Lab Demo : Reverse Engineering a .NET binary

Learning Objectives

- Reverse engineering is trying to convert binary into source code or assembly

- Using dnSpy

- Static Analysis: Analysing code without executing them

- Dynamic Analysis: Running code, setting breakpoints and stepping through, inspecting data, behavior analysis

- dnSpy can do both

Lab Instructions:

- Download PS_DotNet_Lab1.zip from resource section

- Password to unzip is: crackinglessons.com

- Analyze it:
  - and try defeat any anti-analysis mechanism,
  - defeat any obfuscations,
  - find the flag, which is an email address.

Skills

- Using dnSpy as debugger to overcome obfuscation
- Modifying data and memory to alter program behavior
- Letting the program de-obfuscate, or decode or decrypt those obfuscated parts, saving us the trouble to understand how the obfuscation works.

Thank you