REPORT:

코드엔진 Basic

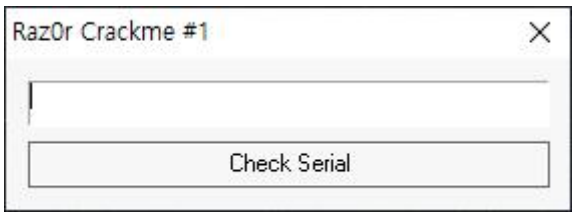
RCE 06 Writeup

COLONY
1824275 정상지

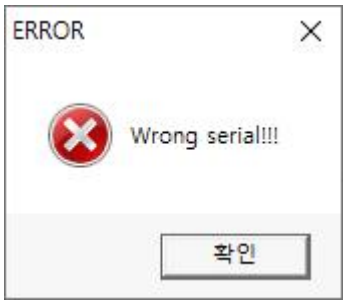
2021.05.23

Unpack을 한 후 Serial을 찾으시오. 정답인증은 OEP + Serial
Ex) 00400000PASSWORD

0. 프로그램 실행

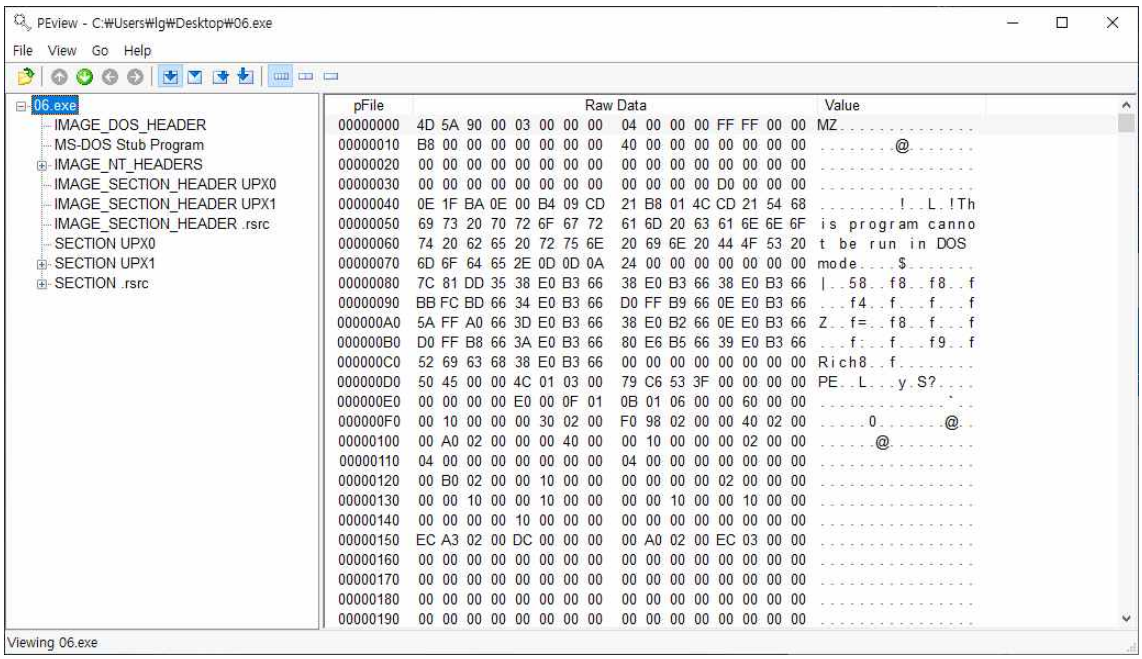


시리얼을 입력하는 창과 시리얼을 체크하는 버튼이 있다



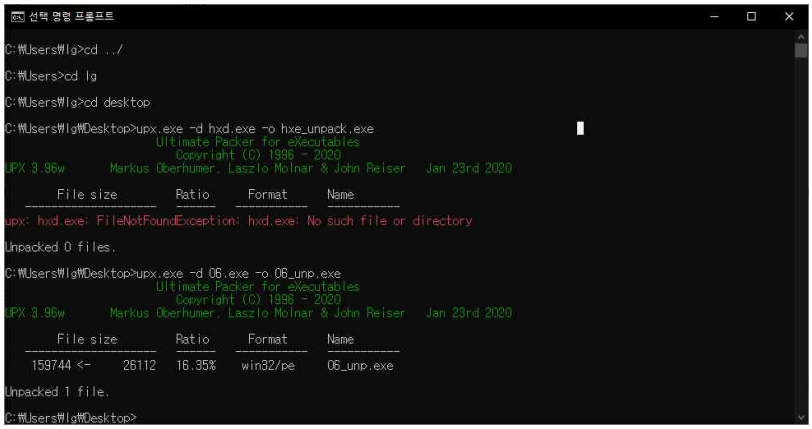
아무 시리얼 값을 넣고 체크했을 때의 에러 출력 문구

1. PE view로 해당 파일 분석

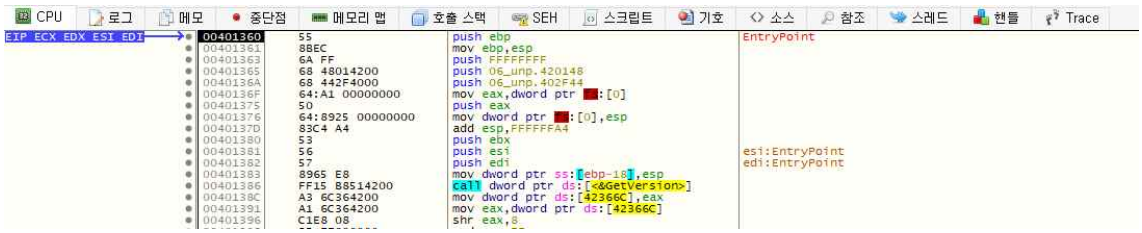


UPX로 패킹되어 있는 모습을 볼 수 있다

2. UPX를 통해 언패킹



3. 언패킹한 파일을 x32dbg로 디버깅

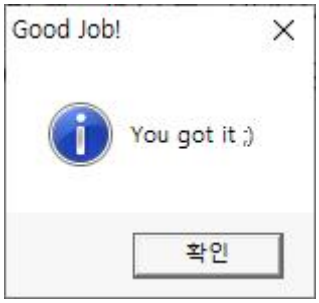


Original Entry Point(OEP)는 00401360으로 확인할 수 있다

문자열 참조를 통해 해당 프로그램이 출력하는 메시지 박스의 문자열을 따라 main문 유추

위의 jne 분기점을 통해 나누어지는 것을 확인 할 수 있다.

문자열 중 AD46DFS547을 시리얼 키 값으로 의심하고 입력했을 때 아래와 같이 성공문구가 나오게 된다.



따라서 정답은 처음 엔트리 포인트인 **00401360 + AD46DFS547**이다