CodeEngn Challenges Basic RCE Level4 풀이

Reverse L04 Start

Author : CodeEngn / Lee Kang-Seok

Korea :

이 프로그램은 디버거 프로그램을 탐지하는 기능을 갖고 있다. 디버거를 탐지하는 함수의 이름은 무엇인가

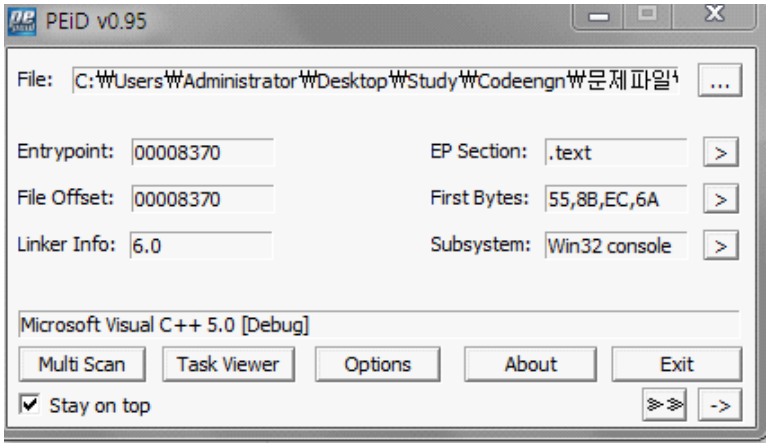
English :

This program can detect debuggers. Find out the name of the debugger detecting function the program uses.

Down

프로그램을 실행해보았다.


정상
정정상상
정정정상상상
정정정정상상상상
정정정정정상상상상상
정정정정정정상상상상상상
정정정정정정정상상상상상상상
정정정정정정정정상상상상상상상상
정정정정정정정정정상상상상상상상상
정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정상상상상상상상상
정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정정상상상상상상상상
정정정상상상상상상상상
정정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정상상상상상상상상
정정상상상상상상상상
정정정정정정정정정정정정정정정정정정정



C,C++로 만들어진 프로그램 같다.

그럼 디버거로 분석을 해보자.

디버거로 attach시킨 후 실행을 해보니

다음과 같이 디버깅 당함 이라고 뜬다.

아마 디버거로 열어보면 디버거를 감지해서 디버깅 당함을 출력해주는것 같다.

안티 디버깅 함수는 찾기가 쉽다.

이 프로그램에 쓰여진 함수를 Search for -> All intermodular calls를 이용해 찾아보면

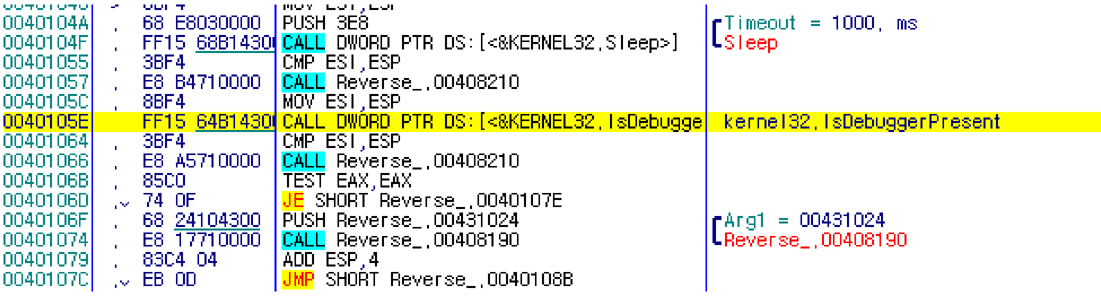
상단에 IsDebuggerPresent 라는 함수가 쓰여진것을 볼수가있었다.

IsDebuggerPresent는 안티디버깅을 하는함수로 잘 알려져있다.

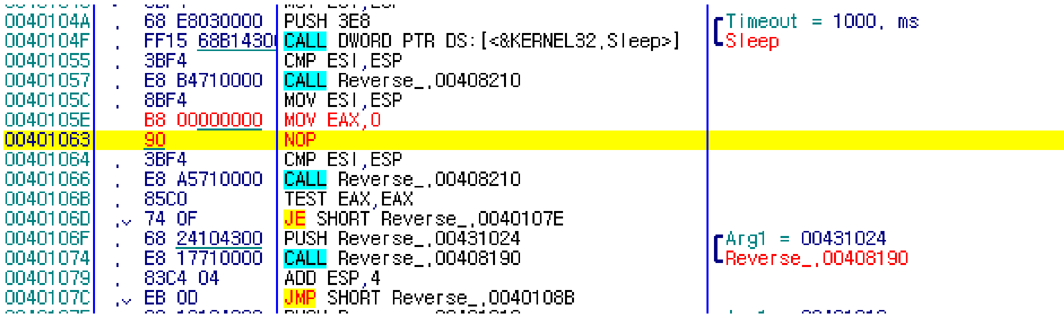
함수를 찾는것만 하지말고 안티디버깅을 우회해 디버깅을 하는중에도 디버깅감지를 못하게 해보겠다.

이 함수는 디버깅을 당하면 1, 아니면 0을 리턴하고 EAX에 저장한다.

이를이용해



0040105E의 어셈을



다음과 같이 바꿔준다.

그리고 크랙한 프로그램을 저장하여 다시 디버거에 attach한 상태에서 실행을 해보면,

다음과 같이 정상으로 뜬다 ! :D

그럼 이제 디버거를 감지해주는 함수가 무엇인지 알 수가 있을것이다.