.404C3C	
0045BBA9	75 1A	jnz 08函数.45B8C5	
0045BBAB	6A 40	push 40	
0045BBAD	B9 64BC4500	mov ecx,08函数.45BC64	45BC64: "Good Boy!!!"
0045BBB2	B4 70BC4500	mov edx,08函数.45BC70	edx: "aa", 45BC70: "we'll done!"
0045BBB3	74 00	jne 08函数.45B8C0	

아까만든 프로그램에서 aa를 넣었을 때 나오는 값을보니
0x7a692df0 으로
상위 16비트가 key 값으로 오는 것을 알 수 있었다.

```
2266 a X : 164c6680
2267 a Y : 4210e170
2268 a Z : 493a5fa0
2269 a a : 7a692df0
2270 a b : 5cbac620
2271 a c : 1a716190
2272 a d : b38d0040
2273 a e : 280da230
2274 a f : 77f34760
2275 a g : a33defd0
2276 a h : a9ed9b80
2277 a i : 8c024a70
2278 a j : 497bfca0
2279 a k : e25ab210
2280 a l : 569e6ac0
2281 a m : a64726b0
2282 a n : d154e5e0
2283 a o : d7c7a850
2284 a p : b99f6e00
2285 a q : 76dc36f0
2286 a r : f7e0320
2287 a s : 8384d290
2288 a t : d2f0a540
2289 a u : fdc17b30
2290 a v : 3f75460
2291 a w : e59230d0
2292 a x : a2921080
2293 a y : 3af6f370
2294 a z : aec0d9a0
```

결국 key값 앞부분 5d88을 이용하여 이름을 찾으면 됨 아까 만든 코드를 수정하여
5d88 저장

```

1 #include<stdio.h>
2
3 int main(){
4     unsigned int c[62],edx,esi,temp=0;
5     int i,j;
6     edx=esi=0;
7     for(i=0;i<10;i++) c[i]=i+48;
8     for(i=0;i<26;i++) {
9         c[i+10]=i+65;
10        c[i+36]=i+97;
11    }
12    for(i=0;i<62;i++){
13        edx=0;
14        esi=c[i];
15        esi+=edx;
16        esi*=0x772;
17        edx=esi;
18        edx*=esi;
19        esi+=edx;
20        esi*=0x474;
21        esi+=esi;
22        edx=esi;
23        temp=edx;
24        for(j=0;j<62;j++){
25            edx=temp;
26            esi=c[j];
27            esi+=edx;
28            esi*=0x772;
29            edx=esi;
30            edx*=esi;
31            esi+=edx;
32            esi*=0x474;
33            esi+=esi;
34            edx=esi;
35            if((esi>>16)==0x5d88)printf("%c %c : %.x\n",c[i], c[j],esi>>16);
36        }
37    }
38    }

```

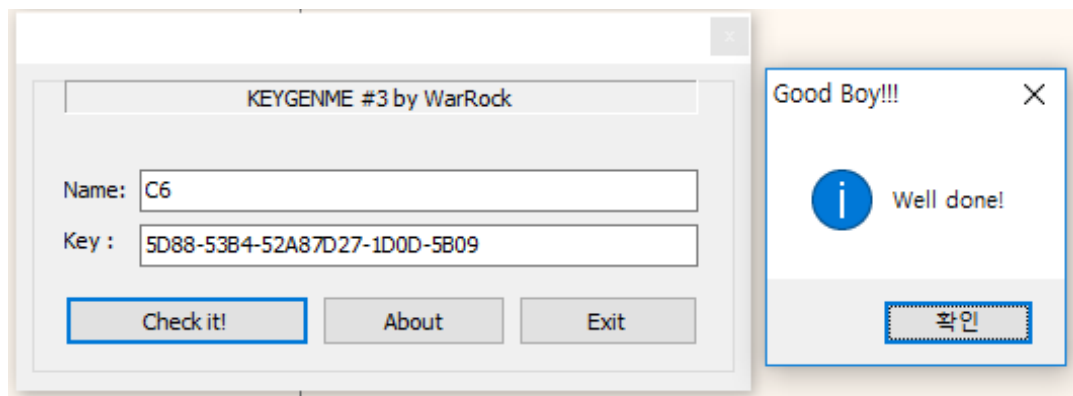
"advance8.c" 38L, 556C

```

[kwl3434@linux ~]$ gcc advance8.c
[kwl3434@linux ~]$ ./a.out
C 6 : 5d88

```

C6이라고 나옴



해시화만 하면

<http://www.convertstring.com/ko/Hash/MD5>

여기 MD5 해시하고자하는 텍스트를 붙여 넣습니다

C6



MD5 해시를 생성!

당신의 MD5 메시지 여기에서 소화 복사합니다.

7E8B9F5CAB4A8FE24FAD9FE4B7452702

7E8B9F5CAB4A8FE24FAD9FE4B7452702

Clear