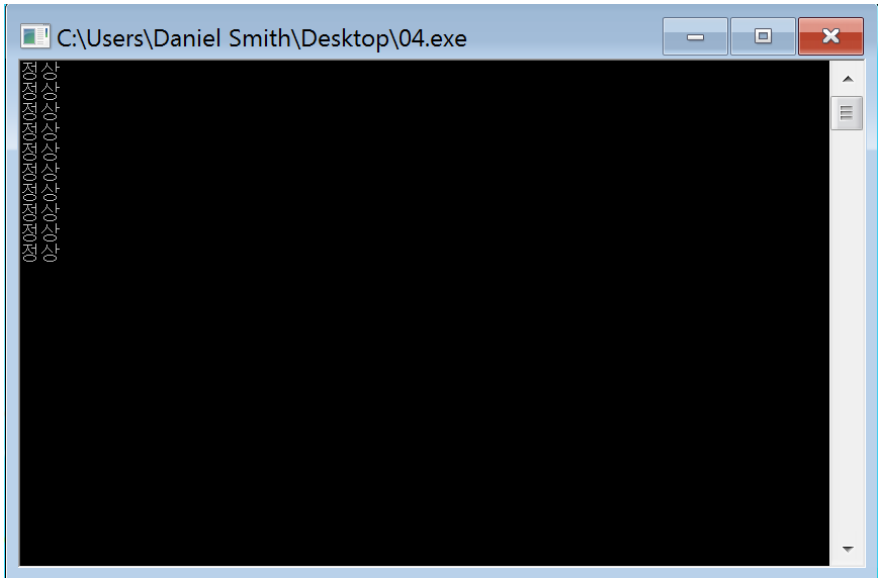
CodeEngn Basic RCE L04 Writeup

Daniel Smith
Feb 18 · 3 min read

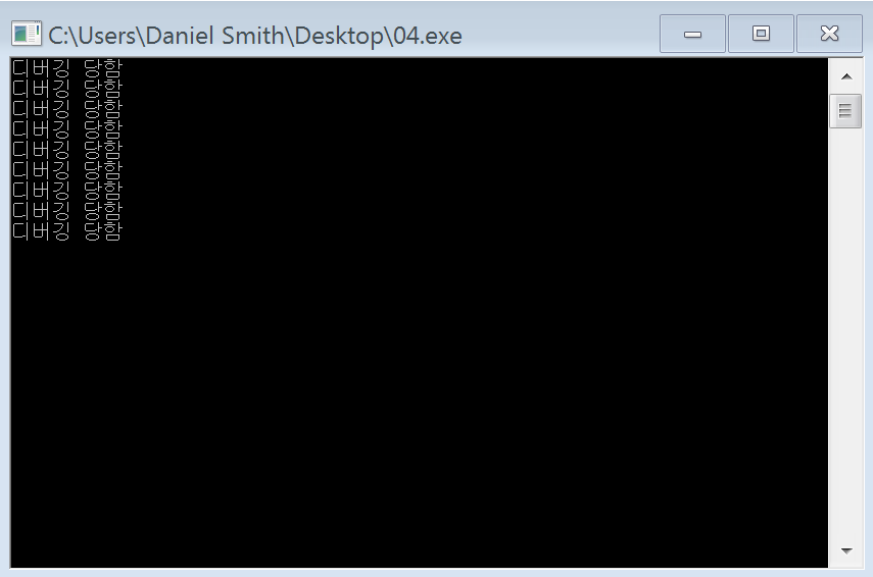
Let's start RCE

```
Filename: 04.exe
Description: 이 프로그램은 디버거 프로그램을 탐지하는 기능을 갖고 있다. 디
버거를 탐지하는 함수의 이름은 무엇인가
Author: CodeEngn
```

Run

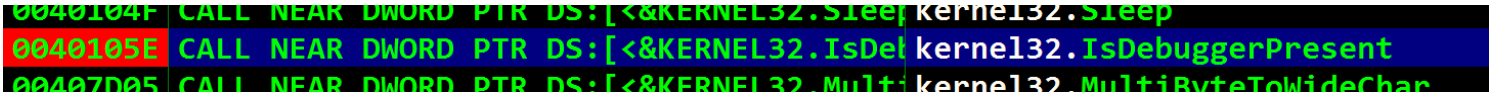


Normal



If got debugged

Analysis



프로그램상에서 호출하는 API 들을 살펴보았을 때, 디버거를 탐지 하는 함수는 IsDebuggerPresent 이라는 것을 알 수 있다.

분석하기 전에, MSDN에서 IsDebuggerPresent 함수의 반환 값을 알아보자.

IsDebuggerPresent function

Determines whether the calling process is being debugged by a user-mode debugger.

Syntax

C++

```
BOOL WINAPI IsDebuggerPresent(void);
```

Parameters

This function has no parameters.

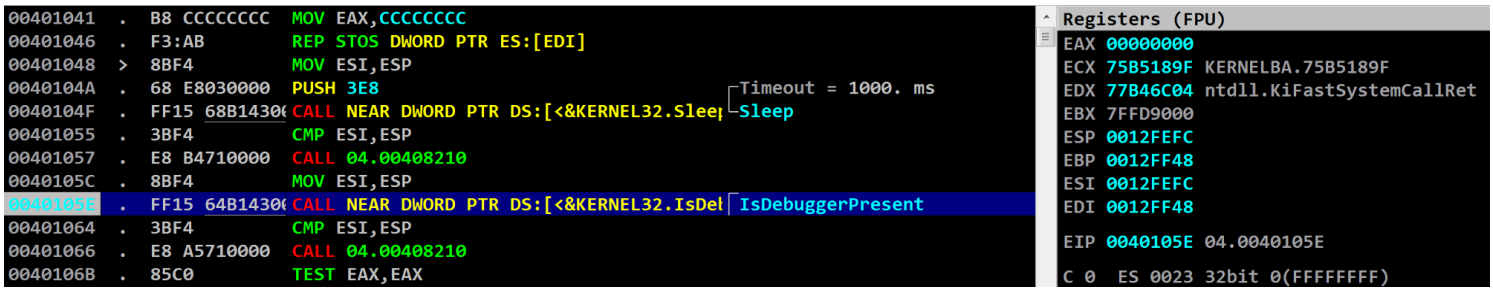
Return value

If the current process is running in the context of a debugger, the return value is nonzero.

If the current process is not running in the context of a debugger, the return value is zero.

MSDN

IsDebuggerPresent 함수는 해당 프로세스가 디버거에서 실행되고 있을 때는 0 이 아닌 값을 반환하고,
그렇지 않을 경우에는 0 을 반환한다



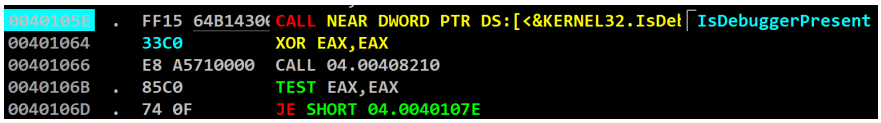
IsDebuggerPresent 호출 이후 레지스터들의 변화를 관찰하기 위해 해당 함수에 BP 를 걸었다

0x0040106D 까지 실행 해본 결과, 예상대로 반환값은 1이 되었고, test(AND 연산 수행) 명령으로 인해 ZF 가 unset 되었고 결과적으로 현재 JE 명령에서 점프를 안할 것이다

디버깅을 당했을때 “디버깅 당함” 을 출력하므로, 0x0040106D 에서 점프하는곳(0x0040107E)이 “정상” 문자열을 출력 하는 구간일것이다

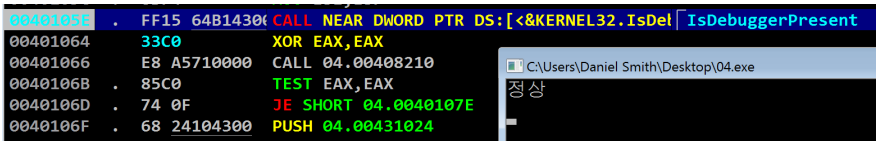
즉, **EAX 를 0으로 바꾸거나, test 명령에서 0 과 0 을 비교**한다면 ZF 가 unset 되지 않아 “정상" 문자열을 출력하는 곳으로 점프하게 될것이다

EAX 를 0으로 바꿔보자



Patched

IsDebuggerPresent 호출 이후 아래 CMP 명령에서 레지스터의 변화가 없어서 CMP 명령을 XOR EAX, EAX 로 패치하였다



이제 디버거에서 실행시켜도 “디버깅 당함” 이 아닌 “정상” 이란 문자열을 출력한다