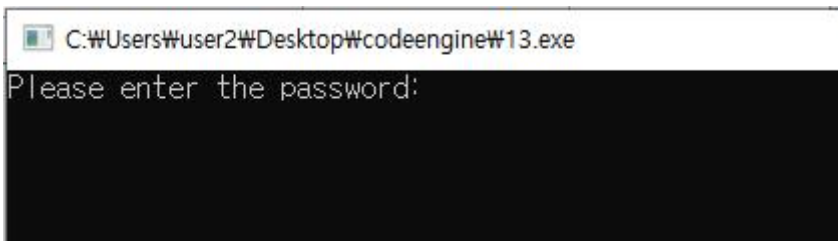
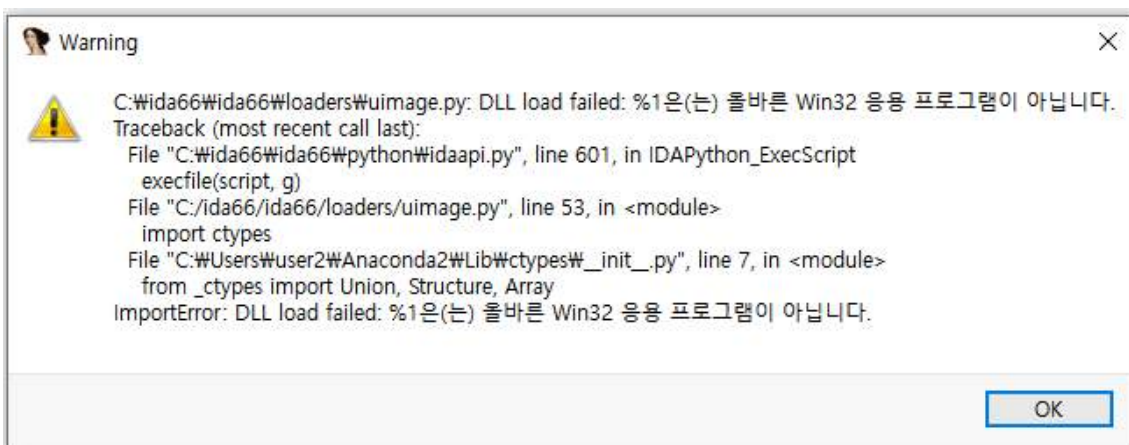


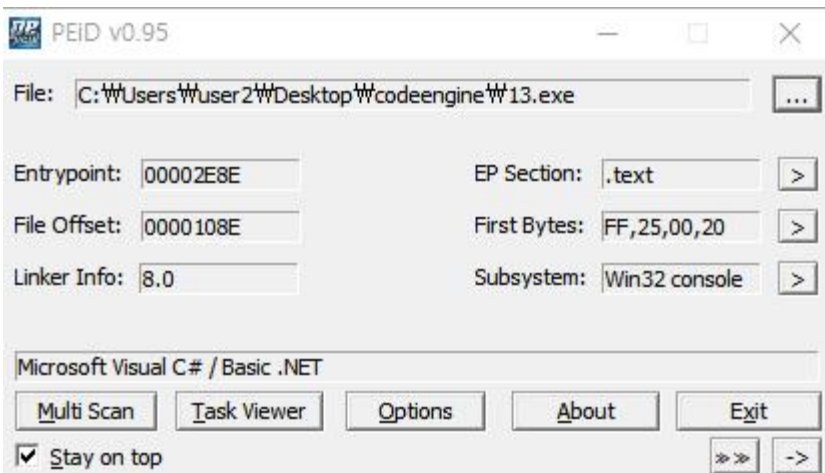
Basic RCE L13
정답은 무엇인가



시작하면 위와 같은 화면밖에 안 뜨고, 올리디버거로 13.exe를 열면 실패한다. (이유 모름) 아이다 역시 실패한다. 올바른 PE구조가 아닌가? 해서 파일구조를 살펴본다. (물론 정상 실행은 되기 때문에 이상함.) 아이다로 여는 것 역시 실패한다.



그 이유를 PEID를 보면 알 수 있다.



이유는 이 프로그램이 visual c# 혹은 .net 로 제작되었기 때문이다. C#코드를 빌드하면 MSIL이라는 중간코드가 만들어지고, 이 코드는 프로그램 실행 시에 JIT Compiler에 의해 컴파일 되어 Native 코드(운영체제가 바로 실행할 수 있는 코드)로 변환되는 것이다. 이러한 IL(Intermediate Language) 방식의 가장 큰 장점은 실행 머신이나 환경(32/64 bit 등등)에 관계없이 동일한 코드를 실행할 수 있다는 것이다.

어떤 운영체제에서도 같은 컴파일러로 중간언어를 만들기 때문에 운영체제에 독립적입니다. 어떤 상황에서도 같은 의미를 가진 소스코드를 작성할 수 있습니다. 운영체제에 맞는 중간언어를 기계어로 변경하는 프로그램(JVM, .NET Framework 등)이 필요합니다. 즉, 플랫폼의 제약이 없습니다.

이러한 장점이 있으나, 디버깅하기에는 곤란하다는 단점이 있다. 중간 언어(IL)로 만들어진 코드는 인터프리터에 의해 Native 코드로 변환되고, 즉 Assembly어를 거치지 않는다는 특징을 가진다.

- 3 ▲ C# is a bad language to compare source code with assembly, because your source code doesn't get compiled to assembly (*). Instead, the source is translated to some intermediate code; running the program means starting an interpreter which takes over and interprets that intermediate code. So the only thing you can trace is that interpreter itself, not the code it's interpreting. (Even if you find a tool that allows you to single-step compiled .net code, it won't be x86 assembly you're single-stepping).

따라서 JetBrains사에서 만든 dotPeek이라는 툴을 이용하자. 이 툴을 이용하면, 13.exe의 원래 코드를 바로 볼 수 있다!!!!!!

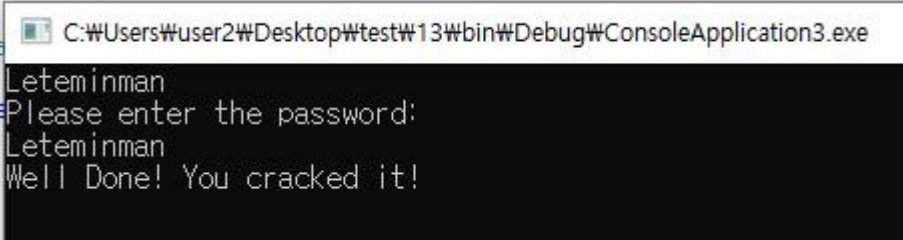


뭔가 엄청난 툴이다.

```
string str = RijndaelSimple.Decrypt(cipherText, passPhrase, saltValue, hashAlg
Console.WriteLine(str); 추가
while (true)
{
    Console.WriteLine("Please enter the password: ");
    if (!(Console.ReadLine() == str))
        Console.WriteLine("Bad Luck! Try again!");
    else
```

다음은 가장 핵심 부분이다. Console.ReadLine()== str 이 되면 else 이하로 넘어가면서 성공 코드가 나오게 된다. str은 Decrypt라는 함수를 거쳐 나오는 것인데, 이를 분석하는 것은 거의 불가능하다. 따라서 그냥 str를 출력하도록 코드에 한 줄을 삽입해주자.

실행!

A screenshot of a Windows command prompt window. The title bar shows the file path: C:\Users\user2\Desktop\test\13\bin\Debug\ConsoleApplication3.exe. The command prompt displays the following text:

```
Leteminman  
Please enter the password:  
Leteminman  
Well Done! You cracked it!
```

실행과 동시에 패스워드가 나온다. while 루틴 전에 출력코드를 넣었기 때문이다.
그대로 패스워드를 입력하니 문제를 해결하였다!