



x86 Software Reverse-Engineering, Cracking, and Counter-Measures

Lab: Cracking LaFarge

Environment Needed:

- Windows Virtual Machine
- Cheat Engine

1. In this folder you will find a crackme.exe (don't run it yet).
2. This is a popular crackme called LaFarge.
 1. Crackmes are software cracking challenge programs. LaFarge was made specifically for people to try and crack it.
 2. **WARNING:** LaFarge crackme.exe plays loud music, make sure the VM is muted.
3. Run crackme.exe:



4. LaFarge wants a username and registration code.

Task 1:

- Use CheatEngine to crack the software to *bypass* the key check (you do not need to find a valid key, just circumvent the key check).

Task 2:

- Use CodeFusion to develop a patch for others to run to bypass the key check.

Task 3 (Bonus):

- Discover a valid key (registration code) for the crackme.

Hints:



x86 Software Reverse-Engineering, Cracking, and Counter-Measures

- Reverse Engineering is all about quickly finding the code of interest. What predictable things happen when you have the *wrong* registration code? How can you use that to isolate the code of interest? Think back to the cracking with Immunity lab