Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | xCryptokGnme #1 |
| 파일명 | xCryptokGnme 01.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.



name과 serial을 입력해 정답 여부를 판단하는 화면입니다.

packing은 따로 되어있지 않습니다.



ollydbg로 실행한 화면입니다. 시작부터 끝의 루틴이 매우 짧고 딱히 정답 체크 및 확인 문자열 들이 보이지 않습니다.



referenced string 검색을 해보니 정답 여부를 출력하는 문자열이 보입니다. 저곳으로 이동합니다.



이동하니 정답 처리 루틴이 보입니다. 분기는 4011F6 주에 있고 string1,2를 비교해 같으면 정답으로 넘어갑니다.



name에 CodeEngn을 입력하고 serial에 11111을 입력한 후 break를 걸고 실행한 모습입니다. name의 값이 특정 루틴에 의해 숫자 문자열로 변경되었음을 확인할 수 있습니다. serial값은 변형되지 않았으므로 숫자 문자열 06162370056B6AC0이 알맞은 serial 값일 것입니다.



정답을 확인한 모습입니다.