

CodeEngn Basic RCE L14

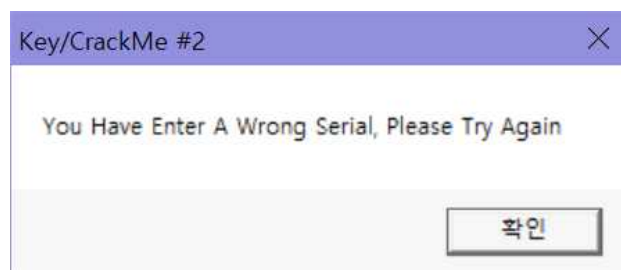
: Name이 CodeEngn 일때 Serial을 구하시오

(이 문제는 정답이 여러개 나올 수 있는 문제이며 5개의 숫자로 되어있는 정답을 찾아야함, bruteforce 필요)

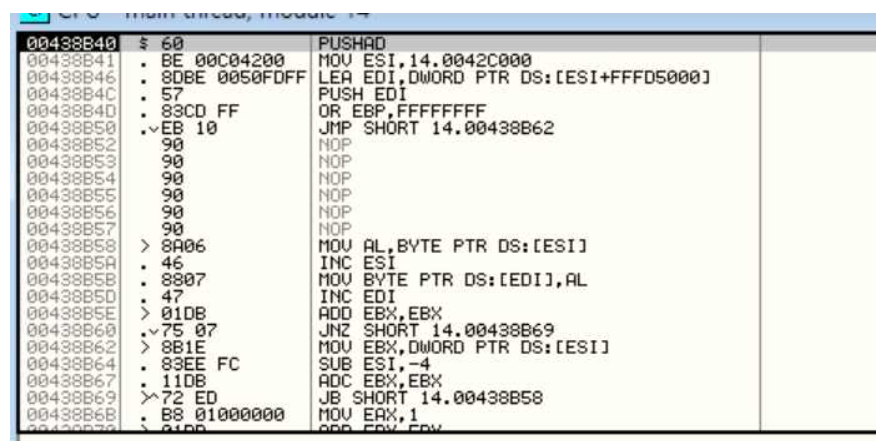
Ex) 11111



exe 파일 실행 시 위와 같은 실행창이 뜨고, 아무거나(df) 누르고 CHECK를 눌렀더니



이런 경고창이 뜬다. serial을 찾아야 하니 올리디버거로 열어주었다.



PUSHAD 가 떴다! pushad가 뜨면 popad를 찾아주어야 한다.

00438C70	. 89F9	MOV ECX,EDI	
00438C72	. 57	PUSH EDI	
00438C73	. 48	DEC EAX	
00438C74	. F2:AE	REPNE SCAS BYTE PTR ES:[EDI]	
00438C76	. 55	PUSH EBP	
00438C77	. FF96 4C940300	CALL DWORD PTR DS:[ESI+3944C]	
00438C7D	. 09C0	OR EAX,EAX	
00438C7F	. 74 07	JE SHORT 14.00438C88	
00438C81	. 8903	MOV DWORD PTR DS:[EBX],EAX	
00438C83	. 83C3 04	ADD EBX,4	
00438C86	. ^EB E1	JMP SHORT 14.00438C69	
00438C88	> FF96 50940300	CALL DWORD PTR DS:[ESI+39450]	
00438C8E	> 61	POPAD	
00438C8F	. -E9 6C83FCFF	JMP 14.00401000	
00438C94	00	DB 00	
00438C95	00	DB 00	
00438C96	00	DB 00	
00438C97	00	DB 00	
00438C98	00	DB 00	
00438C99	00	DB 00	
00438C9A	00	DB 00	
00438C9B	00	DB 00	
00438C9C	00	DB 00	
00438C9D	00	DB 00	

popad 밑에 jmp 한 줄 밖에 없기 때문에 00401000이 OEP이고, 엔터를 눌러서 해당 주소로 이동한다.

0040132A	40	INC EAX	
0040132B	49	DEC ECX	
0040132C	75 DB	JNZ SHORT 14.00401309	
0040132E	56	PUSH ESI	
0040132F	68 38314000	PUSH 14.00403138	ASCII "123123"
00401334	E8 4A000000	CALL 14.00401383	
00401339	5E	POP ESI	
0040133A	3BC6	CMP EAX,ESI	
0040133C	75 15	JNZ SHORT 14.00401353	
0040133E	6A 00	PUSH 0	
00401340	68 62344000	PUSH 14.00403462	ASCII "Key/CrackMe #2 "
00401345	68 B8344000	PUSH 14.004034B8	ASCII " Good Job, I Wish You the Very Best"
0040134A	6A 00	PUSH 0	
0040134C	E8 90000000	CALL 14.004013EE	JMP to USER32.MessageBoxA
00401351	EB 13	JMP SHORT 14.00401366	
00401353	6A 00	PUSH 0	
00401355	68 62344000	PUSH 14.00403462	ASCII "Key/CrackMe #2 "
0040135A	68 86344000	PUSH 14.00403486	ASCII " You Have Enter A Wrong Serial, Please Try Ag
0040135F	6A 00	PUSH 0	
00401361	E8 88000000	CALL 14.004013EE	JMP to USER32.MessageBoxA
00401366	EB 15	JMP SHORT 14.0040137D	
00401368	FF75 14	PUSH DWORD PTR SS:[EBP+14]	
0040136B	FF75 10	PUSH DWORD PTR SS:[EBP+10]	
0040136D	FF75 0C	PUSH DWORD PTR SS:[EBP+0C]	

어셈블리어를 더 쉽게 살펴보기 위해서 실행 후 11111과 123123을 입력하였고, 올리디버거에 123123라는 부분이 에러/성공메세지 전에 띄워지는 것을 볼 수 있다. 즉 시리얼 넘버는 실행 화면에 아랫줄이라는 것을 알 수 있었다.

이제 시리얼 넘버를 찾아야 하니 wrong seial 문구가 뜨는 지점을 기준으로 앞 뒤로 분석해보자 !

```
0040133A    CMP EAX,ESI
0040133C    JNZ 00401353
```

이 부분을 해석해보면 EAX - ESI의 값이 0이 아니라면 00401353으로 이동해서 "YOU HAVE ENTER A WRONG SERIAL"이라는 에러메세지를 출력하도록 하고 있다. 그러면 JNZ 에서 점프를 하지 않아야 "GOOD JOB. ~~~" 이라는 성공메세지를 출력할 수 있다. 즉 EAX - ESI = 0 이 되어야 하고, EAX와 ESI의 값이 같아야 한다.

```
Registers (MMX)
EAX 0001E0F3
ECX 00000000
EDX 00403139 ASCII "23123"
EBX 00000018
ESP 0019F998
EBP 0019F998
ESI 00002E68
EDI 00000111
EIP 0040133A 14.0040133A
C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 0 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 220000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000206 (NO,NB,NE,A,NS,PE,GE,G)
MM0 0000 0000 0000 0000
MM1 0000 0000 0000 0000
MM2 0000 0000 0000 0000
MM3 0000 0000 0000 0000
MM4 8000 0000 0000 0000
MM5 8000 0000 0000 0000
```

레지스터 값에 각각 어떤것이 들어가는지 알아보기 위해서 CMP명령어에 F2를 눌러 BP를 걸고 실행시켰다. 우선 EAX에 들어가있는 값을 10진수로 변환 시켰더니 123123이 나온다. 즉 EAX와 ESI 중에서 EAX의 값이 사용자가 입력하는 시리얼 넘버라는 것을 알 수 있고, ESI가 진짜 시리얼 넘버라는 것을 알 수 있다.

ESI를 10진수로 변환시키면 11880이고, 이를 다시 대입해 보겠다.



성공메세지가 뜬다.

근데 문제에서 이름이 CodeEngn일 때, 시리얼 넘버를 구하라고 했으므로 똑같은 방법으로 시리얼 넘버를 구하면 76193이 나오므로, 답은 76193이다 !