Corelan Team

:: Knowledge is not an object, it's a flow ::

Exploit writing tutorial part 10 : Chaining DEP with ROP – the Rubik's[TM] Cube

Corelan Team (corelanc0d3r) · Wednesday, June 16th, 2010

Table of Contents

Introduction

About 3 months after finishing my previous exploit writing related tutorial, I finally found some time and fresh energy to start writing a new article.

In the previous tutorials, I have explained the basics of stack based overflows and how they can lead to arbitrary code execution. I discussed direct RET overflows, SEH based exploits, Unicode and other character restrictions, the use of debugger plugins to speed up exploit development, how to bypass common memory protection mechanisms and how to write your own shellcode.

While the first tutorials were really written to allow people to learn the basics about exploit development, starting from scratch (basically targeting people who don't have any knowledge about exploit development), you have most likely discovered that the more recent tutorials continue to build on those basics and require solid knowledge of asm, creative thinking, and some experience with exploit writing in general.

Today's tutorial is no different. I will continue to build upon everything we have seen and learned in the previous tutorials. This has a couple of consequences :