Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | CodeEngn Reverse2 L02(Noble 02) |
| 파일명 | Noble 02.exe |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2016/02/06 ~ 2017/02/12 |
| 문제 내용 | \* 비밀번호를 알아내시오. |

문제 풀이:

문제 파일을 실행 시 창 하나가 뜨게됩니다.



비밀번호를 입력하는 창이 보이고 입력 값이 틀릴시 바로 종료됩니다.

프로그램은 별다른 packing 없이 C++로 작성된 것으로 보입니다.



Ollydbg로 실행 후 진행하다보면 주소 40662B에서 메소드 호출을 하고 멈추므로 이 안에서 입력을 받는 것 같으니 내부로 진입하면 위의 화면에서 break를 건 곳에서 입력을 받게 됩니다. 입력을 하고 더 진행해봅니다.



진행을 하다보면 입력한 값의 문자를 하나마다 검사하는 루프문이 있는데 기능을 확인하기 어려우므로 분기점을 찾는 것을 우선으로 합니다.

진행을 하다보면 CALL EDX에서 넘어가는 순간 종료가 됨으로 저 내부에서 처리를 할 것입니다.



내부에 들어가보면 EAX 주소의 처음부터 11번째 값까지 ECX에 대입후 각 특정 값과 대조하는 루틴이 보이고 그 후, 분기점이 보이므로 이 루틴이 정답을 처리하는 과정인 것 같은데 EAX에는 처음에 입력한 비밀번호가 저장되어 있으므로 각 ASCII 코드에 맞는 값만 찾아 쓰면 답이 될 것 입니다. 그 값은

CRAAACKED! 입니다.