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

Lab: Anti-Debugging

Environment Needed:

- Windows Virtual Machine
- IDA
- 010 Editor

This lab illustrates the use and circumvention of code guards to protect programs from modification.

PART I - Pong

1. Using IDA for reverse engineering and 010 for patching, remove the nag screen from pong.exe.
2. * The game may use anti-tampering techniques to prevent modification; ensure that it runs correclty after removing the nag screen.

PART II - Crackme

3. If you successfully remove the nag screen from pong, crackme.exe offers a more complex code guard defense for you to crack.
4. Using IDA and 010, remove the multiple nag screens from the crackme.
5. Once complete, find a valid name and key for the crackme key check.

X86-SOFTWARE-REVERSE-ENGINEERING-CRACKING-AND-COUNTER-MEASURES
ISBN: **1394199880**