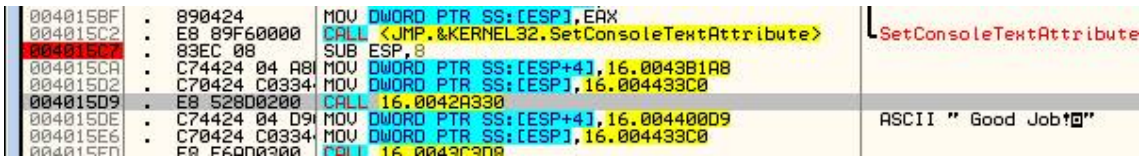
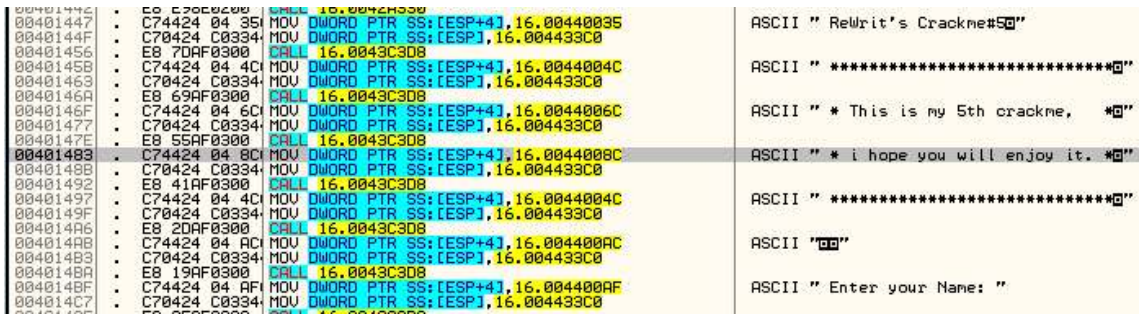
codeengn Basic RCE L16

search reference text string



good job 앞에 있는 이 함수인거 같아서 bp 설정해봤으나, 걸리지 않음. 실패.



CALL 0043C3D8은 print 인 듯하다.

내려가다 보니 0x004015A2에서 JNZ가 있고, 성공과 실패 구문이 나뉜다.

CMP에서 무엇과 무엇을 비교하는지를 중점적으로 살펴보자.
이것저것을 계속 대입해본 결과, EAX에는 내가 패스워드로 입력한 숫자가 들어감을 알 수 있었다. 반면, DWORD PTR [EBP-3C]는 항상 고정된 값이 들어가는 것을 확인하였다.

참고로 여기에는 패스워드로 '12345678'을 입력하였고, 이를 16진수로 표현한 값이 'BC614E'이다. 따라서 ebp-3c의 값을 10진수로 변환해서 패스워드로 넣어주면 정답이다.
정답은 3838184855!