Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | CodeEngn Reverse2 L02(Vallani 04) |
| 파일명 | Vallani 04.exe |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2016/02/06 ~ 2017/02/12 |
| 문제 내용 | \* Name 이 CodeEngn일때 serial 값을 구하시오. |

문제 풀이:

문제 파일을 실행 시 창 하나가 뜨게됩니다.



이름과 serial 값을 입력하는 창이 뜨고 Check 버튼을 누를시 정답 체크를 하게 됩니다.

프로그램은 MASM32라는 다소 생소한 언어(SDK)로 작성되었습니다. packing은 달리 되어 있지 않은것 같습니다.



Ollydbg로 실행 후 referenced string으로 정답 처리 문구로 이동하면 쉽게 분기점을 찾을 수 있는데다 break를 걸고 실행하면 비교값을 알기 쉬운데 serial값과 name이 변형된 값을 비교하므로 string1에 입력된 값을 serial로 입력하면 될 것입니다. 한가지 특이한 점은 StrcmpA의 결과를 CDQ, IDIV EAX로 처리하는데 정답의 경우 EAX에 0이 저장되어 debugger로 진행시 오류가 나게 되는데 그냥 프로그램을 실행하고 테스트하면 잘 작동됩니다. 어떤 방식으로 이 루틴이 정답 처리를 해주는지는 확인해봐야할것 같습니다.



정답을 확인한 모습입니다.