Introduction to Cracking - (Part I)

Introduction

Now as this is the first part, I would start with something very basic. Let's start with decompiling -- the process of extracting the source code from the compiled exe. Yes, you heard it right, **source from exe** ! Let me clear it first that exact decompilation is not possible for many programming languages like C++, VB 6.0 etc.. But there are a few that can be quite satisfactorily decompiled to source-code e.g. Java, .NET (VB, C#, J#, VC++, Delphi.NET), Flash (decompilation from swf to fla) etc...

In this article, I will only talk about decompiling .NET programs (if I get good response then I will continue other decompilation techniques in next parts).

Tools

For decompiling .NET apps, the only tool you need is **.NET Reflector**. It's an excellent decompiler by Red Gate and best of all, it's available for **FREE**. You can just google for .NET Reflector by Red Gate and the first result is what you need. You can grab a free copy with some plug-ins which I think are necessary. So, here is a summary of what you need :

Application

1. .NET Reflector by Red Gate
2. The app you want to decompile (let's call it XYZ.exe)

Plugins :

1. Snippy
2. Code Search
3. Reflexil
4. Deblector
5. SilverlightLoader (if you want to decompile Silverlight)

Setup ...

Now, after downloading Reflector, you've to set it up (won't take long).

1. Extract the zip file to any directory you like.
2. Now extract the plugins to the sub-folder "Plugins".
3. Open Reflector.exe and goto View -> Add-Ins.
4. Click "Add..." and navigate to plugins directory.
5. CodeSearch and Snippy come with only 1 dll, so you can add them right away .
6. But Reflexil and some others come with multiple dll files. You will have to add the correct dll. For ease, generally they are named in the format "<plugin-name>.dll" or "Reflector.<plugin-name>.dll. E.g. Reflexil's plugin is "Reflexil.dll" and Snippy's is "Reflector.Snippy.dll". So add such files. Adding wrong dlls would result in an error, but Reflector won't crash.

After adding plugins to Reflector, it's ready for you to decompile any .NET app .

Decompilation

Before you start decompiling apps, take a look at the small list box below the menu-bar. You can choose the language into which Reflector will decompile the exe. .NET apps built with any .NET language can be decompiled into any other .NET language.

Now, File -> Open -> <select your exe>. Reflector will decompile it for you !
You get the almost EXACT source-code of the app. Decompilation by Reflector is so exact that sometimes, you can directly copy the code from Reflector and re-build the app !

Possible Uses

1. You have lost the source-code of your c00L .NET app and badly want it back !
2. You want to crack the serial for a software built with .NET. When you get the source, you know how the software expects the serial to be, so you can easily crack it. (Details will be in next part ..)

3. Check if your code obfuscation is good enough to protect it from target users. (I will talk in details about obfuscation in next parts...)

Limitations

Several obfuscation schemes can protect .NET apps from being easily decompiled

(but they can't make make it totally un-decompilable). I will talk about cracking some obfuscations in next parts ...

Source: http://www.go4expert.com/articles/introduction-cracking-part-i-t17368/