Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | ReWrit's Crackme 05 |
| 파일명 | Revrit 05.exe |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2016/01/30 ~ 2017/02/05 |
| 문제 내용 | \* Name과 serial의 조합에서 name이 CodeEngn일 때의 serial값을 구하라. |

문제 풀이:

문제 파일을 실행 시 창 하나가 뜨게됩니다.



이름을 입력하는 창이 뜨고 입력하면 password칸이 뜨고 입력하면 정답 여부를 검사합니다. 이번 문제는 별다른 packing은 되어 있지 않고 Dev-C++ 언어로 프로그래밍 되어있습니다.



ollydbg로 파일을 실행한 후 진행한 결과입니다. 이름을 입력하는 구간에서 멈춘 상태입니다.



더 진행해서 name과 password를 입력하고 진행한 상황입니다. name에는 CodeEngn을 password에는 11111을 입력했습니다.

주소 4015A2에서 EAX와 EBP - 3C의 값이 다르면 40163C로 jump하므로 저 위치가 정답 체크를 하는 것임을 유추할 수 있습니다.



주소 4015A2에서 비교되는 값입니다. EAX의 2B67은 입력한 password 11111의 16진수 값이므로 password의 16진수 값이 E4C60D97과 같아야함을 알 수있습니다. 이 값의 10진수는 3838184855입니다.



정답을 확인 받은 화면입니다.