# 第5章 逆向工程

逆向类题目是CTF中难度相对较高的题型，现在已经覆盖Windows逆向、Linux逆向和Android逆向，再加上Flash逆向、Python逆向、.NET逆向、ARM逆向等，对选手的要求可谓越来越高。根据笔者的一些参赛经验，很多成绩优异的战队都是因为在逆向类题目中拿到了足够的分数，因此在CTF中流传着一句话“得逆向者得天下”。

## 5.1 逆向工程概述

在现代社会中，软件被应用于多个方面。典型的软件有电子邮件、嵌入式系统、人机界面、办公套件、操作系统、编译器、数据库、游戏等。同时，各个行业几乎都有计算机软件的应用，如工业、农业、银行、航空、政府部门等。这些应用促进了经济和社会的发展，也提高了工作和生活效率。我们把这些软件开发的过程统称为软件工程。

软件工程是一门研究用工程化方法构建和维护有效的、实用的和高质量的软件的学科。它涉及程序设计语言、数据库、软件开发工具、系统平台、标准、设计模式等方面。而与之相反的技术就是我们本章要学习的软件逆向工程技术，一般也简称为逆向工程。

### 5.1.1 什么是逆向工程

逆向工程，也称为反向工程，是解构人造物体以揭示其设计、结构或从物体中提取知识的过程；它与科学研究相似，唯一的区别在于科学研究是针对自然现象。

——来自维基百科

逆向工程(即RE)一般就是通过对物体或系统的分析，了解其结构和功能，即了解它的实现方法和内在原理，如图5-1所示。这样我们就能对了解不足的地方加以改进，将了解清楚的地方迁移到别的领域。

逆向工程广泛应用于机械工程、电子工程、软件工程、化学工程和生物工程。它最早起源于商业和军事领域，通过逆向对对手的优质硬件进行分析，进而造出自己的产品。需要注意的是，利用逆向并不是复制，因为我们对所分析的物体或系统的内部并没有全部了解，所以往往会存在重构的过程以达到功能一致或类似。