코드엔진 Basic RCE L06

문제

CodeEngn.com [코드엔진]

코드엔진은 국내 리버스엔지니어링 정보공유를 위해 2007년 부터 리버스엔지니어링 컨퍼런스 및 세미나, 워크숍을 현업 실무자들과 함께 운영하고 있는 비영리 커뮤니티입니다.

https://ch.codeengn.com/

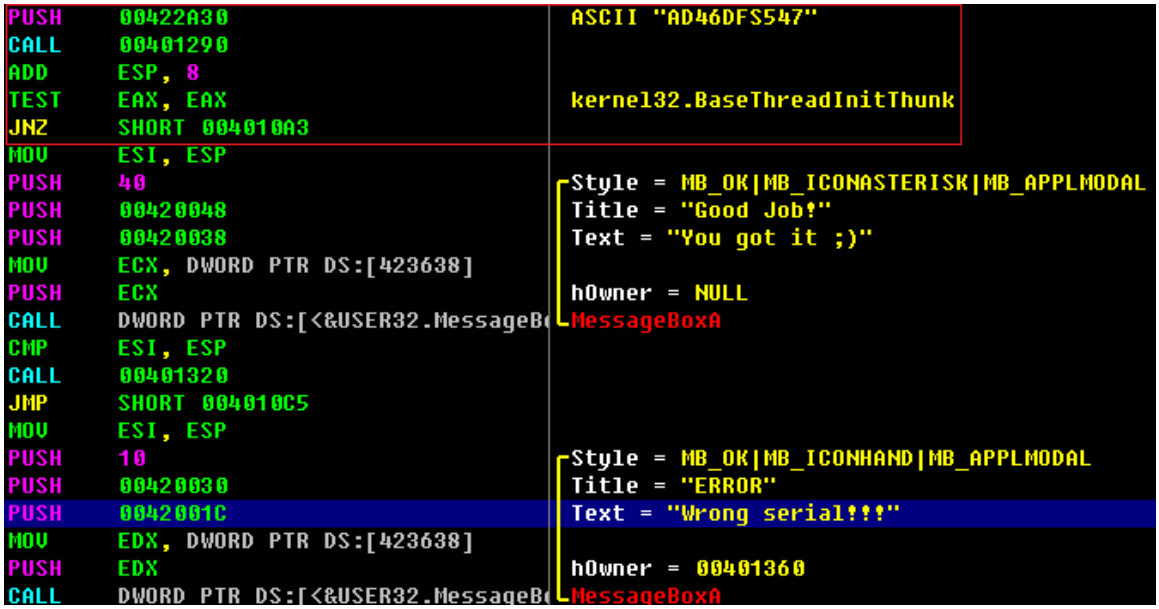
의 Basic RCE L06

해결 과정

- upx로 패킹된 실행코드는 ollyDbg에서 PUSHAD - 압축해제 코드 실행 - POPAD - JUMP OEP 의 형식으로 코드가 나타난다는 것을 검색을 통해 파악
- 실제 ollyDbg에 올려 코드가 이와 같은 형식으로 나타나는 것을 확인하고 OEP의 값을 파악

빨간 선 상자안에 있는 코드가 OEP(Original Entry Point로 점프하는 부분)로 점프하는 부분

- 다음으로, 실행파일을 upx프로그램을 통해 언패킹하여 ollyDbg를 통해 분석
- 시리얼이 맞거나 틀릴 때 나오는 문자열을 검색기능을 통해 찾아 그 문자열들 바로 위에 있을 비교 코드와 비교를 위해 있는 문자열을 파악하여 해결



빨간 선 상자안에 있는 것이 입력 문자열을 확인해 정답인지 아닌지에 따라 점프하는 코드