리버싱 이 정도는 알아야지

Chapter 05. 실전 분석 | 기초 다지기

http://securityfactory.tistory.com

목 차

Chapter 05

실전 분석 | 기초 다지기

SECURITY FACTORY

1. 도전 과제

실전 분석 시간입니다. Challenge 02.exe가 “PrintMe”를 출력하게 만들어보세요. 총 2개의 문제가 있고, 이걸 해결하고 나면 “PrintMe” 문자열이 출력됩니다. 항상 말하지만 문제를 해결하지 못하더라도 직접 시도해보고, 다양한 가능성을 고민해보기 바랍니다.

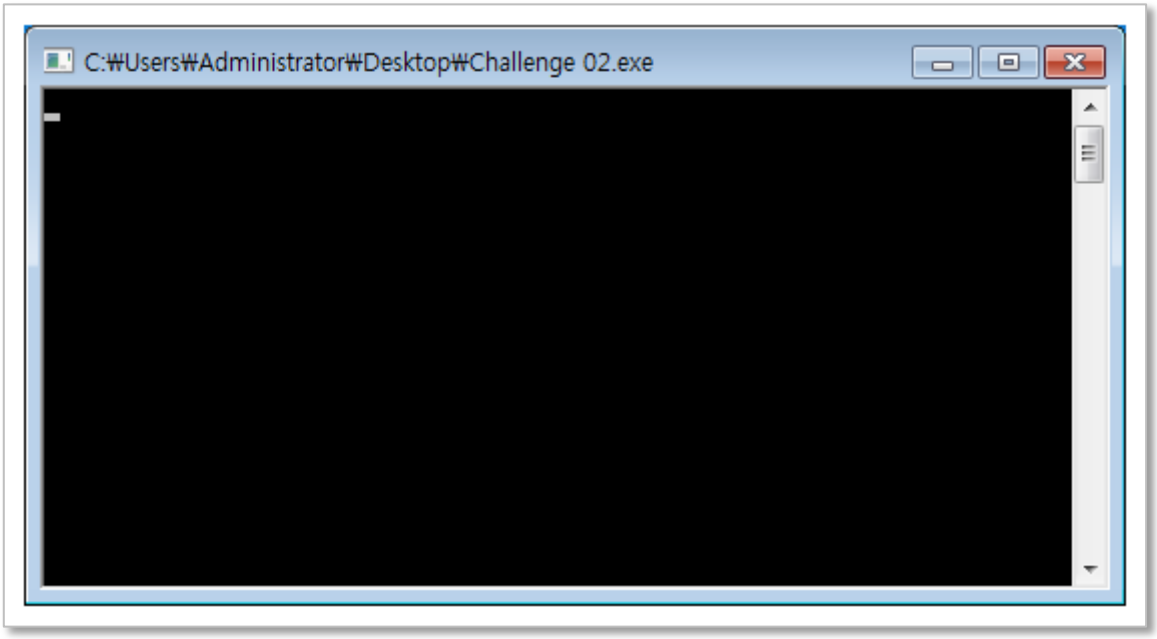

그림 1-1 실행화면_ 문제 해결 전

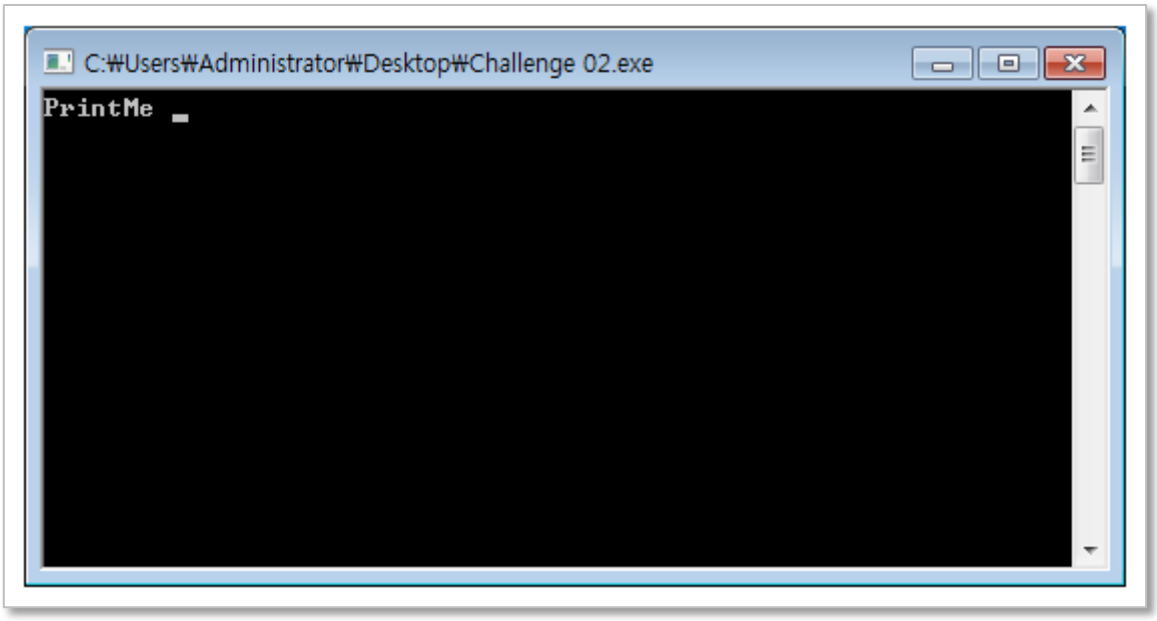

그림 1-2 실행화면_ 문제 해결 후

2. 첫 번째 문제확인 및 해결

다음은 LoadLibraryA( ) API의 MSDN 정보입니다.

LoadLibraryA function

Loads the specified module into the address space of the calling process. The specified module may cause other modules to be loaded.

For additional load options, use the LoadLibraryEx function.

Syntax

```
HMODULE LoadLibraryA(
        LPCSTR lpLibFileName
);
```

Return Value

If the function succeeds, the return value is a handle to the module.

If the function fails, the return value is NULL. To get extended error information, call GetLastError.

※ Note

블로그: http://bitly.kr/udWs
페이스북: http://bitly.kr/OrHQ

3. 두 번째 문제확인 및 해결

※ Note

4. 전체흐름 확인하기

※ Note

리버싱 이 정도는 알아야지

발행일 | 2018 년 11 월
발행자 | SecurityFactory
페북 주소 | http://bitly.kr/OrHQ
이메일 | itseeyou@naver.com


SECURITY FACTORY
http://securityfactory.tistory.com