Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | CodeEngn Reverse2 L07(HMX0101) |
| 파일명 | HMX0101.exe |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2016/02/12 ~ 2017/02/19 |
| 문제 내용 | Name이 CodeEngn일때 Serial은 28BF522F-A5BE61D1-XXXXXXXX 이다.  XXXXXXXX 를 구하시오 |

문제 풀이:

문제 파일을 실행 시 창 하나가 뜨게됩니다.



위의 이름이 CodeEngn일때 serial 값을 찾는 것이 목적입니다.



Ollydbg로 실행하려 하면 에러 메세지와 함께 실행이 되지 않습니다.



packing은 되어있지 않고 C#으로 작성되었으므로 ollydbg 대신 .net reflector 등의 .net decompiler 로 디컴파일을 해봅니다.



디컴파일을 하면 form1에서 버튼 클릭시 이벤트 메소드가 보이는데 정답 처리를 하는 메세지 창을 띄우는 것이 보입니다. 즉, flag 여부를 검사하는 vxzzz 메소드의 결과를 먼저 확인해야 할것입니다. 여기서 vxzzz에 저희가 입력한 text2(serial값)를 uint로 변형한 num3가 인자로 들어가므로 여기서 xxxxx 값이 정해질 것입니다.



vxzzz 메소드의 내용입니다. 맨 앞에선 4개의 인자를 가공하고 while문을 돌면서 숫자 배열을 만들어 저장합니다. 이제 xxxxx값을 찾는 방법은 xxxxx의 길이를 알고 있으므로 brute force로 하나하나 대입하며 찾는것과 이 vxzzz 메소드의 루틴을 역으로 디코드하여 찾는 방법이 있을 것입니다.